DESIGNING AND DEPLOYING PUBLIC WIRELESS NETWORKS
SESSION ACC-2014

Session Topics

• Public WLAN Market Update
• Public WLAN Solutions Today
  – Features
  – Architectures
  – Security
• Public WLAN Solution Evolution
  – Extended Security
  – Roaming
• Public WLAN Extension
• Summary
Session Focus and Assumptions

• Session Focus
  – Public WLAN solution
  – Service Provider deployments
  – End-to-end solution design

• Assumptions
  – Understanding of 802.11 technology and networks
Moving Towards Mainstream

- Innovators
  - Best effort service
  - Small number of isolated hotspots

- Early Adopters
  - Standard service offering
  - Large number of hotspots
  - Worldwide roaming

- Early Majority
  - Standard service offering
  - Large number of hotspots

- Late Majority
  - Standard service offering
  - Large number of hotspots

- Skeptics
  - Best effort service
  - Small number of isolated hotspots

Public WLAN Expanding

- Airports
- Main Office
- Hotels
- Airplanes
- Convention Centre
- Railway Stations
- Home Office
- Coffee Shops
- Bookstores
- Trains
WLAN hotspot operators have publicly stated intentions to build over 65k additional hotspots by end of 2004

“Through 2005, no business model for public WLAN “hotspots” will succeed if its only source of revenue is users paying for connectivity”

GARTNER APRIL 2003
Addressing the ROI Challenge

- **Multiple services, Single Infrastructure**
  - Public and private, wired and WLAN services
  - Bundled service, with PWLAN as complementary option
    - PWLAN and Mobile Data
    - PWLAN and DSL/Cable
    - Managed Guest Access and Wired/WLAN

- **Value Added Services**
  - Web portal offering music, movies, ringtones, etc.
  - Dynamic service upgrades and supplementary services

- **Wholesaling**
  - Offering PWLAN services to other providers

- **Vertical Market Solutions**
  - Higher education, retail chains, government and community

PWLAN Market Key Players

<table>
<thead>
<tr>
<th>Service Provider</th>
<th>Virtual Network Operator (VNO)</th>
<th>Site Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Operator</td>
<td>iPass</td>
<td>Airport</td>
</tr>
<tr>
<td>ILEC/PTT</td>
<td>Boingo</td>
<td>Retail Chain</td>
</tr>
<tr>
<td></td>
<td>GoRemote (GRIC)</td>
<td>Education</td>
</tr>
<tr>
<td>Install &amp; operate end-to-end network</td>
<td>Primary focus is on customer acquisition &amp; interface</td>
<td>May install &amp; operate local network, purchasing Internet access from local provider</td>
</tr>
<tr>
<td>May wholesale to site owners &amp; other providers</td>
<td>Negotiate service access from site owners &amp; service providers</td>
<td>May partner with VNO or partner with/outsource from service provider</td>
</tr>
<tr>
<td>Roaming agreements with other providers</td>
<td>[iPass]</td>
<td></td>
</tr>
</tbody>
</table>
PWLAN Common Deployment Approaches

<table>
<thead>
<tr>
<th>Carrier Class, Large Scale, Multi-Service Solution</th>
<th>Single Site, PWLAN Only Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>• PWLAN one element of provider service offering</td>
<td>• PWLAN for wireless Internet access is sole service</td>
</tr>
<tr>
<td>• Large number of small venues + small number of large venues</td>
<td>• Independent, single location</td>
</tr>
<tr>
<td>• Centrally managed</td>
<td>• Locally managed</td>
</tr>
<tr>
<td>• Central or local access control</td>
<td>• Local access control</td>
</tr>
<tr>
<td>• Highly scalable, available</td>
<td>• Limited scale, availability</td>
</tr>
<tr>
<td>• Higher initial investment but higher potential ROI</td>
<td>• Lower initial cost but limited ROI potential</td>
</tr>
</tbody>
</table>
Baseline User Experience

1. User connects to WLAN and opens Web browser
2. Auto-redirected to login screen
3. Access to free services
4. Login/sign-up to service
5. Billing applies once service accessed
6. User able to access authorised services, e.g. Web, E-mail, VPN, etc.

