Thank you for attending Cisco Connect Toronto 2014, here are a few housekeeping notes to ensure we all enjoy the session today.

- Please ensure your cellphones are set on silent to ensure no one is disturbed during the session
- Please hold all questions until the end of these session to ensure all material is covered
- Let’s Have some fun:
Service Provider WiFi and Small Cells

Agenda

- SP-WiFi Solution Architecture Update
- Passpoint Certified WiFi Update
- Small Cell Overview
- Packet Core Integration options for SP-WiFi
- Practical Examples of SP-WiFi Integration
- Questions?
SP-WiFi Solution Architecture Update
Dealing with non uniform coverage

Macrocell (3G/4G)
- Voice coverage with uniform bandwidth, but not always where people are
- Reduced data capacity edge of cell
- Sub-optimal delivery of high BW to POPs
- High CapEx/OpEx: $400K
- Poor spectral efficiency

Wi-Fi/Femto/Pico
- Delivers targeted coverage and capacity
- Support high-capacity data
- Precision delivery of high BW to POPs
- Lower CapEx/OpEx
- Good spectral efficiency
**SP Wi-Fi Solution: Converged Architecture**

**Metro Wi-Fi**
- Cellular Data Alternative
- MSO/MNO Partnerships
- Walkby user management
- Architecture cadence across

**Cellular Integration**
- 3G/4G Offload
- GTP – 3G Integration
- PMIP – 4G Integration
- Small Cell Integration
- Use cases:
  - Web-Authentication and TAL mechanisms for non-SIM based devices
  - EAP-SIM/AKA for SIM-based devices
  - Open Web Auth and MAC TAL
  - WISPr
  - Location-based Portals
  - Passpoint

**Leading Enablers**
- Location Analytics
- Resi/Comm Wi-Fi – PMIPv6
- AVC/DPI
- QoS – Per client/SSID/AP
- Use cases:
  - CMX – Wayfinding
  - Whitelisting/Blacklisting
  - Parental Control

**Spontaneous Public Wi-Fi**
- Wholesale Provider
- Retailer Providers
- Portal
- DHCP
- AAA

**Internet Services**
- PGW/LMA
- GGSN
- Roaming Partner Core
- HLR
- OCS
- PCRF
- CGF

**Hotspot / SMB**
- NGH (Roaming Partnerships)
- Flexconnect CP/DP split
- SMB/Hospitality vanity SSIDs
- Location-based services
- Use cases:
  - Open Web Auth and MAC TAL
  - WISPr
  - Location-based Portals
  - Passpoint

**Cellular Integration**
- 3G/4G Offload
- GTP – 3G Integration
- PMIP – 4G Integration
- Small Cell Integration
- Use cases:
  - Web-Authentication and TAL mechanisms for non-SIM based devices
  - EAP-SIM/AKA for SIM-based devices
  - Open Web Auth and MAC TAL
  - WISPr
  - Location-based Portals
  - Passpoint

**Leading Enablers**
- Location Analytics
- Resi/Comm Wi-Fi – PMIPv6
- AVC/DPI
- QoS – Per client/SSID/AP
- Use cases:
  - CMX – Wayfinding
  - Whitelisting/Blacklisting
  - Parental Control

**Spontaneous Public Wi-Fi**
- Wholesale Provider
- Retailer Providers
- Portal
- DHCP
- AAA

**Internet Services**
- PGW/LMA
- GGSN
- Roaming Partner Core
- HLR
- OCS
- PCRF
- CGF
Cisco SP Wi-Fi Solution Components

**Core**
- L2/L3 MAC 40K $\rightarrow$ 2M
- ISG 32K $\rightarrow$ 384K
- LBO+3G+4G $\rightarrow$ iWAG
- ASR5K Packet Core: LMA, eWAG, DeWAG, SaMOG
- Scale & HA

**Access**
- Client Scale 7K $\rightarrow$ 64K
- AP scale 500 $\rightarrow$ 6000
- PMIP Mobile Integration (MAG)
- New APs: indoors /outdoors
- Client & AP SSO
- Flexconnect CP/DP split
- vWLC
- 11ac and 3G/4G

**Policy/AAA**
- BH SME/QNS
- QNS 5.3 $\rightarrow$ QPS 6.0
- ASR 1K/5K & WLC Integration with QPS
- Scale, Performance & HA
- CPAR use case support

**NMS**
- Appliance to Virtual
- CPI 1.0 $\rightarrow$ 2.x
- New AP Support
- Scale & Performance
- Reporting & Mapping enhancements
- CPM & PPM ASR5K

*Access + Service and Policy + Packet Core Integration*
3GPP Policy Architecture for WiFi: ANDSF

- 3GPP release 8 introduced ANDSF in LTE reference architecture to convey policies to the device
- ANDSF concepts can be also applied to UMTS architecture
Client functions are extended to support dynamic policies hence providing network control point.

