WiFi Offload Architectures

Peter Gaspar
CSE, SP Mobile, EM East

June 2011

Agenda

- Motivation
- Offload Architectures
- Cisco SP WiFi Solution Core
- Cisco SP WiFi Solution Radio
- Summary

Motivation

Global Mobile Data Traffic Growth

Mobile Video Driving Traffic Explosion

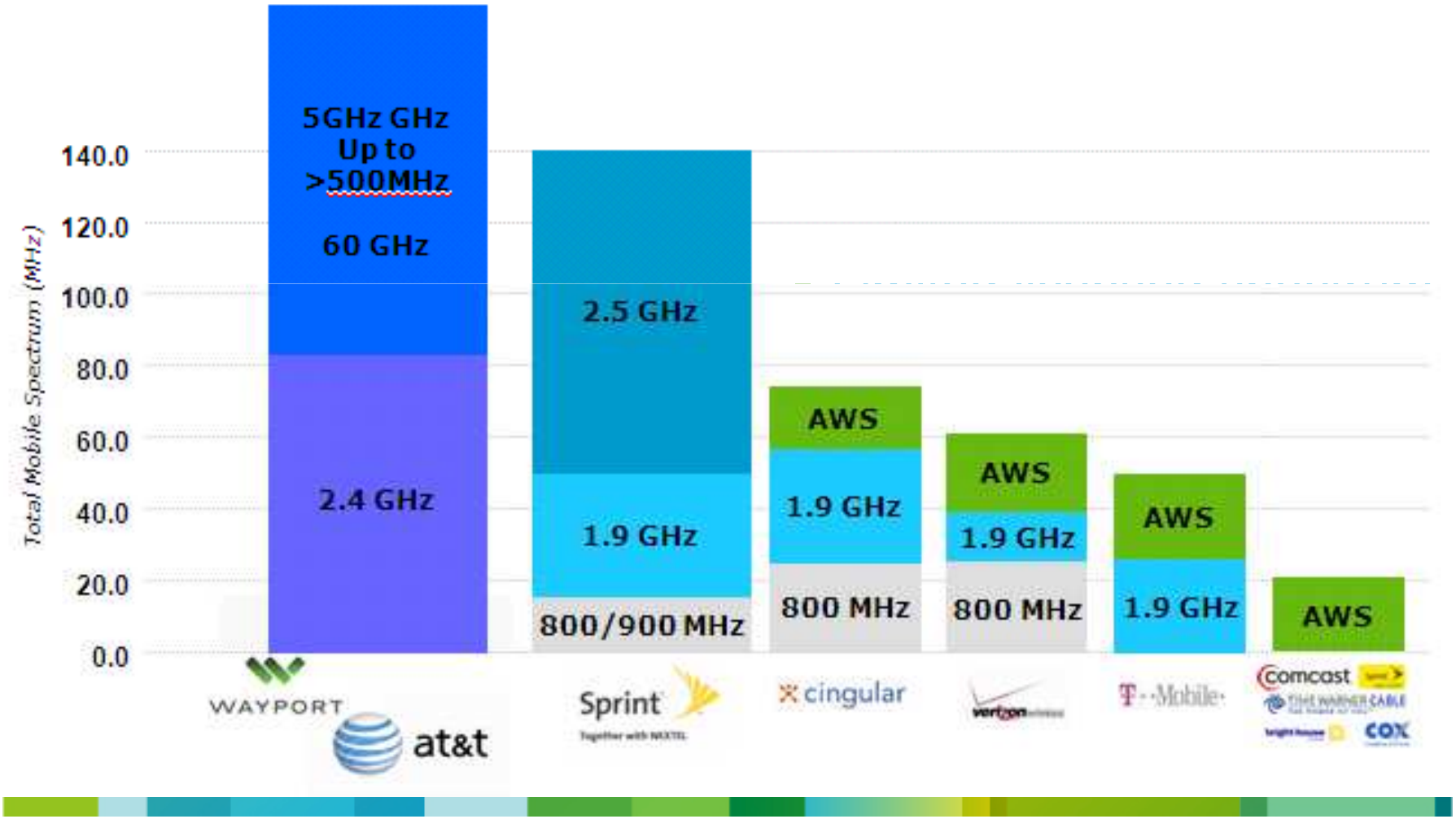
There will be 5B mobile devices and 2B M2M nodes

Global mobile traffic will grow 26X to 6.3 EB/mo

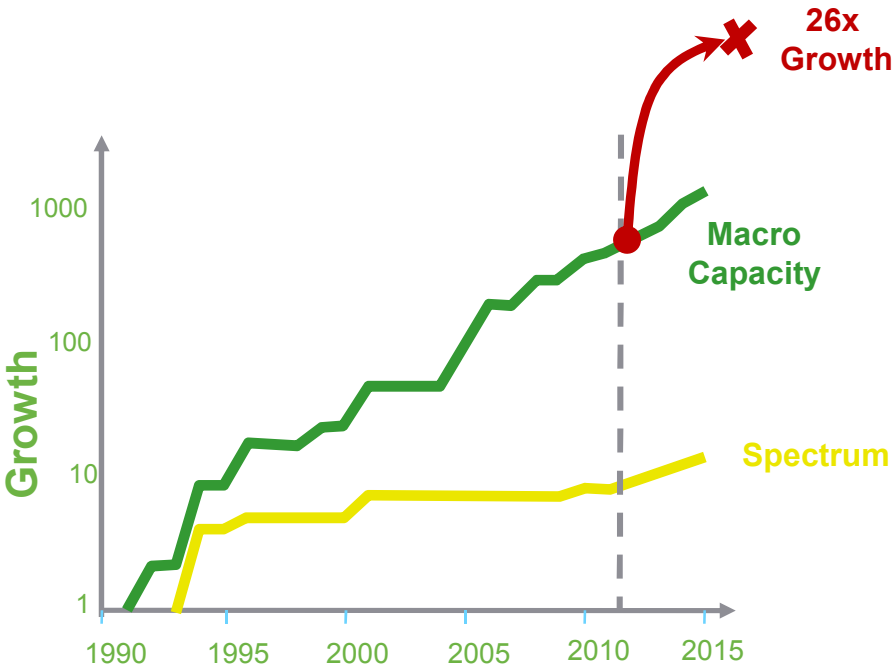
Video will be 66% of all mobile traffic by 2015

Source: Cisco Visual Networking Index (VNI) Global Mobile Data Forecast, 2010–2015

Spectrum is Precious

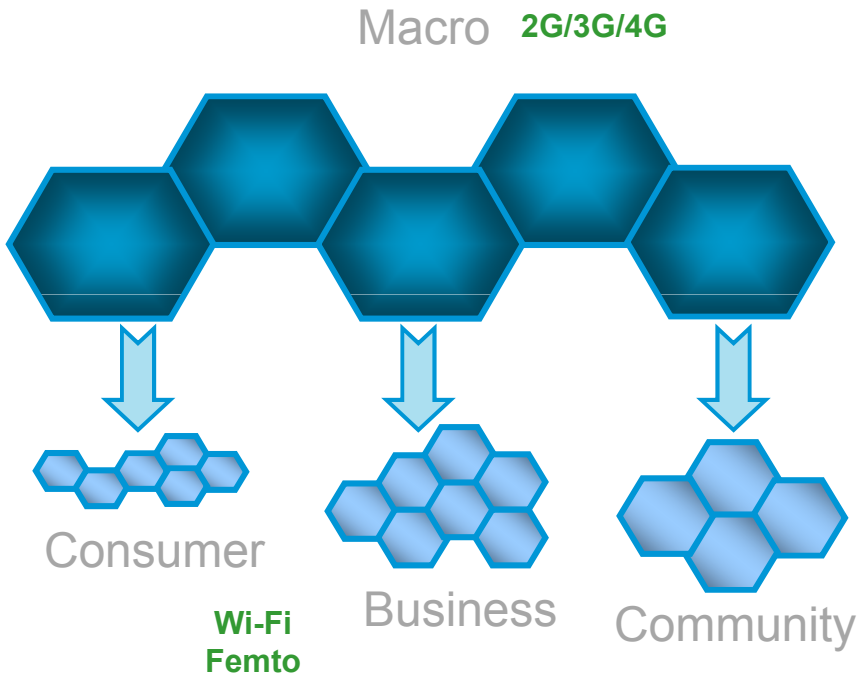


Overall Capacity Not Keeping Pace with Data Demand



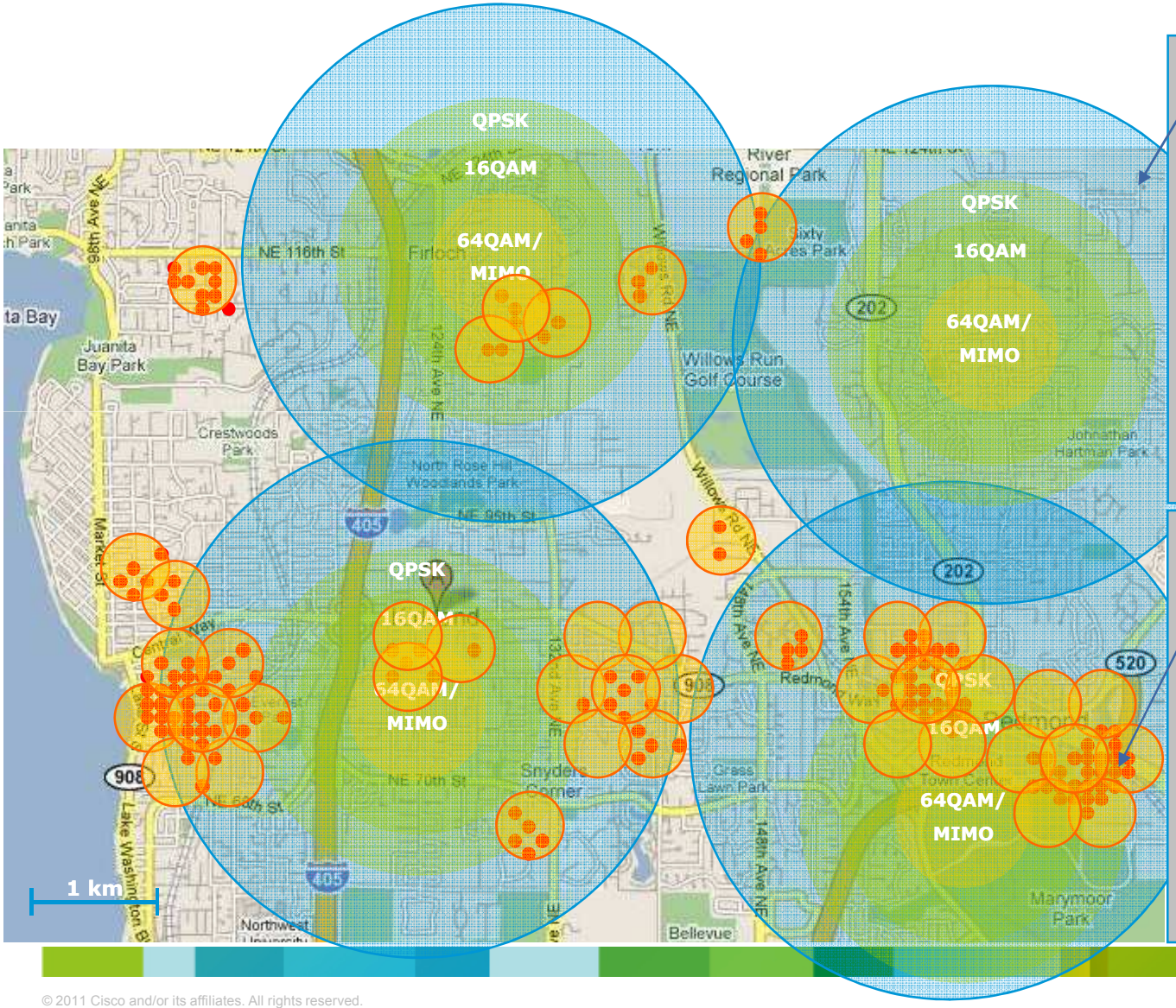
Source: Agilent

Small Cells Increase Existing Capacity



Future networks supporting the mobile Internet will need to integrate smaller cell architectures to scale

What Small Cells Can Deliver . . .



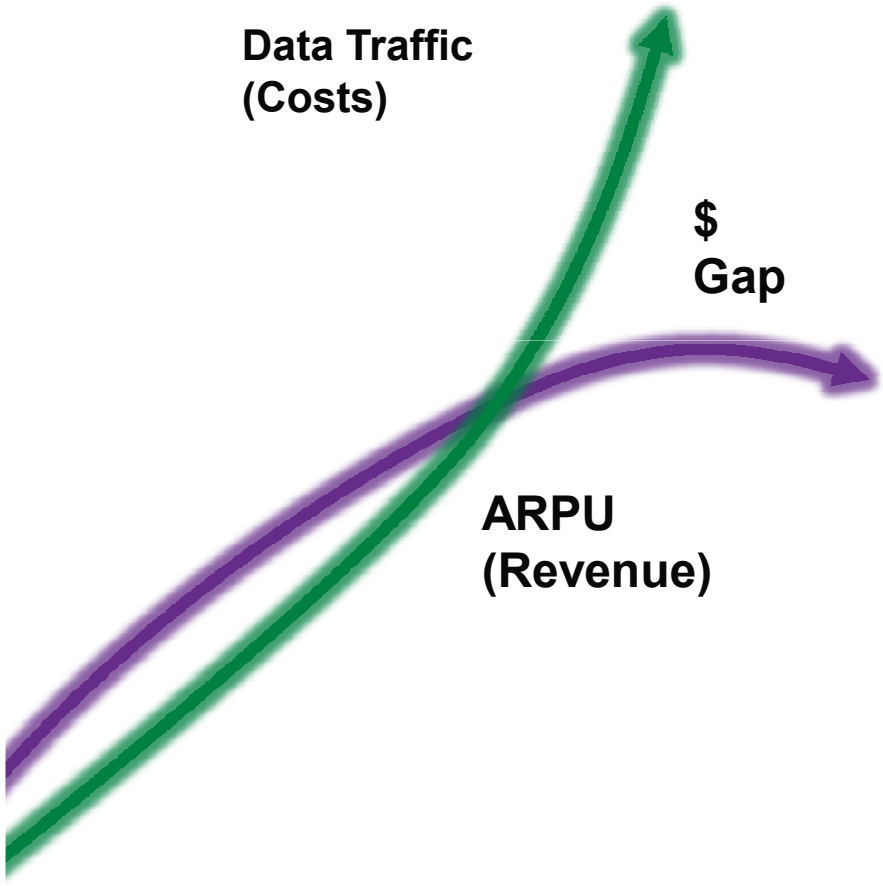
Macrocell (3G/4G)

- Voice coverage with uniform bandwidth, but not always where people are
- Limited data capacity
- Sub-optimal delivery of high BW to POPs
- High CapEx/OpEx: $400K
- Poor spectral efficiency
- New sites: Zoning issues

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
- Low environmental impact

Service Provider Challenge



Increase Revenues

New business models

New services and partnerships

Reduce Costs

Manage "Over The Top"

Optimize use of network assets

Improve Experiences

Three-screen experience and sessions

Video quality experience

Service Provider WiFi Opportunities

Offload of expensive 3G Data

OPEX savings on existing Macro 3G network

CAPEX savings on network expansion / capacity demand growth

New Revenue Models

Localized advertising revenues (Mobile Service Advertising Protocol)

Business to Business Revenue opportunities

Customer Retention

Superior performance advantages in WLAN coverage (4G-like Experience)

More flexible application delivery in WLAN (Facetime, Skype video calls, IPTV)

Offload Architectures

Offload Architectures Characteristics

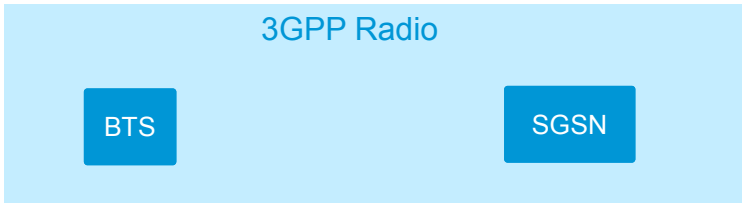
- Used architecture depends on operator's preferences
  - 3rd party WiFi or own build WiFi?
  - Charging requirements for WiFi traffic?
  - Authentication needed for WiFi?
  - Types of devices targeted for offload (smartphones, PCs, any device)?
  - Mobility requirements?
  - Visiting customers and one-time customers integration?
- Selection of the suitable architecture is important to
  - Make sure offload will be utilized by subscribers (simple setup, available devices, benefits for subsriber…)
  - Reach expected level of service quality
  - The cost of the solution is balanced by the benefits
  - Achieve flexibility for future expansion

Offload Architectures

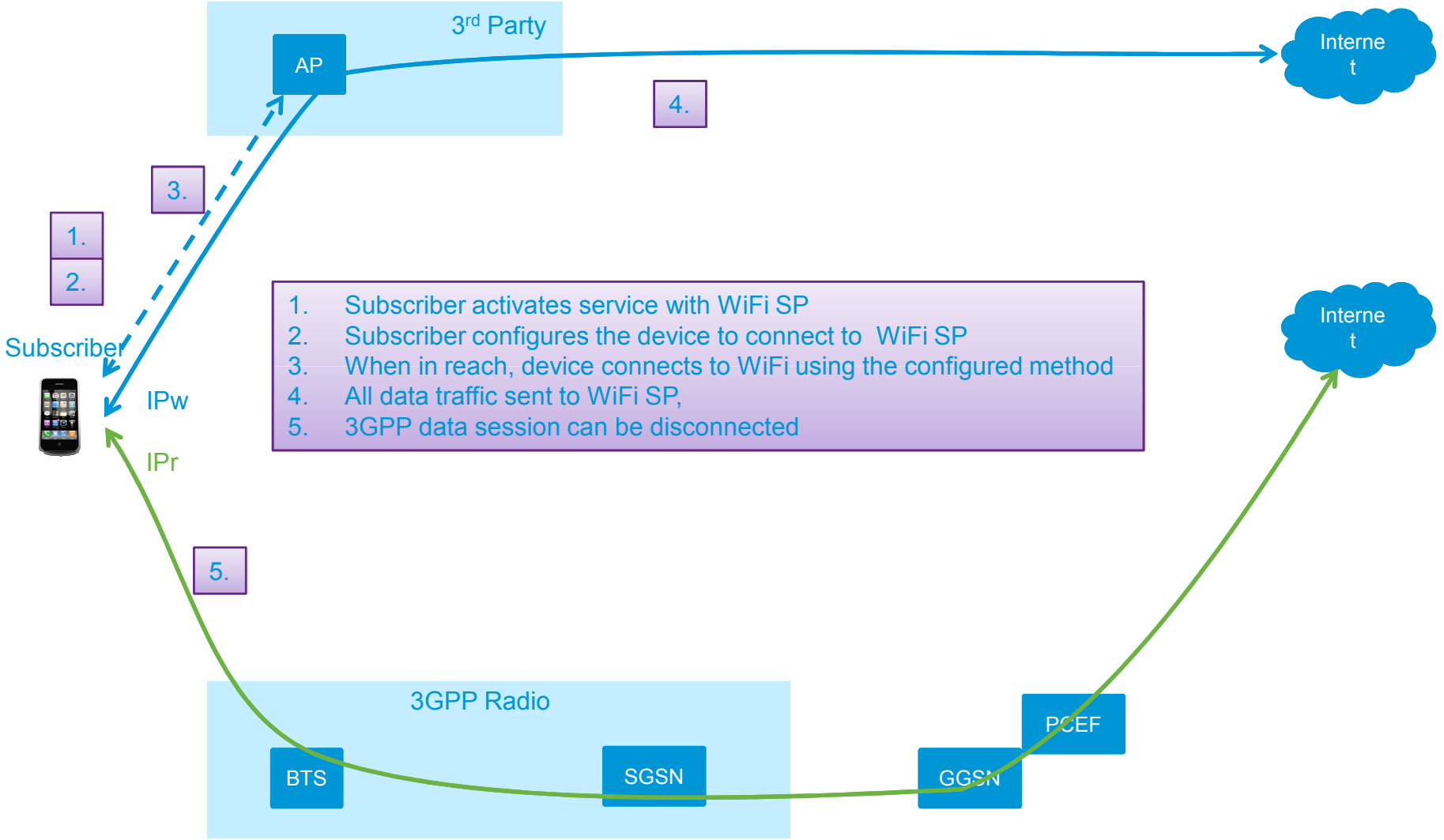
Architecture	Subscriber Involvement	UE Configuration	Policy	Mobility	3rd Party Networks
3rd Party Offload	Authentication				
Transparent Auto Logon					
EAP Authentication					
Hotspot 2.0					
MIP Mobility	Seamless Mobility				
I-WLAN and Mobility					

