

Cisco Expo 2011



Архитектура SP Service Mesh для построения WiFi сетей доступа в Интернет операторами связи

Александр Литвин

innovate *together*

Оцени контент Cisco Expo и получи приз!

Призы ждут всех, кто:

- посетил 2 и более дней конференции
- заполнил общую анкету
- заполнил 5 и более сессионных анкет
- заполнил анкеты по 2 и более плановым демо

Онлайн-анкеты доступны на сайте www.ceq.com.ua.

Анкеты также можно заполнить, воспользовавшись терминалами в зоне общения на первом этаже.



SP Wi-Fi: Drivers for Change

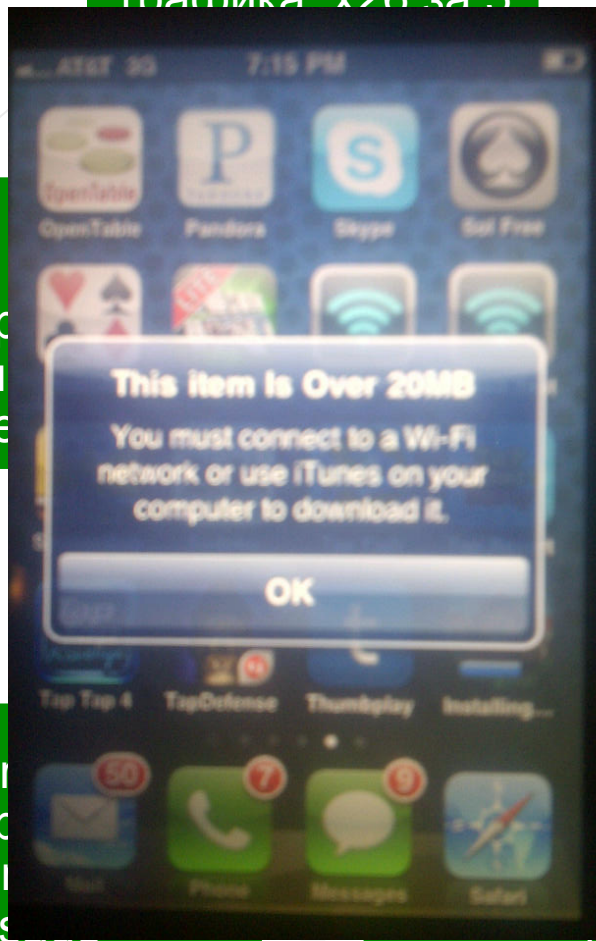
Рост мобильного трафика: x26 за 5

Большая экономия достигается при использовании small/Femto с

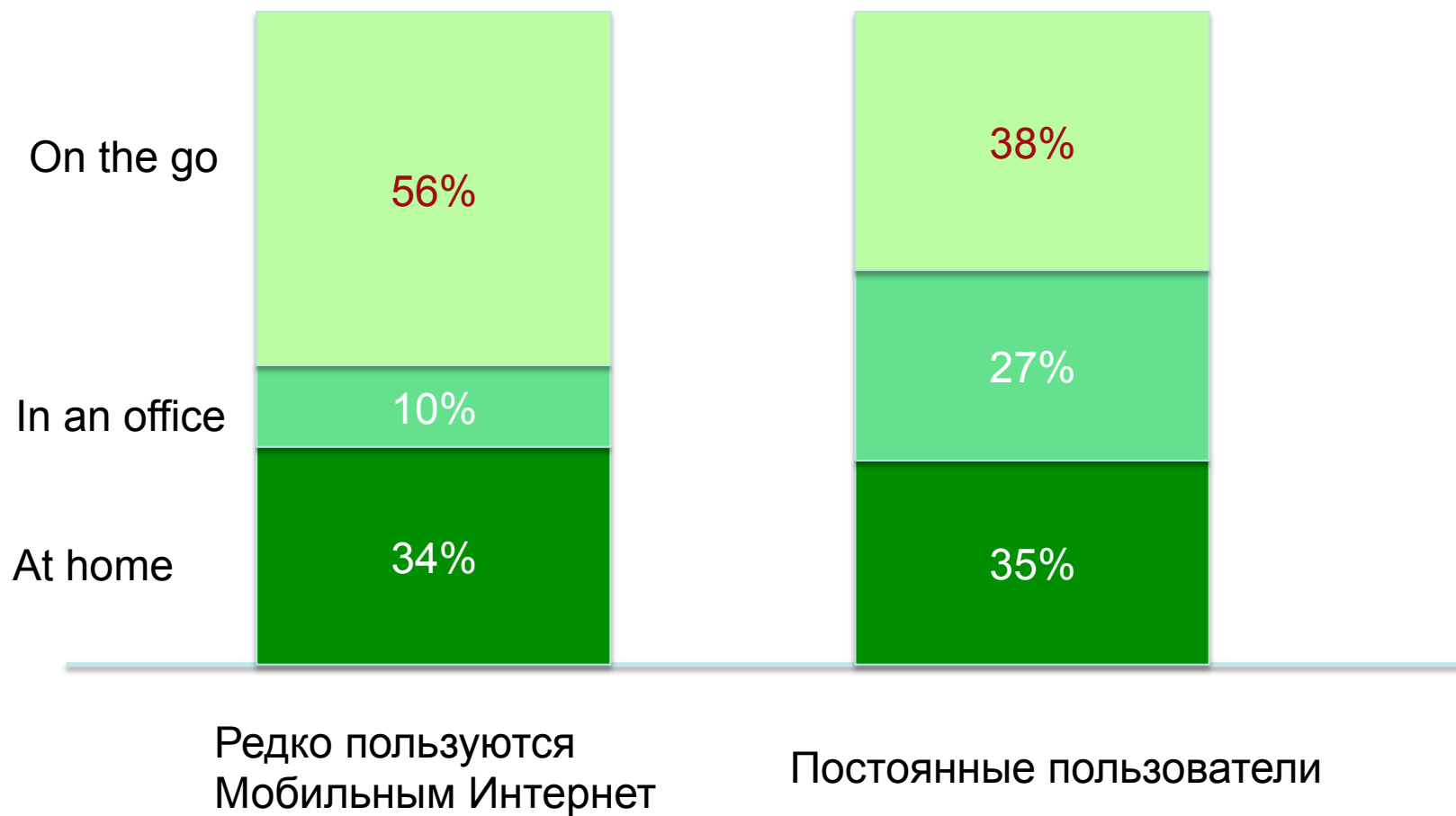
нехватка спектра поддерживает рост кол-ва # cell sites

