



Next Generation Hotspot & SP Wi-Fi

Karrthik Venu

Agenda

❖ *Next Generation Hotspot*

Trends and Drivers

Cisco VNI on WiFi

Technology and Architecture

Hotspot 2.0

MSAP

WBA/WFA Initiatives

Q&A

❖ *SP Wi-Fi*

Trends and Drivers

Business Models

Deployment Strategies

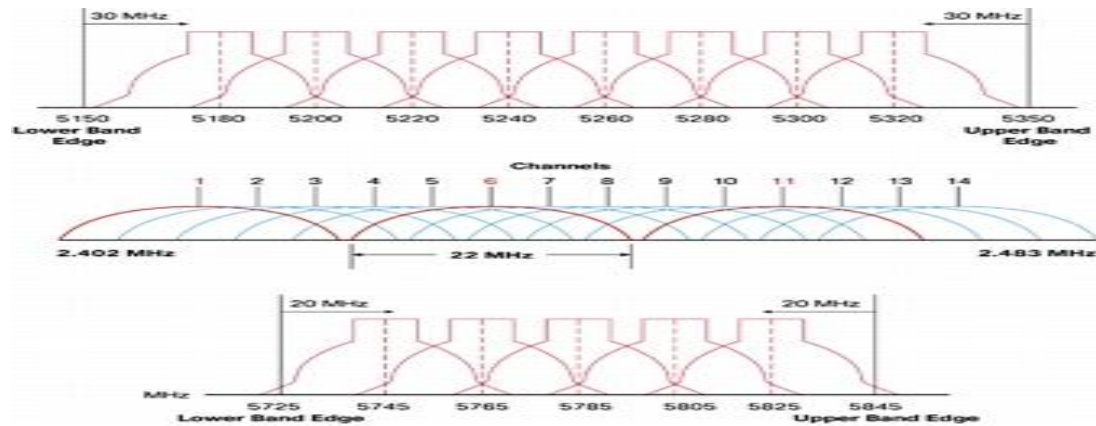
Technology and Architecture

Phased Approach

Q&A

Wi-Fi Regulation

Malaysia Regulations allows following frequencies for License-free operation



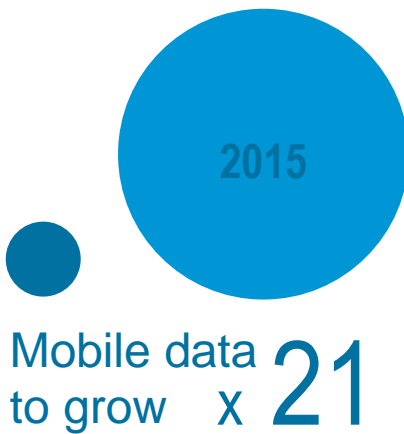
C Domain	Indoor Environment	Outdoor Environment
2.4Ghz	2.400 – 2.500 Ghz	2.400 – 2.500 Ghz
EIRP	27 dbm	27 dbm
Non Overlapping Channel	3 (20 Mhz)	3 (20 Mhz)
5Ghz	5250-5350 MHz 5725-5875 MHz	5250-5350 MHz 5725-5875 MHz
EIRP	30 dbm	30 dbm
Non Overlapping Channel	8 (20 Mhz)	8 (20 Mhz)



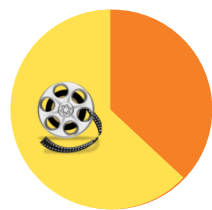
NGH

Trends and Drivers

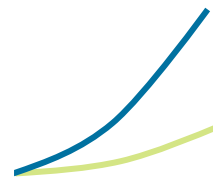
Raise of Data Traffic ..



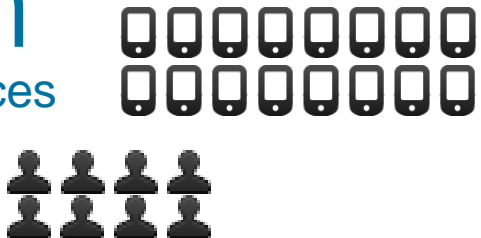
About **70%**
Will be video



Mobile data grow rate will be
x3 faster
than fixed IP
traffic growth



5.5 billion
Connected devices
(1 per capita)



Avg. mobile user to
generate about

1.6 GB /month
Comparing to 97MB
today



Source: Cisco Visual Networking Index 2011

Where its coming from ..

Typical locations accessed by a consumer


Location attractiveness ratings

Subscriber density

Time availability

Quality of experience

Home




L

H

H

Office/ university campus/ libraries




H

H

H

Restaurant, shopping mall




H

M

H

Nursing home/ hospitals




M

M

H

Train/ station, airport/ aircraft, taxi

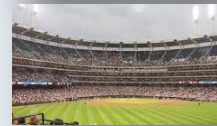


H

H

H

Stadium/ concert arenas



H

H

H

In transit at local/ main streets



M

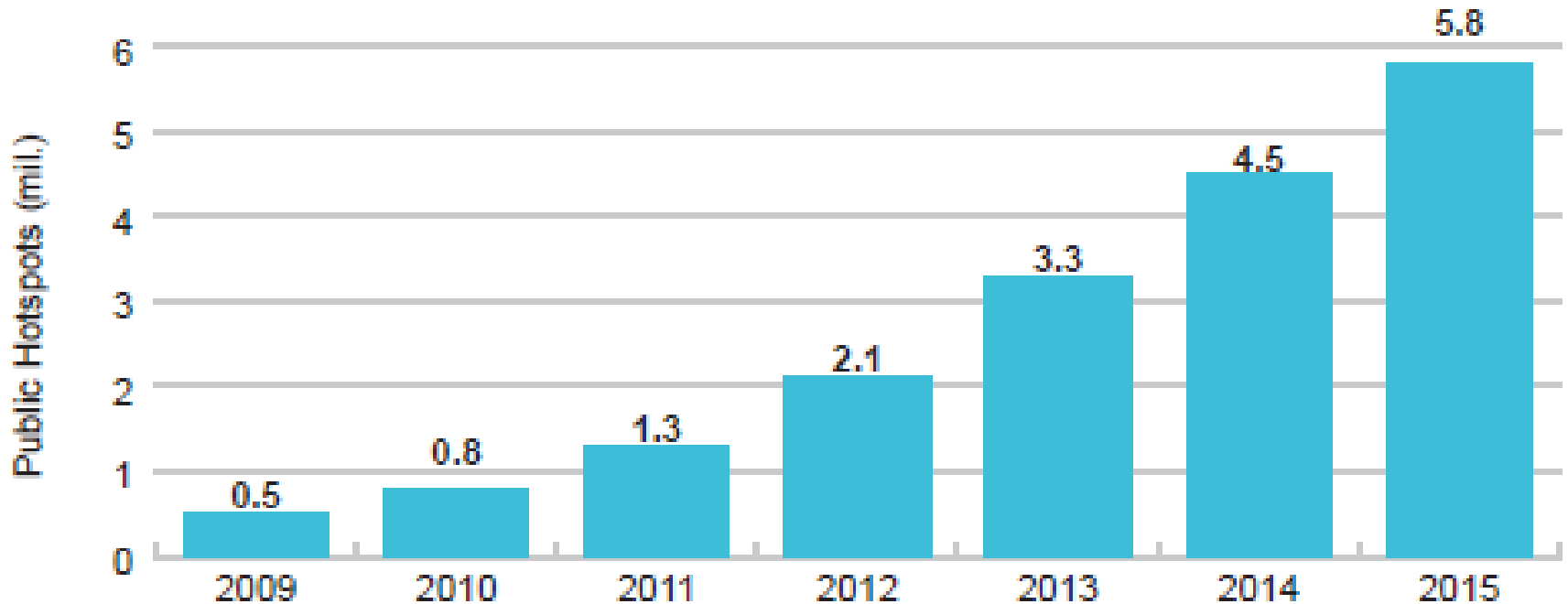
L

L

Ubiquitous Hot Spots .. WBA Report

- WBA's comprehensive survey of 259 service providers and Wi-Fi vendors reveals that global public Wi-Fi hotspot numbers are set to grow from 1.3 million in 2011, to **5.8 million**

