SP WiFi: Deploying Access for 3G and 4G Mobile Networks

Cisco Plus Canada
Session Agenda
Outline and Key Takeaways

- Why SP Wifi?
- What are the Requirements?
- Components of an End-to-End Solution
- Mobile Packet Core Integration
- Call flows for typical deployments
- Case Study
- Summary and Key Takeaways
Why SP Wifi?
SP WiFi: Addressing Service Provider Challenges

- Growth in Mobile Data: 26x over 5 years
- 180% increase in signalling traffic due to smartphones
- Lack of spectrum and inability to rapidly increase # cell sites
- Economics of indoor offload and small cell systems
- A shift from outdoor consumption to indoor
- WiFi already used to support >30% of US smartphone usage

• Easy Connectivity
• Seamless Authentication
• Session continuity
• Application transparency

• Deployment Complexity
• Consistent user experience
Double pressure on SP economics
Illustrative Results for large European Mobile Operator

Decline in voice revenues and difficulty in monetizing data traffic

Network implications of exponential data traffic growth

Source: IBSG Research & Economics Practice, 2011
Doing nothing is not an option
Illustrative Results for a Large European Operator

Cash Flow From Operations

<table>
<thead>
<tr>
<th>Year</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Billions</td>
<td>3.0</td>
<td>3.0</td>
<td>3.0</td>
<td>2.5</td>
<td>2.0</td>
<td>1.5</td>
</tr>
</tbody>
</table>

Source: IBSG Research & Economics Practice, 2011

Financial Metrics

EBITDA Margin

© 2012 Cisco and/or its affiliates. All rights reserved.
Drivers For Change: Scaling Supply
Delivering 26 fold increase in Supply

- Service usage growing unchecked
- Macrocell capacity growth cannot keep up with demand
- Licensed spectrum availability not growing to meet demand
- Smaller Cells are needed to scale supply efficiently & economically
- Licensed and Unlicensed Spectrum will need to be exploited

Source: Agilent
Why Small Cells?
Drivers for Deploying Service Provider WiFi

- Meet Subscriber Demand
  - Increased coverage and service ubiquity
  - Higher Speed enabling richer applications

- High Volume Low Cost Technology
  - SP WiFi is to Mobile (3G/4G) as Carrier Ethernet is to Wired (SDH/PDH)

- Licensed Spectrum Availability
  - Not growing to meet demand

- Hierarchical Network Approach
  - Macro cells & small cells

Drivers for Deploying Service Provider WiFi:
- Spectrum
  - (5MHz vs 10,20 MHz)
  - Multiple carriers
- Efficiency
  - (Bits/Hz, backhaul BW)
  - 3G to HSPA to LTE
- Footprint
  - (#cells/m²)
  - Small Cells
- Macro
- Consumer
- Business
- Community
What are the Requirements?
SP WiFi Vision: End user perspective
Cellular Mobility Experience on Wi-Fi

**Cellular**
Example: GSM Phone

- Turn on phone and get secure cellular connectivity
- Roaming anywhere – no logins or passwords
- Automatic Network Selection
- Access anywhere with my profile & services

**Wi-Fi**
Example: iPhone

- Turn on phone and get secure Wi-Fi connectivity

---

BRKSPM-2200 © 2012 Cisco and/or its affiliates. All rights reserved. Cisco Public
SP WiFi Vision: Cisco Perspective

WiFi Service Requirements

**Ubiquitous Access**
- Automatic service advertisement
- Automatic network selection
- Roaming
- Inter-access mobility

**Common Authentication**
- SIM credentials
- Non-SIM credentials
- Single AAA infrastructure

**Seamless Services**
- Monetization opportunities
- Consistent services
- Session persistence
- Wholesale/Roaming

**Unified Control**
- Traffic path selection
- Billing
- QoS
- Quota mgmt
- “One Subscriber”

Carrier Class Solution for MNOs, MSOs and Hotspot Providers
# SP WiFi

## One Access Technology, Many Deployment Models

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uncontrolled</td>
<td>No SP involvement. User driven offload via unmanaged device.</td>
</tr>
<tr>
<td>Home/Soho Dual SSID (Community)</td>
<td>SP provides dual SSID home device. Private and public (community) SSID</td>
</tr>
<tr>
<td>Hot Spot / Hot Zone</td>
<td>SP installed and managed hot spots in Malls, restaurants, Hotels,…</td>
</tr>
<tr>
<td>High Density Wireless</td>
<td>SP installed and managed hot spots in high density user areas (stadiums,..)</td>
</tr>
<tr>
<td>Metro / Mesh</td>
<td>SP install and manages outdoor Wi-Fi for large dense urban areas coverage</td>
</tr>
<tr>
<td>Enterprise Guest Access</td>
<td>Enterprise Guest Access managed by SP</td>
</tr>
</tbody>
</table>
# SP WiFi

## Key Requirements

<table>
<thead>
<tr>
<th>Carrier Grade</th>
<th>Manageability, Network Reliability and Availability 100s of thousands of APs; Millions (residential); Millions of Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility</td>
<td>Seamless authentication and Fast Roaming/Handoff Wi-Fi to Wi-Fi (inter and intra-vendor), 3G/4G to Wi-Fi</td>
</tr>
<tr>
<td>Roaming</td>
<td>Seamless roaming (with little or no user intervention) Support home and “visited” network scenarios</td>
</tr>
<tr>
<td>Standards Compliant</td>
<td>Critical to support Multi-vendor solution 3GPP compliance important to MNOs</td>
</tr>
<tr>
<td>Integration</td>
<td>Common Billing, Policy and Subscriber Management Leverage MPC/EPC for Wi-Fi network Parental Control / Lawful Intercept / Local Breakout</td>
</tr>
</tbody>
</table>
Components of an End-to-End Solution
**SP WiFi Functional Architecture**