Wi-Fi allowed to support of US usage

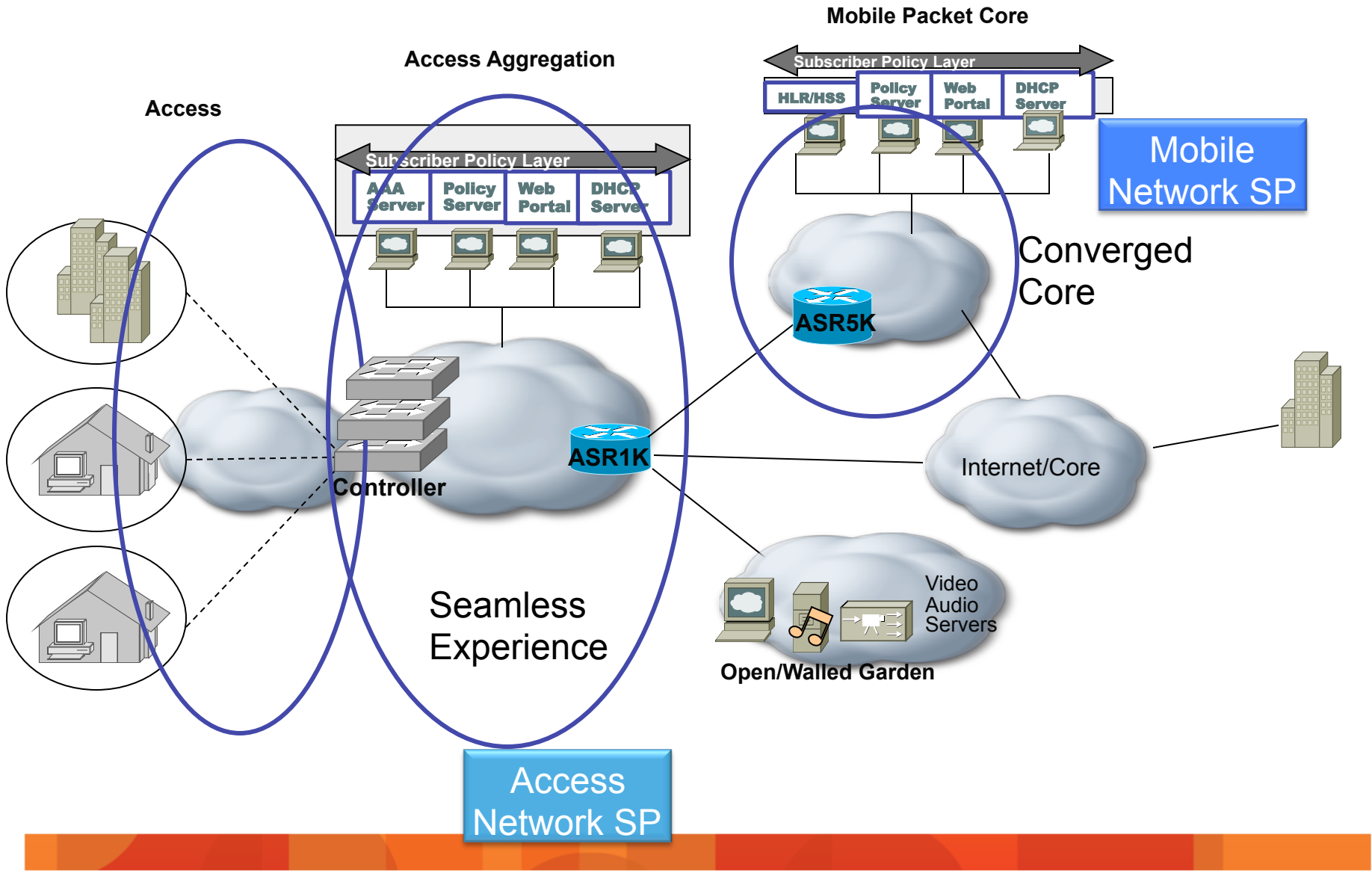
indoor группа является КОЛ-ВО трафика



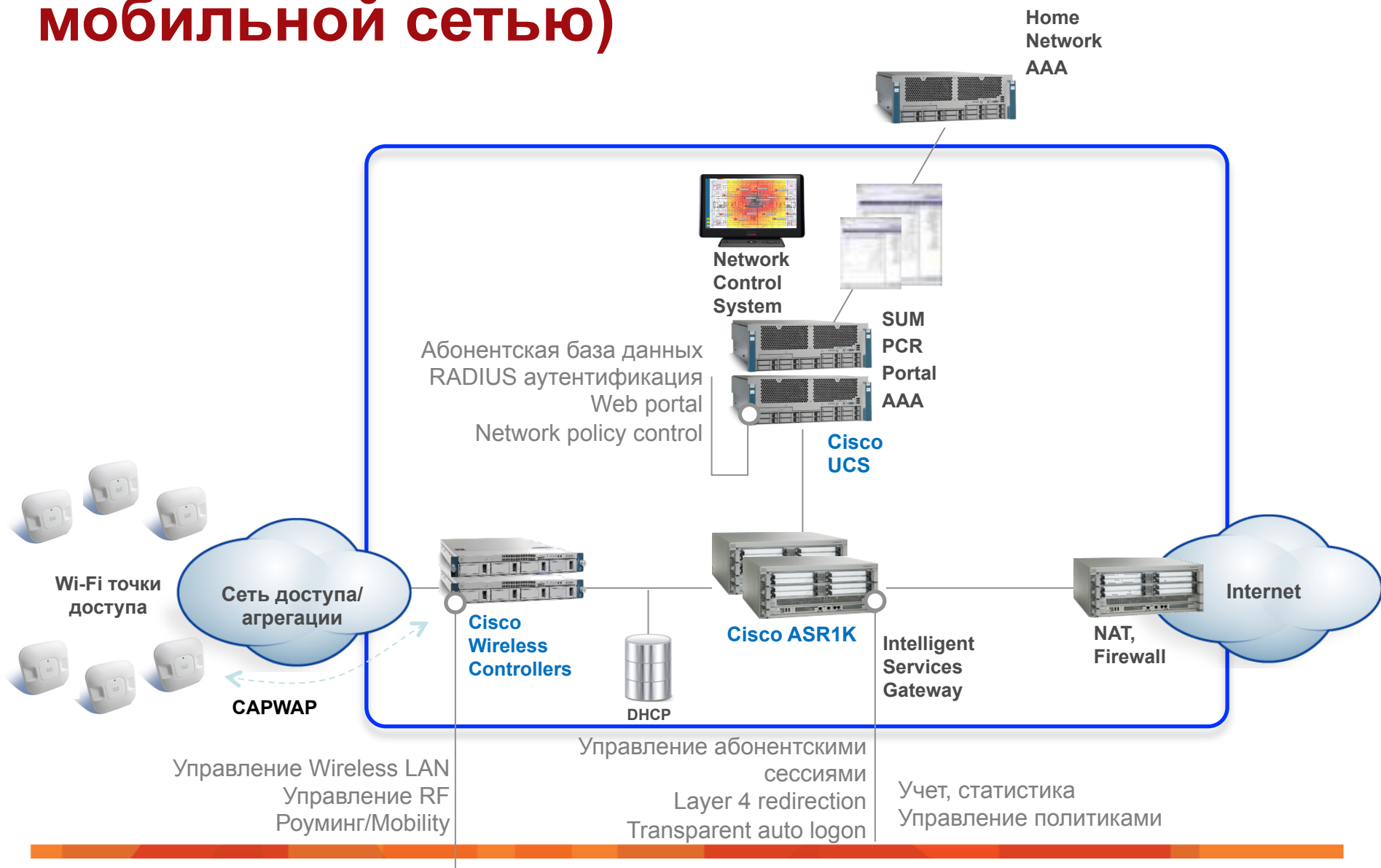
Мотивации к изменениям: Изменение модели использования Мобильного Интернет