Fig. 4: Global number of public Hotspots, 2009-2015

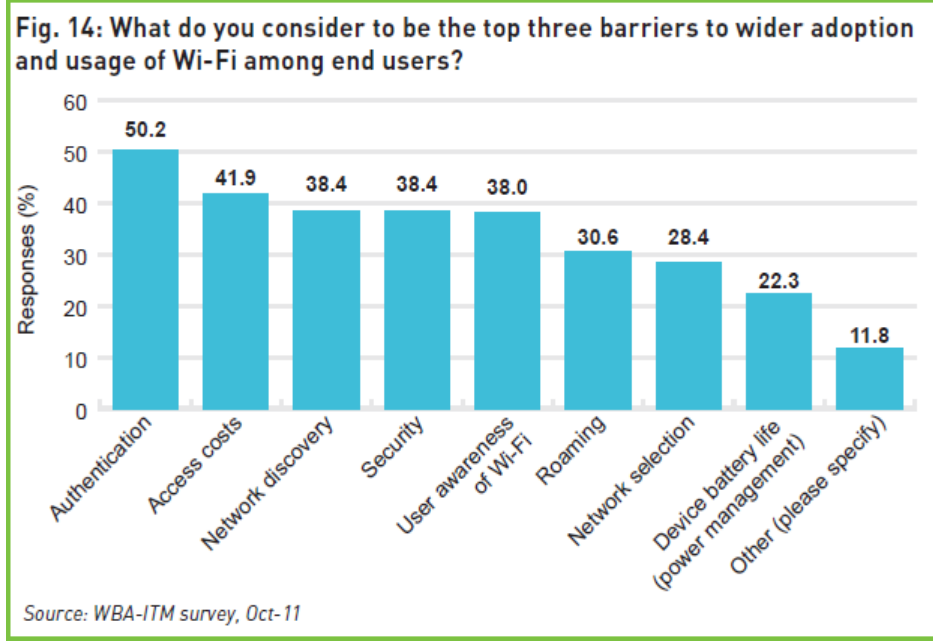
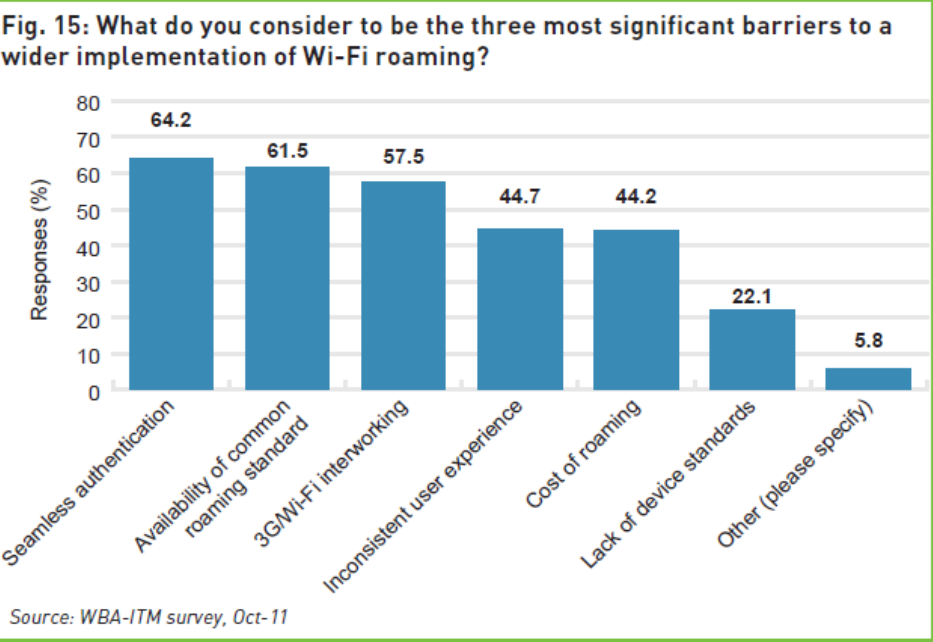


Source: Informa Telecoms & Media

Hurdles in Hotspots ..

Top barriers to wider implementation of Wi-Fi roaming:

Top barriers to further adoption and usage of Wi-Fi:



❑ Network discovery, identification, connection, authentication and security all key for seamless integration of Wi-Fi and cellular networks



NGH

Technology and Architecture

Next Generation Hotspot Vision:

GSM

Example: GSM Phone



Turn on phone and get secure cellular connectivity

NGH

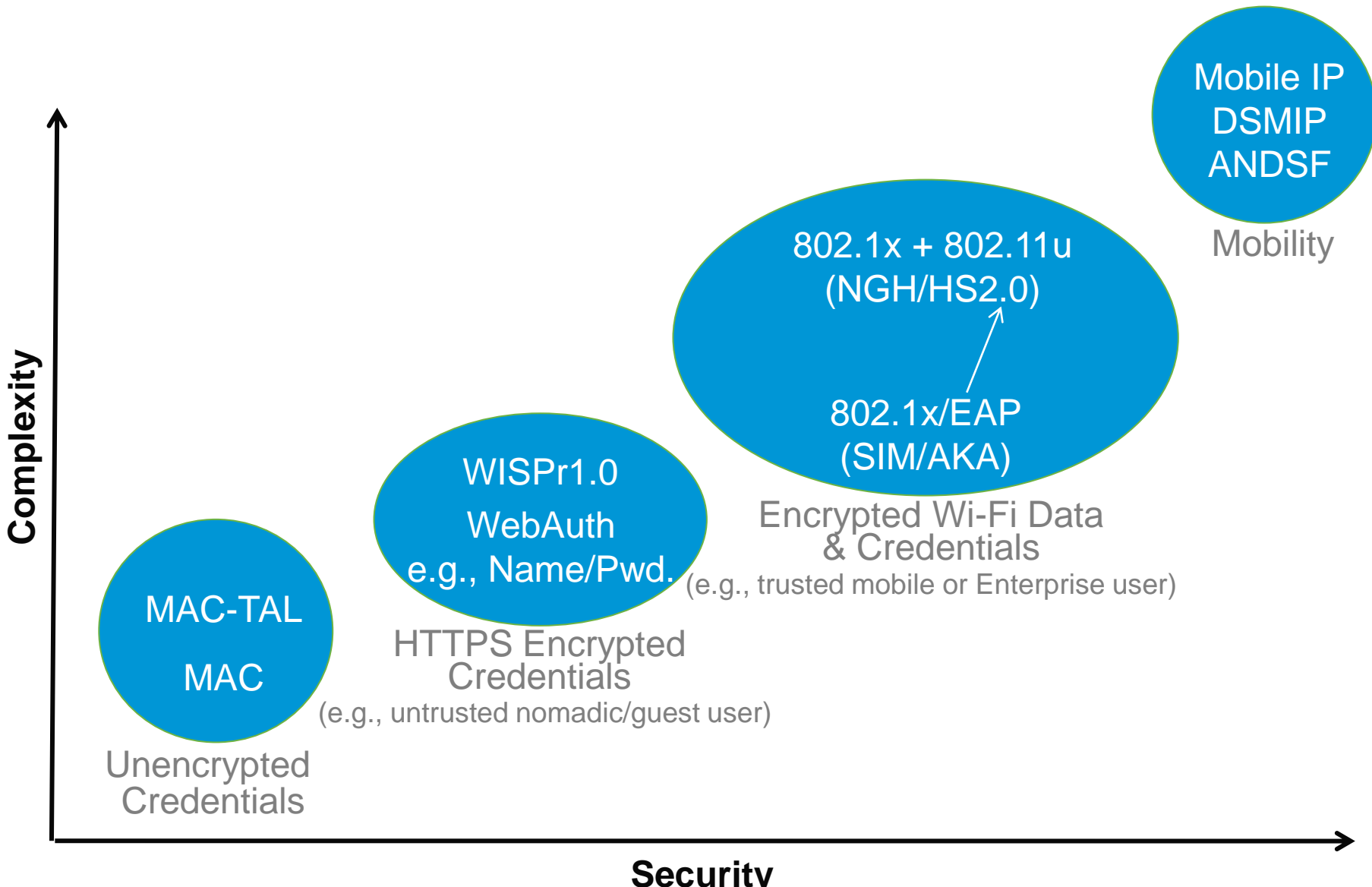
Example: iPhone



Turn on phone and get secure WiFi connectivity

NGH: A cellular-like secure Wi-Fi roaming experience

End User Experience – Today , Tomorrow



The Wi-Fi Alliance's 2-Phase Hotspot 2.0 Certification

- Phase 1: Network Selection and Security (June 2012)
 - 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
- Phase 2: Online Signup and Policy Provisioning (March 2013)
 - 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
 - Secure connection to signup server via WPA2-Enterprise enabled WLAN