Public WLAN Ease of Use

<table>
<thead>
<tr>
<th>Easy Connect</th>
<th>No special wireless configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No client configuration changes</td>
</tr>
<tr>
<td>Easy Access</td>
<td>No detailed instructions to login</td>
</tr>
<tr>
<td></td>
<td>Range of payment options</td>
</tr>
</tbody>
</table>
Provider Branding “Look and Feel”

Value Added Service Offerings

- On-demand services with one-off charging or subscription services for enrollment
  - Movies, Music, Sports highlights, Ring tones
  - Dynamic service upgrades, such as bandwidth speeds
Location Context and Co-Branding

- Critical to winning major chain opportunities
  - Coffee shops, bookstores, hotel chains, airlines
- Required to access wholesale market opportunity

Typical Service Provider Architecture

- Centralized Access Control and Management
- Private Backhaul Network
- Tunnel over Internet as Backhaul
- Distributed Access Control and Centralised Management
- Large Number of Small Hotspots
- Small Number of Large Hotspot Sites
- Service Provider Data Center
  - AAA Server
  - Value Services
  - Billing/Prepaid Partner
- Corporate Network
- VPN
- AAA Server
Typical Small Hotspot Architecture

- Multiple services, single infrastructure
  - Multiple Wireless VLANs
  - Wired and WLAN
  - 802.1Q
  - QoS
  - GRE/IPSec tunnel

Typical Large Hotspot Architecture

- Multiple services, single infrastructure
  - Centralised Management
  - Local access control
  - Local Services

- Terminal 1
  - Airport Public WLAN
  - Airline 1 Private WLAN
  - Airline 1 Lounge Public WLAN

- Terminal 2
  - Airport Public WLAN
  - Airline 2 Private WLAN
  - Airline 2 Lounge Public WLAN

- Internet
  - Service Provider Data Center
  - Web Portal
  - AAA Server
  - Value Services
  - Billing/Prepaid Partner
  - VPN
  - AAA Server
  - Airline Corporate Network

- Airport Wiring Closet
- Airport Private Backhaul Network
- Tunnel over Internet as Backhaul
Large Hotspot, Equal Access Architecture

Airport Wiring Closet
Access Control
AAA Server
Mgmt

Portal offers users ability to select provider

Primary provider’s access controller enforces Layer 3 provider separation on backhaul

Enabling Public WLAN Ease of Use

| Easy Connect | No special wireless configuration | • Open/no WEP access  
• Broadcast SSID |
| Easy Connect | No client configuration changes | • “Plug & Play” support for static IP, private DNS, Web proxy, unresolvable destination |
| Easy Access | No detailed instructions to login | • Automatic redirection to web interface  
• Username/password |
| Easy Access | Range of payment options | • Prepaid, postpaid  
• Vouchers, credit card  
• One-time, subscription |
Enabling “Plug & Play”

- Static IP clients
  - Enable NAT on site router
- Private DNS clients
  - Spoofing and redirect to local DNS
  - Define per-service DNS in service profiles
- Web proxy settings
  - Redirect to local unauthenticated and authenticated Web proxies
    - Lock down access to authenticated proxy service and ports to prevent people using it for free access!
- Unresolvable destination
  - Spoof the destination to trigger redirection
    - Spoofed destination may be informational page, advising user of settings

Enabling Location Context and Branding

- Portal adjusted based on location
  - Location identification based on IP address range today
  - Portals centrally managed to minimise OPEX
- Per hotspot site
  - VLAN based IP pools
- Per access point, per site
  - DHCP Option 82 information from switch enabling VLAN based IP sub-pool selection
Typical Web Login Call Flow

PWLAN User Security Today
PWLAN Network Security

- **Rogue access points**
  - Tools available today to detect rogue APs, plugged into infrastructure or not, using radio management
- **Client spoofing key network infrastructure MAC addresses as type of man-in-the-middle attack**
  - Access point blocks clients spoofing key infrastructure MAC addresses, e.g. next-hop router, access controller
- **VLAN access control**
  - RADIUS based VLAN assignment or SSID authorisation to restrict/enforce user access to particular secure VLANs
  - Separate management traffic VLAN
- **Single account, multiple sessions**
  - Session management on AAA server to restrict number of simultaneous sessions

PWLAN QoS on Hotspot

| Requirement                                                                 | Task                                               | Method                                      |
|                                                                            |                                                   |                                            |
| Protect management and control traffic from high bursts of user data traffic | Rate limit traffic through CPE to prevent overload | Class-based policing                        |
| Segment public and private traffic to meet contracted service levels for private services | Packet classification to partition traffic into multiple classes of service | Classify by setting IP Precedence or DSCP   |
| Offer enhanced QoS services at large sites, with prioritised traffic types within segments | Bandwidth management on uplink to prioritise traffic according to classification | CBWFQ                                       |
|                                                                            | Segment and prioritise different traffic types within each segment | (Apply fundamental QoS principles)          |
PWLAN Management Beyond Fundamental FCAPS Requirements