- AP = Access Point
- MAG = Mobility Access Gateway
- WLC = Wireless LAN controller
- LMA = Local Mobility Anchor
- GTP = GPRS Tunneling Protocol
- IPSG = IP Services Gateway
- EWAG = Enhanced Wireless Access Gateway
- PMIP = Proxy Mobile IP (v6)
- UE = User Entity (mobile terminal)

**Diagram Details**
- **Transparent aggregation**
- **L3**
- **PMIPv6**
- **GTP**
- **IPSec**
- **802.1Q**
- **IPSG**
- **EWAG**
- **Internet**
- **Access Aggregation Core**

**Legend**
- AP = Access Point
- MAG = Mobility Access Gateway
- WLC = Wireless LAN controller
- LMA = Local Mobility Anchor
- GTP = GPRS Tunneling Protocol
- IPSG = IP Services Gateway
- EWAG = Enhanced Wireless Access Gateway
- PMIP = Proxy Mobile IP (v6)
- UE = User Entity (mobile terminal)
End-to-End SP WiFi Integration with Roaming
Enhanced WiFi Access Gateway (EWAG)

Key Capabilities:
- MPC Integration
- Inter-access Mobility
- Roaming
- Wholesale
- Subscriber-aware
- Local Breakout
- Flexible Access Models
- Flexible Authentication

Key Capabilities:
- MPC Integration
- Inter-access Mobility
- Roaming
- Wholesale
- Subscriber-aware
- Local Breakout
- Flexible Access Models
- Flexible Authentication
## Core SP WiFi functional components

### Key Considerations in SP WiFi Network Design

<table>
<thead>
<tr>
<th>Authentication Authorization</th>
<th>Address Allocation</th>
<th>Session Management</th>
<th>Transport Backhaul</th>
<th>Redundancy Load balancing</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA / RADIUS DIAMETER HLR / HSS Integration / Roaming Authentication point EAP / Web Auth Before / After ISG At LMA External DHCP IPv4 / IPv6 Pool depletion Location based Keep alive Idle Timeout Quota enforcement Policy enforcement Session differentiation Session Initiation CAPWAP Fragmentation PMIPv6 (MAG/ LMA) L2TP (AZR) / GTP Autonomous AP MPC integration HSRP/ GLBP 1:1 Redundancy N:1 Redundancy ACE based Single SSID Multiple SSID</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accounting Billing &amp; Policy</th>
<th>Web Ports</th>
<th>Mobility</th>
<th>Network Management</th>
<th>Subscriber Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start and Stop Records (CDR)</td>
<td>When to redirect L4 / HTTP 302 Who redirects Redirection Portals Web Authentication Self service Portals Whitelisting Location based</td>
<td>WiFi only mobility Hierarchical mobility WiFi / Macro Max mobility coverage Roaming agreements Mobility events Anchors / tracking</td>
<td>Security Zero touch rollout Legal Intercept Parental Control Analytics / planning Asset tracking Rogue AP’s</td>
<td>Provisioning Pre-paid / Quotas WiFi only users Transparent logon Service profiles Self service portals</td>
</tr>
</tbody>
</table>

### Authentication

- AAA / RADIUS DIAMETER
- HLR / HSS Integration / Roaming Authentication point
- EAP / Web Auth

### Address Allocation

- Before / After ISG
- At LMA
- External DHCP
- IPv4 / IPv6
- Pool depletion
- Location based

### Session Management

- Keep alive
- Idle Timeout
- Quota enforcement
- Policy enforcement
- Session differentiation
- Session Initiation

### Transport Backhaul

- CAPWAP
- Fragmentation
- PMIPv6 (MAG/ LMA)
- L2TP (AZR) / GTP
- Autonomous AP
- MPC integration

### Redundancy Load balancing

- HSRP/ GLBP
- 1:1 Redundancy
- N:1 Redundancy
- ACE based

### Accounting Billing & Policy

- Start and Stop Records (CDR)
- Who sends them
- Integration with Existing billing
- Gx / Gy / Gz Policy definitions

### Web Portals

- When to redirect
- L4 / HTTP 302
- Who redirects
- Redirection Portals
- Web Authentication
- Self service Portals
- Whitelisting
- Location based

### Mobility

- WiFi only mobility
- Hierarchical mobility
- WiFi / Macro
- Max mobility coverage
- Roaming agreements
- Mobility events
- Anchors / tracking

### Network Management

- Security
- Zero touch rollout
- Legal Intercept
- Parental Control
- Analytics / planning
- Asset tracking
- Rogue AP’s

### Subscriber Management

- Provisioning
- Pre-paid / Quotas
- WiFi only users
- Transparent logon
- Service profiles
- Self service portals
Address Allocation & Management

Considerations

- **When to assign?**
  - Before authentication for Web-auth users
  - Post authentication for EAP / 802.1x

- **Where in the network?**
  - In the access network (eg. EWAG) or in the core (eg. ISG / IPSG Subscriber Service Managers)

- **What to assign?**
  - Location based address assignment with option 82

- **Subnet size?**
  - Oversubscription ratio
  - Lease time
  - Broadcast domain size

- **Overlapping IP address from different administrative domains**
Address Allocation & Management

The Challenge

Challenge: How to Manage UE address Overlap and Routing in Roaming Scenarios
Address Allocation & Management
Separating Roaming Partner Traffic - Single SSID or Multiple SSID?