Network Selection Prior to IEEE 802.11u

- SSID is the sole identifier used for Wi-Fi network selection
- If the Wi-Fi network is open (i.e., no encryption)
 - Whether mobile device's connection manager recognizes the SSID or not, the mobile device can join
 - Authentication notes:
 - In webauth authentication, the captive portal (e.g., visited provider) receives clear-text password (not good for roaming)
 - Mobile devices can be spoofed into providing their password to an Evil Twin AP
- If the Wi-Fi network is encrypted (e.g., WPA2-Enterprise)
 - If the mobile device's connection manager does not recognize the SSID, no further action is taken
 - To join, the mobile device must possess a pre-provisioned profile which contains the binding of {SSID, credential, EAP method(s), AAA server ID, trust anchors}
- There is no way for the Hotspot to signal roaming partners—the only option is for the SP to manage long lists of roaming-partner SSIDs/profiles in the mobile

Network Selection with IEEE 802.11u

- All the legacy methods (i.e., pre-11u) still work! And can be used!
- ***The new question is whether the mobile device has credentials to successfully authenticate with the Wi-Fi access network, NOT whether the SSID is recognized***
- IEEE 802.11 GAS/ANQP provides 3 types of identifiers a mobile device can use to determine whether successful authentication is possible
 - Realms, provided in NAI Realm List
 - PLMN ID, provided in 3GPP Cellular Information List
 - OUI, provided in Roaming Consortium List
- This ANQP-provided information identifies the authentication domains of the hotspot operator and all of its roaming partners
- The hotspot is responsible for carrying out authentication, often using Proxy AAA service
- The home SP is no longer required to manage long SSIDs lists on every mobile device—this responsibility has been transferred to the network

Network Selection with IEEE 802.11u: ANQP Messages Identifying Authentication Domains

- NAI Realm List

A list of **realms** (i.e., username@realm) which can be successfully authenticated

If the mobile device finds a realm in the list matching one of its credentials, successful authentication is possible

Either EAP-TLS (certificate credential) or EAP-TTLS with MSCHAPv2 (username/password credential) is used depending on the credential type provisioned by the Home SP

- 3GPP Cellular Information

A PLMN ID list; a PLMN ID is assigned to every cellular operator and has the form {MCC, MNC}

If the mobile device finds a PLMN ID in the list matching the one from its SIM credential, successful authentication is possible

Either EAP-SIM (2G/3G SIM credential) or EAP-AKA (4G USIM credential) is used depending

- Roaming Consortium List

A list of OUIs (organizationally unique identifier)—essentially the OUI part of a MAC address obtained from IEEE

If the mobile device finds an OUI in the list matching the one it's been provisioned with, successful authentication is possible

This method can be used with Aggregators (e.g., iPass) and for other special purposes

For OUIs in the beacon, this is a very battery efficient roaming method (no ANQP queries needed)

Example: Connection Manager Selecting a Network Using Scanning and Policy

- Mobile device has certificate credential
- Mobile device scanned and found 5 HS2.0 networks
- Mobile performed GAS/ANQP query and discovered that 4 of the 5 hotspots had SP.com as a roaming partner

Policy:
PreferredRoamingPartnerList

FQDN	Priority
bar.com	1
verizon.com	10
orange.com	130
default	128

ANQP Query Responses

Hotspot No.	SSID	Domain Name List ¹	NAI Realm List + 3GPP INfo ²	Policy Priority
1	FT	orange.com	280-00, sp.com	130
2	Ozone	verizon.com	311-480, sp.com	10
3	bar	bar.com	sp.com	1
4	ORD	boingo.com	sp.com, 311-480, 310-260	128
5	dog	cat.com		

Mobile associates to "bar", highest priority network



Can't authenticate



Default priority assigned to hotspot operators not in above list

Notes:
1. Hotspot operator
2. Hotspot roaming partners

NGH Technology Component

Authentication & Roaming

Network Discover & Selection

L2 Authentication

Layer 2 Air Encryption

L3 Authentication

HS Network

Roaming

Hotspot (today)

SSID

None

None

WebAuth
WISPr 1.0/2.0

Untrusted

Manual



NGH (HS2.0 Spec)

802.11u

802.1x

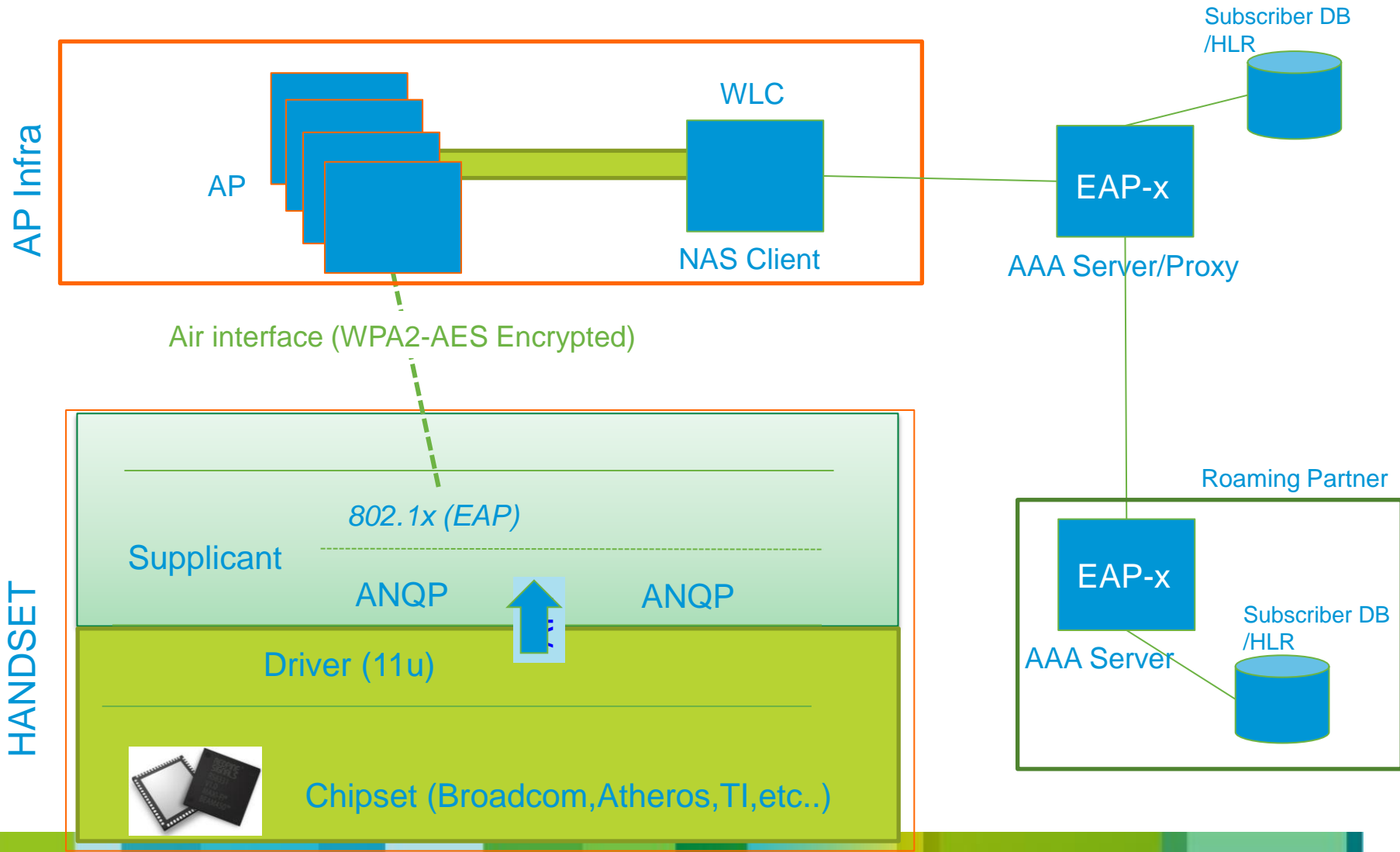
802.11i

EAP-SIM,
AKA, TLS, TTLS

Trusted

Yes

NGH System Component



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

Regular Client



Hotspot 2.0 Client



Can you tell me your network info?
Before I associate?