Доступ + Агрегация + Ядро Сети



Cisco SP Wi-Fi(без интеграции с мобильной сетью)



SP WiFi – функциональные компоненты

Аутентификация Авторизация

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

Назначение Адресов

ISG
At LMA
Внешний DHCP
IPv4 / IPv6

Управление Абонентской сессией

Keep alive
Idle Timeout
Quota enforcement
Policy enforcement
Session differentiation

Транспортная инфраструктура

CAPWAP
PMIPv6
L2TP
GTP

Надежность и Отказоустойчивость

HSRP/ GLBP
1:1 Redundancy
N:1 Redundancy
Single SSID
Multiple SSID

Учет и биллинг

Start and Stop
Records (CDR)
Кто, кому и сколько
Интеграция с
существующим
биллингом

Web Portals

Перенаправление на
портал
Web аутентификация
Портал
самообслуживания
Open Garden

Mobility

Мобильность между
APs, между WLC,
между ISG / MAG
WiFi to Macro
Macro to Wifi
роуминг

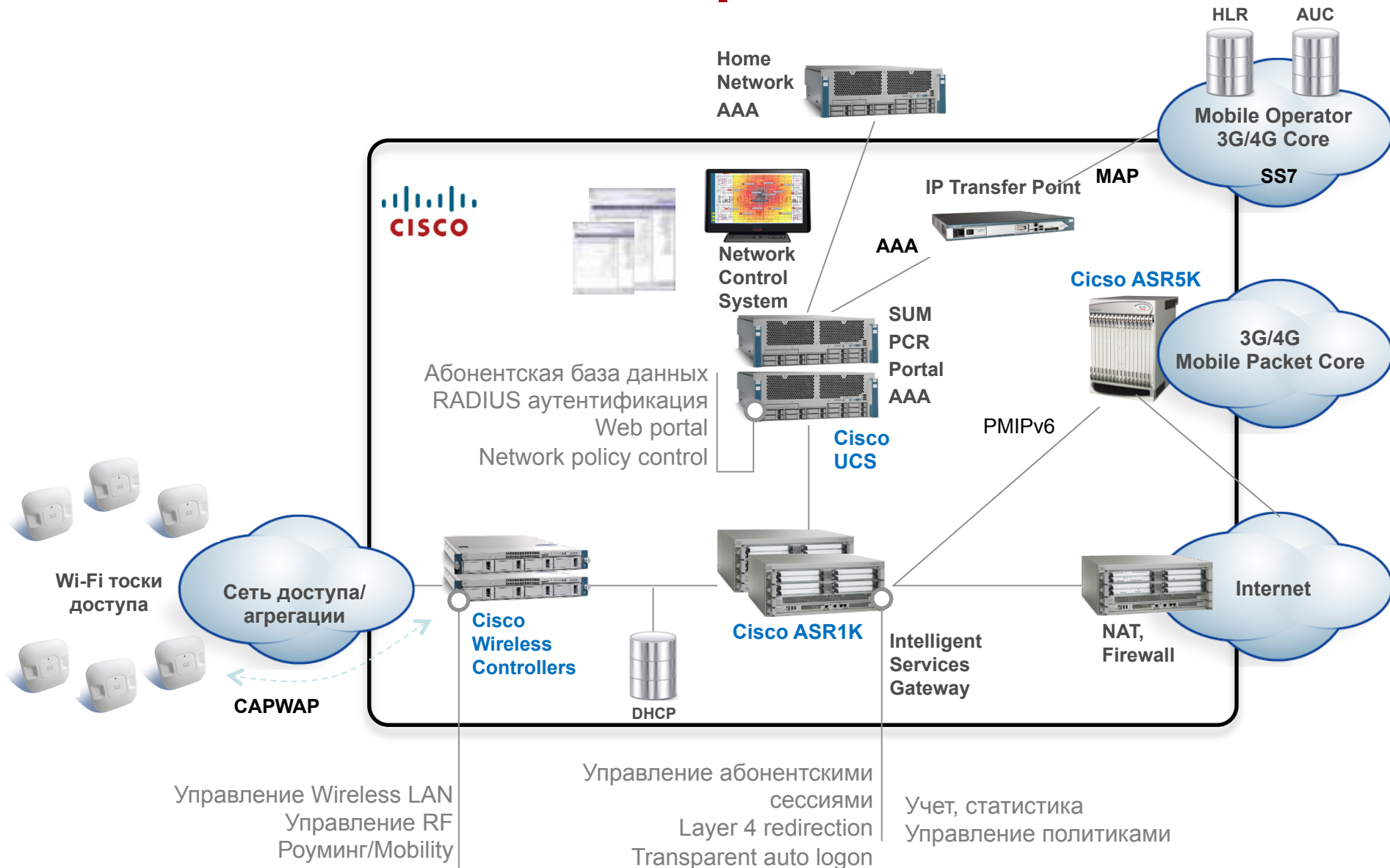
Network Management

WCS
NetFlow
Legal Intercept
Parental Control
Statistics and
Capacity planning

Управление абонентами

Provisioning
Pre-paid / on demand
WiFi only users
Transparent logon
Service profiles