EWAG = Enhanced Wireless Access Gateway
Address Allocation and Management

Key Issues in Roaming Scenarios

- Roaming Partners are independent administrative domains
  - Address pool allocation and overlap will be difficult to coordinate
- Access network design should handle UE address overlap

Options:

- VRF separation on interfaces to roaming partners
- Access network allocates UE IP address with NAT to Home MNO address
  - Clean solution, but leads to address pool fragmentation in PMIPv6 architectures
- Augmented L2 switching at WiFi gateway
  - Use combination of MAC address and GRE-Key or GTP TEID for switching and ARP resolution
IP Host Configuration for WiFi Access

UE/Host Configuration Models

- UEs Require IP Host Configuration; Link model is different for WiFi and UMTS/LTE
- UMTS model allocated a /32 host address directly to the UE and software stack is built to suit this model
- WiFi model is standard IP subnet model: Host Address & Mask plus DNS server address
- LTE with PMIPv6 supports the IP subnet model (PBU along with PCO option)
- WiFi core network supports the IP subnet model (DHCP/ARP control)
- UMTS core integration has challenges:
  - Obtaining subnet mask and default gateway address
  - Obtaining DNS and DHCP server addresses
IP Host Configuration for WiFi Access

Solutions to Consider

1. New Information Element (IE) defined to provide the host configuration
   – Currently applicable only to GTPv2
   – TSG Core Network Working Group 4 working on this
   – Standardization for GTPv1 and then implementation will take time

2. Per-APN static configuration
   – Pragmatic short-term option, but lacks flexibility

3. Dynamic Subnet Extraction
   – EWAG could create a subnet from the allocated IP address (e.g., bit 32 flip)
   – Use GTP Protocol Configuration Options IE for DNS address; Locally configured DHCP server address

4. Proprietary IEs
Subscriber Session Management
Initiation and Termination

- Session creation (First Sign of Life - FSOL)
  - DHCP initiated (L2 connected)
  - Unclassified MAC (L2 Connected)
  - Unclassified IP (L3 routed)
  - Radius proxy (L3 routed)
  - RADIUS accounting start (L3 Routed)

- Session termination options
  - Idle timeouts? Keep alives?
  - DHCP lease expiry
  - Authentication timeout
Session Management

Service considerations

- Service Differentiation
  - Gold / Silver / Bronze / policy enforcement
  - Parental control / DPI
- Quota enforcement
  - Usage based / Time based
- Location based services
- Free services
  - Open garden
  - Whitelisting
- Dynamic service updates
  - Policy push
- Service Control and Policy
  - DPI
- Targeted Push Advertising
  - Intelligent, Location-aware
- Branding
Cisco Tools for Session Management
ASR5000 IP Services Gateway (IPSG)

- Two options for session management on ASR5000:
  - Manage WiFi session as mobile session from another RAT Type
    - Gateway does bearer and session management
    - Leverage charging, billing and inline services capabilities
  - Manage WiFi session using IPSG
    - Gateway does bearer and session management
    - IPSG does subscriber and session inline services

- What is IPSG?
- Standalone or integrated tool for inline session management:
  - DPI, Peer-to-peer control
  - Firewall, NAT
  - PCEF functionality for Policy (Gx) and Charging (Gy)
- Radius based session creation
  - No Diameter/GTP initiators
- Sits at edge of packet core between Gi/SGi reference point and Internet
  - Northbound of GGSN or PGW
Cisco Tools for Session Management
Intelligent Services Gateway on ASR1000

Cisco Intelligent Services Gateway (ISG) Cisco IOS feature that provides Session Management and Policy Management services to a variety of access networks.

Addresses IP and PPP protocol sessions over Ethernet used in SP WiFi while maintaining all subscriber management functions.

Is the subscriber management solution for many Cisco hotpsot and SP-WiFi deployments today.

Is an integral component of EWAG – Enhanced Wireless Gateway on ASR1000.

Deployed at the Internet Edge (Standalone) or in Aggregation (EWAG).

So focal, that the entire device is often referred as an: Intelligent Services Gateway router or simply “The ISG”
Subscriber Dynamic Sessions

IP-Type Sessions are Most Prevalent in SP WiFi

### IP Session: Layer2 Connected

- All traffic associated with the session is IP traffic
- Clients are L2 connected
- Service Manager is L3 Edge and default router
- Access may run PMIPv6 for mobility

![Diagram of IP Session: Layer2 Connected](image)

### IP Session: Routed Connection

- All traffic associated with the session is IP traffic
- Clients are L3 connected (UE IP must be routable in Access domain!)
- Session Manager may be more than one hop away from Client

![Diagram of IP Session: Routed Connection](image)
Dynamic Session Initiation
ISG sessions are initiated at the First Sign of Life (FSOL)

**IP Sessions - FSOL**

FSOL depends on the Session Type. There are options.....