Automatic Setup

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

NAI Realm / 3GPP Cellular Info
Domain Name (hotspot operator's FQDN)
HS2.0 Info

Yes! Here it is:
Realm Name = comcast.com
Auth.type = EAP-TLS

- Makes Wi-Fi easy-to-use and secure like 3G cellular
- 802.11u enabled network is compatible with non-11u devices!

Customer Experience Transformation: Trial of Mobile Concierge with MSAP

Reach customers at the moment of choice

..T..Systems..

T-Systems Multimedia Solutions

Secure Wi-Fi Network Discovery

Special offers today

Receive transient applications without user intervention

http://shopping-mall.app

TARGET WEB COUPON EXPIRES 03-30-2011

digistore

Limit one coupon per guest, one item or offer per coupon. Void if copied, transferred, purchased, sold or prohibited by law. No cash value. Offer good while quantities last. Maximum retail value 5.70 for free item.

9856-0113-9294-1115-1224-4724-47

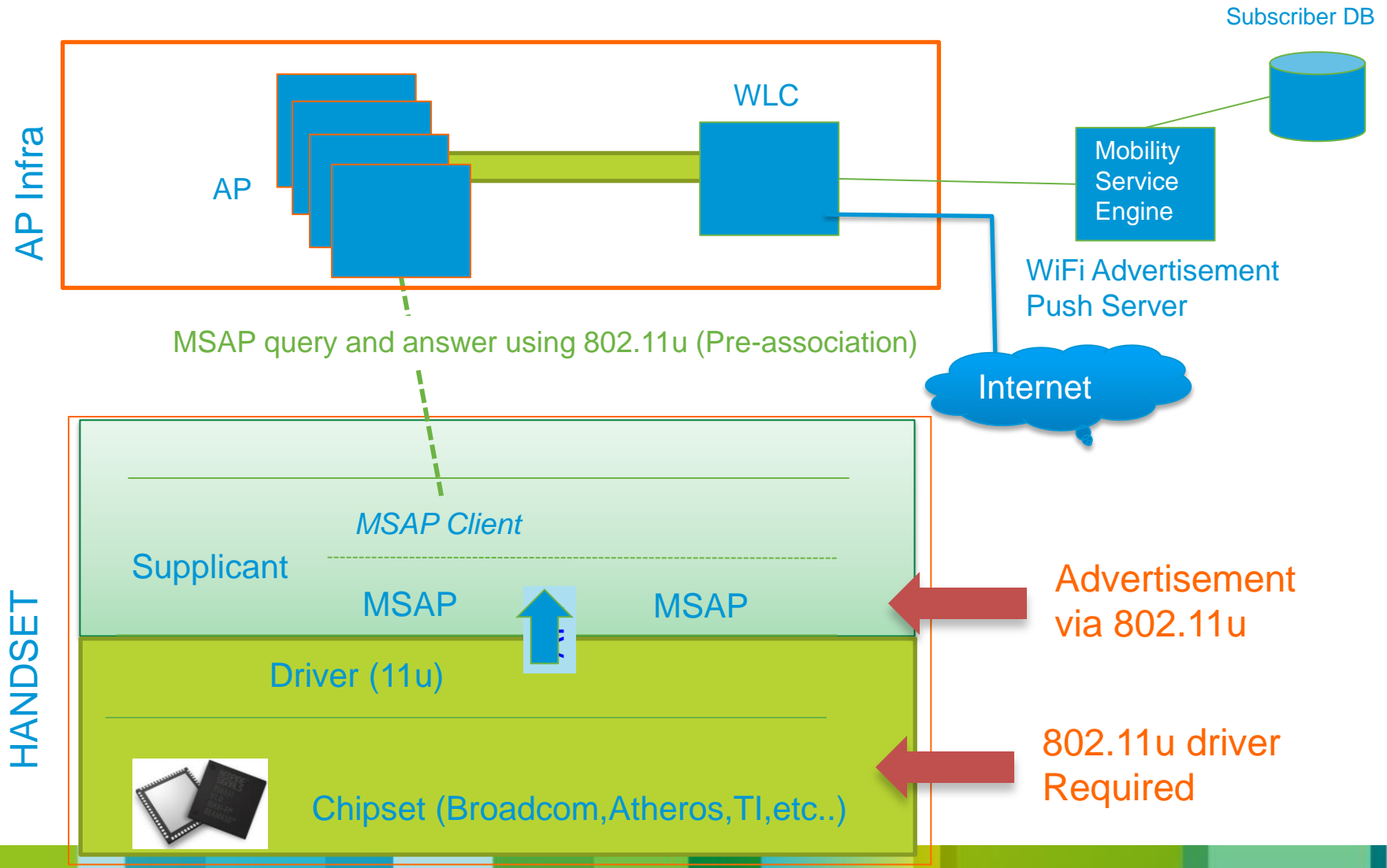
MAP SHOPS

MOBILE WORLD CONGRESS
Barcelona | 14-17 February 2011

T-SYSTEMS MULTIMEDIA SOLUTIONS

A New Mobile Experience for Mobile Subscribers

WiFi Advertising via HotSpot 2.0



NGH Program at WBA



WBA NGH Program 2011



Joint Taskforce

Objectives:

- Make Wi-Fi-Wi-Fi roaming as easy and transparent as GSM
- Common technical implementation for 3GPP-WiFi interworking
- 3GPP-WiFi integration seamless and transparent to the customer

NGH Operators Guide

Best practices guide for operators

- Implement seamless authentication over Wi-Fi networks based on NGH
- Transition from legacy to NGH networks
- Implement 3G/4G data offload over NGH networks
- Use lessons from past WBA seamless authentication trials & the NGH Trial

NGH Trial

End-to-end “Real-World” Wi-Fi roaming trial to

- Test & validate NGH
- Engage ecosystem including operators, equipment providers and roaming hub providers for end-to-end testing
- Provide detailed instructions for NGH based roaming lifecycle and feedback on the Wi-Fi Alliance specifications