3rd Party Offload

Subscriber



3rd Party Offload

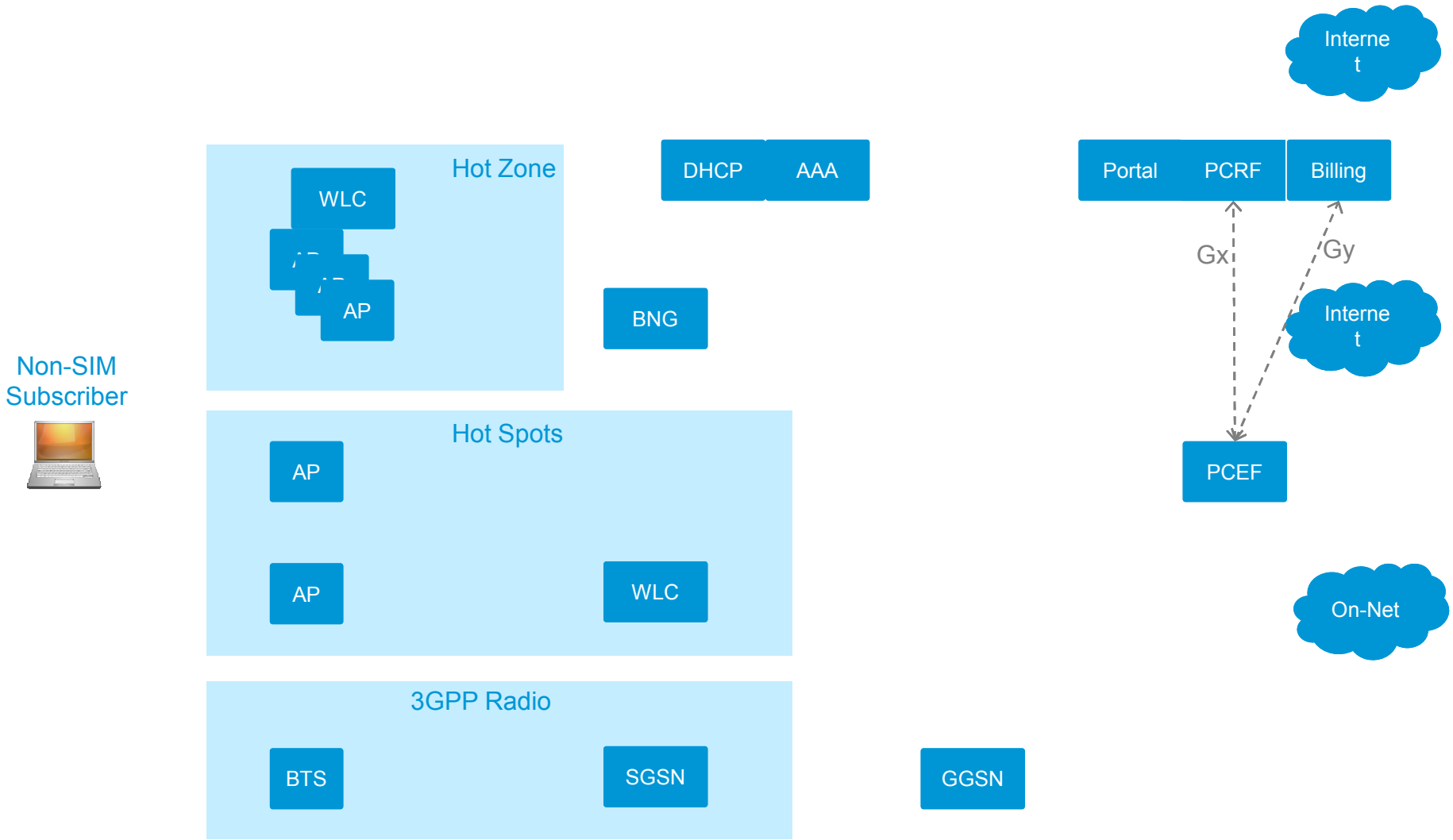


3rd Party Offload

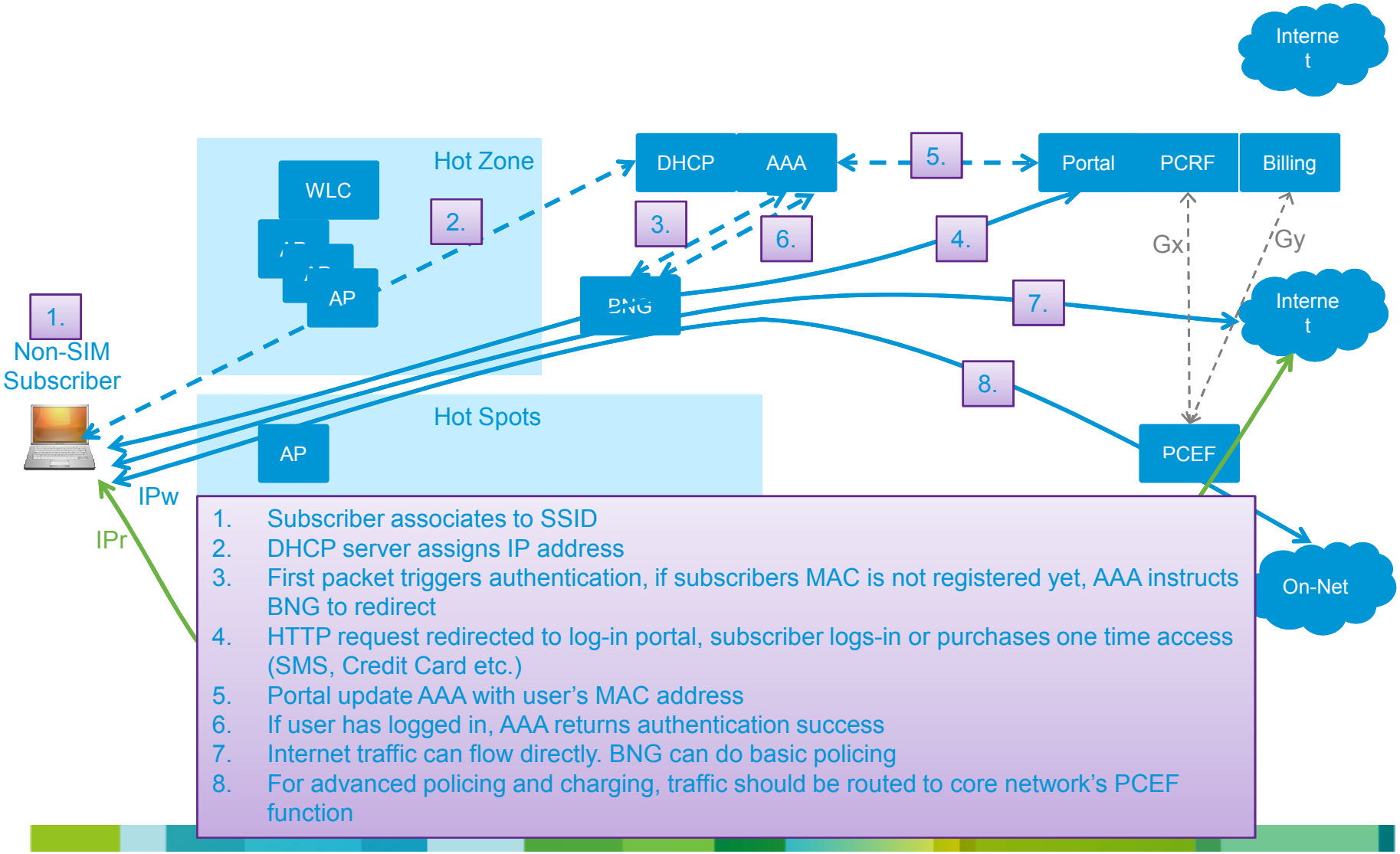
3rd Party

- **Subscriber Involvment**
  - Needs to have service from 3rd party
- **UE Configuration**
  - Configures the SSID and authentication according to 3rd party SPs requirements
  - Configures precedence of WLAN over 3GPP Radio (if not default) and precedence of the SSID
- **Policy**
  - Traffic is not crossing mobile operator's network, so no MO's policies are possible
- **Mobility**
  - Each radio has own IP address. Subscriber needs to configure, which interface is to be used.
  - Because Mobile Operator has no WLAN service agreement with subscriber, mobility is not possible
- **3rd Party**
  - Based on use of 3rd party network

Operator Provided Offload – Transparent Auto Login



Operator Provided Offload – Transparent Auto Login

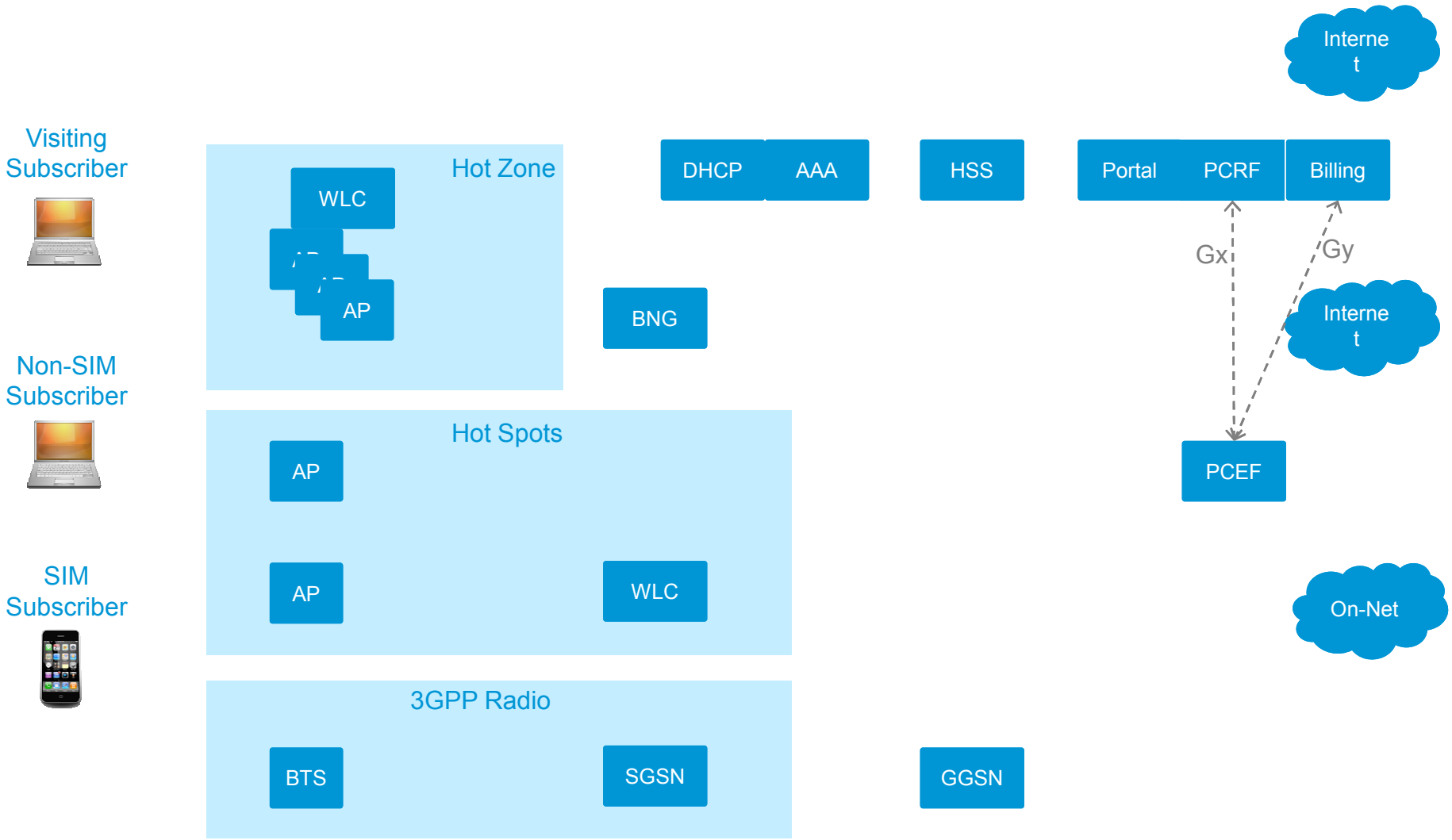


1. Subscriber associates to SSID
2. DHCP server assigns IP address
3. First packet triggers authentication, if subscribers MAC is not registered yet, AAA instructs BNG to redirect
4. HTTP request redirected to log-in portal, subscriber logs-in or purchases one time access (SMS, Credit Card etc.)
5. Portal update AAA with user's MAC address
6. If user has logged in, AAA returns authentication success
7. Internet traffic can flow directly. BNG can do basic policing
8. For advanced policing and charging, traffic should be routed to core network's PCEF function

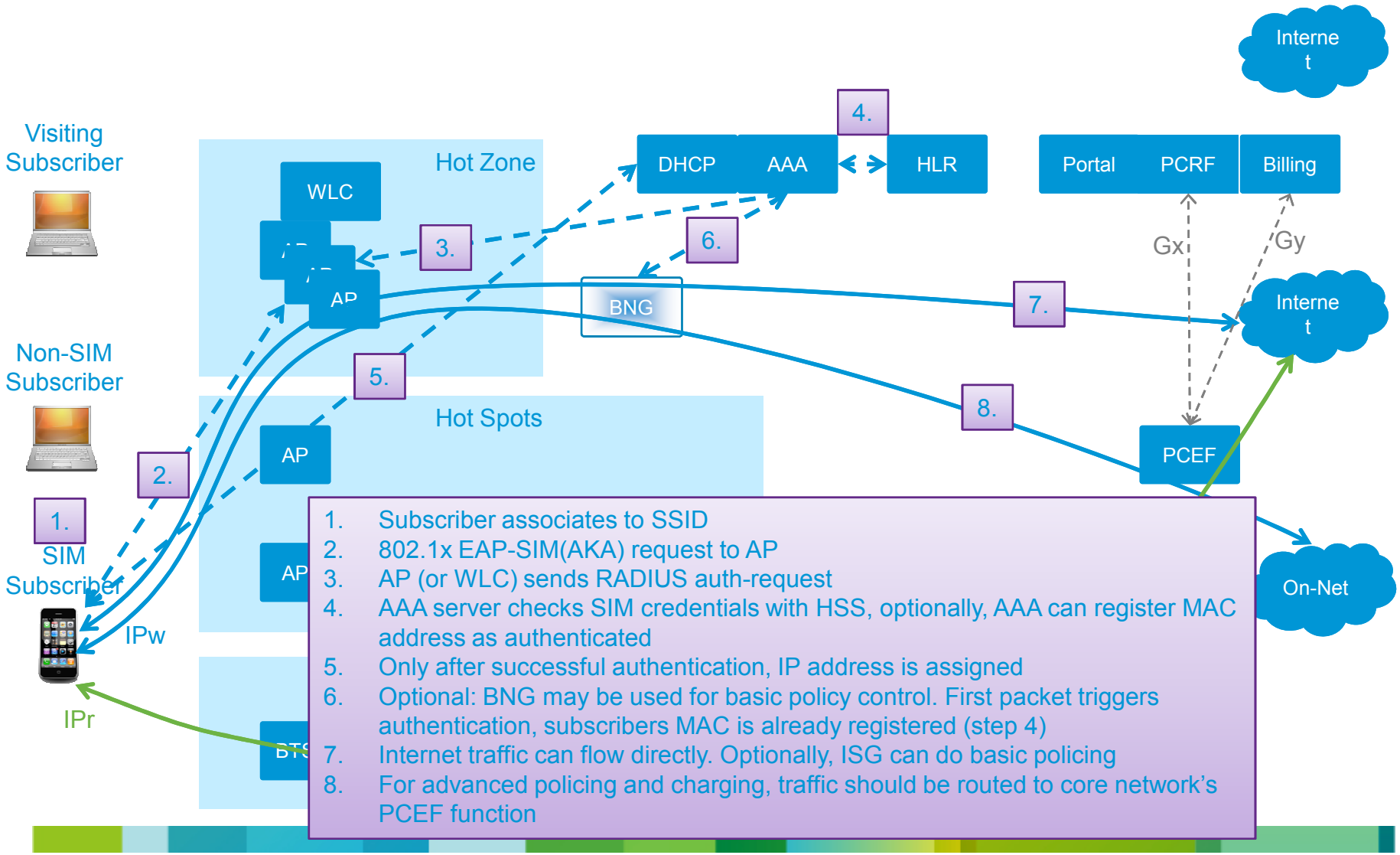
Operator Provided Offload – Transparent Auto Login

- **Subscriber Involvment**
  - Needs to purchase service from Mobile Operator, so he is provided with username and password
- **UE Configuration**
  - Configures the SSID
  - Configures precedence of WLAN over 3GPP Radio
  - Needs to enter username/password every time login expires
- **Policy**
  - Traffic to be charged and policed, needs to be routed to the core of the network
  - Basic policing can be implemented on ISG
- **Mobility**
  - Each radio has own IP address. Subscriber needs to configure, which interface is to be used.
  - No seamless mobility.
  - Mobile IP and I-WLAN can be added to the architecture to provide mobility
- **3rd Party**
  - If 3rd party has roaming agreement with mobile operator, registered users may login in visited network
  - Subscriber needs to know the correct SSID