- **Unclassified MAC or IP**
  - Data Traffic
  - IP packet with unknown MAC or IP source address
    - Use MAC for L2-connected IP sessions
    - Use IP for routed IP sessions

- **DHCP**
  - DHCP discover
  - DHCP Discover message
    - ISG must be DHCP Relay or Server

- **RADIUS**
  - RADIUS Access Request OR Accounting Start
  - RADIUS Access/Accounting Start
    - ISG must be a Radius Proxy for Account Start/Stop
    - Typically used in PWLAN and WiMAX environments
Authentication Options
Two main authentication models

- **EAP/802.1x – WLC or AP Authenticator / ISG - Authorization**
  - AAA is the authentication server
  - Seamless authentication but requires client config. (certificates, username/pwd, etc)
  - EAP-SIM/AKA helps if proper supplicant SW available on terminal device

- **Weblogin – Portal-based Authentication and Authorization**
  - Open SSID
  - Requires no client configuration, completely Web-based
  - Subsequent Logins are transparent/automatic using device MAC address
  - Vulnerable to MAC Spoofing
ISG Services for Session Management

- **Service**: A collection of features that are applicable on a subscriber session
  
  \[ \text{Service} = \{ \text{feat.1}, \text{feat.2}, \ldots, \text{feat.n} \} \]

<table>
<thead>
<tr>
<th>Features</th>
<th>Service Administration</th>
<th>Traffic Conditioning</th>
<th>Traffic Forwarding Control</th>
<th>Traffic Accounting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portbundle (PBHK)</td>
<td></td>
<td>QoS: Policing, MQC</td>
<td>Subscriber Address Assignment Control</td>
<td>PostPaid</td>
</tr>
<tr>
<td>Timeouts: Idle, Absolute</td>
<td></td>
<td></td>
<td>GTP or PMIP tunnel assignment(^1)</td>
<td>Tariff Switching</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Interim</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Broadcast</td>
</tr>
</tbody>
</table>

- **Primary Service**: Contains one “traffic forwarding” feature and optionally other features; only one primary service can be active on a session

1. New feature with EWAG – Q4-2012
## Defining Services

<table>
<thead>
<tr>
<th>Location</th>
<th>Download</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AAA Server</strong></td>
<td>1. Premium HSI service should be activated on the session</td>
</tr>
<tr>
<td>- Services defined in Service Profiles</td>
<td>2. RADIUS Access-request Username: Premium_HSI</td>
</tr>
<tr>
<td>- Standard and Vendor Specific RADIUS attributes used</td>
<td>Password: &lt;service pwd&gt;</td>
</tr>
<tr>
<td>- On demand download on a need basis</td>
<td>3. RADIUS Access-accept Features associated w/ service</td>
</tr>
<tr>
<td></td>
<td>4. Service Activated on session</td>
</tr>
<tr>
<td></td>
<td>- Service Stored in local cache while in use by at least 1 sessions</td>
</tr>
<tr>
<td><strong>Policy Manager</strong></td>
<td></td>
</tr>
<tr>
<td>(supporting the SGI Interface)</td>
<td></td>
</tr>
<tr>
<td>- Services defined in XML</td>
<td></td>
</tr>
<tr>
<td>- Pre-download of all existing services</td>
<td></td>
</tr>
<tr>
<td><strong>ISG</strong></td>
<td></td>
</tr>
<tr>
<td>- Services pre-configured using CLI</td>
<td></td>
</tr>
<tr>
<td>- Services defined on Service Policies: policy-map type service &lt;name&gt;</td>
<td></td>
</tr>
</tbody>
</table>

### SGI Request
- Premium, Standard, Basic HSI service definitions

### SGI Response
- Definition of all existing Services typically pre-downloaded on Box
- Services permanently stored in local database

---

© 2012 Cisco and/or its affiliates. All rights reserved. Cisco Public
How Services Are Activated on a Session?

### During Subscriber Authentication/Authorization
- Subscriber is successfully authenticated
- RADIUS Response includes Services and Features to activate on Session (from User Profile)

### Via an External Policy Manager/Web Portal
- Service Activation request sent by External Policy Managers via a RADIUS CoA or a SGI Request message

### Via the On-Box Policy Manager
- Policy Plane determines what actions to take on session based on events
  - actions “include” applying a service
  - Control Plane ensures actions are taken – i.e. provisions the data plane
  - Data Plane enforces traffic conditioning policies to the session
Location based services
Simple VLAN based

SSID: XYZ

Same SSID from different AP groups mapped to separate VLAN groups

VLAN 10
VLAN 20

VLAN 10
VLAN 20

VLAN 30
VLAN 40

Separate policies on VLAN's Redirect traffic to different Portals.

AP-Groups (500 max)

VLAN-Groups (512 max)

Portals

Web Portal (Library)

Web Portal (Stadium)
Mobility Management
Essentials for Mobility

- Common anchor point for all access technologies
- A common subscriber identifier across all access technologies
  - Eg. MAC address, MSISDN…. key for inter-access mobility
- Address allocated from a common DHCP pool
- A common authentication scheme
- Common session identifier
  - For common billing and subscriber service across WiFi/3G/4G
- Ability to track subscriber
Mobility Management
PMIPv6 - Hierarchical mobility

Subscriber authentication Tracking

Common IP pool
Common Anchor
Same Subscriber ID
Same Session ID

Common IP pool
Common Anchor
Same Subscriber ID
Same Session ID

802.11(x) CAPWAP L2 PMIPv6
Mobility Management

Domain Mobility with PMIPv6

- Host-based Mobility: Mobile IP - MIPv4, MIPv6
  - Requires client implementation of Mobile IP stacks; client signalling needed
  - Drawback: requires client support (ubiquity?)