- Rapid, straightforward hotspot activation and network/service level provisioning
  - Zero/one touch deployment based on carefully defined workflows
  - Inventory management and remote monitoring/management

- Radio management
  - Rogue/neighbor AP detection
  - Radio interference detection
  - Site survey/re-survey and mapping

- Scalable, available architecture
  - Thousands of elements, distributed locations

PWLAN Security Concerns

- User Authentication
  - Username/password vulnerable to attack
  - Rogue networks

- Air Link Sniffing
  - Non VPN/IPSec traffic vulnerable

- Network Security
  - Rogue devices can get onto network

- Session Hijacking
  - IP & MAC spoofing create vulnerability
Security Upgrade: WPA and 802.1x/EAP

- **WPA**
  - subset of 802.11i draft
  - WPA = 802.1x + EAP + TKIP + MIC

- **802.1x/EAP**
  - Port based authentication
  - Variety of EAP methods offering strong authentication mechanisms
  - Dynamic per session key distribution for encryption
  - Mutual authentication to secure against rogue networks
  - Ability to perform VLAN assignment or SSID authorisation
  - Mitigates MAC spoofing attacks
  - “Single Sign-On” => no more web login!
**WPA, 802.1x/EAP Overview**

- **Client** with EAP Supplicant
- **Access Point**
- **Backhaul Network**
- **Authentication Server with server side EAP**

- **Security capability discovery**
- **Client associated to AP**
- **EAP Authentication**
- **RADIUS**
- **Client and network authenticated**
- **Client assigned IP address**
- **Key Generation**
- **RADIUS Based Key Distribution**
- **Client data encrypted using independently derived encryption keys**

---

**Deploying 802.1x/EAP**

- **Client**
  - Supplicant for particular EAP type
- **Access Point**
  - Support for 802.1x/EAP
  - Support for multiple SSIDs
  - Multiple wireless VLANs to support secure and Open access
- **AAA Server**
  - Support for particular EAP type
- **Tunnel over Internet as Backhaul**
- **Hotspot Infrastructure**
  - 802.1Q VLAN to support multiple secure and Open wireless VLANs and/or WPA migration mode
- **Additional Equipment**
  - Depending on EAP type, possible additional systems and/or interfaces

---
Addressing PWLAN Security Concerns with WPA, 802.1x/EAP

<table>
<thead>
<tr>
<th>User Authentication</th>
<th>EAP types with strong authentication available</th>
<th>Mutual authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Air Link Sniffing</td>
<td>Dynamic per session key distribution for encryption</td>
<td></td>
</tr>
<tr>
<td>Network Security</td>
<td>802.1x/EAP device-device authentication</td>
<td>VLAN assignment or authorisation</td>
</tr>
<tr>
<td>Session Hijacking</td>
<td>Per session encryption protects user from session hijacking</td>
<td></td>
</tr>
</tbody>
</table>

WPA, 802.1x/EAP Challenges

- **Client EAP support**
  - EAP framework natively available in Windows XP and 2000
  - Software supplicant for particular EAP type required
- **Client dynamic key support**
  - Available in Windows XP
    - First Microsoft O/S with standard interface to 802.11 card
- **WPA client card support**
  - WPA client cards available today but limited proliferation
  - WPA migration mode enables mix of clients on same VLAN or additional VLAN for WPA clients
- **Industry /market standardisation on EAP type**
  - Large number of different EAP types available today
    - LEAP, PEAP, EAP-TTLS, EAP-SIM, etc…
EAP-SIM for GSM Mobile Operators

- EAP authentication mechanism based on GSM-SIM card
  - SIM cards are the baseline authentication method for these operators
  - All GSM phones authenticate to network using credentials on SIM card
  - Trusted authentication method
  - Uses same SIM cards for WLAN authentication
  - IETF draft under development
  - Leverages Existing Infrastructure
    - Provisioning chain, roaming agreements, etc.