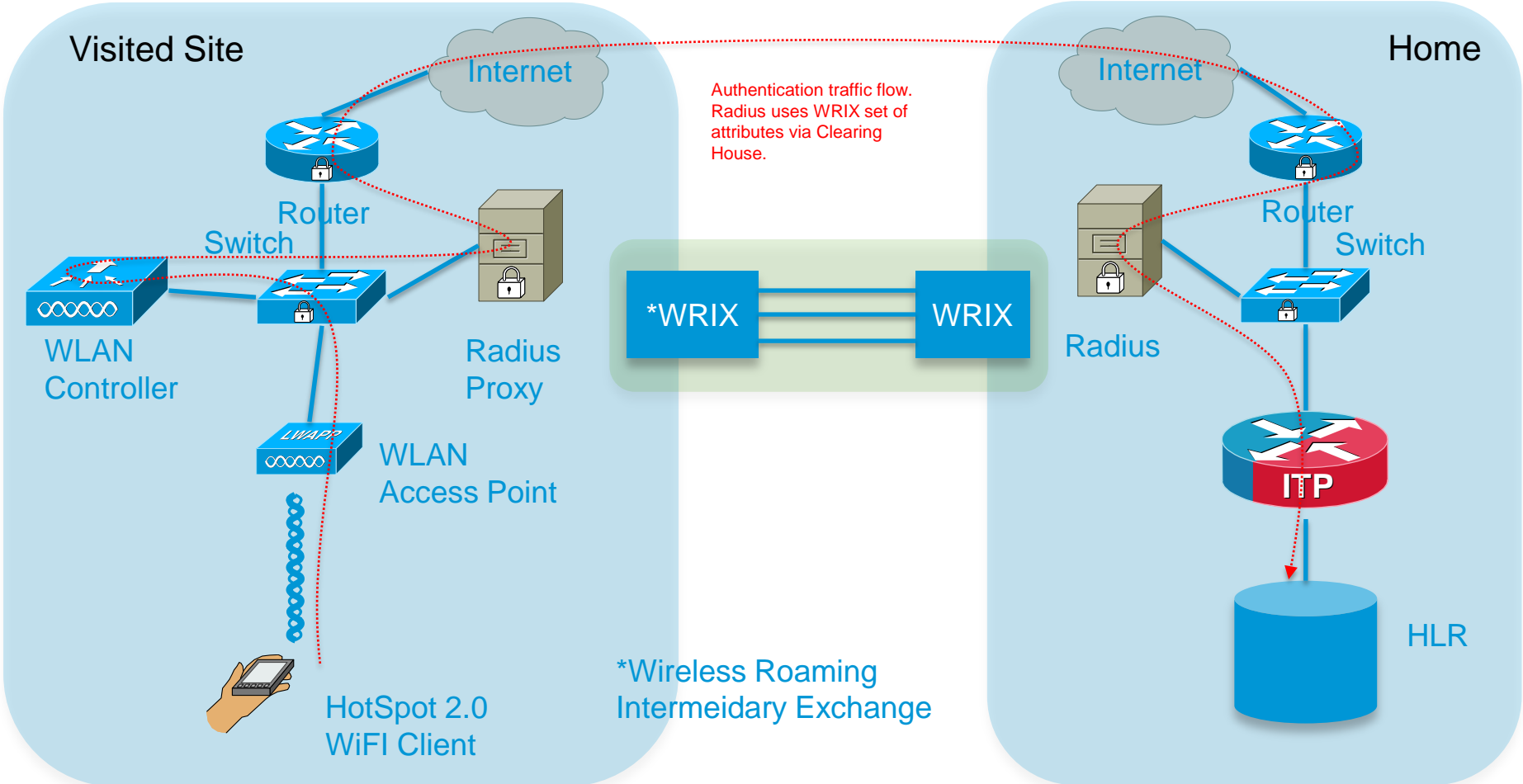
Enhancement to support NGH Roaming

Cooperation Framework

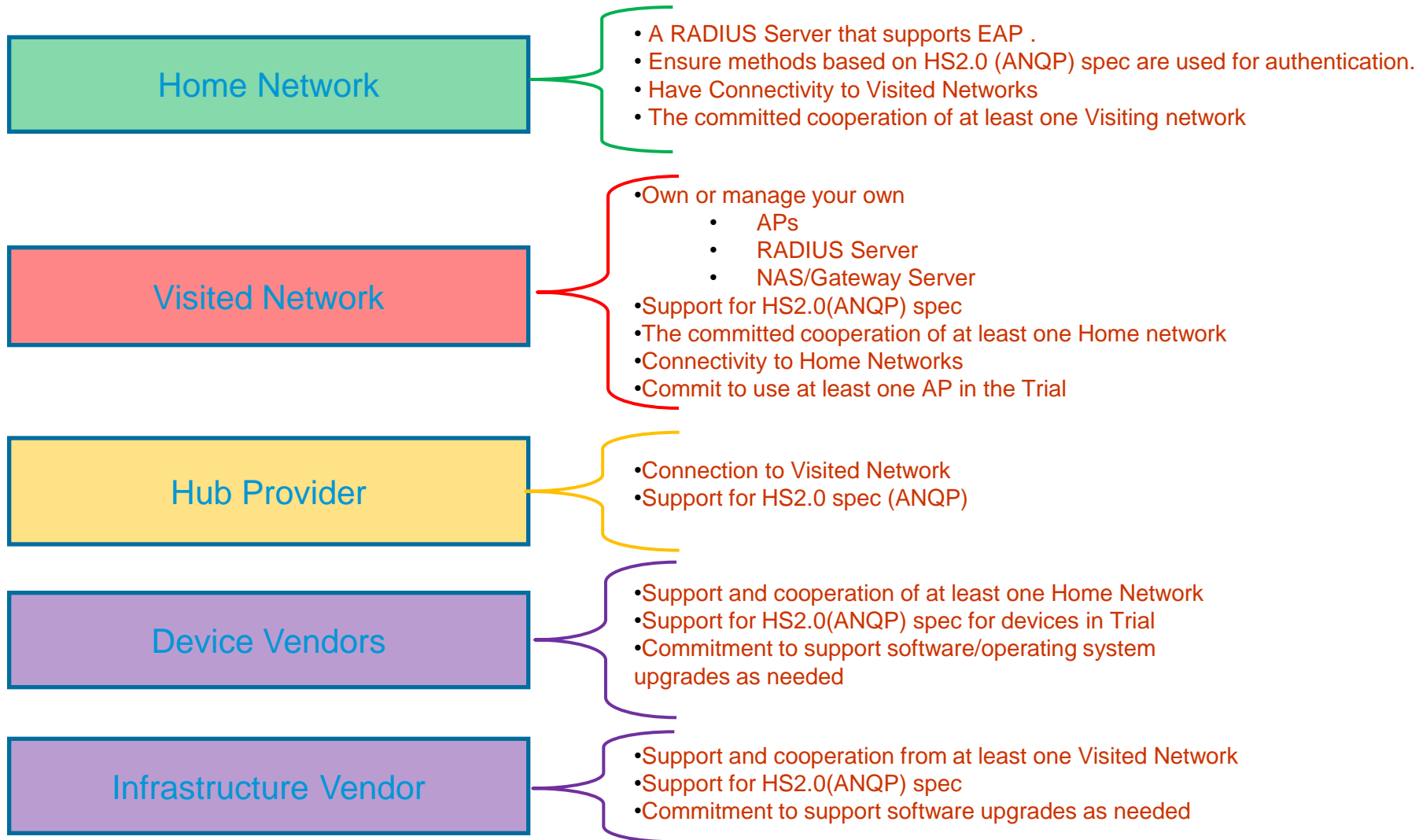
Objectives:

- Have a complementary focus and cooperation that maximizes the benefits of innovation for end users, manufacturers and service providers within the Wi-Fi industry
- Join effort to promote the benefits of WBA’s NGH program & Wi-Fi Alliance CERTIFIED Passpoint™ program among the wide ecosystem associated with the Wi-Fi industry