Client policy decision based on subtype, device type, network capability, APN types, cost, SLA, Security, Charging, etc.
ANDSF Solution Approach

- Off-load UMTS/LTE traffic to WiFi provided that user experience on WiFi will be equivalent to microcellular

- Device client is critical in solving the problem
  - Client enables managed WiFi offload where SP controls criteria and conditions for traffic offload
    - Access type
    - Access and network conditions
    - Location
    - APN
    - Device
    - Roaming status
    - Time
    - Data usage
    - Application
    - Subscriber status/service
    - TFT (5 tuple filters)

- The client can also expose info required to collect analytics

- Network needs to provide necessary triggers to enable these policies
ANDSF List of Usecases

1. Standard ANDSF and S14 interface
2. Initial policy download including filtering based on location
3. New SSID list based on location change
4. Connection fallback on poor access conditions
5. Control of WiFi access for roamers
6. WiFi access for over the quota prepaid users
7. Selective traffic routing
8. Analytics
## Client Technology Roadmap

### Device Platforms
- Android
- Windows
- iOS
- BlackBerry

### Policy Enforcement
- Policy Engine
- Static
- ANDSF
- OMA DM

### Application Enablement
- Video Client
- IMS Voice
- DRM
- CDP
- LLDP
- RSVP
- Traffic Optimization

### Traffic Routing
- IP Flow Mobility
- Policy based Routing

### Network Attachment and Mobility
- VPN
- DSMIP
- MIP
- HS2.0
- I-WLAN

### Authentication
- EAP
- WISPR

### Connection Management Framework
- Monitor & Feedback
- QoS Network Monitoring
- Policy Based Access Selection

### Timeline
- Available
- 6 months
- 12 months

### Technology Standards
- UMTS
- CDMA
- LTE
- WiMax
- WiFi
- Ethernet
Passpoint Certified WiFi Update
Imagine a World…

- **You Enter a Venue…**
  - …and get onto the Wi-Fi network as simply, seamlessly, and securely as cellular
    - no SSID, no username, no password, no Web Auth, etc.
    - a new customer can immediately sign-up online at the venue

- **You are Automatically Notified of Special Services**
  - pre-installed apps automatically launch upon notification (or can download new apps as needed from a local server)

- **You have Instant Access to cool venue specific services and content**
  - Indoor Maps, Product Finder, Call for Help, Product Reviews, Loyalty info, etc.

- **This is the Promise of Hotspot 2.0**
Sample Scenario

Manual Setup

1. Power-on or unlock the phone
2. Select Wi-Fi network (vulnerable to rogue AP)
3. Go to WebAuth
4. Browse webpage and enter right credential, usually ID/PWD
5. Choose roaming plan
6. Start Internet

Automatic Setup

1. Power-on or unlock the phone
2. Handset automatically validates network and initiates connection

- Makes Wi-Fi easy-to-use and secure (like cellular)
- 802.11u enabled network is compatible with non-11u devices!

Can you tell me your network info… …before I associate?

Yes! Here it is!
Realm Name = operator.com
Auth Type = EAP-SIM
Wi-Fi CERTIFIED Passpoint™
Program Scope

Discovery
- Provide network information (including operator network information) before association to allow optimized selection
  RELEASE 1

Registration
- Create new account (if needed)
  RELEASE 2

Provisioning
- Provision credentials and subscription policy on the device (if needed)
  RELEASE 2

Secure Access
- Leverage WPA2 Enterprise for authentication and encryption provide notification of session expiration, renewal
  RELEASE 1

Technical elements of certification

- 802.11u elements
- Operator Policy – Wi-Fi Alliance Specification
- Online Signup – Wi-Fi Alliance Specification
- WPA2 Enterprise
Passpoint™ Releases

- WPA2-Enterprise with agreed credentials/EAP methods
- AP and mobile certified for IEEE 802.11u GAS and ANQP interoperability
- Mobile certified for network selection algorithm for roaming, applying user preferences and preferred association to Home SP’s hotspot
- AP certified for implementing peer-to-peer traffic inspection and filtering (for user protection via firewall) including …
  - Blocking of local peer-to-peer traffic attempting to traverse AP (TDLS, DLS and Wi-Fi Direct)
  - IPv4 Proxy ARP and IPv6 Proxy Neighbor Discovery

**Release 2: Online Signup and Policy Provisioning (anticipated in 2014)**
- Mobile certified for enhanced network selection using operator policy
- Mobile certified for operator policy provisioning providing preferred and blacklisted hotspots
- Mobile certified for in-venue, secure online signup and credential provisioning
  - User can get a subscription in any Hotspot when needed
  - Username/password and certificate provisioning
  - Supports provisioning credentials & policy for an existing subscription to a new / un-provisioned mobile device