PEAP (Protected EAP)

- Protected EAP (PEAP)
  - Tunneled EAP method
    - Encrypted TLS tunnel
    - EAP inner method

- Greater security
  - May be possible to hide user's true identity
    - Any EAP (inner) method allowing use of anonymous or generic user name for tunnel establishment can protect user's true identity
  - Protection from dictionary attacks
  - May not be subject to MITM attacks

- Provisioning and certificates
  - Only server side certificate required
  - Root CA used by client to authenticate network
PEAP Types

- **PEAPv0 (Microsoft)**
  - MS-CHAPv2 inner
  - Vulnerable to MITM attacks

- **PEAPv1 (Cisco)**
  - EAP-GTC inner (=username/password or OTP)
  - No native client in Microsoft O/S
  - Vulnerable to MITM attacks

- **PEAPv2 (IETF standard under development)**
  - Any EAP inner
  - NOT vulnerable to MITM attacks

Network Facilitated Nomadic Roaming

- **AAA Proxy**
  - Typically, realm used to identify provider
  - May proxy direct to home provider’s AAA servers or through clearinghouse
  - Dependent upon agreements in place
Voice over WLAN

- Potential value-add and service extension for providers with flexible, extensible architecture
  - Already a reality in the Enterprise
  - Common in certain verticals
- Starting to see emergence of dual mode phones
- Driving need for fast, secure roaming

Seamless Roaming with Mobile IP

- Standards based solution for seamless roaming
  - No service interruption
- Hides client network move by preserving IP address
- Lose location identification based on IP address range
Beyond the building!

- Outdoor coverage
  - Metropolitan areas
  - Sea ports
- Transportation
  - Trains
  - Planes
  - Automobiles
PWLAN Market Summary

- PWLAN is here to stay…but not as a standalone service!
  - Key to business model is “not just PWLAN” but service bundling and value-add service extensions
- Build a network that can evolve as the service models evolve
  - Flexible, multi-service standards based architecture
- Still early in lifecycle but evolving into more mature technology and service
  - Ongoing development of roaming and interworking agreements will drive ubiquity of service
PWLAN Design Summary

• Simple, easy access
  ➢ Ease of use is key to service success

• Trusted, quality service
  ➢ Security must be addressed to attract and retain users
  ➢ Availability and quality also key to retaining customers

• Multiple billable, customisable services
  ➢ Flexible, multi-service network to deliver and enable multiple, customisable services, as well as ability to meet evolving standards

• Carrier class solution
  ➢ Scalable to enabling expansion as demand increases
  ➢ Available to ensure quality, reliable service
  ➢ Centralised management to control OPEX

Q and A
Other Sessions of Interest

- ACC-2011
  - Securing 802.11 Wireless Networks
- ACC-2012
  - Design and Deployment of Outdoor Wireless LAN/Bridging Networks
- ACC-1011
  - Introduction to Wireless Mobile Networks
- ACC-4010
  - Advanced 802.11 Designs for Voice enabled Enterprise Roaming
- PRD-7026
  - Wireless LANs - Security, Interoperability, and New Product Directions
- NMS-2T30
  - Deploying QOS to protect voice, video and critical data

Reference Materials

- Cisco Service Provider Mobility Solutions
  - www.cisco.com/go/mobile
- WPA
  - http://www.wi-fi.org/OpenSection/index.asp
- Wi-Fi Hotspots Directory
  - http://www.wi-fitechnology.com/Hot_Spots+main.html
- IETF
  - http://www.ietf.org
Recommended Reading

- **802.11 Wireless LAN Fundamentals**
  - [1-58705-077-3]

- **Wireless Networks First-Step**
  - [1-58720-111-9]
  - Available August 2004

- **802.11 Wireless Network Site Surveying and Installation**
  - [1-58705-164-8]
  - Available September 2004

---

Complete Your Online Session Evaluation!

**WHAT:** Complete an online session evaluation and your name will be entered into a daily drawing

**WHY:** Win fabulous prizes! Give us your feedback!

**WHERE:** Go to the Internet stations located throughout the Convention Center

**HOW:** Winners will be posted on the onsite Networkers Website; four winners per day
Cisco PWLAN Solution Architecture

- Location Context and Provider/Customer Branding
- Small, Medium and Large Hotspots
- Web and 802.1x/EAP Authentication
- Multiple VLANs, Public and Private WLAN Services
- Rich, Flexible Access and Service Control
- Mobile Data Services Integration
- Managed Guest Access