- Network-based Mobility: Proxy Mobile IP – PMIPv6 (RFC-5213)
  - Only network entities participate in mobility related signaling on behalf of clients
  - Advantage: transparent to UE; no client required
Mobility Management
Domain Mobility with PMIPv6 cont’d

- PMIPv6 Entities:
  - Local Mobility Anchor (LMA):
    topological anchor point for UE;
    assigns and manages UE address and access network location
    Switches UE downstream/upstream data to appropriate MAG via PMIP tunnelling (GRE-based encapsulation)
  - Mobility Access Gateway (MAG):
    manages mobility signalling for the UE;
    tracks UE location subnet-to-subnet;
    Switches downstream/upstream UE data between correct access subnet and PMIP tunnel to LMA
    notifies LMA of location changes for MAG handoff
Local Mobility Management

Intra Controller roaming

- Intra-Controller roam happens when an AP moves association between APs joined to the same controller
- Client must be re-authenticated and new security session established
- Controller updates client database entry with new AP and appropriate security context
- No IP address refresh needed
Local Mobility Management
Inter Controller Layer 2 roaming

- L2 Inter-Controller roam happens when an AP moves association between APs joined to the different controllers but client traffic bridged onto the same subnet.
- Client must be re-authenticated and new security session established.
- Client database entry moved to new controller.
- No IP address refresh needed.
Local Mobility Management
Inter Controller Layer 3 symmetric roaming

- Foreign controllers will send Layer 3 roaming client’s packet back to its anchor controller through EtherIP tunneling
- Source IP address of the packet will be the foreign controller’s management IP address
- Upstream routers that have Reverse Path Forwarding (RPF) will forward on packets
- No IP address refresh needed
Mobile Packet Core Integration
Integrating WiFi into Mobile Packet Core
Clientless and Client-based Options Summary

- **Devices**
  - Clientless – IPSG or ISG (IP)
  - Clientless EWAG (PMIPv6)
  - Clientless eWAG (GTPv1)
  - Clientless 3GPP2
  - Clientless 3GPP
  - Secure Client based iWLAN

- **IP Core**
  - Trusted Wi-Fi
    - Un Tunneled User Data (IP)
    - Per User PMIPv6 or GTP Tunnel
  - Untrusted Wi-Fi
    - Per User IPSec Tunnel

- **Mobile Packet Core**
  - Converged, Policy, Charging and Billing Systems
  - 3GPP AAA
    - IP Core

- **Devices**
  - EWAG
  - HSGW
  - SGSN
  - TTG
  - P-GW
  - GGSN

- **3G Cellular**
  - Per User PMIPv6 Tunnel
  - Per User GTP Tunnel

- **WLAN AAA**
  - 3GPP AAA

- **Untrusted Wi-Fi**
  - Per User IPSec Tunnel

- **Converged, Policy, Charging and Billing Systems**
  - IP Core
  - GTP (Gn)
Integrating WiFi into Mobile Packet Core

Client-based iWLAN

- **Client based integration – iWLAN**
  - Defined in 3GPP 23.234
  - WiFi infrastructure can be trusted or untrusted
  - No dependencies on WiFi infrastructure other than IPSec needs to get through any firewalls
  - TTG to terminate IPSec tunnel required in MPC
  - Existing MPC infrastructure reused – PCRF, OCS, Billing, LI
  - TTG only interfaces to AAA and GGSN – no other MPC integration is needed
  - Seamless mobility via Home Agent based on Client Mobile IP or PMIP from GGSN
  - **Device IPSec client needed**
Integrating WiFi into Mobile Packet Core

Clientless EWAG

- **Enhanced Wireless Access Gateway – EWAG**
  - Clientless WiFi Integration into the mobile packet core
  - A mediation device between WiFi access and 3GPP Core
  - Clean partition of RAT types
  - Interworking between IP-based Access Network and Mobile Core control planes
  - Authentication via Mobile AAA infrastructure
  - PMIPv6 and GTP capability
  - Existing MPC infrastructure reused – PCRF, Billing, Lawful Intercept…
Enhanced WiFi Access Gateway
Common Subscriber Management and Routing Functions

- Subscriber and Service Aware Aggregation Function
  - Key to support for Local Breakout, Wholesale access
  - Per-subscriber APN selection and control

- Policy-controlled subscriber routing, mobility services (PMIP, GTP)
  - Anchoring to the GGSN, PGW or local-breakout based on subscriber profile
  - Subscriber service management for home network as well!
  - Interprovider Roaming with policy control

- Policy interface options:
  - Radius-based (WiFi evolution) and/or Gx-based (MNO evolution)

- Integrated Accounting for Wholesale and Retail Services

- IP Aggregation support:
  - DHCP Server and Relay capability
  - Support for routed and switched access networks
  - Efficient solution for IP control-plane to Mobile network control plane interworking – i.e. link model mediation
  - Address Pool overlap management in access network
Key EWAG Functions for 4G Integration

PMIPv6

- **Packet Core Interface:**
  - PMIPv6 over S2a is standardized method of integrating trusted non-3GPP access networks with a 3GPP Evolved Packet Core
  - 3GPP 29.275 defines PMIPv6 based S2a interface

- **Session Triggers:** DHCP, IPv6 Router Solicitation, Radius Proxy and Unclassified MAC for tunnel initiation

- **Transport:** IPv4 and IPv6 as per RFC-5844 and RFC-5213

- **EAP Methods:** Agnostic to generic EAP methods (EAP-SIM/AKA and MSISDN)