**Release 3: (program requirements under development)**
WFA Passpoint™
Certified Information Elements

Beacons - Broadcasted

Interworking Info.
  Venue Group,
  Venue Type
  HESSID
  Access Network Type
  Internet Service
  WebAuth Required
Advertisement Protocol Info
  ANQP
Roaming Consortium Info
  OIs Info
BSS Load Element

ANQP info - Query based

802.11u Std
  Venue Name
  Roaming Consortium list
  Network Authentication Type
  NAI Realm list
  3GPP Cellular Network Info.
  Domain Name list
  IP address type
HotSpot 2.0 ANQP element
  HS Query list
  HS Capability list
  Operator Friendly name
  WAN Metrics
  Connection Capability
  Operating Class Indication
  NAI Home Realm Query

Other Network Features

802.11v BSS Transition
Proxy ARP
Multicast/Broadcast Filter
Peer-to-Peer block
Information Element Configuration

Handset Policy

Access Point Attribute

WLC Attribute

Operator Policy (Subscription MO)

Venue Info
- Venue Name*
- Venue Group
- Venue Type

802.11u IE
- Internet Access indicator
- Network Types
- Network Authentication Types (WebAuth)
- HESSID
- OUIs
- Realm list (EAP-Type info)
- Cellular Information list
- Domain list

HotSpot 2.0 IE
- Operator Name*
- WAN Metrics
- Connection Capability
- Operating Class

AP/WLC can set all the IE parameters but handset connection policy may only use a subset of it
Packet Flow

Wi-Fi Client

Beacon with 802.11u Interworking IE
- Probe Request
- Probe Response
- GAS Initial Request
- GAS Initial Response
- GAS Comeback Request
- GAS Comeback Response
- Authentication (null)
- Authentication Response
- Association Request (SSID)
- Association Response (AID)
- 802.1X (EAPOL-Start)
- 802.1X (EAP-Identity Request)
- 802.1X (EAP-Identity Response)
- 802.1X (EAP-Auth. Exchange)
- 802.1X (EAP-Success)
- 4-Way Handshake (PTK, GTK)

Used if response requires GAS fragmentation

AP/WLC

Number of queries and query content is mobile implementation dependent

Pre-association protocol using 802.11 public action frames for GAS L2 transport

ANQP provides NAI Realm, 3GPP PLMN ID, etc. so mobile can select roaming candidate network

802.11u doesn’t change your typical WLAN authentication procedure below this dotted line

Realm and EAP Method learned from GAS exchange

AAA Server

HS2.0/802.11u-enabled connection manager supplies SSID to join

Authentication (null)
- RADIUS (EAP-Auth. Exchange)
- RADIUS (Access-Accept)

SP WiFi & Small Cell
Cisco and/or its affiliates. All rights reserved.
Cisco Public
Samsung WLAN
Join decision-making process

1. Start
   - Active Scan for Network
     - Found Roaming Consortium OI in the Probe Response, that matched Home OI or RC OI List on the phone
       - ANQP – 3GPP CI Matches cred.conf info? (static or read from IMSI)
         - Yes
         - ANQP – NAI Realm List Obtain Real Names and EAP Type Info matched w/ Home Realm?
           - Yes
           - Case 1 - EAP-SIM or AKA Based on IMSI 1st digit
           - Case 2 - EAP-TTLS or TLS Based on EAP Type Info
         - No
       - No
     - ANQP – Domain Name list Found matched?
       - Yes
       - Home Network
       - No
       - Visitor Network
         - WiFi Roaming Enabled? (Older SGS3 Option)
           - Yes
           - 802.1x
           - No
         - No

SP WiFi & Small Cell
Cisco and/or its affiliates. All rights reserved.
Cisco Public
Small Cell Review
Cisco Mobility Portfolio Innovations

Access
- SP Wi-Fi
- 3G Small Cell
- Converged Small Cells
- Mobile Backhaul Solution with ASR 901, 901S, 903

Transport
- ASR9000, CRS-1/CRS-3

Core
- ASR5000, ASR5500
- With Enhanced Services

Software
- Quantum™
  - Network Abstraction Suite
  - Policy Suite
  - Analytics Suite
  - RAN Optimization Suite
  - WAN Orchestration Suite

Cisco Mobility Solutions

- Cost Effective Coverage & Capacity
- Persistent & Seamless Connectivity while Managing Traffic Growth
- Increase Service Creation Velocity & Deploy New Service
AT&T 3G MicroCell

- AT&T 3G MicroCell launched April 2010
  http://www.wireless.att.com/learn/why/3gmicrocell/
- Largest 3G femtocell deployment worldwide
- True zero-touch provisioning
  Over 90% of femto installations done without customer care intervention
  Fully automated provisioning and management control

BEST COMMERCIAL FEMTO LAUNCH

AT&T’s 3G MicroCell National Deployment

“AT&T’s 3G MicroCell deployment with Cisco caught the judges’ eyes for two crucial reasons. First and foremost, it emphasized the importance of the customer at the heart of the femtocell experience, positioning technology very much as an enabler, rather than an end in itself. Secondly, the deployment is on a national scale, which given the US market’s size adds an additional layer of complexity”, agreed the judges.