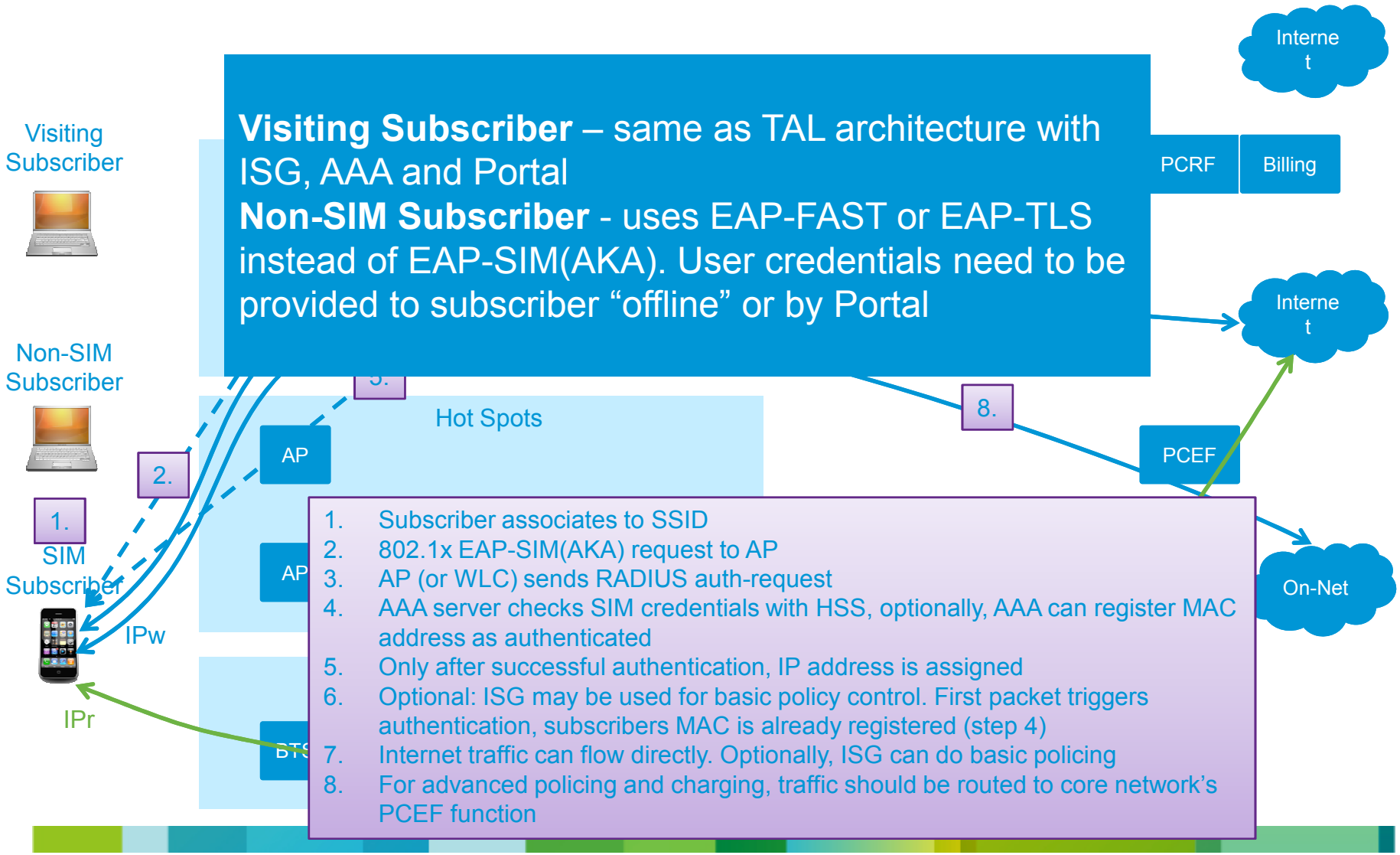
Operator Provided Offload - EAP



Operator Provided Offload - EAP



Operator Provided Offload - EAP



Visiting Subscriber – same as TAL architecture with ISG, AAA and Portal

Non-SIM Subscriber - uses EAP-FAST or EAP-TLS instead of EAP-SIM(AKA). User credentials need to be provided to subscriber "offline" or by Portal

1. Subscriber associates to SSID
2. 802.1x EAP-SIM(AKA) request to AP
3. AP (or WLC) sends RADIUS auth-request
4. AAA server checks SIM credentials with HSS, optionally, AAA can register MAC address as authenticated
5. Only after successful authentication, IP address is assigned
6. Optional: ISG may be used for basic policy control. First packet triggers authentication, subscribers MAC is already registered (step 4)
7. Internet traffic can flow directly. Optionally, ISG can do basic policing
8. For advanced policing and charging, traffic should be routed to core network's PCEF function

Operator Provided Offload - EAP

- **Subscriber Involvment**
  - Non-SIM subscriber needs to purchase service and receive credentials
- **UE Configuration**
  - Configures the SSID
  - Configures precedence of WLAN over 3GPP Radio
  - One time configuration for EAP authentication
- **Policy**
  - Traffic to be charged and policed, needs to be routed to the core of the network
  - Basic policing can be implemented on ISG
- **Mobility**
  - Each radio has own IP address. Subscriber needs to configure, which interface is to be used.
  - No seamless mobility.
  - Mobile IP and I-WLAN can be added to the architecture to provide mobility
- **3rd Party**
  - If 3rd party has roaming agreement with mobile operator, registered users may login in visited network
  - Visited network may not support EAP. In such case subscriber needs to know his username/password and log-in to visited login page
  - Subscriber needs to know the correct SSID

Next Generation Hotspot

Roam, Authenticate, Monetize

Mobile Service Advertisement Protocol (MSAP)

RELIABLE
Carrier class solution

SEAMLESS
Simplifies network discovery and selection for seamless cellular data offload

SECURE
Extends existing SIM-based authentication techniques over encrypted Wi-Fi

PROFITABLE
Enables location-based and value-added services

Hotspot 2.0

- **Subscriber Involvment**
  - Non-SIM subscriber needs to purchase service and receive credentials
- **UE Configuration**
  - Configures the SSID
  - Configures precedence of WLAN over 3GPP Radio
  - One time configuration for EAP authentication
- **Policy**
  - Traffic to twork
  - Basic po
- **Mobility**
  - Each rac rface is to be use
  - No seam
  - Mobile IP y
- **3rd Party**
  - If 3rd par may login in v
  - Visited network may not support EAP. In such case subscriber needs to know his username/password and log-in to visited login page
  - Subscriber needs to know the correct SSID

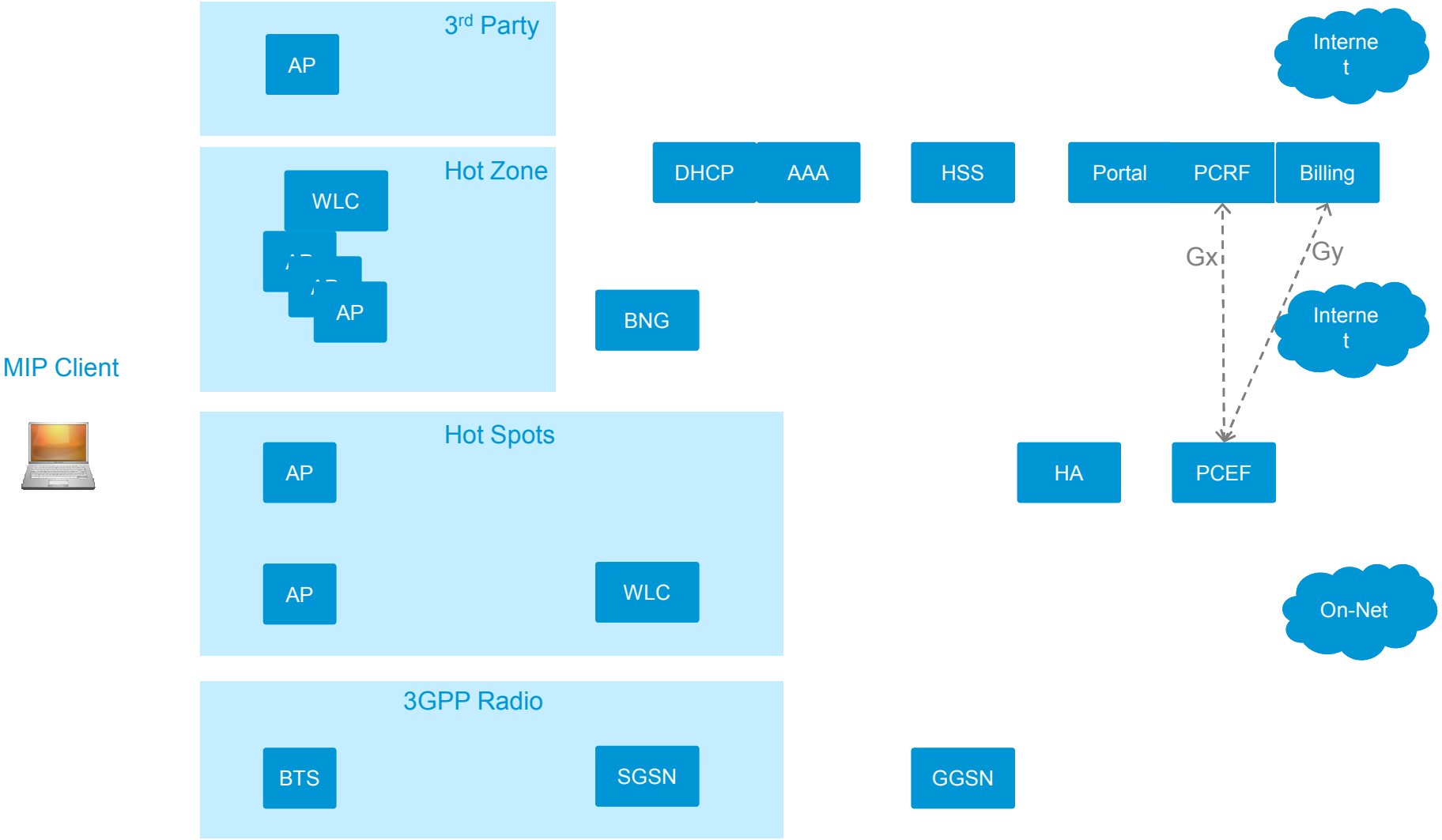
WBA initiative Hotspot 2.0 greatly simplifies subscribers interaction needed for WLAN connections by specifying standardized set of protocols:

- 802.11u
  - exchange of services provided on AP
  - which SSID provides service of subscribers home operator
- 802.1x
  - EAP-SIM
  - EAP-TLS
  - EAP-FAST
- Roaming – WRIX specification

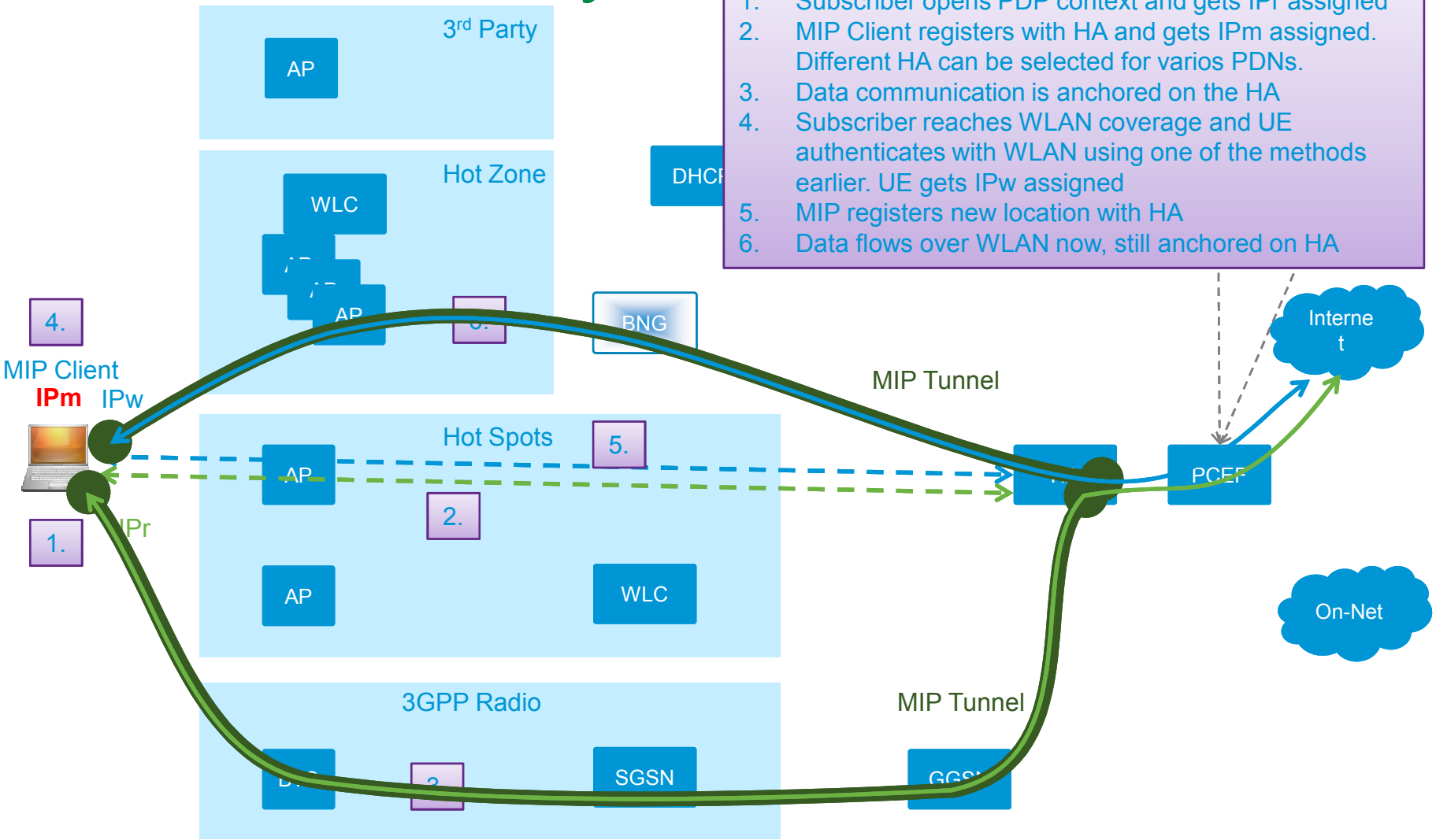
Seamless Mobility

- Characteristics
  - UE has two active radios, two IP addresses
  - No interconnection between RAN controllers of the two networks
  - Each RAN provides internal mobility
  - WLAN RAN may be operator's own or 3rd party
  - Authentication differs between WLAN and 3GPP
  - Encryption not provided by WLAN
- Consequence
  - UE decides when to handover between radios without knowledge of the RAN and therefore client software is required
  - Anchor point is needed (Home Agent or Local Mobility Agent) to work with client for service continuity
- Mobility is independent of access architecture (TAL, EAP etc.). Access must be authenticated before mobility tunnel is created.