NGH Trial



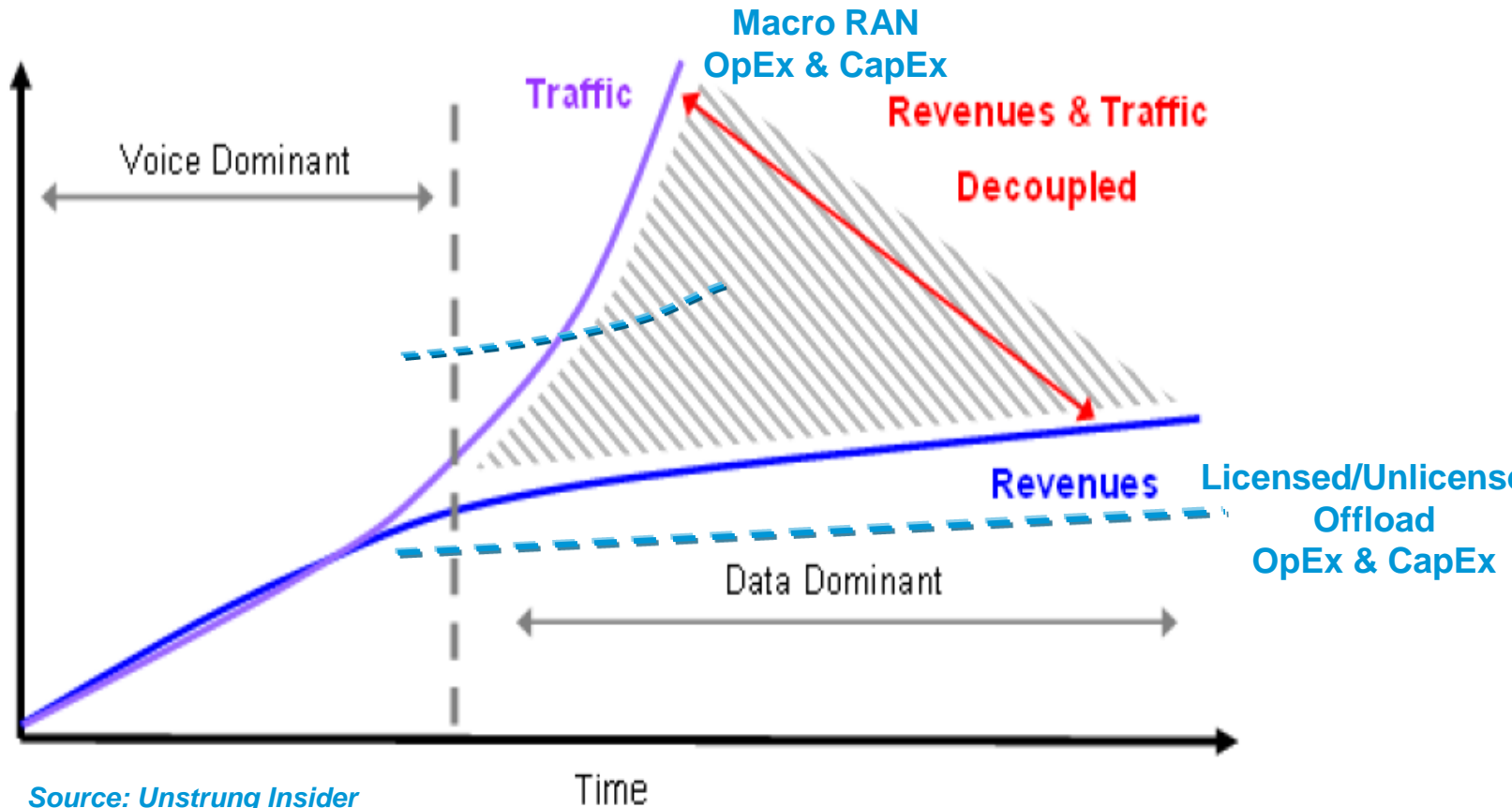
Expectations for Trial Participants



SP Wi-Fi

Trends and Drivers

Mobile Operator Financial Reality



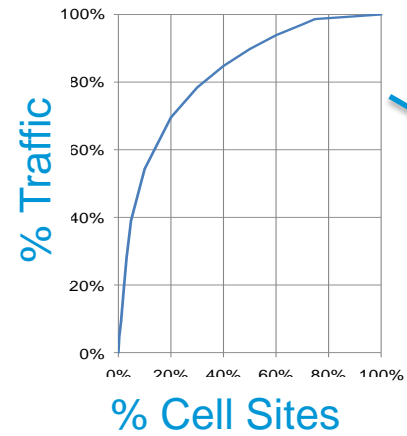
Source: Unstrung Insider

The Licensed/Unlicensed Offload OpEx & CapEx Spend is quite flat!

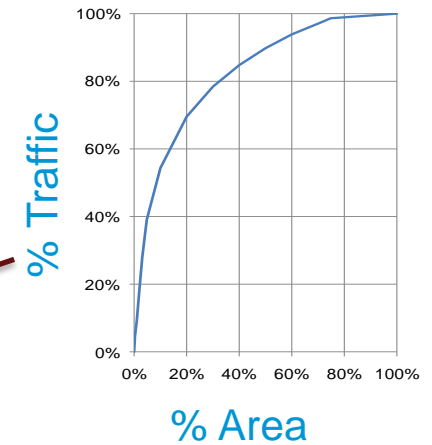
Offload price reductions will drop the line from \$2/subscriber/month (today) to \$1/subscriber/month in 3 years

The economics of mobile networks are complex

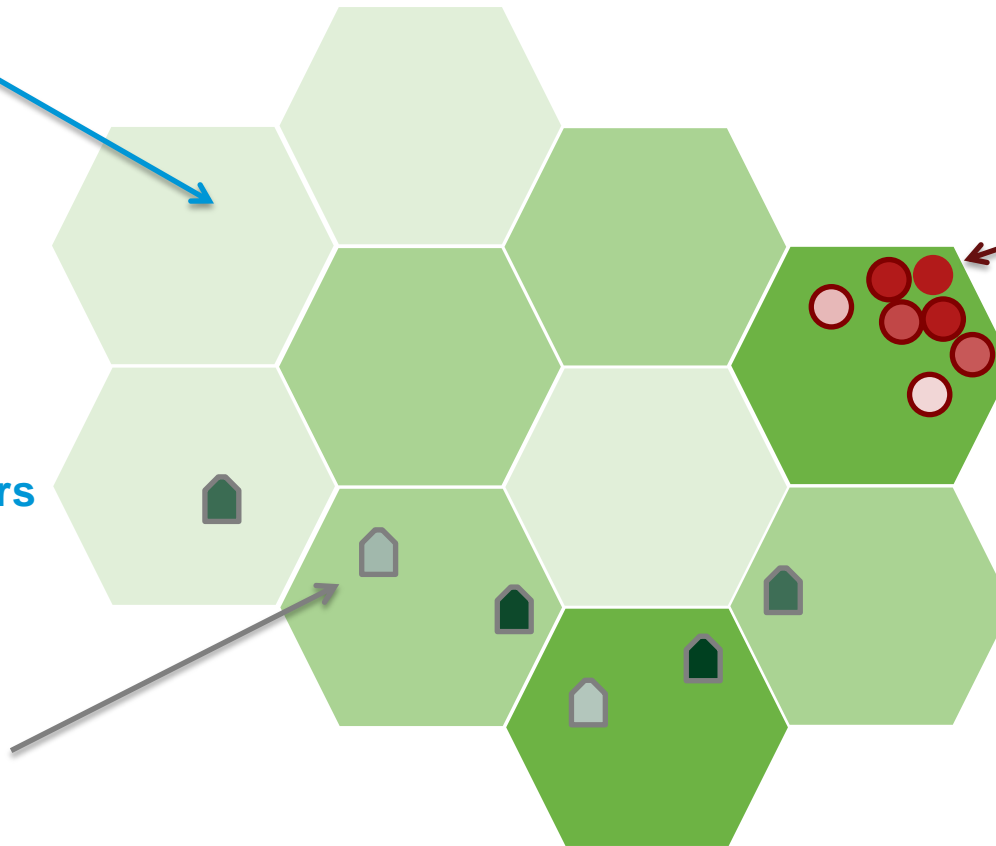
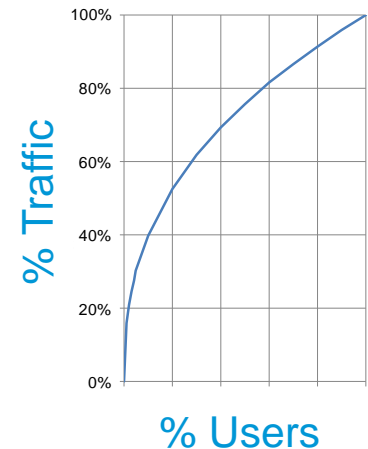
Distribution of Cells