Cisco Public WLAN Solution

- Wi-Fi Zone
  - Cisco Access Points
    - Cisco Access Zone Router
      - 1200, 1300 and 1100 series
- Cisco Access Control
  - Service Selection Gateway (SSG) with Subscriber Edge Services Manager (SESM)
- Cisco Mobile Exchange
  - Cisco SSG & SSM
  - Cisco Access Registrar
  - Cisco AAA Server
    - Access Registrar
- Cisco Management
  - WLE, CiscoWorks, CIC, CNS Configuration Engine
- Cisco Load Balancing
  - IOS Load Balancing
- Cisco Content Billing
  - Content Services Gateway (CSG)
Cisco Public WLAN Solution with EAP-SIM

Cisco Aironet Access Points
- Support for 802.1x/EAP

Cisco Access Control
- SSG RADIUS proxy
- EAP transparency for single sign-on

Cisco EAP-SIM Supplicant
- Technology enabler for EAP-SIM

Cisco Access Registrar
- Support for EAP-SIM with HLR Proxy

Cisco Mobile Exchange

Cisco ITP MAP Gateway
- Network user API (MAPUA) for specific MAP primitives
- Standard SS7 connectivity via TDM, HSL, M2PA
- Terminates and/or translates all SS7 events and messages

Cisco Access Control

Cisco ITP MAP Gateway

Cisco Access Registrar
- Support for EAP-SIM with HLR Proxy

Cisco Public WLAN Solution with EAP-SIM

Cisco Aironet WLAN Access Points

1200 Series AP
- Dual-band capable (802.11a+b or 802.11a+g)
- Rugged metal enclosure
- Variety of antennas available
- Outstanding performance

1100 Series AP
- Single band (802.11b)
- Plastic housing
- Integrated omni antenna
- Outstanding value

1300 Series Outdoor AP/Bridge
- Single band 802.11g
- Outdoor enclosure
- Multi-function
- Multiple antenna options

All featuring...
- Inline power
- IOS feature set
- Plenum-rated
- Support within Cisco Structured Wireless-Aware Network (SWAN)
Cisco Access Zone Router Platforms

Low End  Mid Range  High End

800 Series  1700 Series  2600 Series  3600 Series  3700 Series
Fixed Configuration  Modular Configuration  Modular Configuration  Modular Configuration

Performance/Density

Cisco Access Zone Routers

- What is a Cisco AZR?
  - Baseline Router Features
    - WAN Connectivity
    - 802.1Q VLANs
    - Dynamic Address Assignment
    - QoS/Policy Based Routing
  - PWLAN Specific Feature Enhancements
    - IP Spoofing Protection
    - Layer 2 user detection and session termination
    - Switch port based location identification
    - Client static IP support
Cisco Service Selection Gateway (SSG) Router Platforms

Cisco Subscriber Edge Services Manager (SESM)

- Fully extensible and customisable SDK based on Java Runtime Environment (JRE)
- SESM server works in conjunction with SSG to provide subscriber and service management
  - Captive portal (Web redirect to login)
  - Open (Free) and walled garden (premium services)
  - Location branding
  - User Self-Care
  - Advertising
  - QoS Policing
  - HTTP proxy and DNS proxy and spoofing services
Cisco Access Registrar

- Cisco AAA server developed specifically for the service provider market
  - High performance
  - High flexibility
    - Extension points for custom logic
  - Range of authentication types
    - Including LEAP, PEAPv0, PEAPv1, EAP-SIM, EAP-MD5, EAP-TLS, EAP-GTC, EAP-MSCHAPv2
  - Proxy RADIUS
  - Prepaid billing support
  - External interfaces
    - ODBC, LDAP

Cisco Content Services Gateway

- Content aware billing
  - Differentiate services at higher layers
    - Layer 3 IP
    - Layer 4 TCP/port or UDP/port
    - Layer 7 HTTP, WAP, FTP
  - Usage record generated on per user, per content connection basis
- Blade for Cat6500 and 7600 switching platforms
PEAP: Two Phase Authentication

Supplicant → Access Point → Network → RADIUS Server

- EAPOL Start
- EAP-Request/Identity
- EAP-Response/Identity (NAI)

Start EAP Authentication
Ask Client for Identity
Access Request with NAI

Client Derives Session key

Server-side TLS

Client-side Authentication

EAP Success
(RADIUS Access Accept (Pass Session Key to AP))

- EAPOL-Key (multicast)
- EAPOL-Key (session parameters)

Perform Sequence Defined by PEAP

Deliver broadcast key encrypted with session key and session parameters