Limited to 7 macrocells within 1x1km area

Busy areas require 50m radius microcells

Busiest 200x200m area requires 6 microcells plus 3 carrier picocells/public femtocells

All microcell deployed with 3 carriers (2xU2100 1xLTE2600).

Microcell range limited to 150m due to building loss and corner loss

Source: O2 UK in Small Cells Summit, London June 2012
Cisco Small Cell Solution

Comprehensive, Intelligent 3G/LTE/Wi-Fi Small Cells

Minimize deployment OPEX with zero/low touch provisioning

Best of breed SON solution ensuring Macro radio co-existence

- Built on industry standards; 3GPP architectures
- Innovative features and capabilities solving coverage & capacity challenges
- Proven optimization & monetization models with robust Policy & Subscriber services
- End-to-end, validated, carrier-grade network solutions (radio, access, backhaul, core, policy/charging)
Small Cell Solution
Reference Solution Architecture

USC Small Cell

DMZ

RAN Management System (RMS)

H(e)NB GW

ASR5K

Network and Element Management
RAN Optimization/SON

SP OSS

SP MSC

SP SGSN or GGSN

EPC

SP NMS

Bootstrap-PKI
Small Cell Typical Connectivity

- **Subscriber Network**
- **HNB**
- **Cisco**
- **CloudBase**
- **IPSec Tunnel**
- **TLS**
- **DMZ Network**
- **ASR5K**
  - **HNB-GW**
  - **SeGW**
- **NTP**
- **RMS Serving**
- **RMS Upload**
- **RMS Central**
- **RMS**
- **L3 with IPSec Address**
- **CN Network**
  - **SGSN**
  - **MSC**
  - **OSS Network**
  - **OSS**
- **Network Management**
  - **CN**
  - **Network**
  - **CloudBase**

This diagram illustrates the typical connectivity for a small cell network, showing the flow of data through various network components and security measures such as IPSec and TLS tunnels.
Cisco Universal Small Cell Series

**USC 7000 Series**
- Concourse
- Venue

**USC 5000 Series**
- Enterprise
- Hotspot

**USC 3000 Series**
- Home
- Small Office/Home Office (SoHo)

"Mobile Internet delivered in the modern urban landscape"

Concourse - "High density, high intensity"

Enterprise - "All business is mobile today"

Home - "Mobile as the center of your lifestyle"

Small Office/Home Office (SoHo) - "In touch with the world with my mobile business device"
3G Small Cell Module for Aironet AP3600 Series
USC5310 Product Description - 3G/HSPA+ Plug-in Module

- 16 User 3G Open Mode Module
- <100mW Transmit Power (same as ETSI 802.11)
- Compatible with 3600i/3600e Wi-Fi
- Power provided by the Aironet through PoE+ (IEEE 802.3at) or external PSU.
- R99 WCDMA Voice Calls
- HSDPA+ 21Mbps / HSUPA 5.76Mbps (Peak Rates)*
- Available in 3GPP I (Rest of World) and Band II/V (USA/LATAM)

### Product Offer – 3G + Wi-Fi

<table>
<thead>
<tr>
<th>Capability</th>
<th>3G/HSPA + 802.11n</th>
</tr>
</thead>
<tbody>
<tr>
<td>RF</td>
<td>Band II/V or I 802.11n 2.4/5GHz</td>
</tr>
<tr>
<td>RF Power</td>
<td>100mW at Ant. Port</td>
</tr>
<tr>
<td>Antenna</td>
<td>1x1 SISO 802.11n 4x4 3SS / Beamforming</td>
</tr>
<tr>
<td>RF BW</td>
<td>5 MHz</td>
</tr>
<tr>
<td>Base Platform</td>
<td>USC Software Platform</td>
</tr>
<tr>
<td>3G Throughput</td>
<td>21/5.7 Mbps HSDPA+ (peak rate)*</td>
</tr>
<tr>
<td>3G Feature Set</td>
<td>16 Active users; 200 idle ;3GPP R99 &amp; R8 HSDPA+ ; Iuh / TR-069, TR-196v1, Open Mode</td>
</tr>
<tr>
<td>Mobility</td>
<td>3G Active CS/PS and Idle Mode Reselection</td>
</tr>
<tr>
<td>SON / HetNet</td>
<td>3G : Network Listen 802.11 : Clean Air</td>
</tr>
<tr>
<td>Power Supply</td>
<td>Provided by the Aironet Product</td>
</tr>
<tr>
<td>Size / Weight</td>
<td>1.5L ; 1.4kg (complete unit)</td>
</tr>
<tr>
<td>Deployment</td>
<td>Desk/Wall/Ceiling</td>
</tr>
</tbody>
</table>