Distribution within Cell



Distribution of Users

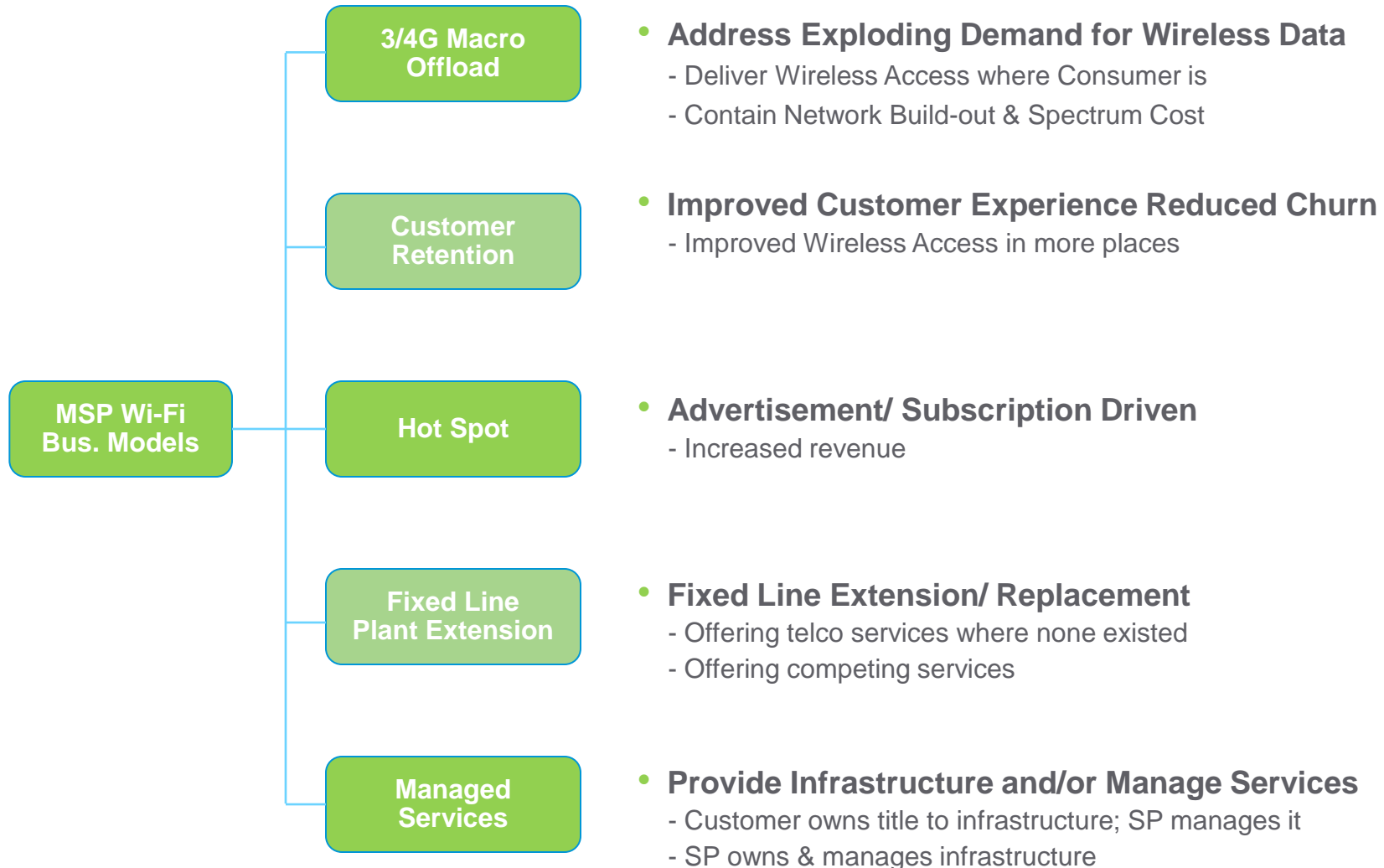


Distribution of Traffic

- 3G
- 3G or Wi-Fi
- 4G, 3G or Wi-Fi

Source: Cisco IBSG Research & Economics Practice, 2011.