- **PMIP Info Elements:** Supports all necessary IEs for interface to the MPC

- **Policy:** Cisco UE Service VSA for provisioning of differentiated access per subscriber
  - Phase 1.5 includes 3 different service options “IPv4”, “IPv6” and “dual”
Key EWAG Functions for 3G Integration

GTP-based 3G Integration

- **Packet Core Interface:**
  - GTP over Gn’ Interface as per TS 29.060
  - GTP control support: PDP context creation, deactivation, PDP echo

- **Session Triggers:** DHCP, IPv6 Router Solicitation, Radius Proxy and Unclassified MAC for tunnel initiation

- **Transport:** IPv4, IPv6

- **EAP Methods:** Agnostic to EAP method (EAP-SIM/AKA with MSISDN or user@realm subscriber ID)

- **GTP Info Elements:** Supports all necessary IEs for interface to the MPC
  - eg. Protocol Configuration Options, MSISDN, APN
SP WiFi Roaming Architecture
Enabling Roaming and Wholesale Service with EWAG

Hotspot
Public/Large Venue
Community WiFi
Policy and Charging
PCRF Integration Architecture – Mobile Packet Core

Interfaces and Functions

- PB – Policy Builder
- PS – Policy Server
- CS – Charging Server
- SM – Unified Subscriber Manager

ASR5000

Mobile Gateway
AAA Integration Architecture – WiFi Core Network

Interfaces and Functions

OSS/BSS
- HSS
- Billing
- Inventory & Provisioning
- CRM

Radius Server
- Subscriber Profiles & Policies

Portal
- Broadband Access Policy Infra

SOAP/XML

Radius

Portal API

EWAG
(ASR1000 with ISG)

Internet

WiFi Access

PB – Policy Builder
PS – Policy Server
CS – Charging Server
SM – Unified Subscriber Manager

BroadHop Service Manager
AAA and MPC Interworking

Interfaces and Functions

- OSS/BSS
  - HSS
  - Billing
  - Inventory & Provisioning
  - CRM

- Radius Server
- Subscriber Profiles & Policies
- Broadband Access Policy Infra Portal

- BroadHop SME
- ITP- IP Transfer Point
  - MAP Gateway for MAP/Radius
  - Interworking

- MPC Authentication Interworking
- CAR
- Local HLR
- SS7 Network
- Interface to Local HLR if Applicable

- Internet Gateway
- Internet
- EWAG (ASR1000 with ISG)
- WiFi Access

- Roaming Partner
- HLR
- Internet Gateway

- CRM
- HSS
- Billing
- Inventory & Provisioning
- CRM

- Radius
- Portal API

- SOAP/XM L
Call flows for typical deployments
### PMIPv6 with EAP-SIM Based Authentication

#### Call Flows (1/2)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Open Association</td>
<td>Device connects to AP+WLC.</td>
</tr>
<tr>
<td>2. EAP Request/ID</td>
<td>AP+WLC sends EAP Request/ID to Device.</td>
</tr>
<tr>
<td>3. EAP ID Response/ID</td>
<td>Device sends EAP ID Response/ID to AP+WLC.</td>
</tr>
<tr>
<td>4. RADIUS Access Request</td>
<td>AP+WLC sends RADIUS Access Request to AAA. (username= EAP ID, calling station ID = MAC, called-station-ID = SSID)</td>
</tr>
<tr>
<td>5. EAP-SIM Method, Recover IMSI from Pseudonym or Fast Re-Auth ID</td>
<td>Recover Subscription Profile (IMSI) from AAA.</td>
</tr>
<tr>
<td>6. EAP SUCCESS</td>
<td>Device sends EAP SUCCESS to AP+WLC.</td>
</tr>
<tr>
<td>7. RADIUS Access Accept (EAP Success, PMIPv6 VLAN override)</td>
<td>AP+WLC sends RADIUS Access Accept to Device. (EAP Success, PMIPv6 VLAN override)</td>
</tr>
<tr>
<td>8. Source MAC Address: DHCP Discover</td>
<td>AP+WLC discovers the source MAC address through DHCP.</td>
</tr>
<tr>
<td>9. RADIUS Access Request (Calling Station ID = Source MAC address)</td>
<td>AP+WLC sends RADIUS Access Request to AAA. (Calling Station ID = Source MAC address)</td>
</tr>
<tr>
<td>10. RADIUS Access Accept(User Profile)</td>
<td>AP+WLC sends RADIUS Access Accept to Device. (User Profile)</td>
</tr>
</tbody>
</table>

### Notes
- **Configure authorized IMSIs on the Subscriber database with WiFi Subscriber Profile.**
- **WiFi Subscriber Profile:** Realm, WiFi APN, Charging Characteristics, IPv4/IPv6 service
- **IMSI Authenticated, but MSISDN unknown**
- **User Profile VSAs:**
  - CISCO-SERVICE-SELECTION (APN)
  - CISCO-MOBILE-NODE-IDENTIFIER (IMSI@realm)
  - CISCO-MSISDN
  - 3GPP-CHARGING-CHARS
  - CISCO-MN-SERVICE (IPv4)
PMIPv6 with EAP-SIM Based Authentication

Call Flow 2/2

Device

AP+WLC

DHCP/MAG

P-GW

PCRF

SPR/Sub DB

AAA

HLR

EWAG

DHCP Offer (a.b.c.d)

DHCP Req/Ack

(Primary DNS recovered from PBA)