* SCS 2.0 Supports 14 codes = ~15 Mbps Peak Rate
USC 5030 Dual Module Holder

- Module holder only
  - 1x GbE RJ45 ports

- Provides 2x10W via Cisco module connector

- Module Configurations
  - 1x3G
  - 1xLTE (When available)
  - 2x3G (Planning)
  - 2xLTE (When available)
  - 1x3G + 1xLTE (When available)

- Power PoE+ and/or 48V DC
- Compatible with USC 5310 and USC 541x

22 x 22 x 6 cm; ~1kg

Target FCS – May 2014

Available Next Month!
USC5416 LTE Module

- Partner to USC 5310 Module
- Module supports (auto-selects)
  - 1x1 SISO with 6W PSU (AP3600/AP3700)
  - 2x2 MIMO with 10W PSU (USC5030)

- LTE FDD
  - Upto 20 MHz iBW
  - 16 Active Users
  - 128 RRC Connected Users

- 100mW Output Power

Target FCS – December 2014

Standard Module Size; ~500g
RAN Management Solution (RMS)

RMS provides a standard based, scalable solution for Cisco Universal Small Cell Solution

- Lower time to deployment and OPEX
- Provides a centralized management entity for the small cell network
- Easy to use graphical applications in user interface
- Based on Commercially available HW
- Provides interfaces and integration API for OSS/BSS

Key Functions of RMS

- Activation of Access Points
- Configuration of Access Points
- Software upgrade of Access Points
- Status monitoring of Access Points
- Collection of raw AP KPI data
- Access to AP alarm data
- Troubleshooting of Access Points
- RADIUS service for AP auth on HNB-GW and whitelist
- DHCP service for allocating IPSec addresses
Cisco Small Cell AP-SON Capabilities

Self-Configuring
Zero-Touch Activation

- Device Activation & Automatic Network Connectivity
- Network Listen Mode
- Automatic Carrier & PSC/PCI Selection
- Initial Power Settings
- Automatic Neighbour Relations Generation
- IP Timing/Macro Synchronisation
- SW Upgrade & Initialisation
- Configuration Profiles
- Backhaul DL/UL Bandwidth Determination

Self-Optimising
Cognitive RRM Algorithms

- Continuous Network Listen
- Optimisation of Carrier & PSC /PCI Selection
- Dynamic DL/UL Power Adaptation
- Automatic P-CPICH/Common Reference Signal Power Tuning
- UE Targeted DL/UL Power Overshoot
- Automatic Neighbour Relations Management
- Backhaul DL/UL Bandwidth Tracking
- Adaptive UL Traffic Shaping

Self-Healing
Advanced System Monitoring

- HW & SW Fault Detection
- SW Process Restarts
- Chip Restarts
- Factory Recovery
- Adaptation of Power Settings & Neighbour Relations
- Determination of, & Fast Restart Following Backhaul Failures
- Load Control/Balancing in Response to Available Backhaul Bandwidth
ActiveRadio® In Action
Self-Configuration & Self-Optimisation

1. Power on
   Load correct software & basic connectivity parameters from CloudBase.

2. (Optional)
   Location locking
   Initial environment scan & optional GPS location locking.

3. (Optional)
   Local spectrum license
   Management boot inform & further provisioning.

4. Full environment scan & configuration
   Select frequency, PSC/PCI & initial power. Populate neighbour list & configure cell stickiness.

5. System authorisation
   Report of final config & gateway authorisation.

6. Enable radio & operational for calls

7. Auto power & rate adaptation
   Using information gathered from UEs.

8. Continuous network listen
   Periodic interference level checks. Ongoing environment adaptation whilst in service.
Cloudbase® Activation
- from factory to subscriber service

1. Small Cell Produced
2. Manufacturing Information
3. Small cell Records
4. Customer, retailer or Web interface orders service
5. Shipment Ordered
6. Subscription Details
7. Small cell delivered
8. Customer connects and powers up unit
9. Unit Activation
10. RMS Provisioning
11. Auto-configuration
12. Service to Subscriber
Packet Core Integration Options for SP-WiFi
Building a User-centered Solution
SP Wi-Fi Experience - User Endpoint (UE)