Cisco SP Wi-Fi – интеграция с МРС



SP WiFi архитектура в 3GPP

Построение “Trusted Non-3GPP” сети доступа

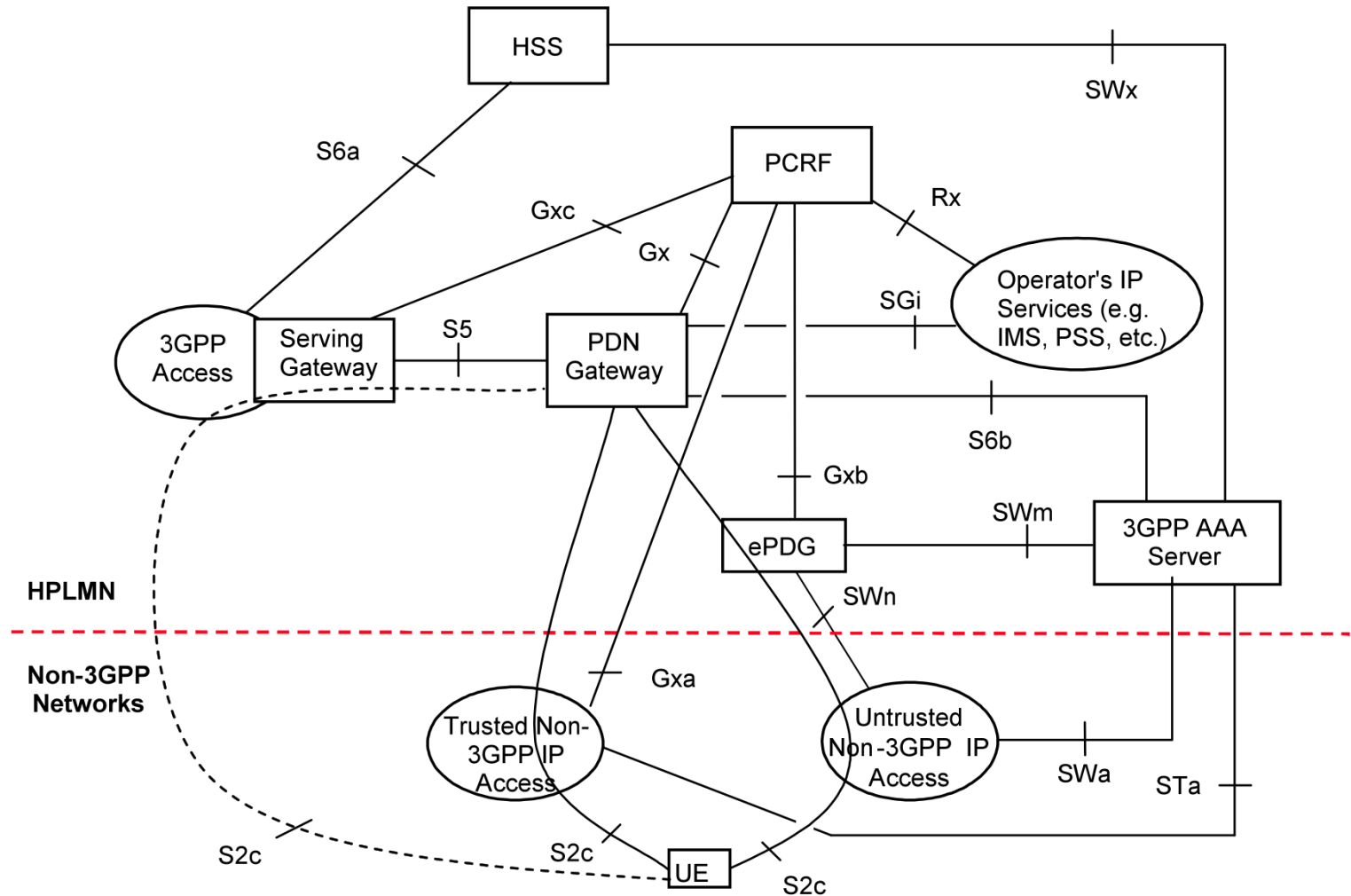
- До 3GPP Release 8, все non-3GPP сети доступа, включая и WiFi, считались “not trusted”

“WLAN security was considered poor in both strength and ease of use, compared with that taken for granted in 3G networks and devices.... Hence it made sense for the mobile network operators to use .. IPsec between the UE and ePDG for the security of the user data.”

- 3GPP Release 8, все изменил, при этом non-3GPP сети доступа (включая WiFi) считаются “trusted”:

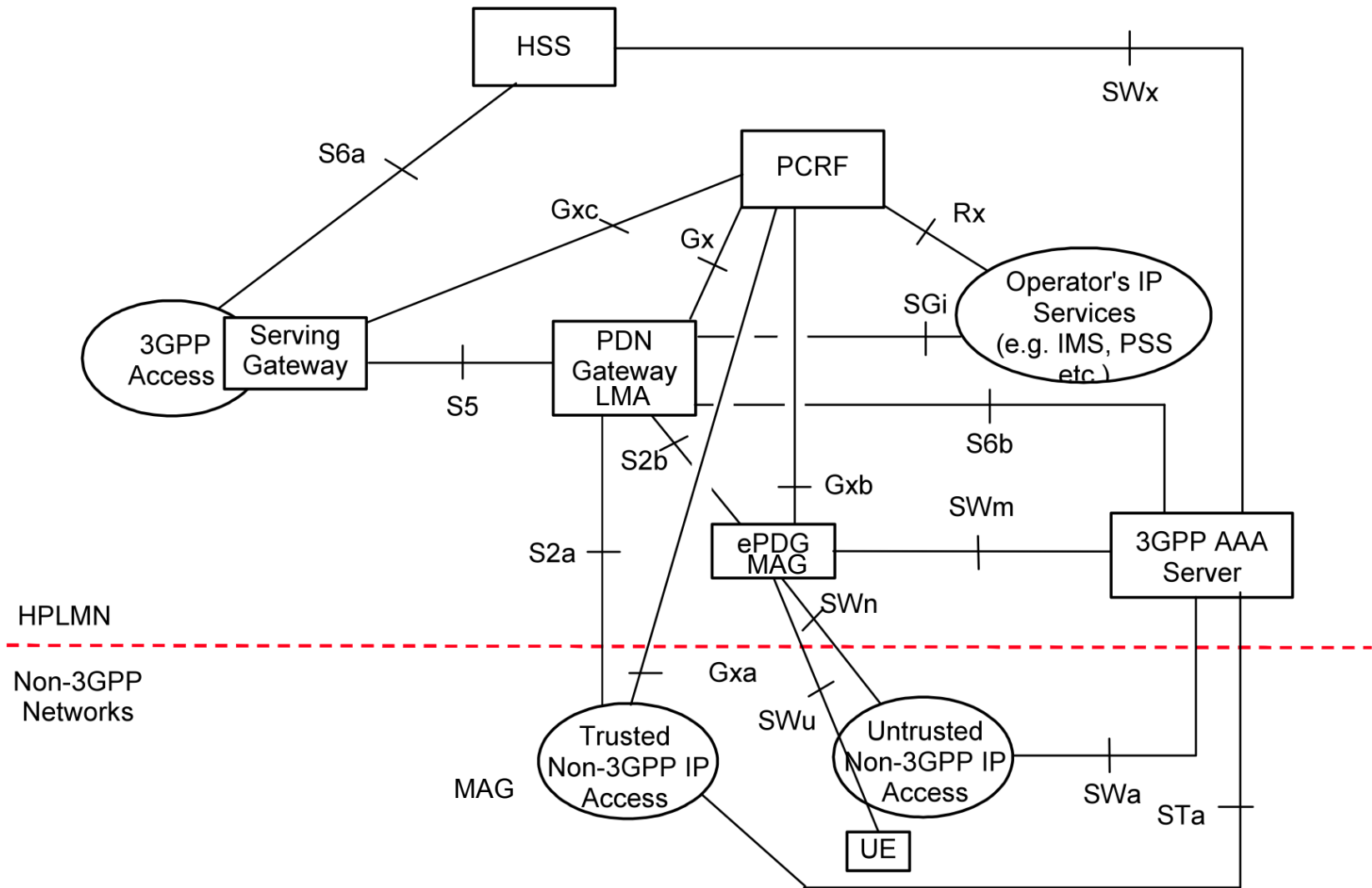
“Now, with the deployment of 802.1x, 802.11u, 802.11i and Hotspot 2.0, it may be considered by some operators that the security strength and ease of use is as acceptable as 3G/LTE security. For example, for the radio air link, the operator controlled hotspot with 802.11i could be treated as the trusted Non-3GPP Access.”

Mobile IP Mobility – 3GPP спецификация



3GPP TS 23.402

ПрохуМІР – 3GPP спецификација



3GPP TS 23.402

PMIPv6 versus GTP

Почему PMIPv6?

- Операторы фиксированной связи рассматривают PMIPv6 как универсальную архитектуру
- Стандартизированный IETF протокол, предоставляющий мобильность без специального клиентского ПО
- Совместим с 3GPP client based DSMIP mobility, но используемый в non-3GPP сетях
- Применим и в 3GPP2 инфраструктуре
- Простой стек протокола (с.f. GTP)

Почему GTP?

Решение для случая, когда оператору необходимо интегрировать SP WiFi инфраструктуру с существующим GGSN и сервисной инфраструктурой (Gx/Gy/Ga)

Возможность использовать стандартный (Gp/S8) GTP based роуминг



Использование WLC (Wireless LAN Controller) для аутентификации

- Общая архитектура решения для ISG и MAG имплементации
- Burden of authentication more evenly distributed amongst WLC's
- Пользователи прошедшие авторизацию получают доступ за пределы WLC
- AAA сервисы могут выбираться на базе SSID
- ISG не находится на пути прохождения RADIUS запросов
- “Trusted модель” с точки зрения ISG. Трафик только авторизованных пользователей будут обслуживаться ISG