Mobile IP Mobility



Mobile IP Mobility

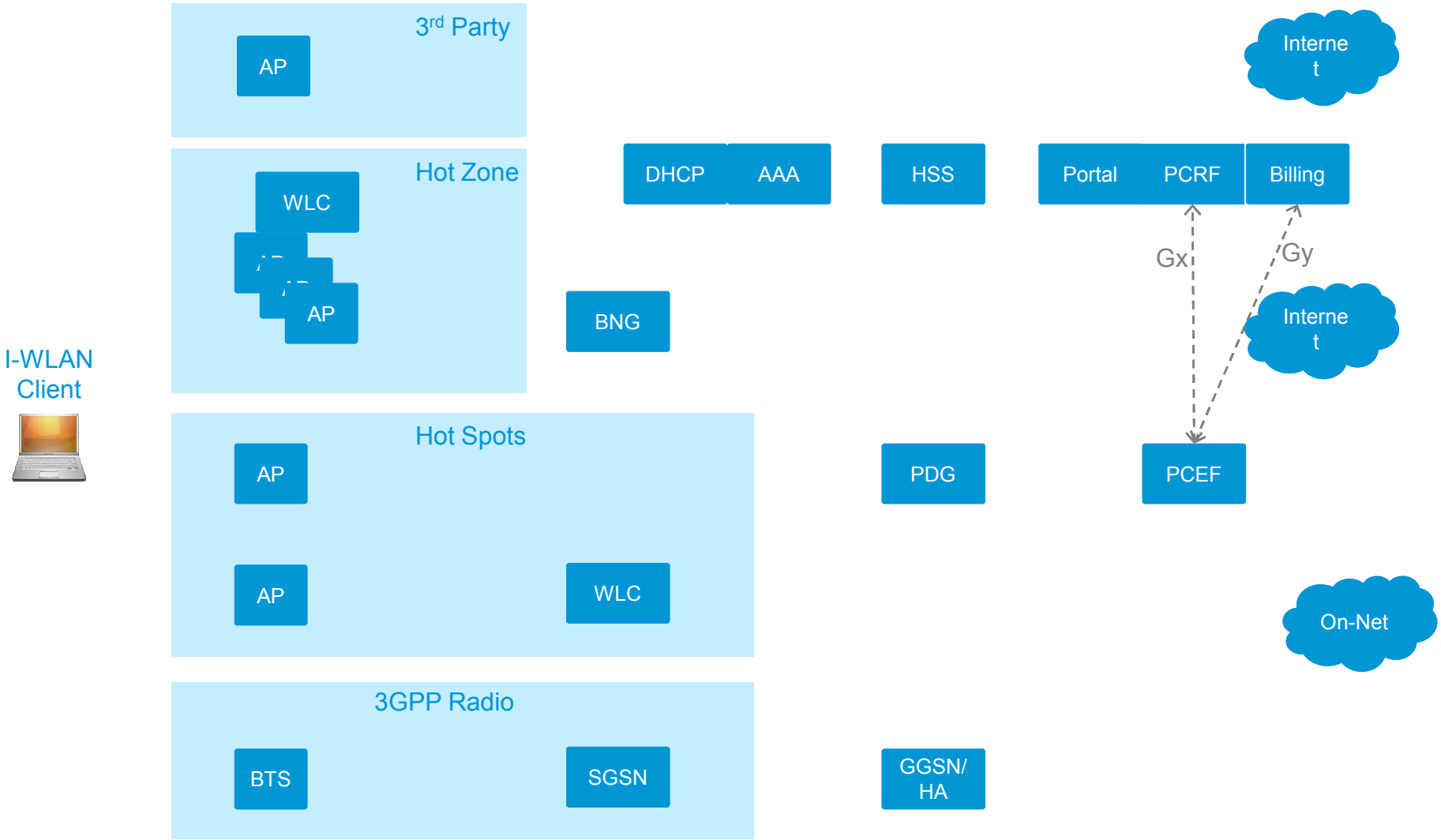


Mobile IP Mobility

1. Subscriber opens PDP context and gets IPr assigned

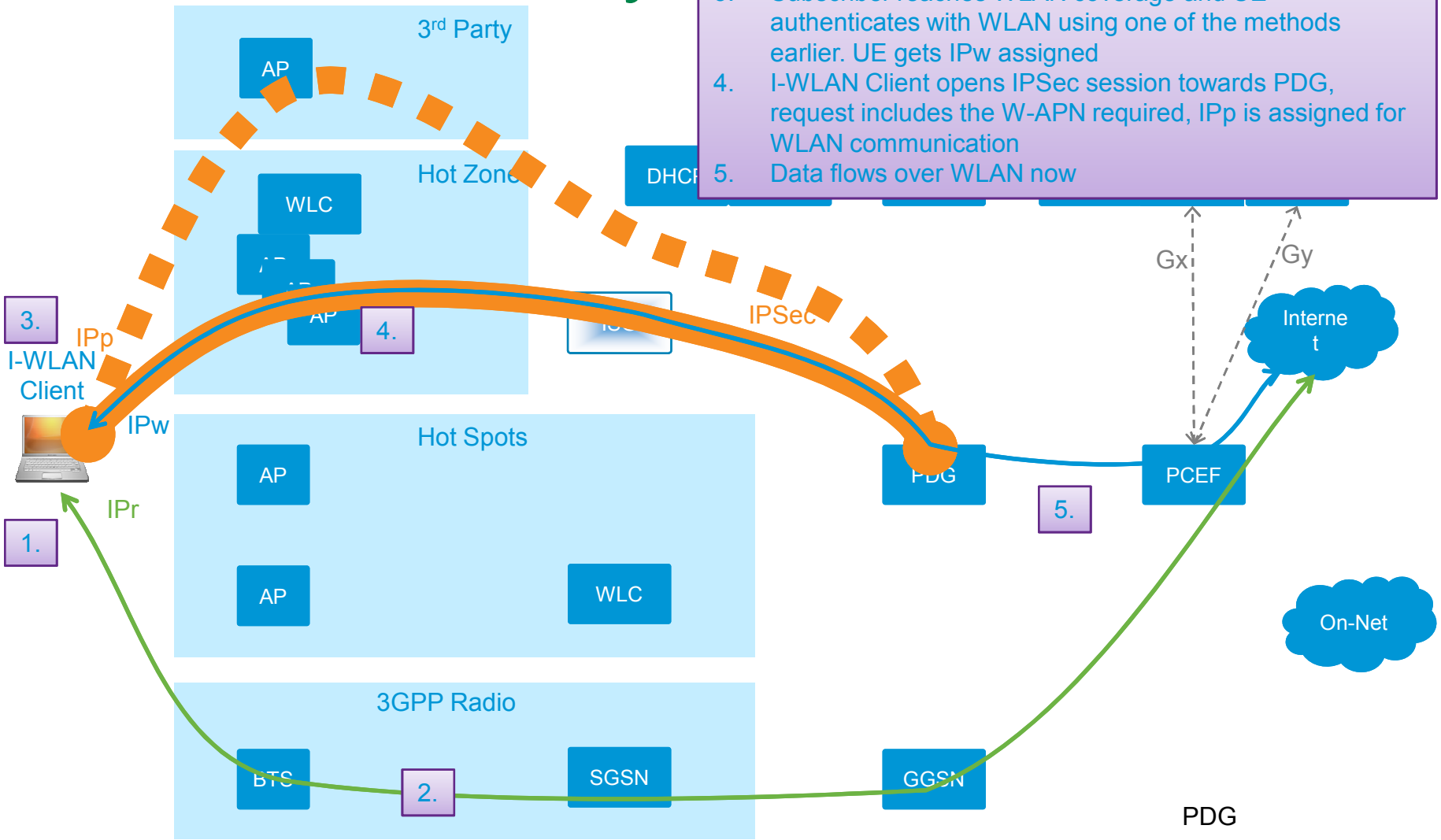
- **Subscriber Involvment**
  - Mobile IP client download and installation
- **UE Configuration**
  - Depends on the authentication method used by WLAN
- **Policy**
  - All traffic is anchored at HA
  - PCEF function is close/integrated to HA, all traffic can be policed
- **Mobility**
  - Seamless mobility
  - Client Software decides when the handover is needed
  - All communication from Internet goes to Ipm
  - User data over WLAN are NOT encrypted
- **3rd Party**
  - If 3rd party has roaming agreement with mobile operator, registered users may login in visited network
  - Works over 3rd party networks, unencrypted

I-WLAN



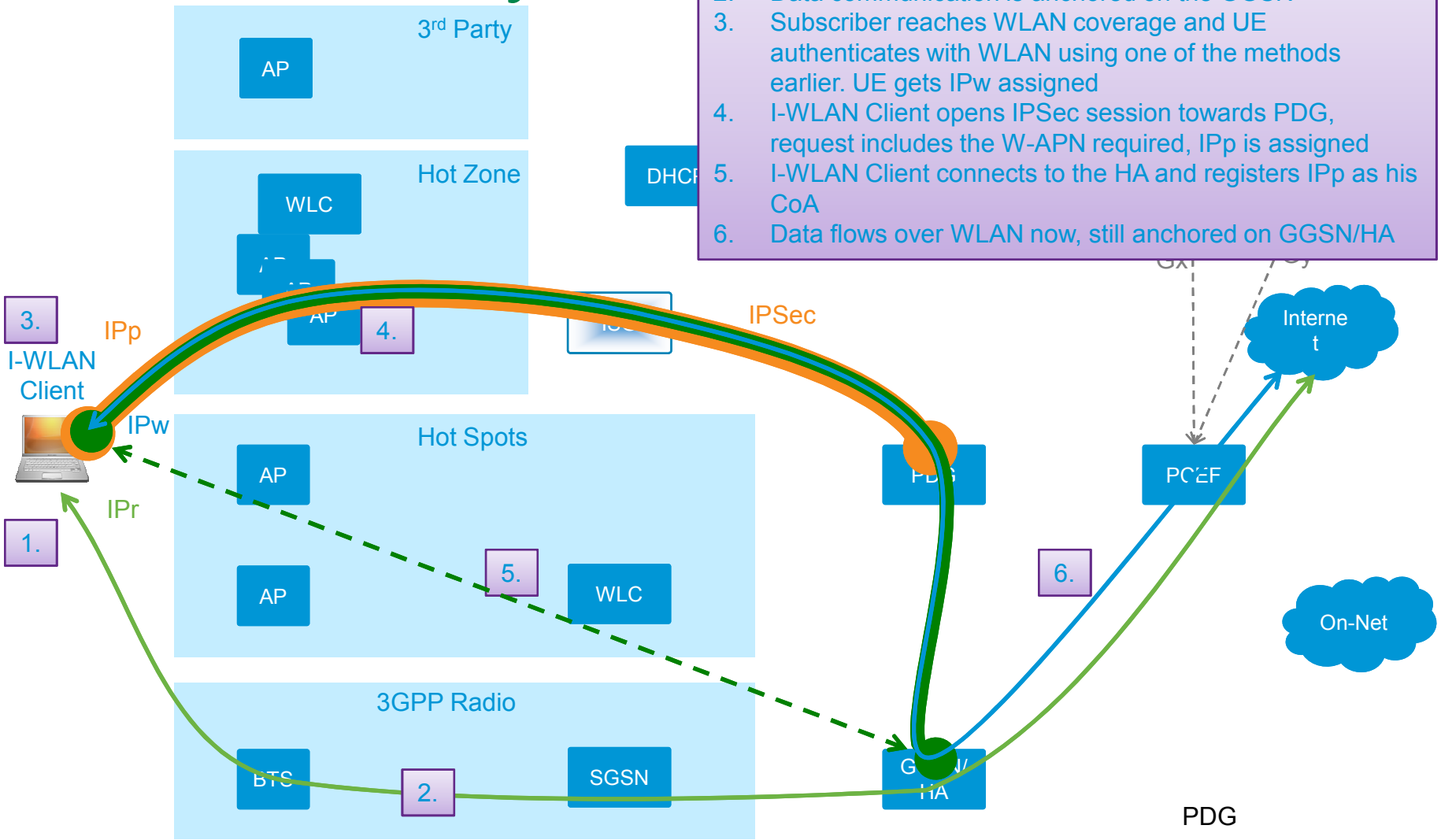
I-WLAN No Mobility

1. Subscriber opens PDP context and gets IPr assigned
2. Data communication flows through the GGSN
3. Subscriber reaches WLAN coverage and UE authenticates with WLAN using one of the methods earlier. UE gets IPw assigned
4. I-WLAN Client opens IPSec session towards PDG, request includes the W-APN required, IPp is assigned for WLAN communication
5. Data flows over WLAN now



I-WLAN Mobility

1. Subscriber opens PDP context and gets IPr assigned, this should also be his Home Address
2. Data communication is anchored on the GGSN
3. Subscriber reaches WLAN coverage and UE authenticates with WLAN using one of the methods earlier. UE gets IPw assigned
4. I-WLAN Client opens IPSec session towards PDG, request includes the W-APN required, IPp is assigned
5. I-WLAN Client connects to the HA and registers IPp as his CoA
6. Data flows over WLAN now, still anchored on GGSN/HA



I-WLAN Mobility

1. Subscriber opens PDP context and gets IPr assigned

- **Subscriber Involvment**
  - I-WLAN client download and installation
- **UE Configuration**
  - Depends on the authentication method used by WLAN
- **Policy**
  - All traffic is anchored at GGSN/HA
  - PCEF function is close/integrated to GGSN, all traffic can be policed
- **Mobility**
  - Seamless mobility
  - Client Software decides when the handover is needed
  - All communication from Internet goes to IPr (assigned from GGSN)
  - User data over WLAN are encrypted
- **3rd Party**
  - If 3rd party has roaming agreement with mobile operator, registered users may login in visited network
  - Works over 3rd party networks, encrypted

Offload Architectures - Summary

Architecture	Subscriber Involvement	UE Configuration	Policy	Mobility	3rd Party Networks
3rd Party Offload	Yes	Yes	Yes	Yes	Yes
Transparent Auto Logon	Yes	Yes	Yes	Yes	Yes
EAP Authentication	Yes	Yes	Yes	Yes	Yes
Hotspot 2.0	Yes	Yes	Yes	Yes	Yes
MIP Mobility	Yes	Yes	Yes	Yes	Yes
I-WLAN and Mobility	Yes	Yes	Yes	Yes	Yes

Offload Architectures - Summary

Architecture	Subscriber Involvement	UE Configuration	Policy	Mobility	3rd Party Networks
3rd Party Offload	yes	yes	no	no	yes
Transparent Auto Logon	yes	yes	If routed to core	Expandable	If Roaming
EAP Authentication	Non SIM Subscribers	minimal	If routed to core	Expandable	If EAP Roaming
Hotspot 2.0	Non SIM Subscriber	no	If routed to core	Expandable	If Roaming
MIP Mobility	Client Installation	no	yes	yes	Yes, non encrypted
I-WLAN and Mobility	Client Installation	no	yes	yes	Yes, encrypted

Corporate Access

- Possible only with tunneling architectures (tunnel to HA or PDG)
- Packed Data Network (PDN-GW) selection
  1. AAA server assigns the appropriate PDN-GW based on UE identity
  2. Preconfigured on client device

  Format:

  FQDN (<APN-NI>.apn.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org)

  IP Address and APN
- APN is signaled during tunnel set-up to the PDN-GW

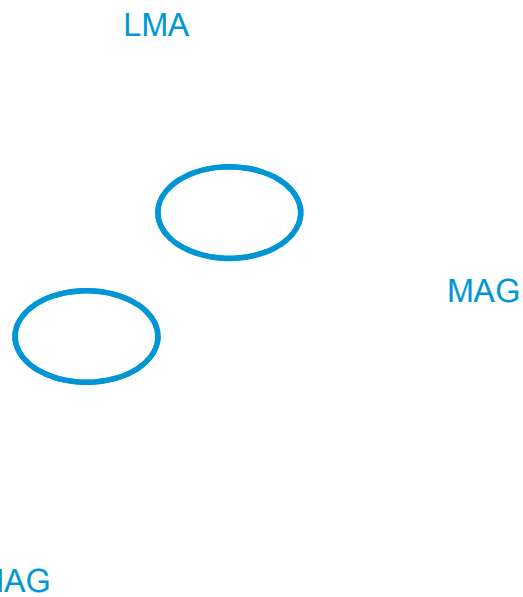
Mobile IP Mobility – 3GPP Reference

3GPP TS 23.402

Future Developments

- Clientless mobility (3GPP TS 23.402)
  - Proxy MIP
  - Client gets identical IP address assigned from both radio types
- MSAP (Cisco proprietary)
  - Advertisement push
  - Localized and targeted
- Breakout for Seamless mobility
  - Send cheap traffic directly to Internet
  - Send traffic to core only if policy needed
- Voice integration
  - IMS integration (client)

ProxyMIP – 3GPP Reference



3GPP TS 23.402

3GPP S2a Attach

3GPP TS 23.402

3GPP S2b Attach

3GPP TS 23.402

3GPP S2a/S2b Mobility

3GPP TS 23.402

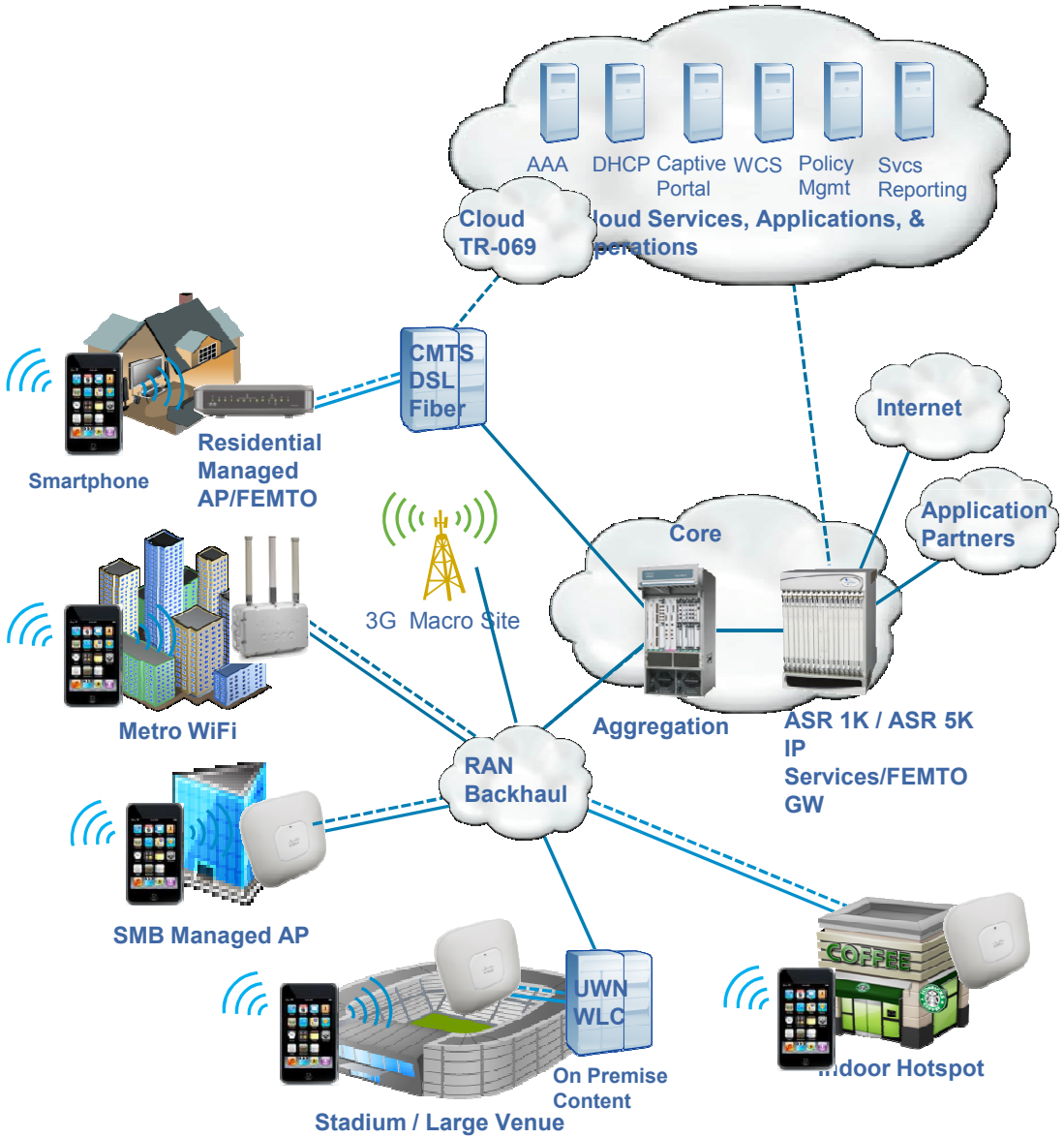
SP WiFi – Building The Business Case

	Offload	New Revenues
Operator Benefits	Macro network savings (OPEX) Cost efficient network expansions (CAPEX)	Advertisement revenues Service for one-time customers Roaming Charges B2B revenues
Enablers in the Architecture	EAP-SIM Authentication (WLAN/3G Mobility) Roaming Preconfigured devices	Cisco MSAP Portal based authentication Roaming
Subscriber Communication	Flat WLAN rate for monthly fee 4G coverage (speed) Loose policies in WLAN coverage Rural (Villages) Broadband Coverage	Time-limited use of WLAN with online payment (CC, SMS) Roaming for visiting customers Managed WLAN coverage Managed Enterprise WLAN with UC Wholesale WLAN Targeted and localized advertisement

Reduction of Churn (more services, better network quality, innovation leadership…)

Cisco SP WiFi Solution Core

End-to-end SP WiFi Network Architecture



- **Unlicensed RAN complement to 3G/4G Mobile Broadband networks**
  - Reduces RAN congestion
  - Improves Indoor Coverage
  - 3G Data offload at high traffic locations
  - Low Network TCO
- **Flexible & Scalable**
  - Scales from Metro/indoor to Residential
  - Cloud based Operations & Services Mgmt
- **Standards Based**
  - 802.11 a/b/g/n
  - 802.11u – 802.1x Authentication
  - CAPWAP Mobility & Radio Resource Mgmt
  - DOCSIS 3.0 & MEF
  - TR-069 RGW Provisioning & Mgmt
  - 3G Offload – 3GPP iWLAN
    - IPSEC - Untrusted Network Access
    - Client / Clientless Mobility - CMIP/PMIP/DSMIP

ASR5k Product Portfolio

In-line Services*

- Enhanced Charging Service
- Intelligent Traffic Control
- Stateful Firewall
- Content Filtering
- Peer-to-Peer Detection & Control
- Dynamic Policy
- Heuristic DPI
- TPO

+

Network Function Modules*

- Session Control Manager: P-CSCF, I-CSCF, S-CSCF
- GGSN
- HA
- A-BG
- PGW
- SGSN
- PDSN
- HSGW
- ASN GW
- TTG PDG
- Femto GW
- MME
- SGW