User Endpoint is a subscriber's carrier experience

Coverage, Performance, Ease of use

**Seamless**
- Authentication
- Network Roaming
- Session Roaming
- Policy Roaming

**Goals:**
- Seamless Roaming across many providers networks (HS 2.0)
- Zero Configuration (ANDSF)
- Zero footprint (Client Less)
- Support no-UE devices

**Authentication Options**
- EAP-SIM
- EAP-AKA
- WISPr
- Web Logon
- MAC TAL

**Standards**
- ANDSF
- HS 2.0
# WiFi Passpoint vs. ANDSF

<table>
<thead>
<tr>
<th>WiFi Passpoint</th>
<th>ANDSF</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Using</strong></td>
<td>WiFi</td>
</tr>
<tr>
<td><strong>What</strong></td>
<td>Operator Roaming (11u)</td>
</tr>
<tr>
<td></td>
<td>Network Quality &amp; Info (HS20)</td>
</tr>
<tr>
<td></td>
<td>WiFi enhancement</td>
</tr>
<tr>
<td></td>
<td>Security enhancement</td>
</tr>
<tr>
<td><strong>How</strong></td>
<td>.11u Probe Scanning</td>
</tr>
<tr>
<td></td>
<td>ANQP</td>
</tr>
<tr>
<td></td>
<td>Combine 802.1x supplicant</td>
</tr>
<tr>
<td><strong>By</strong></td>
<td>WiFi Alliance, Passpoint Certification</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cisco SP Wi-Fi Services & Policy Enforcement

Identify

Authorize

Policing

QoS

Forwarding

Accounting

Wireless Access Gateway (WAG) Routers

ASR5K

ASR9K

ASR1K

Carrier-Grade

SP WiFi & Small Cell
Cisco and/or its affiliates. All rights reserved. Cisco Public
Mobile Packet Core Integration: WiFi into 3G Packet Core

All Client-less and Client-based configurations supported

- **WLAN AAA**
- **3GP P AAA**
- **Converged, Per subscriber Policy, Charging and Billing Systems**

**Devices**

- **Clientless – IPSG (IP)**
- **Clientless MAG (PMIPv6)**
- **Clientless eWAG (GTPv1)**
- **Clientless 3GPP2**
- **Clientless 3GPP**
- **Secure Client based iWLAN**

**Trusted Wi-Fi**

- VPN
- MAG
- eWAG

**IP Core**

- Un Tunnelled User Data (IP)
- Per User PMIPv6 Tunnel
- Per User GTP Tunnel
- Per User PMIPv6 Tunnel
- Per User GTP Tunnel
- Per User IPSec Tunnel

**Untrusted Wi-Fi**

- Per User IPSec Tunnel

**3G Cellular**

- HSGW
- SGSN

**Mobile Packet Core**

- TTG
- GTP (Gn)
- GGSN
- P-GW

**Multiple Applications Simultaneously Running on Session-Centric Operating System**

- WLAN AAA
- 3GPP AAA
- 3GPP2 AAA
Mobile Packet Core Integration: WiFi into 4G Core

All Client & Client-less options supported

- Secure Client based iWLAN
- S2c - DSMIPv6
- S2c - DSMIPv6
- Clientless 3GPP
- S2a - PMIPv6

Untrusted WiFi
- IPSec (SWu)
- S2c - DSMIPv6

Trusted WiFi
- S2c - DSMIPv6
- S2a PMIPv6

4G Cellular

WiFi AAA/BackEnd

Mobile AAA

Policy/Billing

MAG

SGW

ePDG

PGW

S1

S2b

Mobile Packet Core

SP WiFi & Small Cell
Cisco and/or its affiliates. All rights reserved.
Cisco Public
Cisco SP Wi-Fi Solution Standards

Air Interface
- IEEE 802.11a
- IEEE 802.11b
- IEEE 802.11g
- IEEE WMM/802.11e IEEE 802.11h
- IEEE 802.11n

AAA Functions
- IEEE 802.1X
- RFC 2716 PPP EAP-TLS
- RFC 2865 RADIUS Authentication
- RFC 2866 RADIUS Accounting
- RFC 2869 RADIUS Extensions
- RFC 3579 RADIUS Support for EAP
- RFC 3580 IEEE 802.1X RADIUS Guidelines
- RFC 3748 Extensible Authentication Protocol

Control & Provisioning AP
- RFC 5415 CAPWAP Protocol Specification
- RFC 5416 CAPWAP Binding for 802.11

Clientless
- AP

Encryption
- WEP and TKIP-MIC: RC4 40, 104 and 128 bits
- AES: CBC, CCMP, CCMP
- DES: DES-CBC, 3DES
- SSL and TLS: RC4 128-bit and RSA 1024- and 2048-bit
- DTLS: AES-CBC
- IPsec: DES-CBC, 3DES, AES-CBC