MSP Economic Drivers

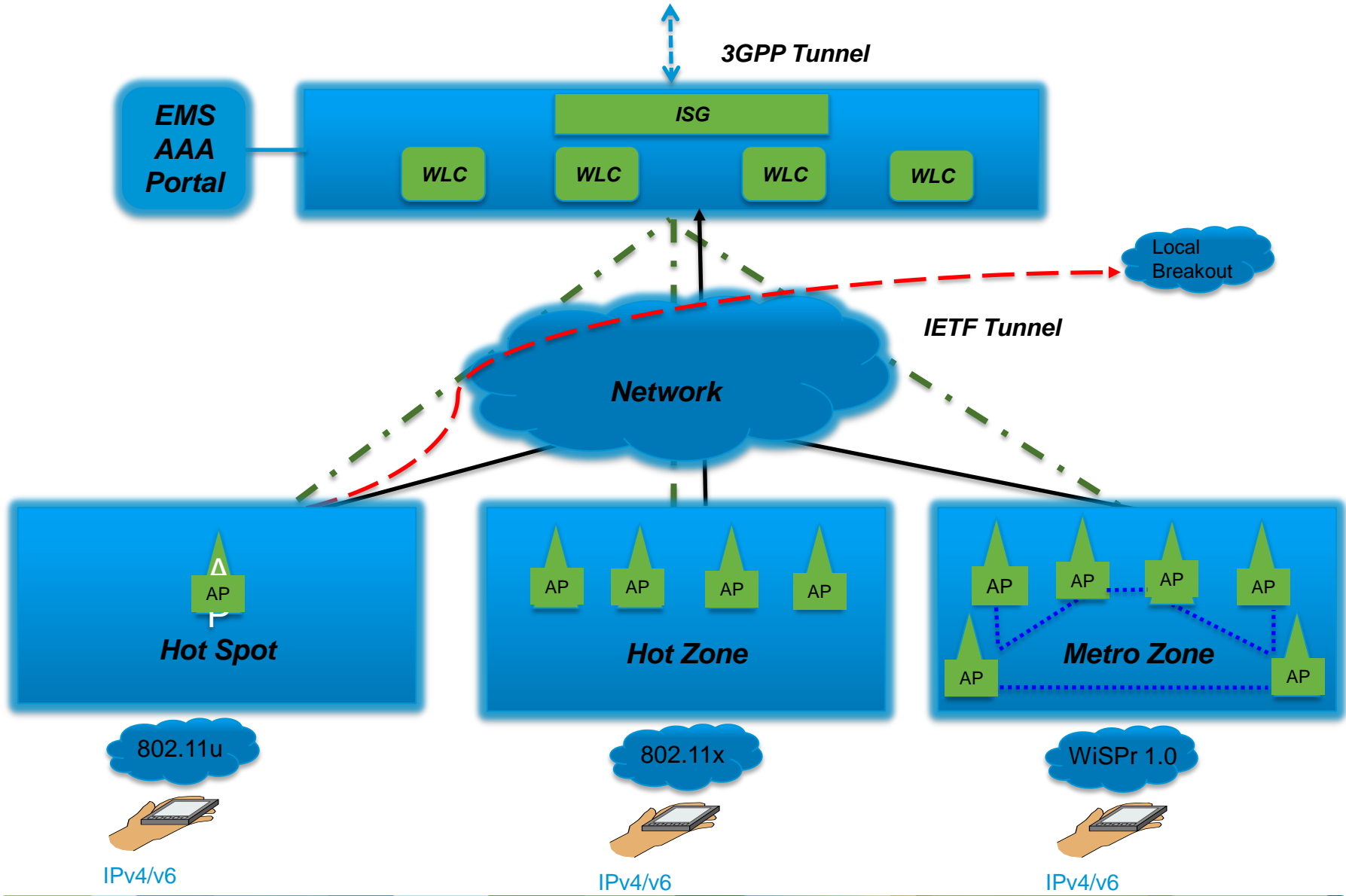




SP Wi-Fi

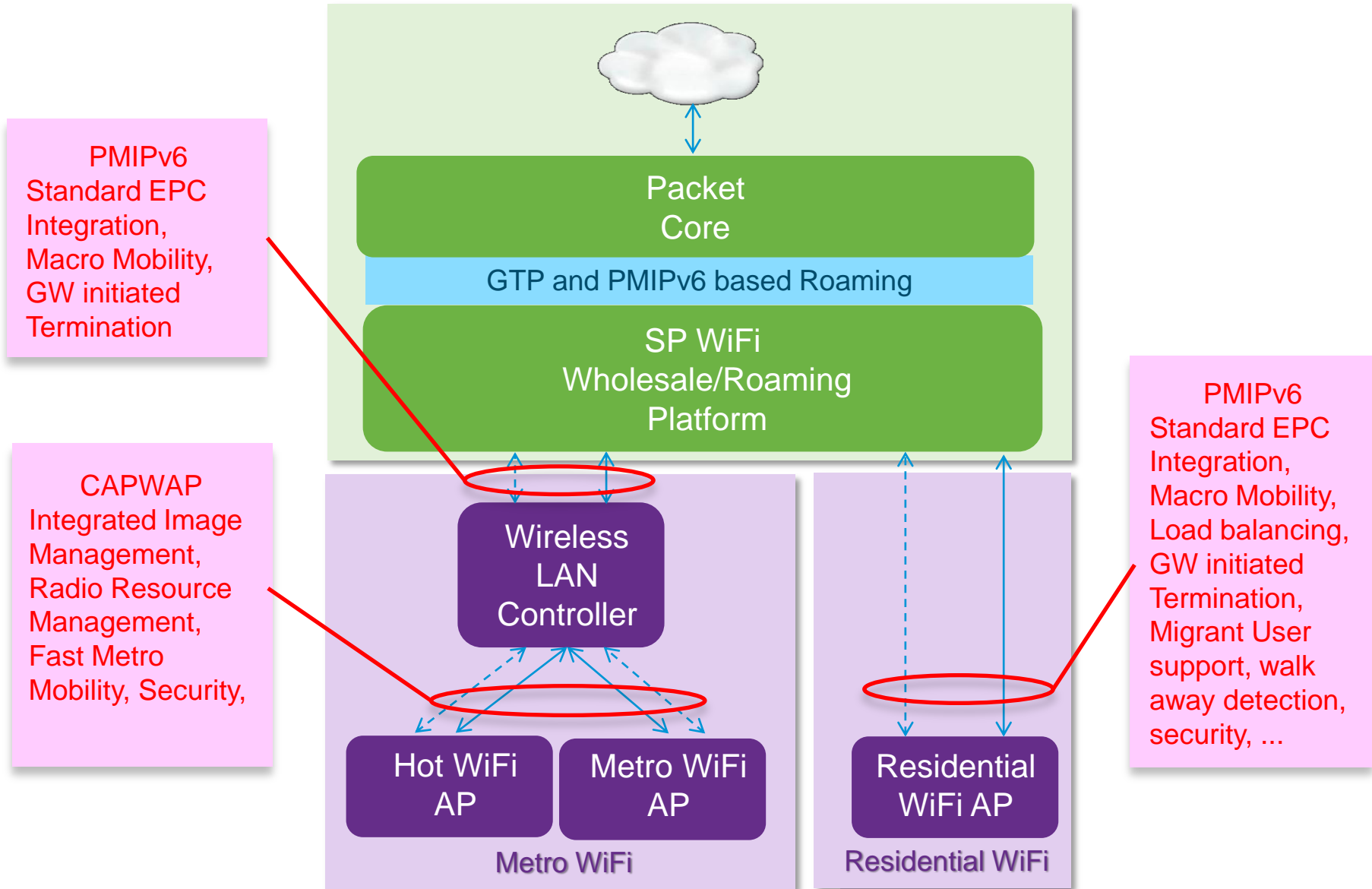
Technology and Architecture

Cisco SP Wi-Fi Unified Architecture

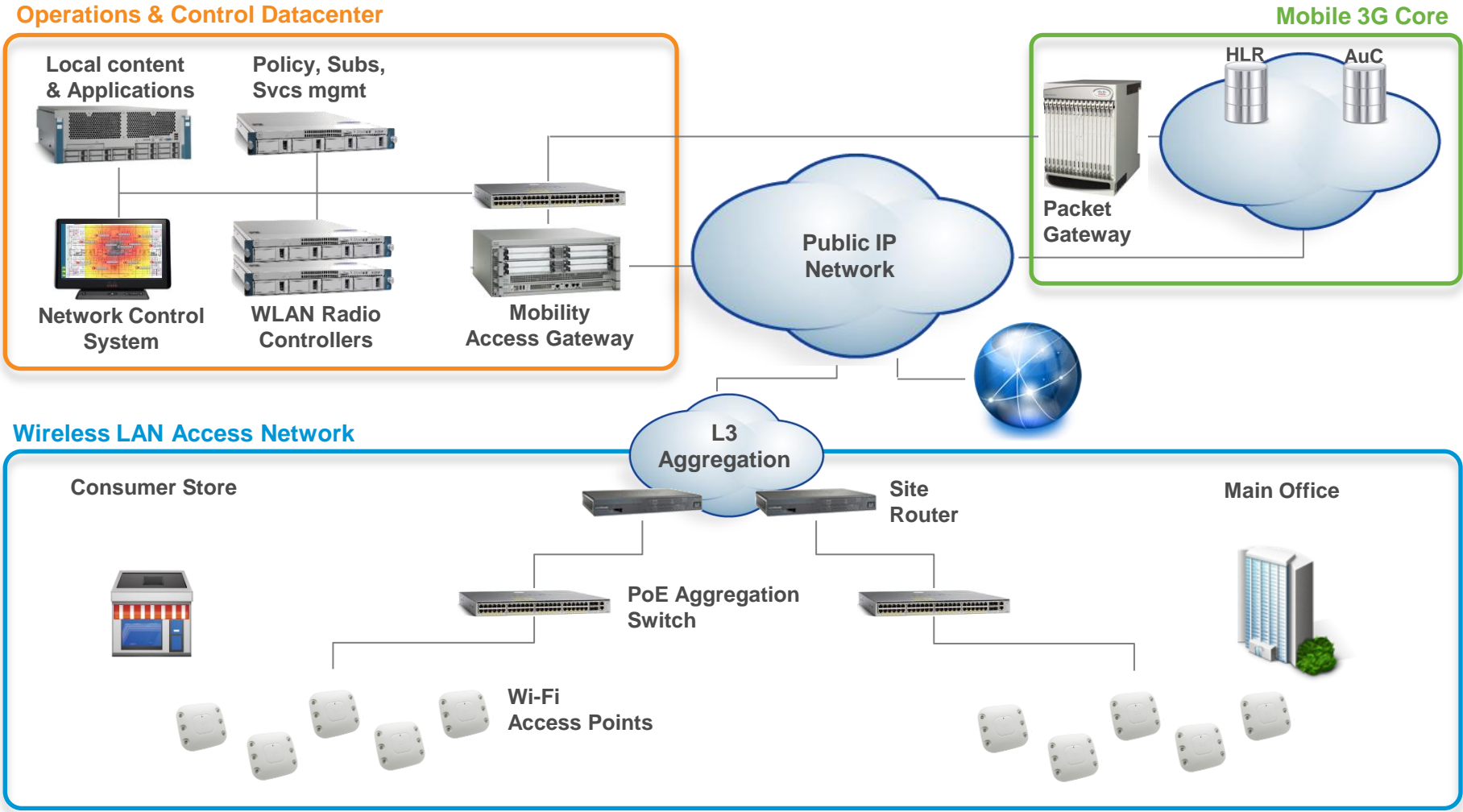


Cisco SP WiFi Unified Architecture

Delivering Converged Policy and Wholesale Services



SP-WiFi 3G Offload Approach Implementation



SP-WiFi: Key Benefits for Service Providers

3G-like experience

Extend the mobile service in a transparent manner



New revenues

Generate new revenue streams via innovative wireless services



High-speed access

Provide higher speeds for smartphone users cost-effectively



Brand enhancement

Associate service provider brand with innovation & consumer experience



Reduce churn

Increase customer loyalty & stickiness offering a complementary service



Thank you.