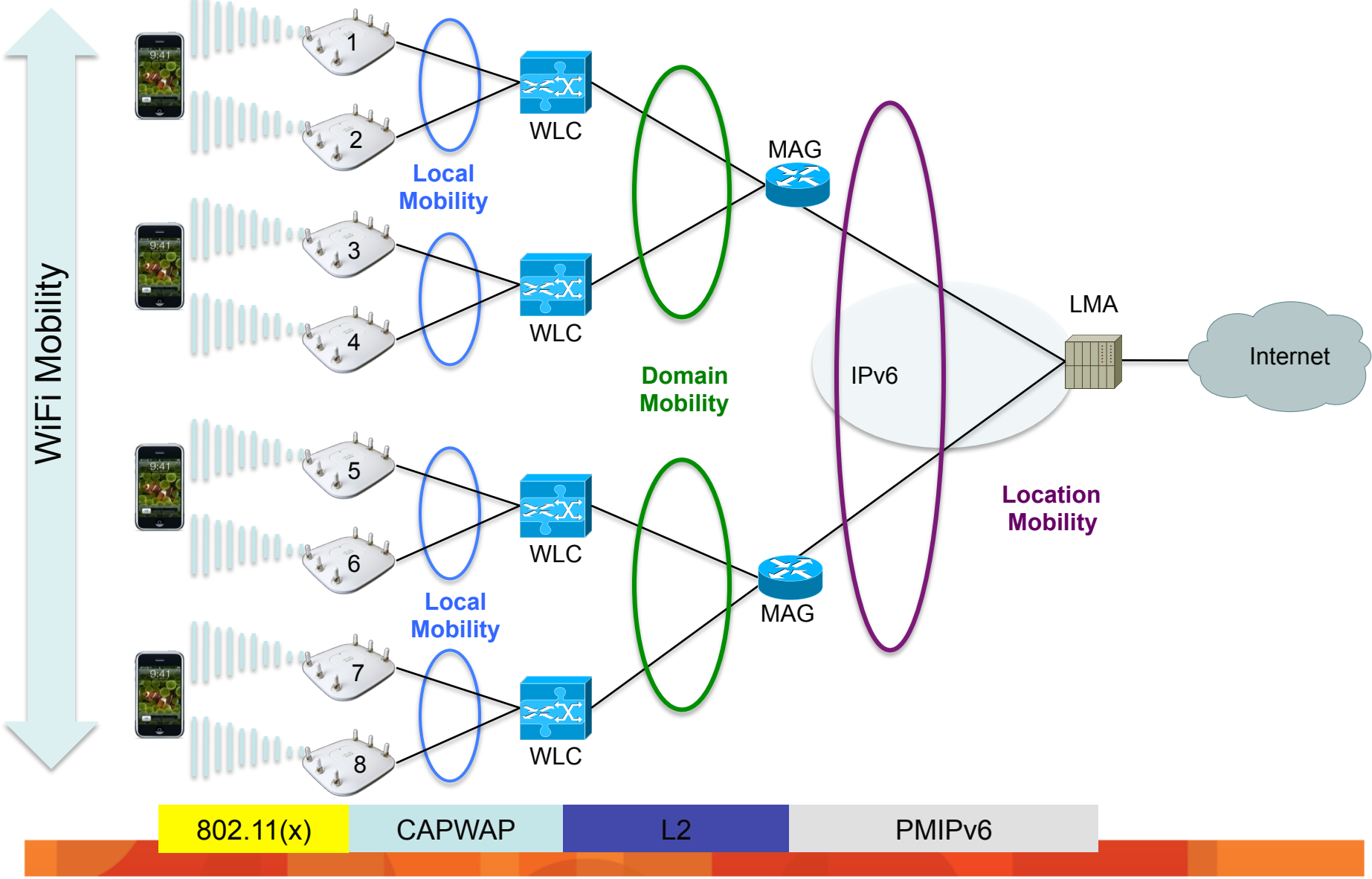
PMIPv6 терминология

- **LMD – Local Mobility Domain;**
Сегмент сети, который поддерживает PMIP. LMD включает в себя один LMA и несколько MAG.
- **LMA – Local Mobility Anchor;**
Весь трафик от и к мобильному устройству маршрутизируется через LMA. LMA содержит таблицу маршрутов к каждому мобильному устройству подключенному к LMD.
- **MAG – Mobile Access Gateway;**
MAG выполняет сигнальный обмен относящийся к стеку Mobile IP от имени мобильного устройства.
- **MN – Mobile Node;**
Устройство подключенное через беспроводную сеть доступа к LMD
- **CN – Correspondence Node;**
Любое устройство (host) в Internet или LMD, которое обменивается трафиком с MN