PBU

Gx:CCR-I

Gx:CCA-I

PBA

Open PGW-CDR

With container for WiFi Service, subscriber ID = MSISDN

RF: Diameter ACR

RF: Diameter ACA

PMIPv6

IPv4 HoA = 0.0.0.0

MN-ID (imsi@realm), SSMO (APN), MSISDN, CHARGING CHARACTERISTICS, ATT = WiFi

Gx:CCR-I: IMSI, MSISDN, APN, RAT Type

Subscriber ID Type = E.164, RAT = WiFi

SP: Recover Subscriber Profile

Policy Profile to Apply

PBA: IPv4 Home Address (HoA)

PCO: Primary DNS

SPR/Sub DB

PCRF

PBU

Gx:CCA-I

Gx:CCR-I

Open PGW-CDR

With container for WiFi Service, subscriber ID = MSISDN

RF: Diameter ACR

RF: Diameter ACA

PMIPv6

IPv4 HoA = 0.0.0.0

MN-ID (imsi@realm), SSMO (APN), MSISDN, CHARGING CHARACTERISTICS, ATT = WiFi

Gx:CCR-I: IMSI, MSISDN, APN, RAT Type

Subscriber ID Type = E.164, RAT = WiFi

SP: Recover Subscriber Profile

Policy Profile to Apply

PBA: IPv4 Home Address (HoA)

PCO: Primary DNS

SPR/Sub DB

PCRF

PBU

Gx:CCA-I

Gx:CCR-I

Open PGW-CDR

With container for WiFi Service, subscriber ID = MSISDN

RF: Diameter ACR

RF: Diameter ACA

PMIPv6
Case Study:
Super Bowl XLVI
Case Study

- This case study was presented at the event only
- Please contact your Cisco SE for details if needed
Summary & Takeways
Summary

- SP WiFi access is a business reality today for MNOs and Hotspot providers alike
- Mobile Packet Core integration is a multifaceted problem
  - attention needed to multiple factors
- WiFi access and aggregation uses IP control plane mechanisms.
  - WiFi Access Gateways need proper interworking support
- Wholesale access and roaming is a key consideration
  - WiFi Access Gateway need to support multiple roaming partners; 3G, 4G core interfaces
- Rich service management needed for subscriber differentiation and monetization
- There is no single solution for all access types, but all types of access should be supported at the service layer
- The results of a good deployment will deliver outstanding user experience!
ISG Subscriber Session
Traffic Forwarding Capabilities

**Subscriber Session**

- **Session-Features**
  - Apply to the entire session
  - e.g. per-user ACL, Policing, MQC, Accounting

- **Traffic Classification**
  - (using traffic classes: class-map type traffic)

- **Flow-Features**
  - Apply to the classified flow
  - (a portion of entire session traffic)

- **Forwarding Service**
  - Forwarding
    - (at L2, e.g. GTP)
    - or Routing
    - (at L3, e.g. PMIP, VRF)
  - Mutually exclusive

**TC1Service**: priority 10
**TC2Service**: priority 20

**TC = Traffic Class**
(similar to Traffic Flow Template)
Building the Identity and Assigning Service

An Example

DHCP Exchange Starts

T0

Subscriber Session

MAC Addr: 00:DE:34:F1:C0:28
IP Addr: ?
Username: ?
Service: DEFAULT_SRV

DHCP Exchange Completes(*)

T1

Subscriber Session

MAC Addr: 00:DE:34:F1:C0:28
IP Addr: 10.1.1.211
Username: ?
Service: DEFAULT_SRV

Subscriber Authentication(*)

T2

Brian Subscriber Session

MAC Addr: 00:DE:34:F1:C0:28
IP Addr: 10.1.1.211
Username: Brian
Service: PPU_SRV

Dynamic Service Update

TN

Brian Subscriber Session

MAC Addr: 00:DE:34:F1:C0:28
IP Addr: 10.1.1.211
Username: Brian
Service: PREMIUM_FR_SRV

Identities

IP Addr: 10.1.1.211
Username: Brian

Services

DEFAULT_SRV

PPU_SRV

PREMIUM_FR_SRV

DEFAULT_SRV

Only permits management traffic through the session

PPU_SRV

Pay Per Use Service:
- Permits all traffic
- 512K/1Mbps US/DS
- Accounting enabled on session

PREMIUM_FR_SRV

Flat Rate Premium Data Service:
- Permits all traffic
- 1M/8Mbps US/DS

(*) Order of operations not representative of a real call flow

For Your Reference
MAG-to-MAG Mobility

Call Flow

IPv4 HoA: a.b.c.d

Standard EAP-SIM flows and PMIPv6 Tunnel Establishment

Open Association
EAP Request/ID

PMIPv6

Standard EAP-SIM flows

EAP SUCCESS
(Source MAC address)

RADIUS Access Request (Calling Station ID = Source MAC address)

RADIUS Access Accept (User Profile)

PBU: IPv4 HoA: a.b.c.d

Gx:CCR-U

Gx:CCA-U

PBA: IPv4 HoA a.b.c.d

Update BCE

PMIPv6

BRI trigger = Inter MAG H/O

BRA

ARP Response

IPv4 HoA: a.b.c.d

BRI = Binding Revocation
BCE = Binding cache Entry

Cisco Public
EAP Authentication – ISG on ASR1000

Authorization at the ISG

Device → AP → WLC → AAA → DHCP → ISG → Internet

802.1x (1) → RADIUS (2) → EAP Negotiation (3) → EAP Authentication / Authorization (4) → DHCP Discover (5) → DHCP Offer (7) → DHCP Request / ACK (8) → Acct Start (9) → IP Traffic (10) → RADIUS (11) → RADIUS (12) → IP Traffic (13) → RADIUS (13) → IP Traffic (14)

User record cached
User Authorized
Service profile downloaded
User session created
Service Applied
Policies enforced
EAP authentication with PMIPv6

Authorization at the MAG

Device → AP → WLC → AAA → DHCP/MAG → LMA → Internet

802.11x (1) → EAP Negotiation (3) → RADIUS (2) → EAP Authentication / Authorization (4) → DHCP Discover (5) → DHCP Relay (6) → RADIUS Access Request (7) → RADIUS Access Accept (8) → PBU (9) → PBA (10) → DNS option added to offer

Note: example uses Integrated DHCP Server. External Server also possible.