Control = Green
Bearer = Blue

+

Platforms

ASR5K

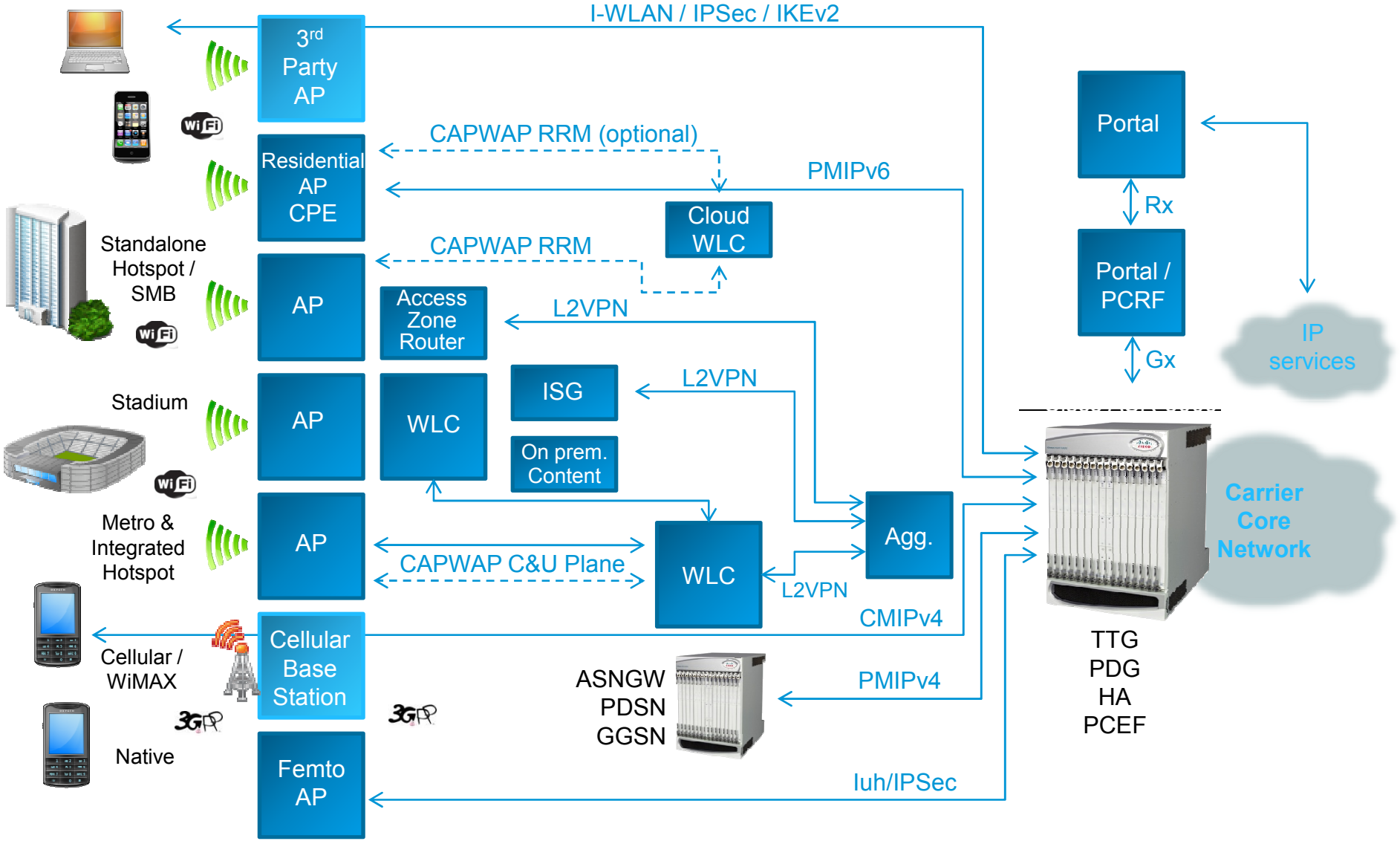
EMS

*Current and future solutions

Cisco ASR 5000

- Performance
  - Provides both superior security and performance across all un-trusted applications
    - 1M+ tunnels; 1,000 transactions/sec
    - 4 M sessions fror Femto GW, 1 M HNB
  - HW based IPSec encryption
- Integration
  - Able to integrate SeGW into existing core nodes (PDSN/GGSN) w/software upgrade lowering OpEx and CapEx
    - Simple migration path for incumbent 3G operators (software upgrade)
    - Even with separate platforms, lower entry cost – same qualified platform and cards
  - Cross functional application security solutions, e.g., WLAN and Femto
  - Mobility on I-WLAN through integrated HA functionality
- Intelligence
  - Sophisticated application intelligence for In-line Services available w/o new external elements across all access networks for accelerated ROI
  - Number of “off the shelf” services: DPI, policy control, content filtering, firewall, …
- Reliability
  - Same 99.9999% reliability as existing mobile core applications
  - Most ATCA architecture do not allow true stateful redundancy
- Evolution to ePDG for complete LTE solution
  - Existing platform evolves to LTE together with next generation ePDG

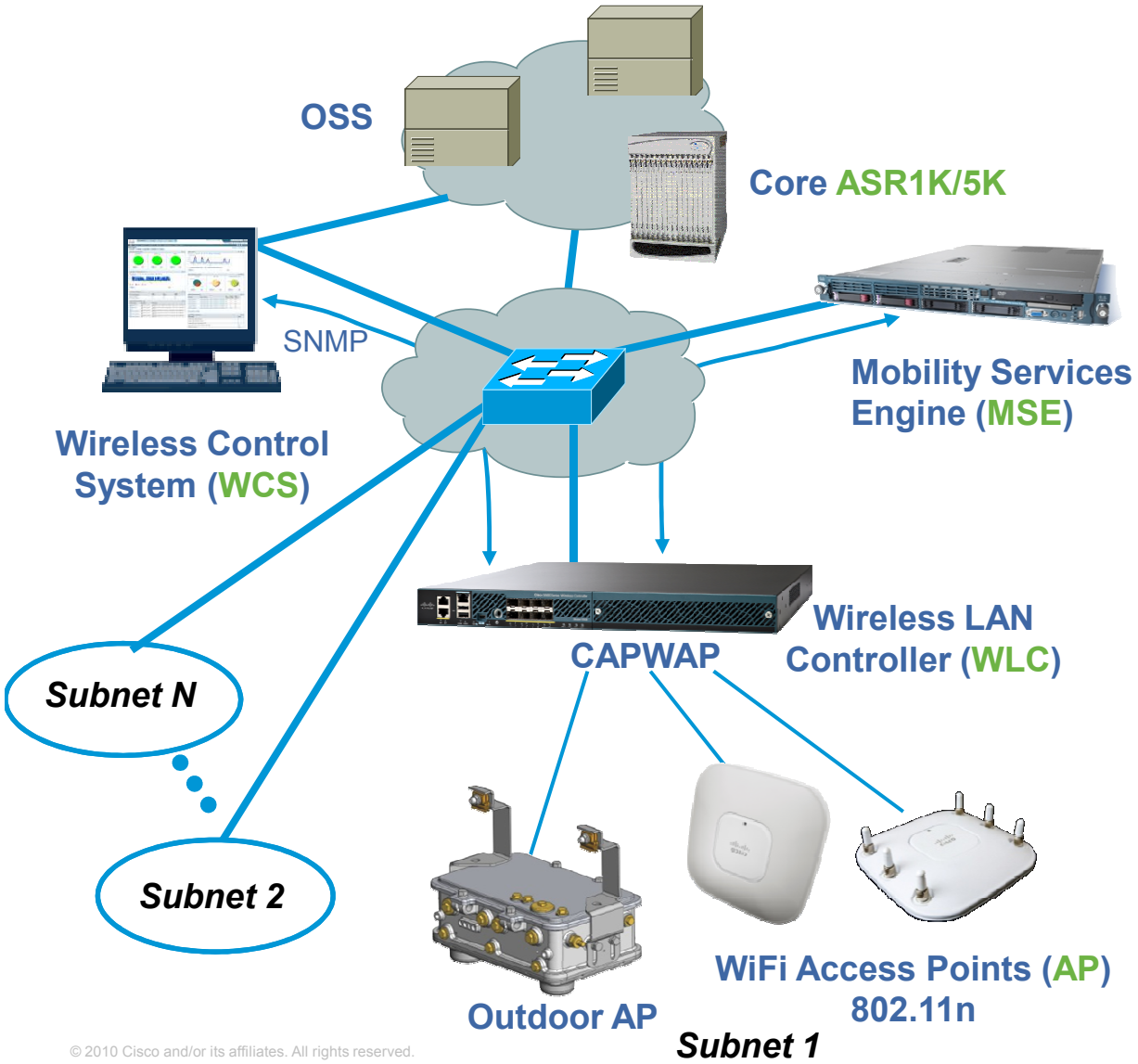
Cisco Offload Framework



Cisco SP WiFi Solution Radio

Cisco Unified Wireless Architecture

Logical Overview



- **802.11a/b/g/n**
- **Highly scalable**
- **RRM for Real-time RF visibility & autonomous local control**
- **Easily configurable**
  - WLAN controllers & APs
  - Standard I/F (CAPWAP)
- **Built-in support for Voice & Mobility Services**
  - Unified Communications
  - Context–Aware Services (Location)
  - Adaptive Wireless Intrusion Prevention (wIPS)
- **Fault-tolerant Controller**

Controller-Based Architecture

- Why a WiFi controller-based architecture?
  - All successful commercial mobility networks based upon concept of centralized control or aggregation of the radio access network (RAN)
  - All use the Radio-network-controller (RNC) as access layer controller & aggregator
  - Next-Gen 4G LTE wireless networks also support centralized RAN control & further allow its separation from the user-plane (i.e. MME/SGW)
- RNC provides mobility networks with
  - RRM: to maximize coverage & capacity thru. network-wide RF quality & interference-awareness, resource allocation (RF channels, BW, Power, …)
  - Controlled Handoff via local anchoring
  - Single inter-op point (e.g. foreign networks) to reduce IOT & OPEX
  - Context-aware service adaptation (e.g. multicast/broadcast, voice codec optimization, …) & support of multiple services (voice, data, Ethernet or IP)

RNC: Radio Network Controller
RAN: Radio Access Network
OPEX: Operational Expenditure
IOT: Inter-Operability Testing
MME: Mobility Management Entity
SGW: Serving Gateway
RRM: Radio Resource Management

WLC: Cisco's WiFi "RNC" architecture
Wireless LAN Controller

- Controls Handoff Between APs
  - Manages "neighbour-Lists" within/between WLC
  - Uses RF Parameters in Mobile-Assisted Handoff
  - Fast & seamless handoff for L2 & L3 services (802.11r)
- LAN, MAN or WAN connected (Layer 2 or L3 transport)
  - Not limited by size of L2 domain or transport technology
- CleanAir provides industry-leading active interference mitigation based on centralized RRM
  - Capacity and coverage booster for all environments incl. those with "unwanted" APs
- Adaptive wireless intrusion detection/prevention (wIPS)
- Context-aware services (e.g. VideoStream, VoWiFi CAC)
  - Multi/uni-cast admission control & media-adaptation needs central network view
- Inter-network mobility (e.g. 3G-WiFi) via IP (e.g. PMIP)
  - Edge-based mobility for very infrequent "roaming" cases
- Supports control/data split in-line with next-gen wireless (LTE)

LAN: Local Area Network
MAN: Metropolitan Area Network
WAN: Wide Area Network
WLC: Wireless LAN Controller
wIPS: Wireless Intrusion Prevention System
PMIP: Proxy Mobile IP
CAC: Connection Admission Control

Controller-based vs Controller-less WiFi

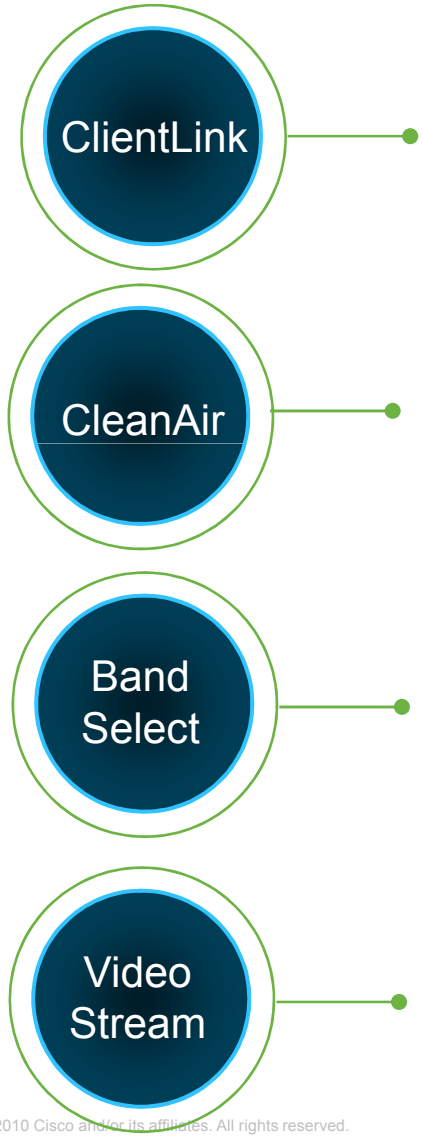
	Controller Based (L2/L3)	Controller-Less (L3-only)
Data mobility (layer 2 & layer 3)	✓	✓
Real-time mobility (layer 2 & layer 3) *(pre-802.11r; CCX)*	✓	✘
Network capacity optimization *(RRM - interference mitigation)*	✓	✘
Comprehensive security+ intrusion detection *(e.g. rogue AP)*	✓	✘
Best user experience *(Context-aware voice/video optimization)*	✓	✘
Large scale deployment manageability	✓	✘
Future proof architecture	✓	✘

One architecture – many applications

- HotZone (stadium, public venues, metro, etc)
  - Contiguous coverage area served by Unified WLC (centralized mgmt, mobility, CleanAir, RRM, etc)
  - Typically, WLC co-located with access gateway (e.g. ASR1K) for charging & Internet offload
  - Single WLC typically serves 10-1000 APs (1-10K users)
- HotSpot (public access retail, etc)
  - Single facility (few APs) usu co-located with access router (e.g. AZR) for charging & Internet offload
  - Typically a discontinuous coverage area (limited mobility)
  - C-plane only FlexForward WLC (centralized mgmt., RRM, CleanAir, aWiPS, etc)
  - Single WLC serves 2-5Ks HotSpot APs
- SMB (managed services, etc)
  - Dual SSID (for MSP) usu. with bundled services (e.g. VPLS, IP-PBX, FMC, etc)
  - Similar coverage as HotSpot and FlexForward WLC
- Residential (MDU)
  - Clusters of semi-contiguous SP coverage -> interference constrained -> RRM/CleanAir
  - FlexForward or Unified WLC

Radio – RF Performance Matters

Not all access points are the same



Best in class RRM coupled with “legacy beamforming” to deliver focused power to clients.

Improves Network Throughput and Coverage

Sophisticated “Spectrum Intelligence” to monitor the airwaves, detect, locate & classify interference, alert IT and automatically reconfigure the network to avoid.

Improves Network Reliability

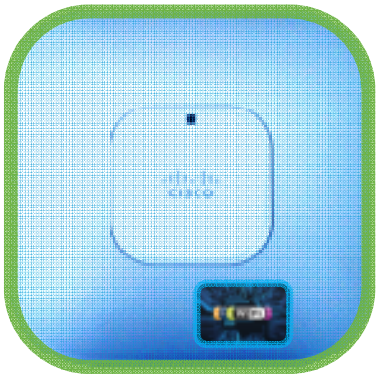
Optimized RF utilization by moving 5 GHz capable client out of the congested 2.4 GHz channels.

Improves Network Throughput

Extends reliable multicast into the wireless network by converting multicast to unicast at the AP

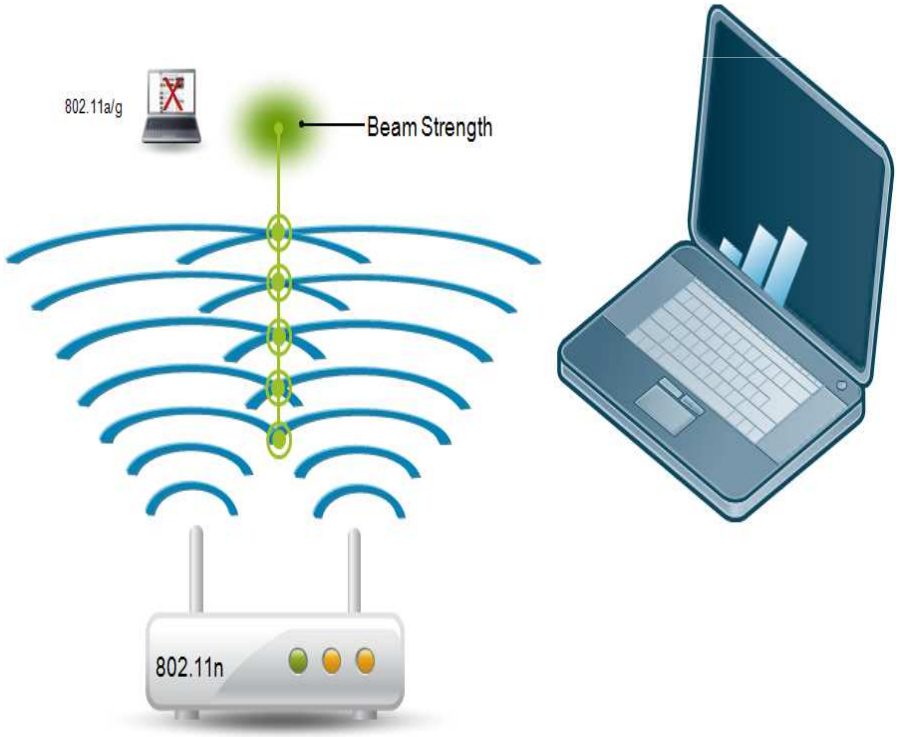
Efficient Video over WLAN

What is Clientlink Technology?