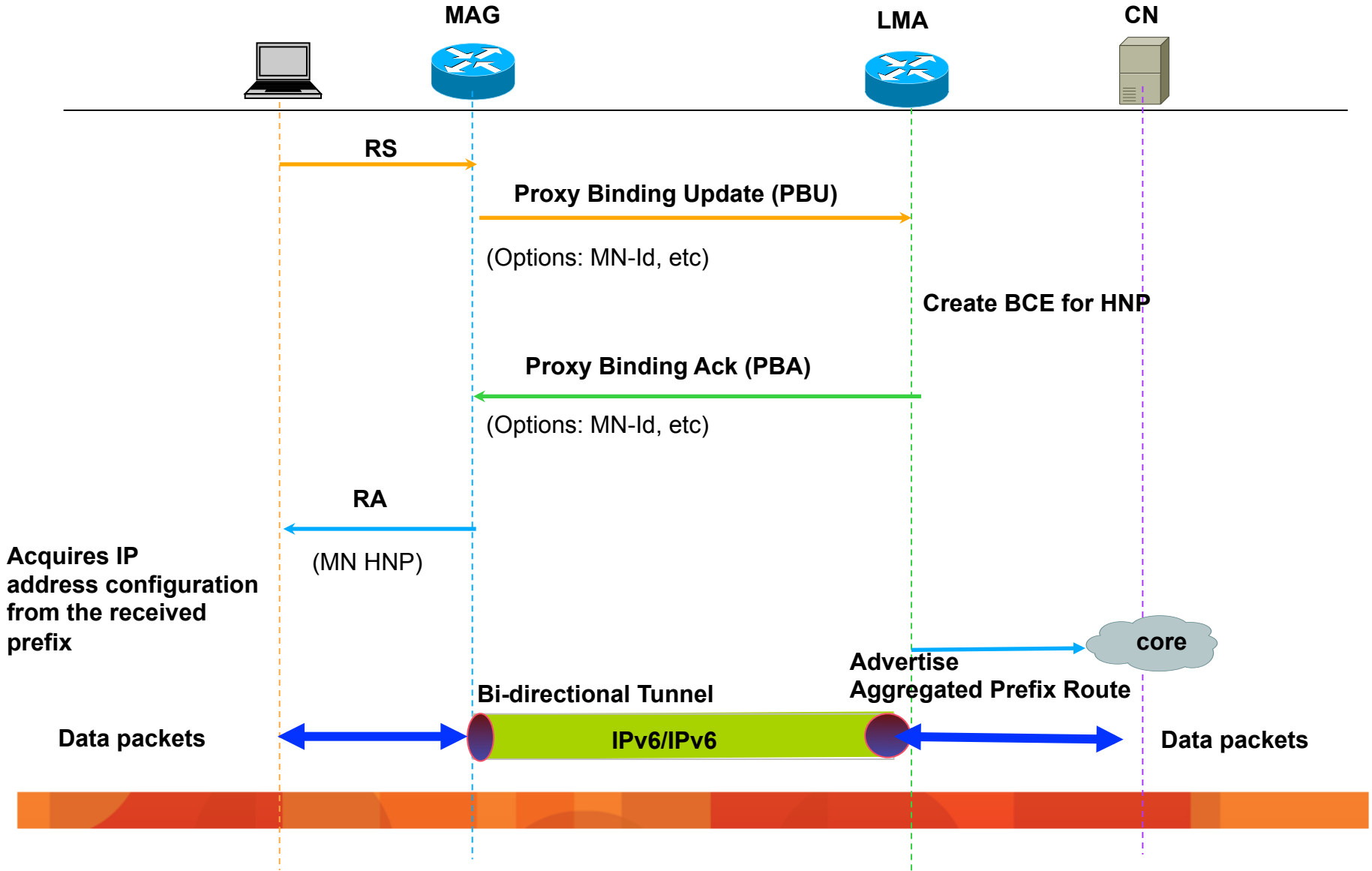
PMIPv6 терминология

- **BN – Binding Cache;**
Запись в таблице кэш LMA, которая содержит MN-ID, MAG proxy-CoA и MN-prefix
- **PBU – Proxy Binding Update;**
Сигнальный пакет PMIP, который MAG отправляет LMA для подключения нового MN. PBU содержит поля MN-ID (e.g. MN's MAC), MAG address (proxy-CoA) и handoff индикацию (т.е. индикацию того, что это либо новое подключение или переключение мобильной сессии от соседнего MAG)
- **PBA – Proxy Binding Acknowledge;**
Ответ LMA в сторону MAG. Ответ содержит MN-ID, MAG address и префикс назначенный мобильной станции
- **Proxy-CoA – Proxy care of address;**
IP address интерфейса MAG – это адрес туннеля на стороне MAG. LMA инкапсулирует пакеты адресованные MN в туннель, destination которого MAG proxy-CoA.