Security Standards
- IEEE 802.11i (WPA2, RSN)
- RFC 1321 MD5 Message-Digest Algorithm
- RFC 1851 The ESP Triple DES Transform
- RFC 2104 HMAC: Keyed Hashing for Message Authentication
- RFC 2246 TLS Protocol Version 1.0
- RFC 2401 Security Architecture for the Internet Protocol
- RFC 2406 IPsec
- RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPSec
- RFC 3686 Using AES Counter Mode with IPsec ESP
- RFC 4347 Datagram Transport Layer Security
- RFC 4346 TLS Protocol Version 1.1

Trigger
- RFC 1542 BOOTP
- RFC 2131 DHCP
- RFC 826 ARP

Mobility Support
- RFC 3775 Mobility Support in IPv6
- RFC 5213 Proxy Mobile IPv6
- RFC 5844 IPv4 Support for Proxy Mobile IPv6
- RFC 5846 Binding Revocation for IPv6 Mobility

S2a Interface
- 3GPP TS 23.402 Architecture Enhancements for Non-3GPP Accesses

Policing & Charging
- 3GPP TS 23.203 Policy and Charging Control Architecture
- 3GPP TS 29.212 Policy and Charging Control over Gx Reference Point
- 3GPP TS 32.240 Charging Architecture and Principles
- RFC 4006 Diameter Credit-Control Application

3GPP AAA
- MAP
- TCAP
- SCCP
- M3UA
- SCTP
- IPv4
- L1/L2

ASR5K
- PGW / LMA

Offline Billing
- PCRF
- OCS
- HLR

MAP Protocol
- 3GPP TS 29.002 Mobile Application Part (MAP) Specification
Cisco SP WiFi Functional Building Blocks

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
Access Gateway
PMIP = Proxy Mobile IP (v6)
UE = User Entity (mobile terminal)
WA = Web based Authentication

Access Aggregation Core
Use-Case 1: S2a access for 4G

**MAG on WLC, LMA on ASR5K: architecture for S2a**

- Cisco SP-WiFi Whole-Offer Solution: Model 2.x
- Uses S2a Interface on ASR5K
- Provides Signalling & Dataplane
- L2 and L3 mobility for inter & intra WLC groups
- Policy & Charging via Gx/Gy interface → Replicated via IP Diffserv
- Dynamic LMA selection via AAA intelligence
- WiFi treated as a 4G-like RAT
Use-Case 1.5: S2a access for 4G
MAG on AP, LMA on ASR5K: architecture for S2a

- Utilize Cisco vWLC and/or Flexconnect WLC
- Cloud-like deployment of WLC for RRM and management
- Local Break Out for AP
- AP will have MAG (R7.5+)
- Centralized WebAuth

**Diagram:**
- AP/MAG
- AP
- WLC
- AAA
- DNS DHCP
- Portal
- LMA
- GTP
- Subscriber Policy Enforcement
- MAG
- L3
- eWAG
- ASR5K
- WAG
- Internet
- Protected Area

**Network Components:**
- **Access:** UE, AP, WLC
- **Aggregation:** AP, WLC, LMA, GTP, eWAG
- **Core:** L3, ASR5K, Internet

**Security Protocols:**
- PMIPv6
- IPSec
- 802.1Q
- GTP
- R7.5
- R7.4
- R14.0

**Key Systems:**
- Cisco vWLC
- Flexconnect WLC
- Cloud-like deployment
- Local Break Out
- AP with MAG
- Centralized WebAuth
Case 1.7: WebAuth + S2a access for 4G

MAG & WebAuth on WLC, LMA on ASR5K: architecture for S2a

- WebAuth Service on WLC (internal, custom, external)
- Authenticated users are placed in MAG or VLAN for Local Break Out
- External AAA/Portal with Radius CoA needed
Use-Case 2.1: eWAG for 3rd Party WiFi

IP Native on 3rd Party WLC, eWAG on ASR5K

• 3rd party AP/Controller presents subscriber after authentication as L3 traffic
• AAA or DHCP triggered eWAG session creation
• Local Break Out supported
Use-Case 2.2: sGRE, GTP for 3rd Party WiFi

**sGRE 3rd Party WLC, ASR1K, GTPv1 on ASR5K**

- Aruba/ALU solution for use of sGRE as tunneled traffic
- Use ASR1K as sGRE to GTP WAG (scaling)
- Use ASR1K for WebAuth & Local Break Out
- Proxy subscribers to ASR5K using GTPv1
- DiffServ QoS to sGRE re-marking (needs to be explored)
- Q's around L2 and L3 mobility requirements

**Diagram Details:**
- AP/MAG, AP, WLC, AAA, DNS, DHCP, Portal, Flexconnect, PMIPv6, LMA, GTP, Policy Enforcement, L3, Internet, R7.4, 802.1Q, sGRE, IPSec, sGRE, L2, L3, GTPv1, L3, PMIPv6, WA, L3, ASR1K, ASR5K, R14.0.
Use-Case 2.3: GTP for 3rd Party WiFi