- User record cached
- PMIPv6 trigger
- User Authorized LMA / NAI downloaded
- Binding created on LMA
- DNS option added to offer

Device
AP
WLC
AAA
DHCP/MAG
LMA
Internet

Note:
ex
ample uses Integrated DHCP Server. External Server also possible.

Device
AP
WLC
AAA
DHCP/MAG
LMA
Internet

Note: example uses Integrated DHCP Server. External Server also possible.

Device
AP
WLC
AAA
DHCP/MAG
LMA
Internet

Note: example uses Integrated DHCP Server. External Server also possible.
3G/GTP Session Call Flow

EAP SIM Authentication and Radius Control

Device | AP+WLC | L3 Router | EWAG | GGSN | AAA | ITP | HLR

- Open Association
  - EAP Request/ID
  - EAP ID Response/ID

EAP-SIM Method

- EAP SUCCESS
  - RADIUS Access Accept (EAP Success)

DHCP Discover (MAC address)
- DHCP Offer (IPv4)
- DHCP Req/Ack

Data packet (Src IP=IP)

RADIUS Access Request
- RADIUS Access Accept
  - Create PDP Ctx Req
  - Create PDP Ctx Res

GTP

Data packet (Src IP=IP)

Configure authorized IMSIs on the AAA Server and there MSISDN mapping

Username=EAP ID, Calling Stn ID = MAC, Called Stn ID = SSID

VSA = MAP: getauthinfo

VSA = MAP: authtriplet

Cache mapping between IMSI, MAC, address and SSID

User Authorized at EWAG
User Profile VSAs:
m-nai=IMSI@realm, APN, MSISDN

Username=EAP ID, Calling Stn ID = MAC, Called Stn ID = SSID

GGSN Allocated IP address
EAP authentication – IPSG on ASR5000
Authorization at IPSG, Accounting start as session initiator

Client starts EAP

User traffic encrypted using EAP derived WEP keys

WLC forwards all traffic to VLAN_EAP. All VLAN_EAP traffic VPN to mobile core

User MAC and IMSI cached after successful EAP

AAA looks up user IMSI/MSISDN based on MAC

User session on IPSG

User traffic

EAP-SIM/AKA authentication

DHCP Req/Resp

Radius Acct Start (Framed IP, mac)

Radius Acct Response

Radius Acct Start (Framed IP, IMSI/MSISDN)

Radius Acct Resp
Web Authorization for SP WiFi Access

Why is it needed?

- Web portal based access continues to be demanded by MNOs and WiFi Access providers
- Many mobile devices do not have SIM cards or SIM-based clients apps
  - WiFi iPAD and iPod touch are two major examples
  - Will every WiFi connected device get a SIM? When?
- BYOD will be a major use case for WiFi access going forward
- Exploit visiting “non-subscribers” – a good “churn” opportunity for you
  - Need a portal login and splash page to offer your service
- However there are many integration challenges….
Web authentication – ISG on ASR1000

L4 redirection at the ISG

Device → AP → WLC → AAA → DHCP → ISG → Portal → Internet

- Open association
- DHCP Discover (3)
- DHCP Offer (5)
- DHCP Request / ACK (6)
- DNS Query (7)
- DNS Response (9)
- HTTP Request (10)
- HTTP Response (11)
- User Login (12)
- RADIUS Auth (14)
- RADIUS CoA (13)
- CoA Ack (15)
- Radius Acct Start (16)

Unauthenticated Session
User Profile cached
Authenticated Session
Broadband Community WiFi – Initial Setup
Using Existing Broadband Connectivity to Deliver WiFi Access

Wireless Association
ISP PPP Session Setup
L2TP Tunnel Establishment
PPP Session Establishment
Radius Accting Start
DHCP Discovery Relayed to LNS
DHCP Discover Relayed to LNS
DHCP Offer/Req/Ac
DHCP Offer/Req/Ac
DHCP Offer/Req/Ac

WiFi Client now has an IP address

Association to Hotspot SSID triggers L2TP/PPP connection
LNS Assigns IP Address to Residential GW “Hotspot”
RG Hotspot registers with the ISG. This clears any previously existing sessions for this RG
Broadband Community WiFi cont’d – Web-Auth Flow
Using Existing Broadband Connectivity to Deliver WiFi Access

- Residential Gateway “hotspot”
- UE
- BNG
- LNS
- ISG
- AAA Accounting
- Policy Server
- AAA
- Portal
- Internet

ISG First Sign of Life. Initial Services Applied – eg. HTTP redirect
Traffic redirect to Portal for Login
Successful Login. Notify ISG via Radius CoA
ISG queries AAA Server for User service profile which is returned in Radius Access-Accept Message
User service and policy profile applied to user session. Internet access established