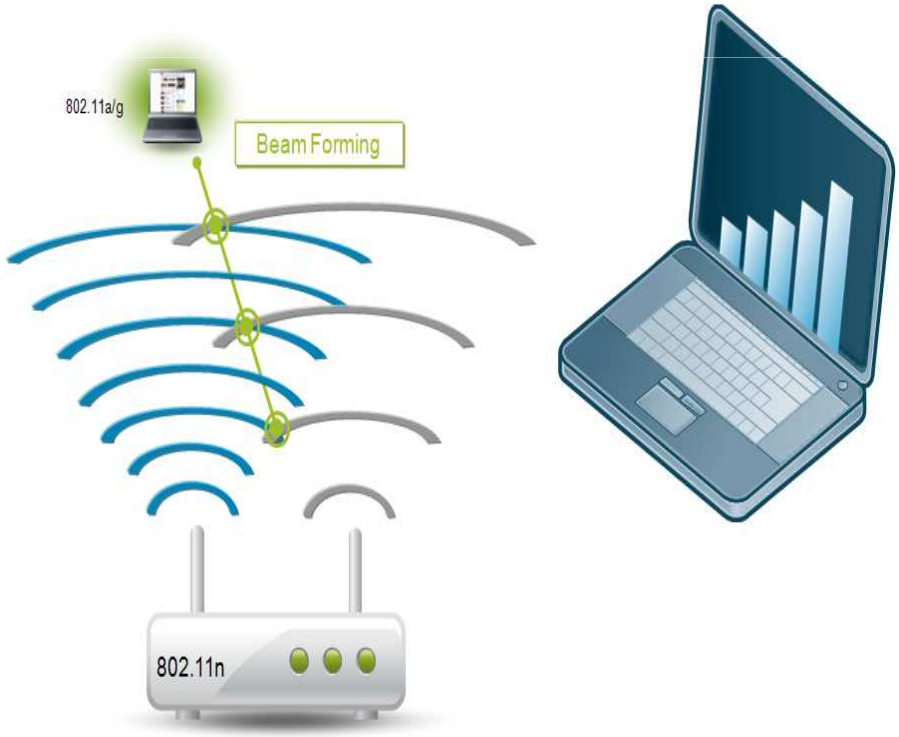


- Silicon-level intelligence that focuses DL RF energy (Beamforming) directly to 802.11a/g clients
  - Higher Signal Strength ► Higher Throughput (up to 85%)
  - Higher Signal Strength ► More Range (~20%)

w/o Clientlink



w/ Clientlink

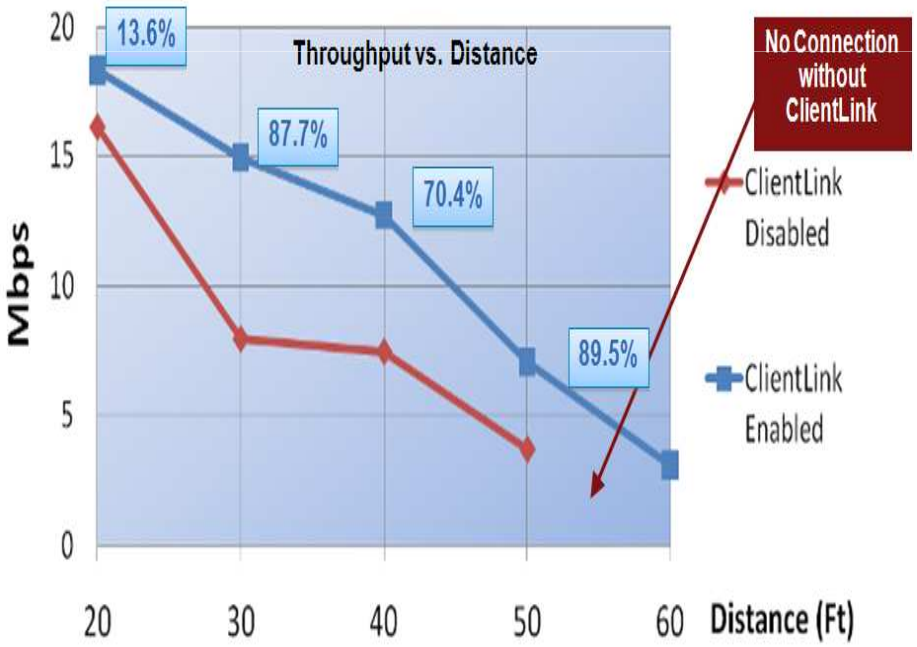


DL: Downlink

Benefits of Clientlink Technology - Capacity

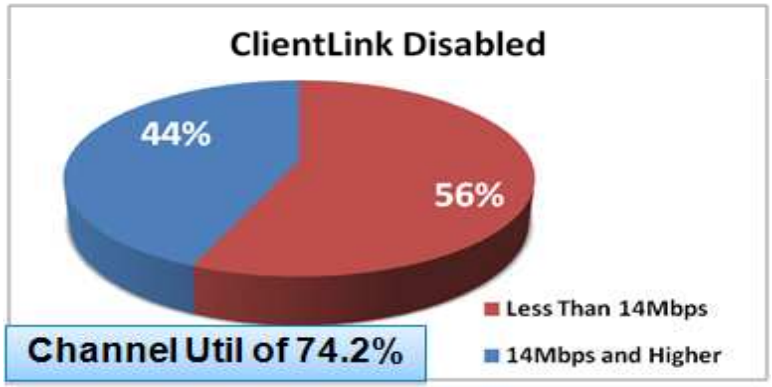
Up to 87% higher performance per 11a/g device

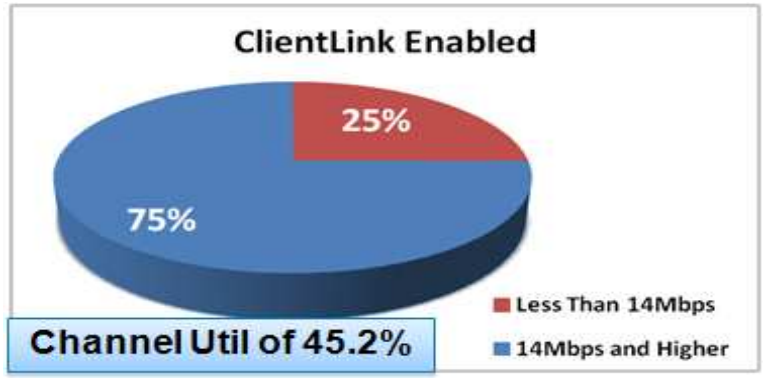
- Beam Forming directs signal to improve performance & coverage for any standards based 802.11a/g device



~27% Network Capacity Improvement

- Faster data transmission, less retries = more efficient use of RF channel
- Faster 11a/g transactions opens airtime for 11n devices, providing them improved experience



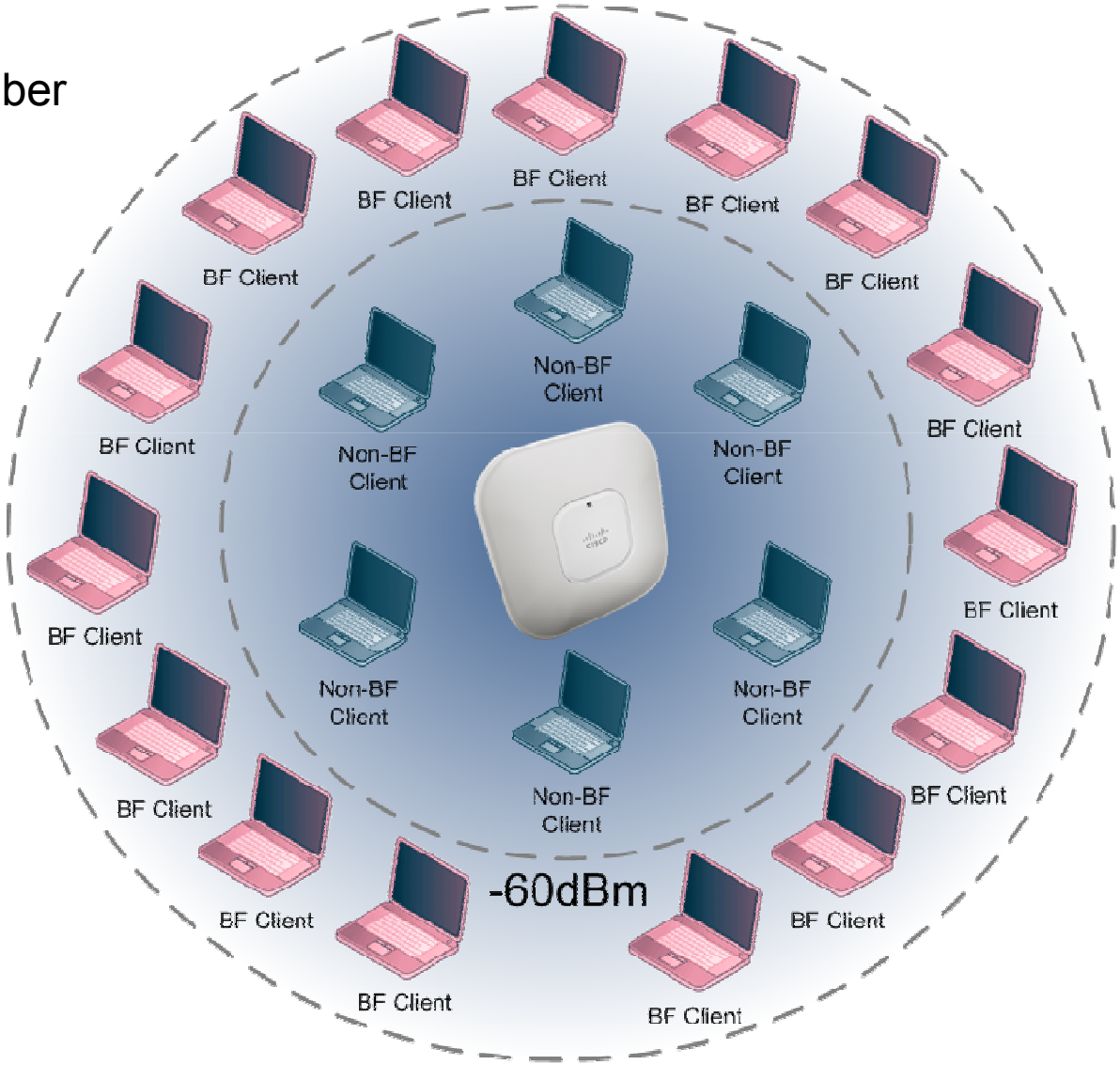


Miercom

Clientlink Essential Facts

15 Beamforming Clients per Radio (Dual Band AP: 30 Clients)

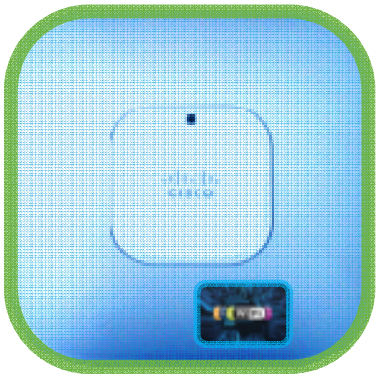
- 15 is **not** the maximum number of clients per radio
- Example:
  - 15 Beamforming Clients
  - 6 Non-Beamforming Clients
  - Total of 21 clients



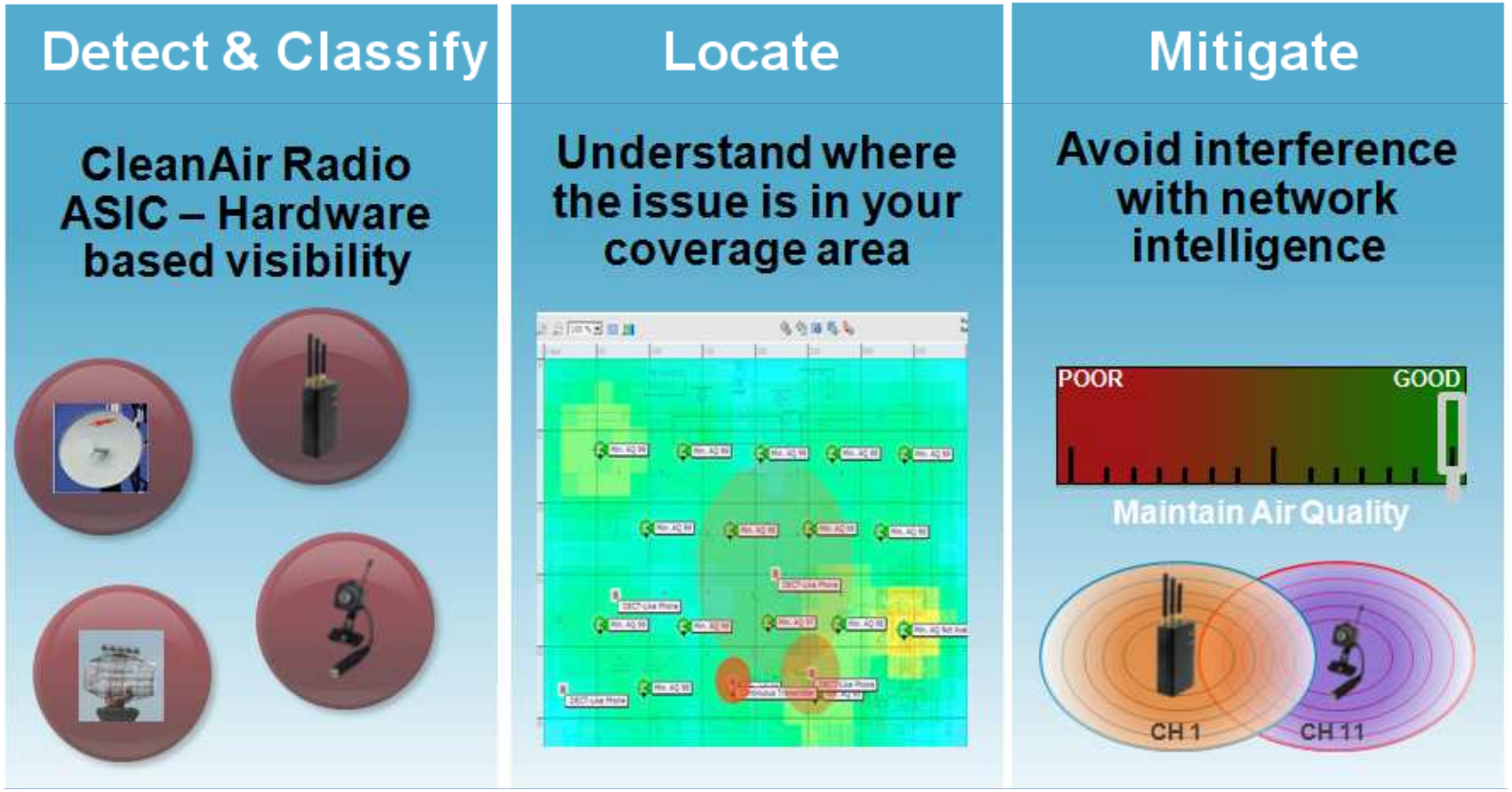
Benefits of Cisco Clientlink Technology

Features	Benefits
▪ Up to 87% throughput improvement for 11a/g devices	**Support Mixed Client Environment** *Migrate devices at own pace (protect legacy investment)*
▪ ~27% overall network throughput improvement	**Higher User Density** *Online collaboration, higher BW applications*
▪ ~20% range improvement for 11a/g devices	**Fill Coverage Holes** *Uninterrupted coverage, better RF planning*
▪ Non-proprietary solution – works within the 802.11 standard	**Full Advantage of 11a/g Ecosystem** *Works with any standards based 11a/g device*

What is CleanAir Technology?



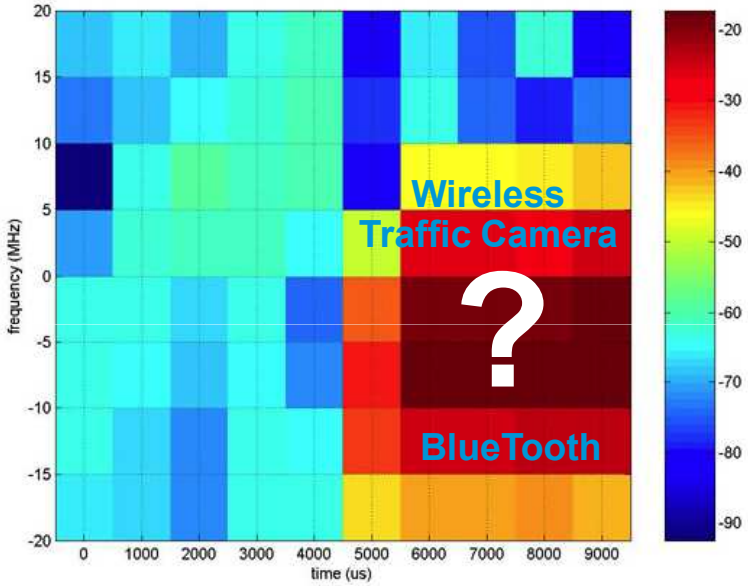
- Silicon-level intelligence to automatically mitigate the impact of wireless interference, optimize network performance and reduce troubleshooting costs
  - Classification processed on Access Point
  - Interference impact and data sent to WLC for real-time action
  - WCS and MSE store data for location, history, and troubleshooting



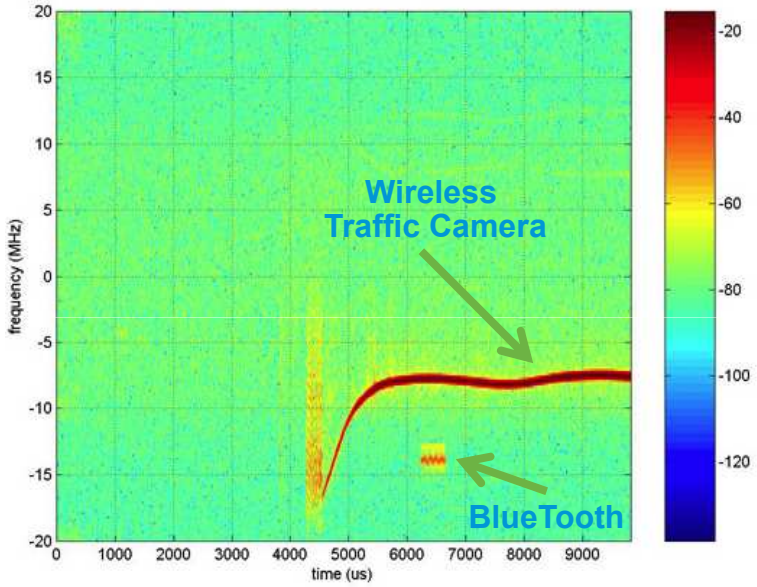
High Resolution Spectral Advantage

The Industry's ONLY in-line, high-resolution spectrum analyzer …

Typical SW Implementation
Spectral Resolution at 5 MHz



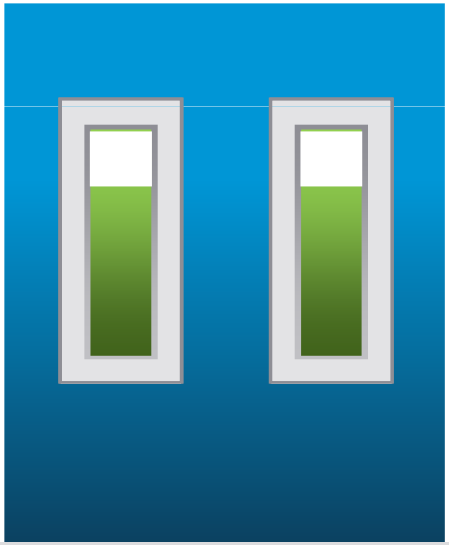
Cisco CleanAir Wi-Fi chipset
Spectral Resolution at 78 to 156 KHz

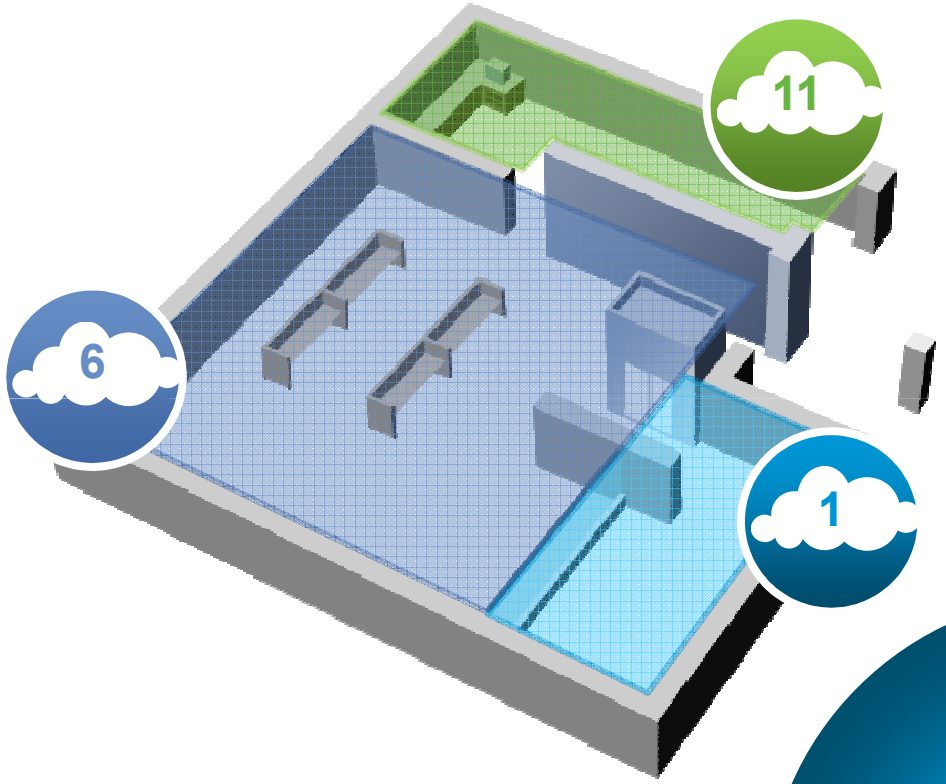


… provides the ability to detect & avoid common <u>outdoor interferers</u>

- Rogue APs / Jammers
  - ► WiFi Inverted Signal, WiFi Invalid Channel
- Outdoor Interferers
  - ► Wireless Video Camera, WiMAX, RADAR
- Other Interferers
  - ► DECT wireless phones, …