GTP via 3rd Party ePDN, ASR1K, GTPv1 on ASR5K

- Aruba/ALU solution for use of sGRE as tunneled traffic
- Use GTPv1 directly into ASR5K: sGRE anchor is the 7750
- Diffserv QoS to sGRE re-marking (needs to be explored)
- Q’s around L2 and L3 mobility requirements

- 802.1Q
- sGRE
- IPSec
- GTPv1
- L2
- L3
- AAA
- DNS DHCP
- Portal
- AP/MAG
- AP
- WLC
- MAG
- WA
- LMA
- LMA
- Subscriber Policy Enforcement
- GTP
- eWAG
- WAG

Access → Aggregation → Core

SP WiFi & Small Cell
Cisco and/or its affiliates. All rights reserved. Cisco Public
Use-Case 2.4: SaMOG, Inter-Carrier Roaming

PMIPv6 & 3rd Party WLC via sGRE, SaMOG on ASR5K towards Home/Visited EPC

- Aruba/ALU solution for use of sGRE as tunneled traffic
- Use ASR5K as sGRE to EPC Core (SaMOG)
- Use ASR5K TWAP for Authentication and Trusted WLAN Access Gateway (TWAG) for data path integration.
- Proxy subscribers to ASR5K using GTPv2 (home and visited)
- DiffServ QoS to sGRE re-marking (needs to be explored)
ASR5K SaMOG based SP Wi-Fi EPC Integration

CAPWAP CNTRL. & Data plane tunnels

PMIPv6 used to establish Dynamic L3-GRE tunnels

EAP messages over RADIUS from WLC to TWAP

EAP messages over DIAMETER

UE data traffic tunneled over GTP

Update the P-GW address for the UE session

UE Authorization Profile download AKA, AKA' Credentials

External IPv4 Networks
Practical Examples of SP-WiFi
Wi-Fi as a hotspot technology: a wireline service

Wi-Fi as a mobile offload technology: a cellular network optimization tool

Wi-Fi as a platform for:
- Service innovation
- Revenue growth
- Experience transformation
Example: Super Bowl XLVI
Connected Stadium

- Fan facing Wi-Fi access for Super Bowl activities
- Carrier-neutral Wi-Fi access – free to all fans
- Provided by Verizon wireless
- Objective: increased fan experience and 3G offload
- High speed data as well as Voice & SMS worked well
- 604 in-stadium Access Points

Downstream
Peak: 75 Mbps
Total: 225.3 GB

Upstream
Peak: 42 Mbps
Total: 144.6 GB

Total attendance: 68,658
Unique Associations: 12,946 (19%)
Simultaneous access: 8,260 (12%)
Use Case: Super Bowl XLVII
Connected Stadium

• Fan facing Wi-Fi access for Super Bowl activities
• Carrier-neutral Wi-Fi access – free to all fans
• Provided by Verizon wireless
• Objective: increased fan experience and 3G/LTE offload
• High speed data as well as Voice & SMS worked well
• 1229 in-stadium Access Points

<table>
<thead>
<tr>
<th></th>
<th>Downstream</th>
<th>Upstream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak</td>
<td>185 Mbps</td>
<td>400 Mbps</td>
</tr>
<tr>
<td>Total</td>
<td>442 GB</td>
<td>683 GB</td>
</tr>
</tbody>
</table>

Total attendance: 71,024
Unique Associations: 9,556 (13%)
Simultaneous access: 5,569 (8%)
Example: Montreal Formula 1 Event

WiFi Network Observations

- Cisco worked with a Canadian Telecom Service Provider to install and operate a WiFi network for the Montreal F1 event
  - The network covered 2 bleachers, 2 VIP areas; roughly 50 K Square feet
  - 50 APs (3600 and 1552 from Cisco)
  - Fiber backhaul – 200Mbps

- Network statistics over 3 days:
  - Just under 3,300 users at peak (race day)
  - Peak Upstream Bandwidth = 52Mbps (race day)
  - Peak Downstream Bandwidth = 28 Mbps (race day)
  - Total traffic over three days 144Gb
  - Average users at the same time = 2,200
Questions?
Check out our SP-WiFi and Small Cell Solution setup at our World of Solutions Showcase
Thank you
Complete Your Paper Session Evaluation – Wednesday April 16

Give us your feedback and you could win 1 of 2 fabulous prizes in a random draw.

Complete and return your paper evaluation form to the Room Attendant at the end of the session.

Winners will be announced today at the end of the session. You must be present to win!

Please visit the Concierge desk to pick up your prize redemption slip.

Visit them at BOOTH# 407