Self Healing and Optimization

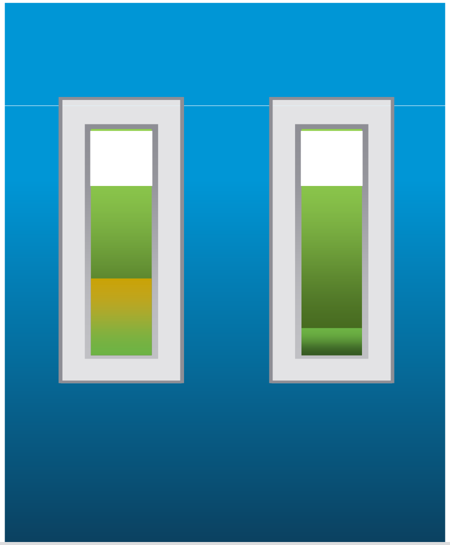


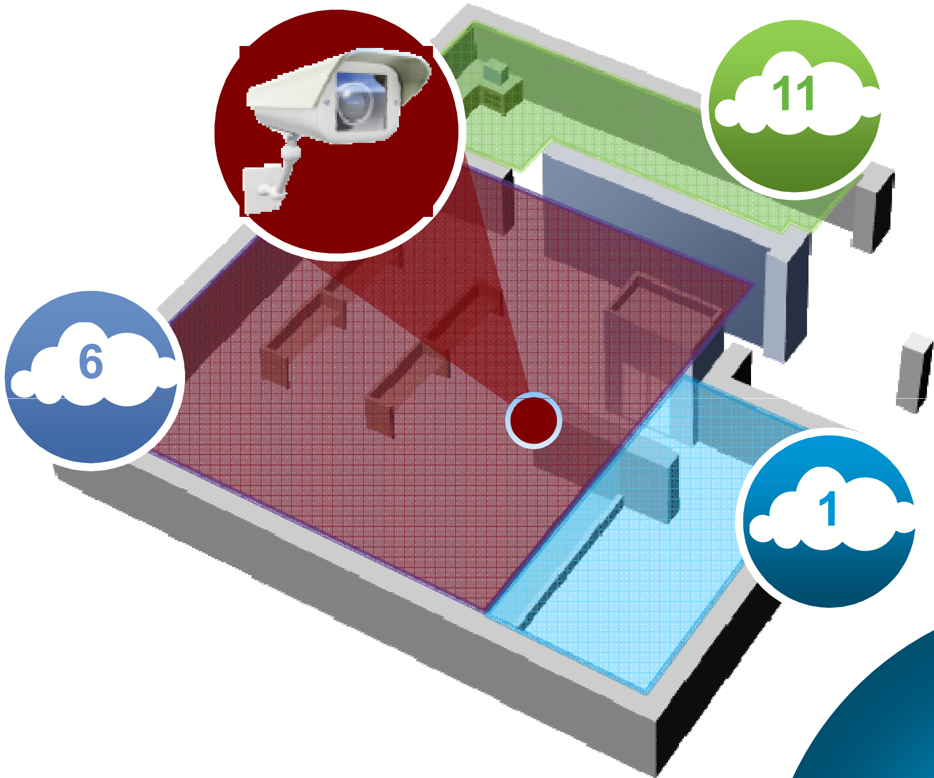


Wireless LAN Controller

Channels 11, 6 and **1** are optimized for maximum performance and minimum interference

Self Healing and Optimization



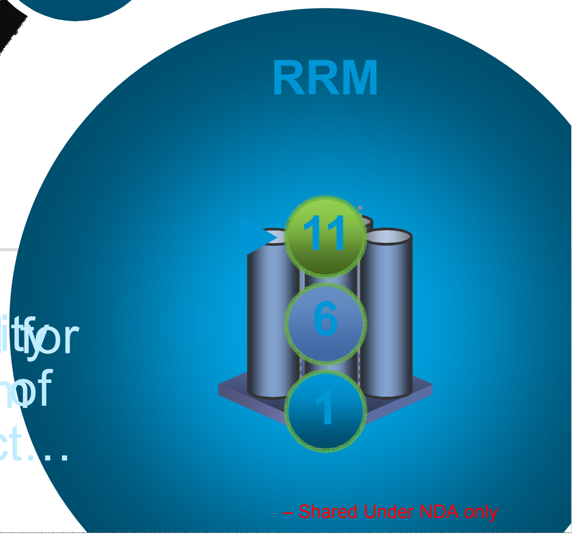


Wireless LAN Controller

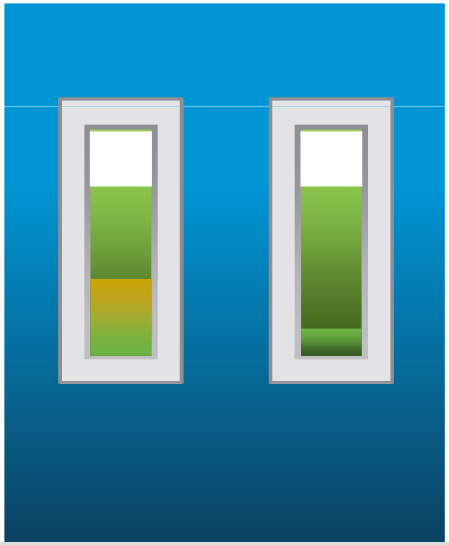
Interference on Channel 6, Air Quality

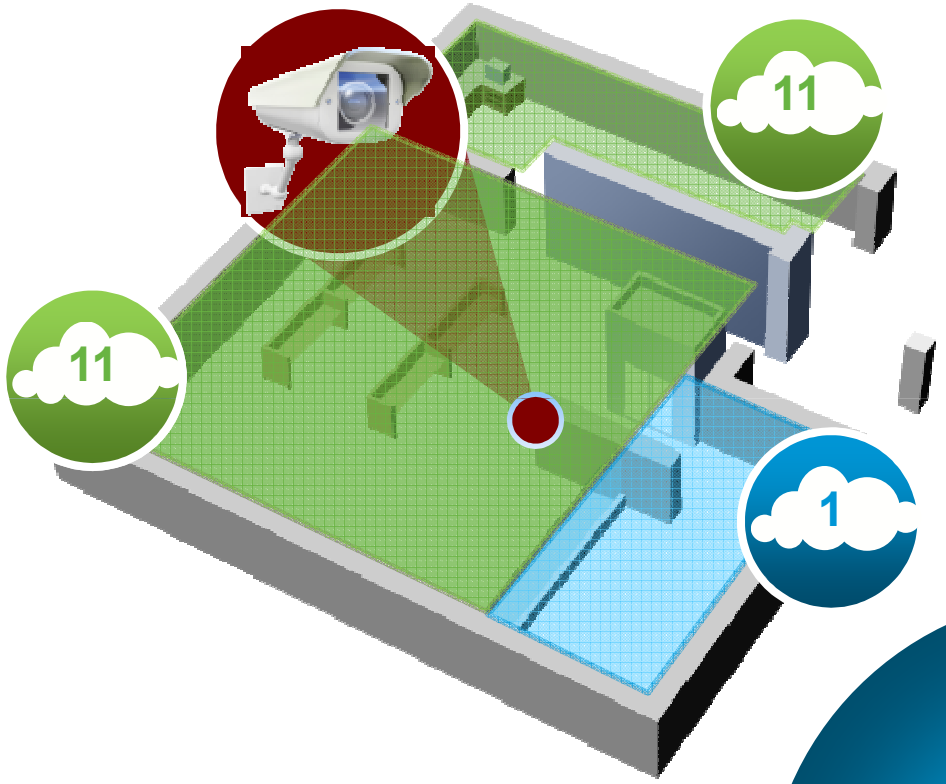
Channels 1, 6 and 11 are optimized for maximum performance allowing minimum interference

Scanning available channels in the list of preferred channels to resolve conflict...



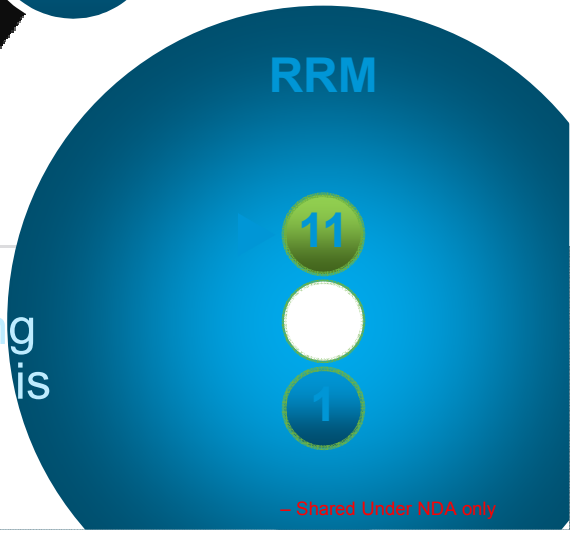
Self Healing and Optimization





Wireless LAN Controller

Conflict resolved. Information is being relayed to RRM. Conflicting channel is blocked from future use.



Benefits of Cisco CleanAir technology

Features	Benefits
▪ AirQuality Aware RRM ▪ Event Driven RRM ▪ Persistent Device Avoidance	**Self Healing and Optimizing** *Reduces Downtime, Maximizes Resilience*
▪ Remote Client Troubleshooting ▪ Spectrum Expert Connect ▪ Location, Impact Analysis and History Playback	**Troubleshooting Forensics** *Lowers Problem Resolution Time/Cost*
▪ New Rogue Threats Detection (off-channel, inverted) ▪ DOS Jammer Detection	**Wireless Security** *Improves Visibility to New Threats*
▪ Unwanted Device Notification ▪ Unwanted Device Location	**Policy Enforcement** *Enables Enforceable Rules*

RRM: Radio Resource Management

What is BandSelect Technology?
Access Point Assisted 5 GHz Band Selection

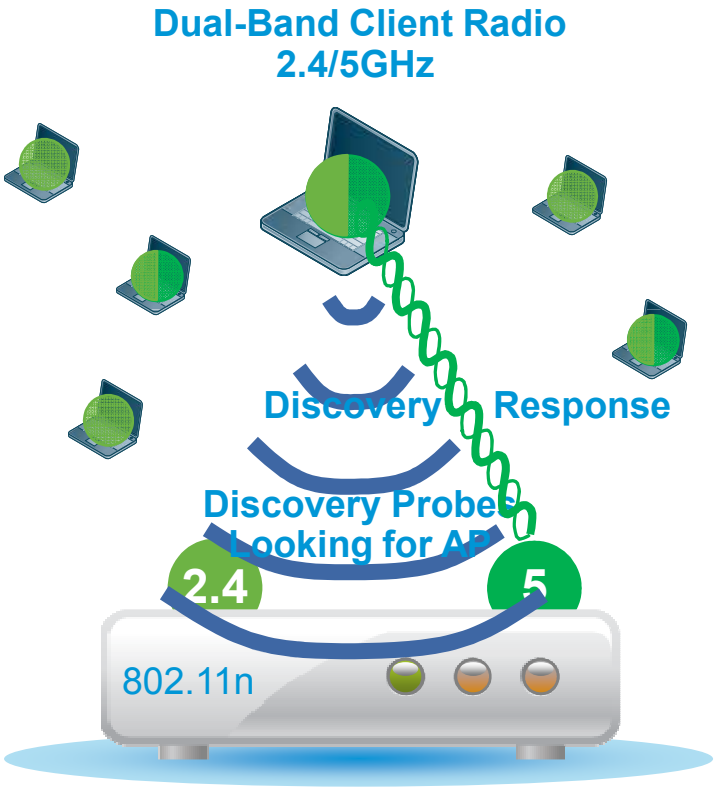
Challenge

Dual-Band clients persistently connect to 2.4 GHz

Solution

BandSelect directs clients to 5 GHz optimizing RF usage

- Better usage of the higher capacity 5GHz band
- Frees up 2.4 GHz for single-band clients



Optimized RF utilization by moving 5 GHz capable client out of the congested 2.4 GHz channels

BandSelect Algorithm

- Probe suppression

  Identify dual-band clients (2.4GHz & 5GHz capable)
  - Suppress immediate probe response on 2.4 GHz channels
  - Wait for dual-band clients to scan into 5 GHz channels

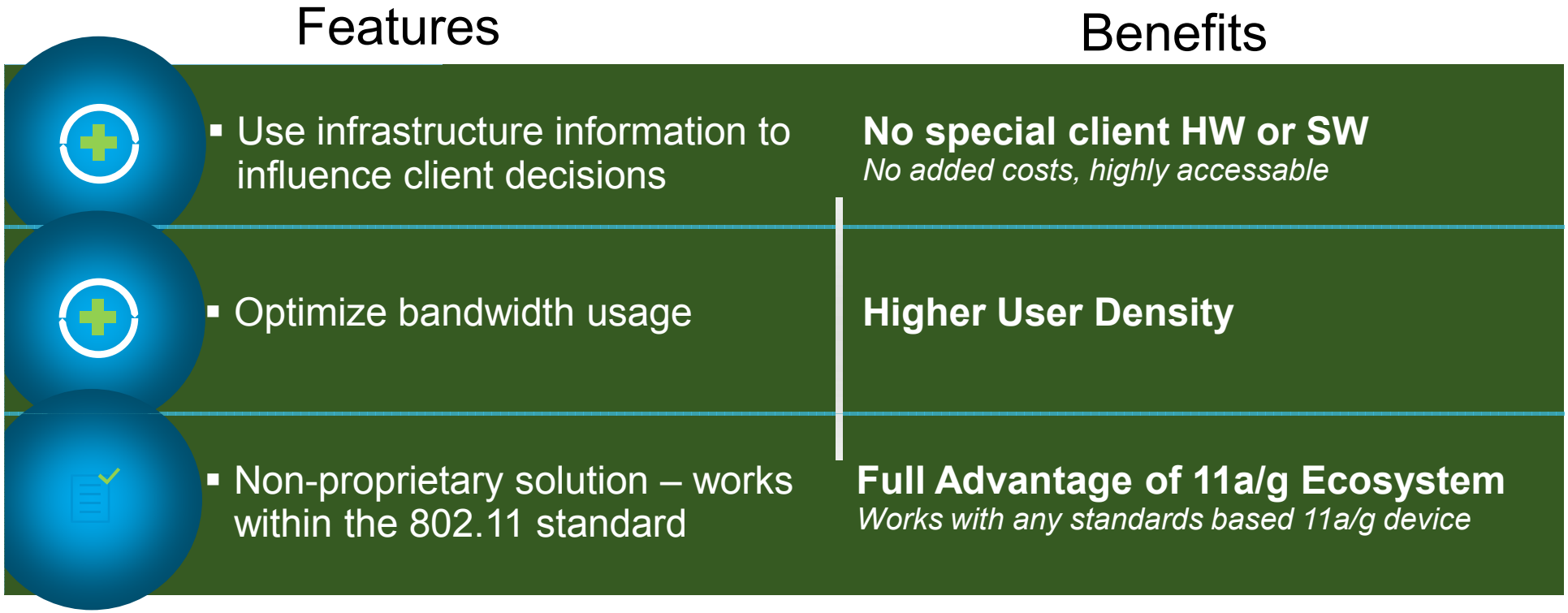
  Do not respond to dual-band capable client on 2.4 GHz

- Accommodate 2.4GHz clients & dual-band clients that fall back to 2.4GHz
  - Time-out dual-band client 2.4GHz probe response suppression
  - Mark 2.4 GHz only clients & respond with probes

- Distributed algorithm
  - Algorithm runs on AP firmware
  - Global configuration for the algorithm parameters on controller

  Per WLAN ‘override’ control

Benefits of Cisco BandSelect Technology



Cisco Wireless

Performance Protection for 802.11n

More Bars Everywhere

- Beam forming improves throughput for 11a/g devices

Interference Mitigation

- Detect, Classify, Locate and Mitigate

Intelligent Network Utilization

- Move 5GHz capable clients out of congested 2.4GHz channels

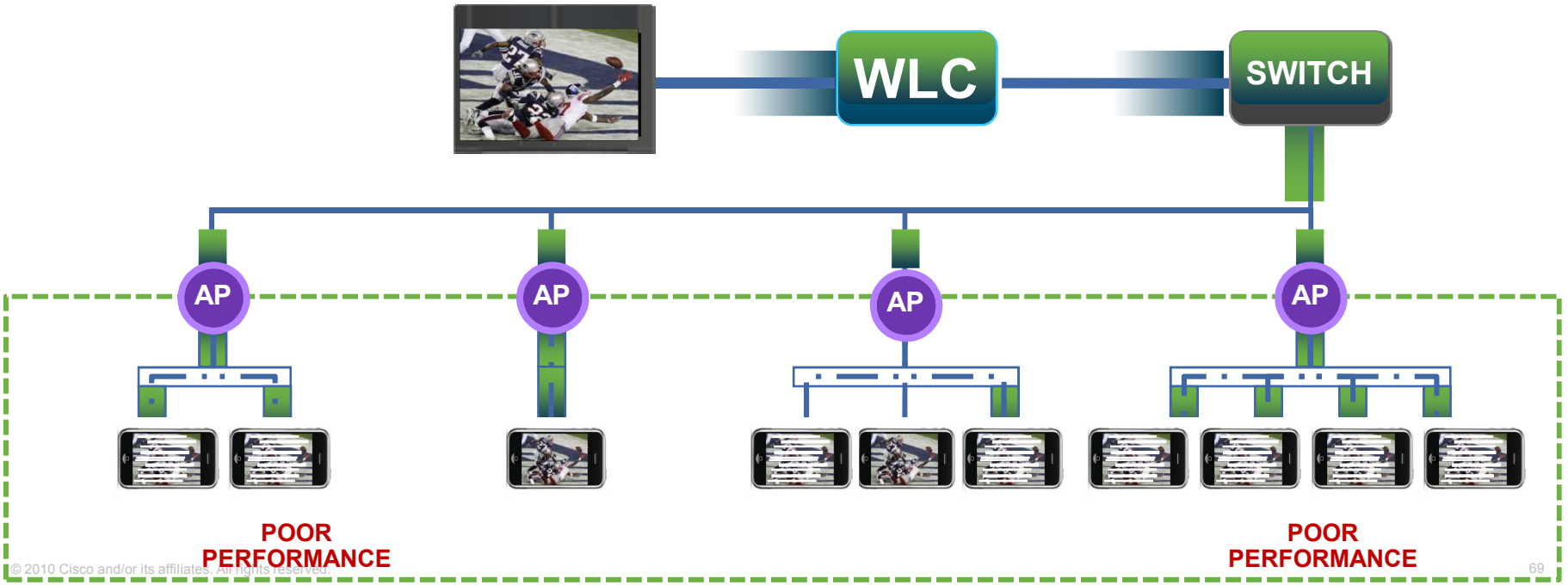
Cisco 802.11n

- First enterprise-class Wi-Fi certified product
- 65% market share
- Comprehensive product portfolio

Streaming Video Challenges
Radio Frequency Limitations

- Can't deliver multicast video over RF at scale
- Video overloads network and degrades other application performance
- Unable to deliver quality video

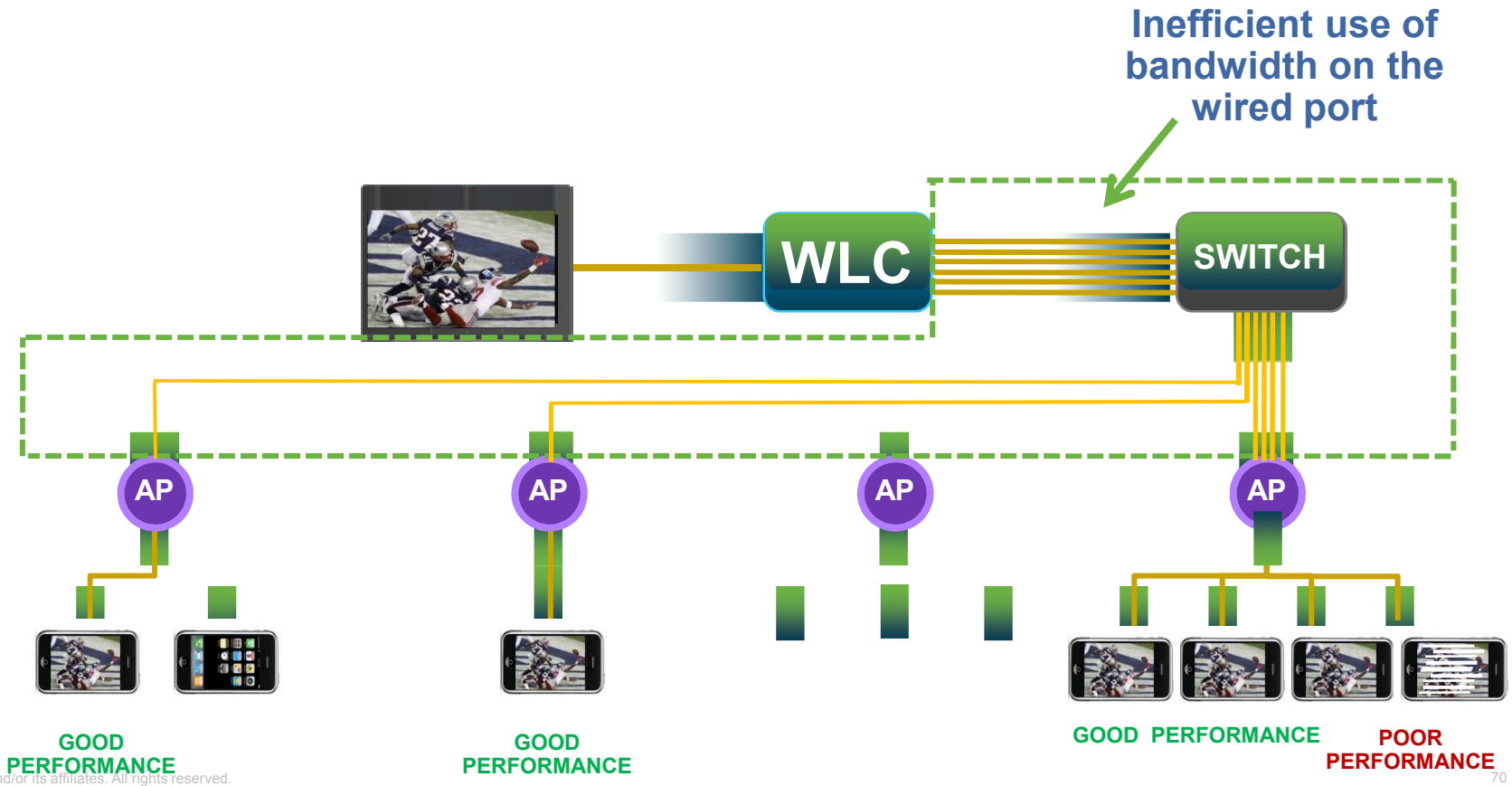
Video Streaming Without Reliable Multicast



Streaming Video Challenges

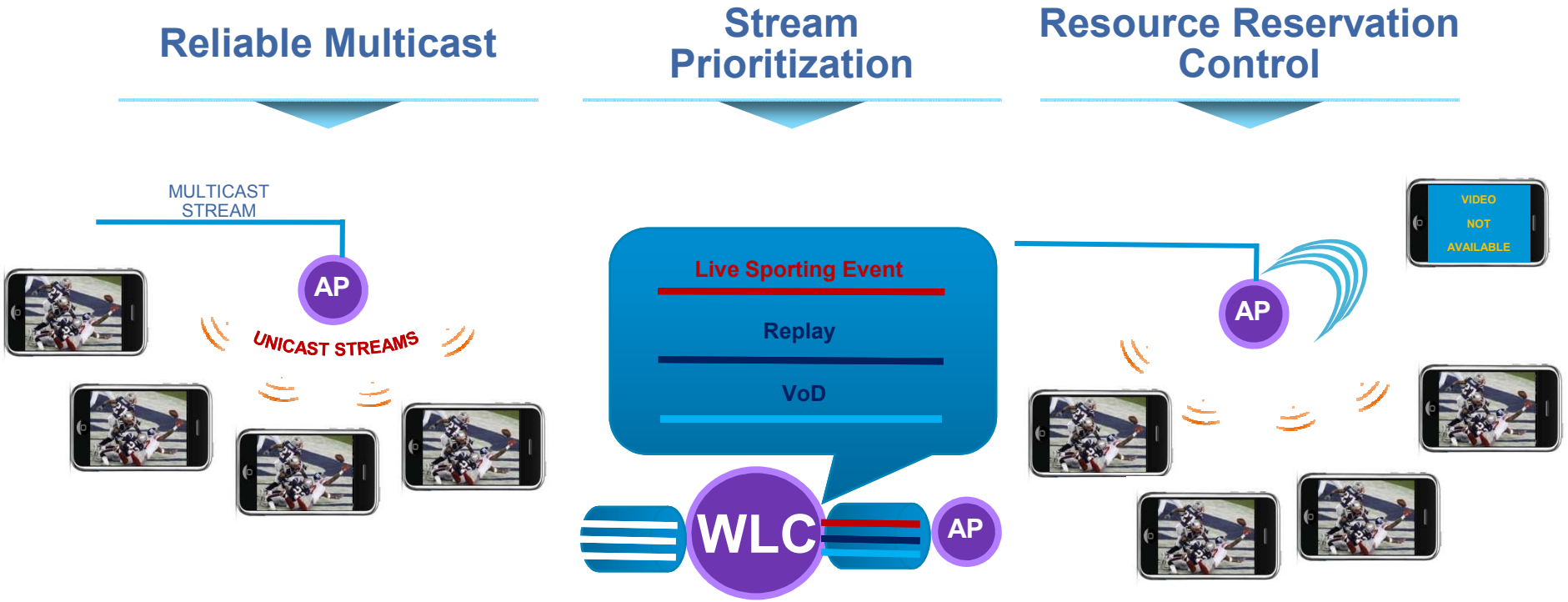
Poor Wired to Wireless Network Integration

- Reliability at WLC improves quality but NOT overall scale
- No identification of respective priority
- Inefficient use of overall network



VideoStream Technology

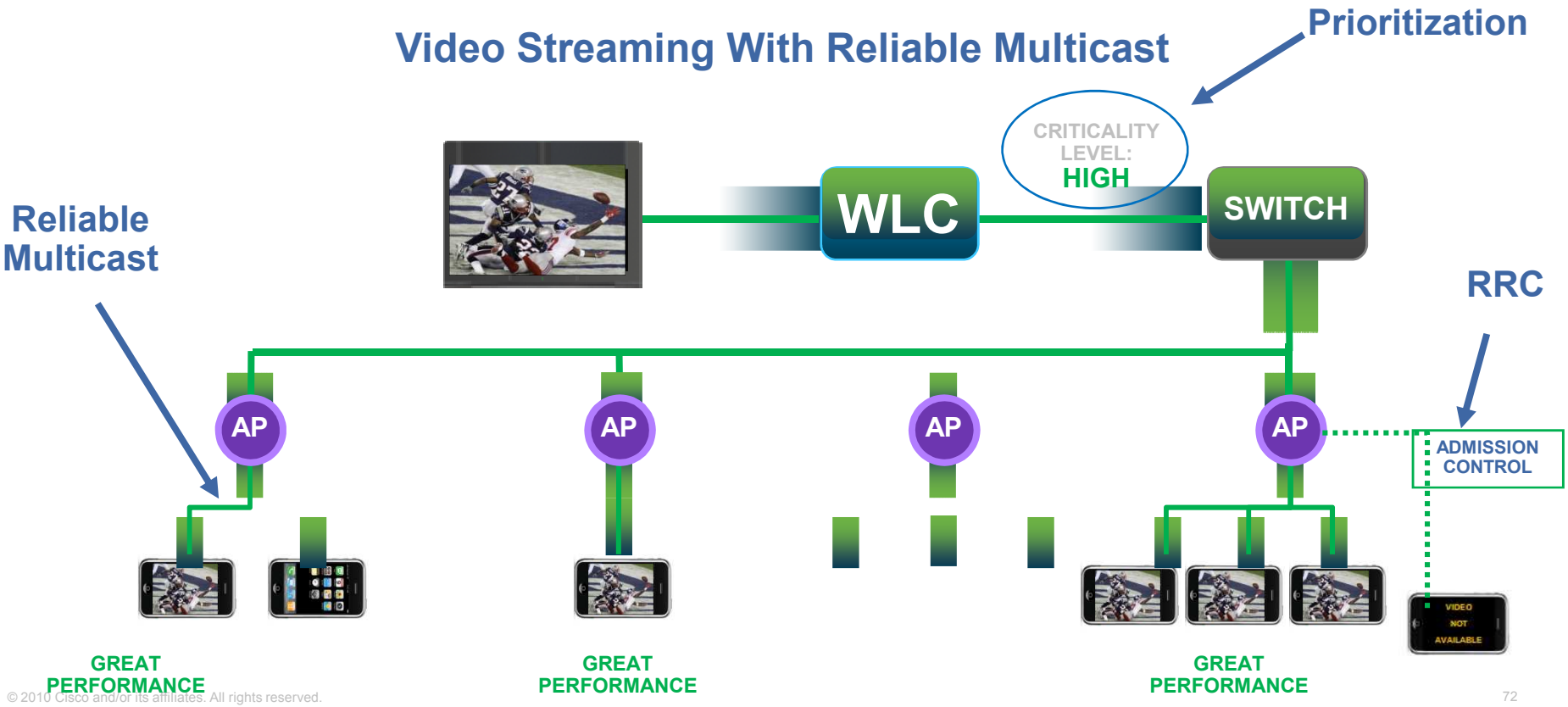
- Cisco VideoStream Technology enables reliable and consistent delivery of quality video over the wireless network



Media Ready WLAN with VideoStream

Wireless Investment Optimized for Video

- Improves quality and scale of streaming content:
  - Solves challenges with RF and wired / wireless integration
  - Brings wired video quality to wireless
  - Stream prioritization protects important content precedence



What Does the Cisco Outdoor Wireless Solution Provide?

- **Complete Indoor and Outdoor Networking Solution**

  Part of the Unified Wireless Network for a complete end-to-end wireless solution for the mobile workforce

- **Scalable Mesh Architecture**

  Designed to scale to various size networks from campus deployments to extensive outdoor environment such as large metropolitan areas

- **Mobility Services and Applications**

  Designed to support robust integrated security services, guest network (public access) and vertically-focused applications

- **Open Architecture**

  Allows an ecosystem of partners to extend services to third party applications and services such as video surveillance, automated meter reading, etc.

Outdoor 11n AP Summary

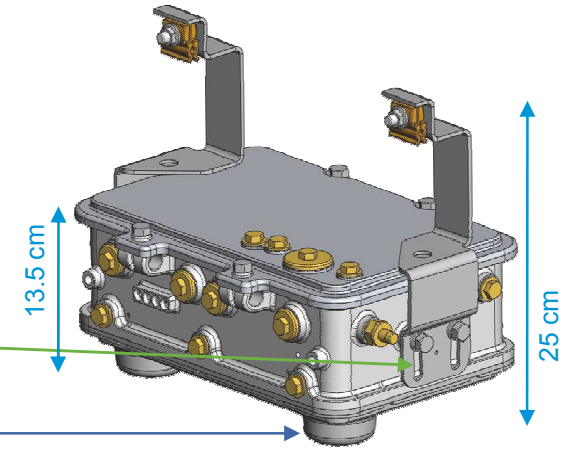
Leveraging Cisco's 11n Leadership & Expanding Value Differentiation

- New Industrial Form Factor & Mount

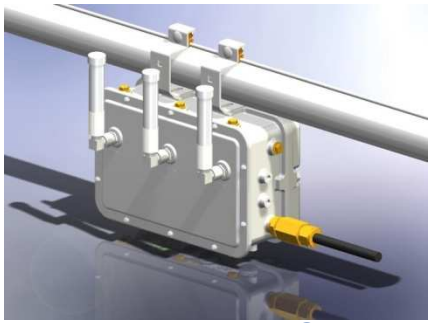
  Low-Profile: chassis & antenna only 25 cm high
  (easily complies with 30 cm cable-strand height restrictions)

  Bracket for horizontal Chassis orientation
  Strand Slope Adjustment Capability

  3-Element Dual-band (2.4 & 5 GHz) Antenna array in a single low-profile radome



NEW 802.11n



Current a/b/g

OPS

- Replaces up to 6 single-band stick antennas (for dual-band 2X3 MIMO radios)
- Optimizes field-of-view by placing antennas to bottom
- Eliminates possibility of "non-connected" antenna
- Reduces deployment complexity/Eliminates cables
- Eliminates possibility of cable-antenna tangle/break-off
- Reduced Cost

U-NII-2 5.250-5.350 GHz (100 MHz) + new DFS req't (0.5 μs)
U-NII-Worldwide 5.470-5.725 GHz (255 MHz) + new DFS req't (0.5 μs)
U-NII-3 5.725-5.850 GHz (125 MHz)
vs. others meet old DFS req't. (0.8 μs) ► not FCC certified for U-NII-2

U-NII Unlicensed National Information Infrastructure
DFS Dynamic Frequency Selection; radar avoidance

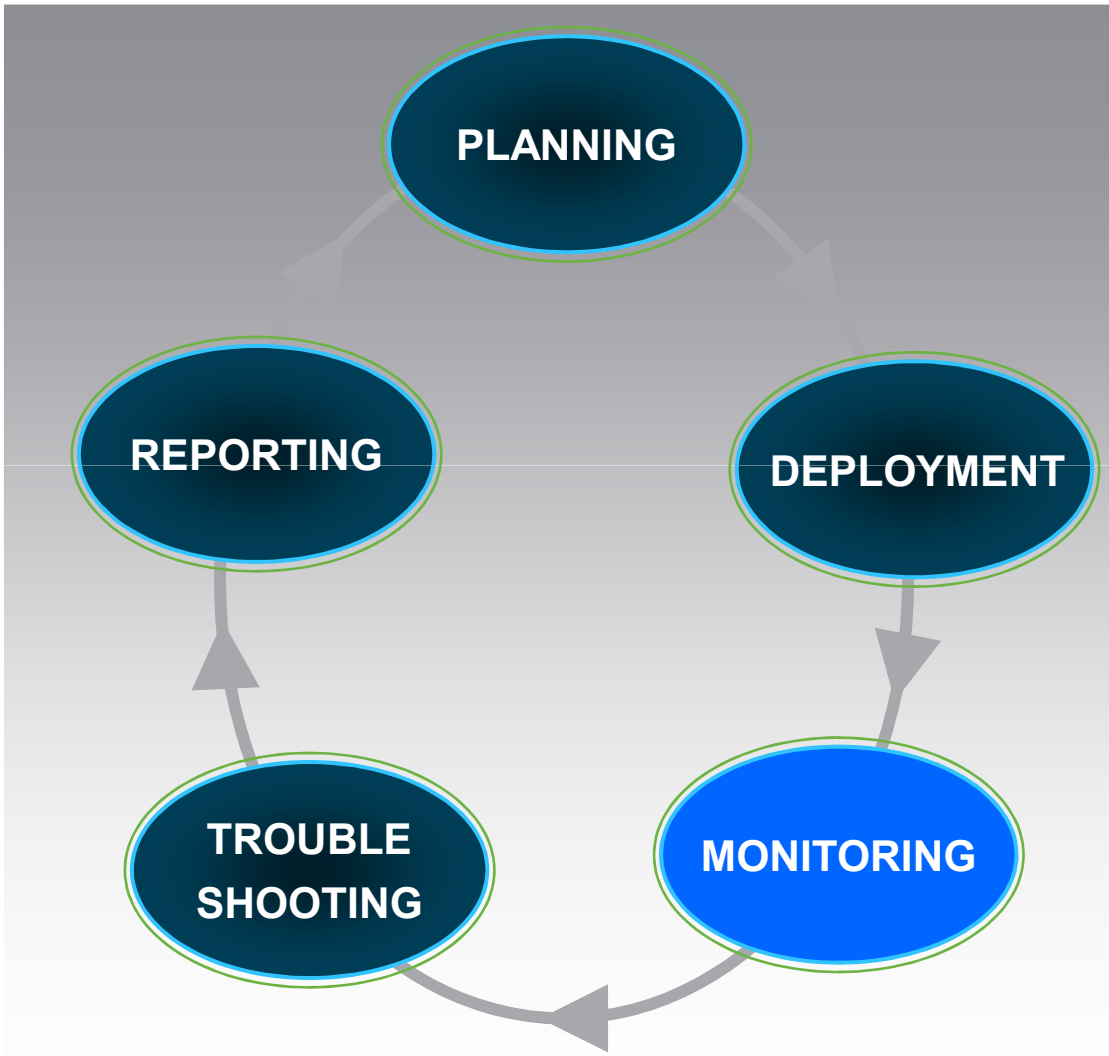
Cisco Outdoor 11n Access Point

RF Superiority Reduces Cost

- Higher Coverage & Throughput; Less APs req'd.
  Provide Same Coverage to a given area with up to 25% less APs
- Less APs = Lower Direct Expense
  - Reduced CAPEX (Hardware, Installation, Peripheral)
  - Reduced OPEX (Network OPEX & Maintenance OPEX)
- Spectrum Intelligence reduces Indirect Expense
  - ClientLink: Delivers stronger signals to legacy Clients
  - CleanAir: Locates & isolates Interferer
  - Band Select: Moves 5GHz capable client out of 2.4GHz channel
  - RRM: Avoids high interference channels
  - RESULTS: Improved Customer Experience

Cisco Wireless Control System (WCS)

Comprehensive WLAN Lifecycle Management



- Ensure Network High-Availability
- Complete visibility & control of the RF environment
- Comprehensive lifecycle management in a single centralized platform
- Easy trending, capacity planning & troubleshooting
- Lower OPEX & CAPEX

Summary

Cisco SP WiFi for Mobile Offload

- Offload Architectures
  - Each MO has different motivation for Offload
  - Multiple technologies can be deployed depending on requirements
  - Flexibility is needed to adopt the architecture to new business models
- Flexible and Modular Core
  - Different levels of offload integration are supported
  - Step-by-step deployment as requirements grow
  - Integrated core functions in the ASR 5000
  - Developed in-line with 3GPP standards
- Outstanding Radio Performance
  - Years of experience
  - Controller based for better RRM, Security and Mobility
  - CleanAir, ClientLink, BandSelect, VideoStream
  - Industry leading outdoor access points


cisco

I-WLAN Mobility