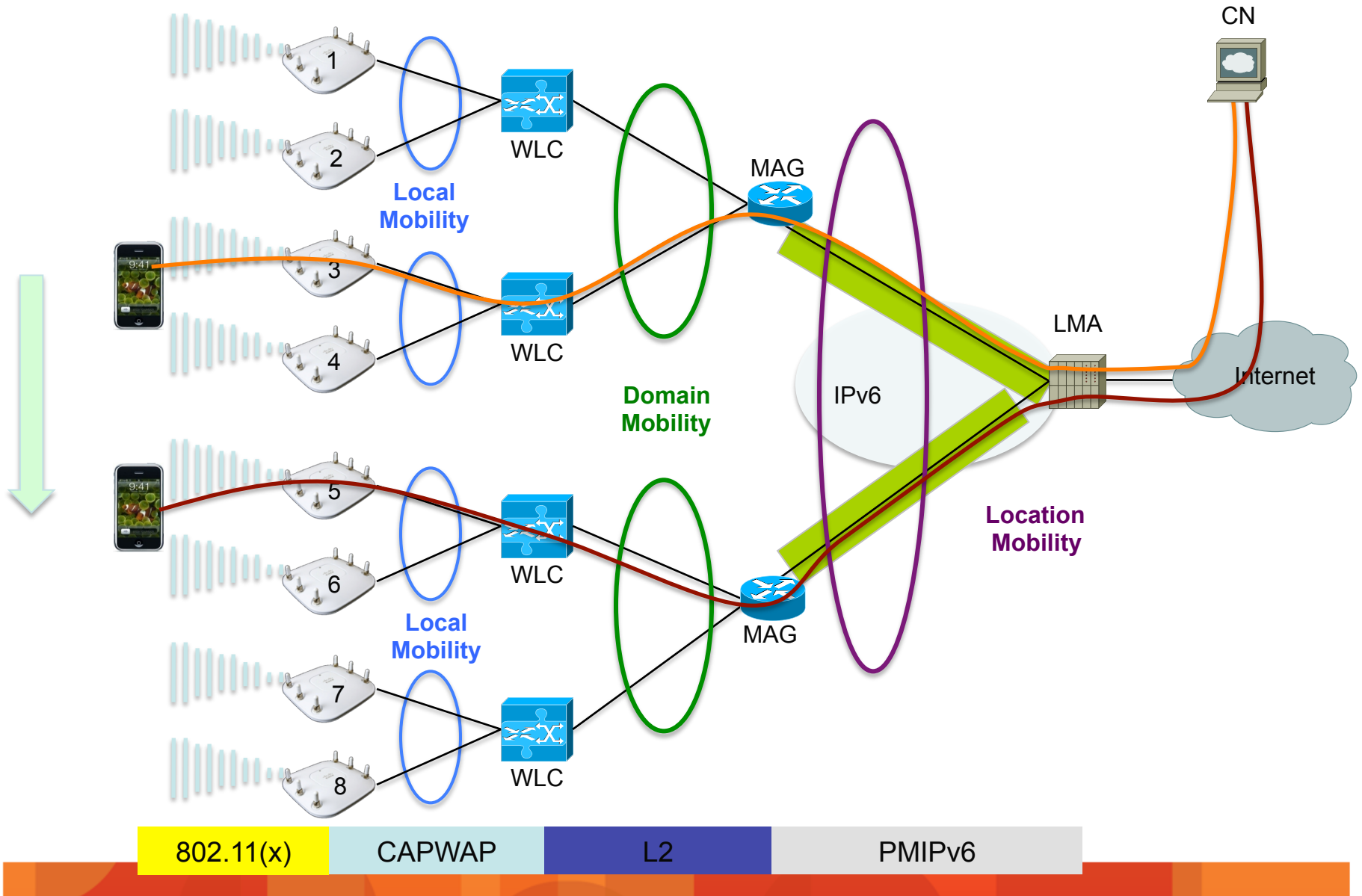
PMIPv6 – Иерархия



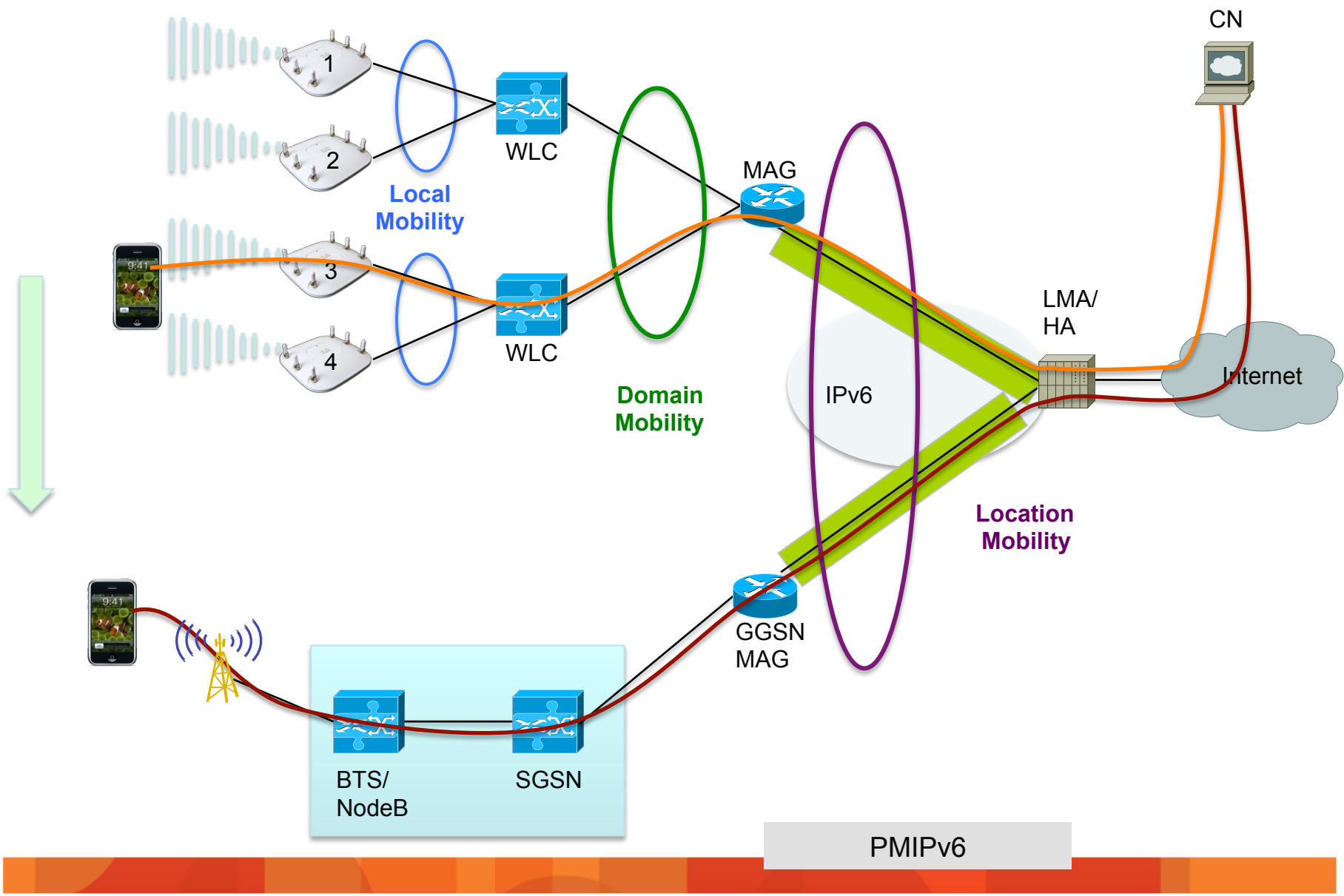
PMIPv6 Call flow



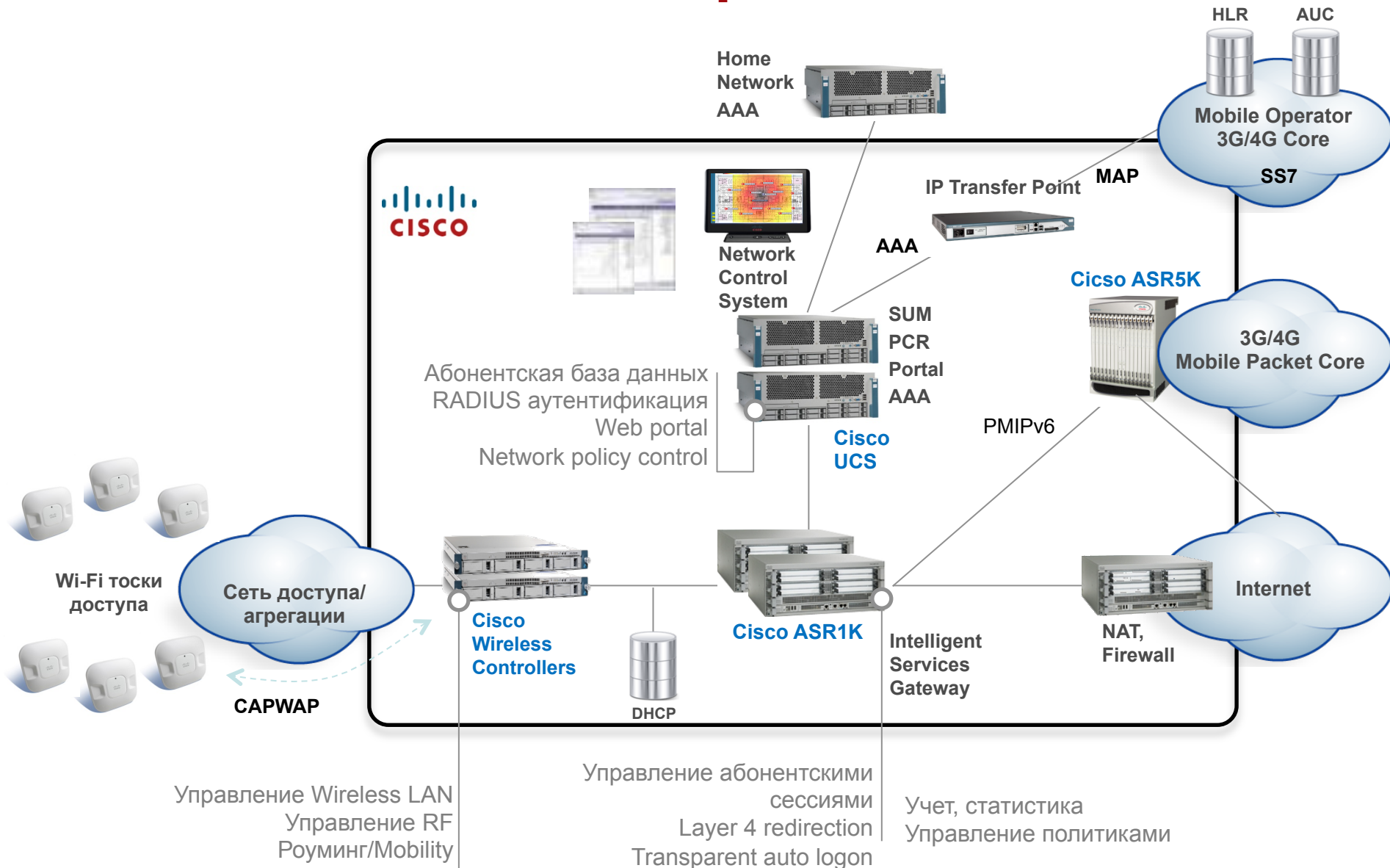
PMIPv6 – интер-MAG мобильность



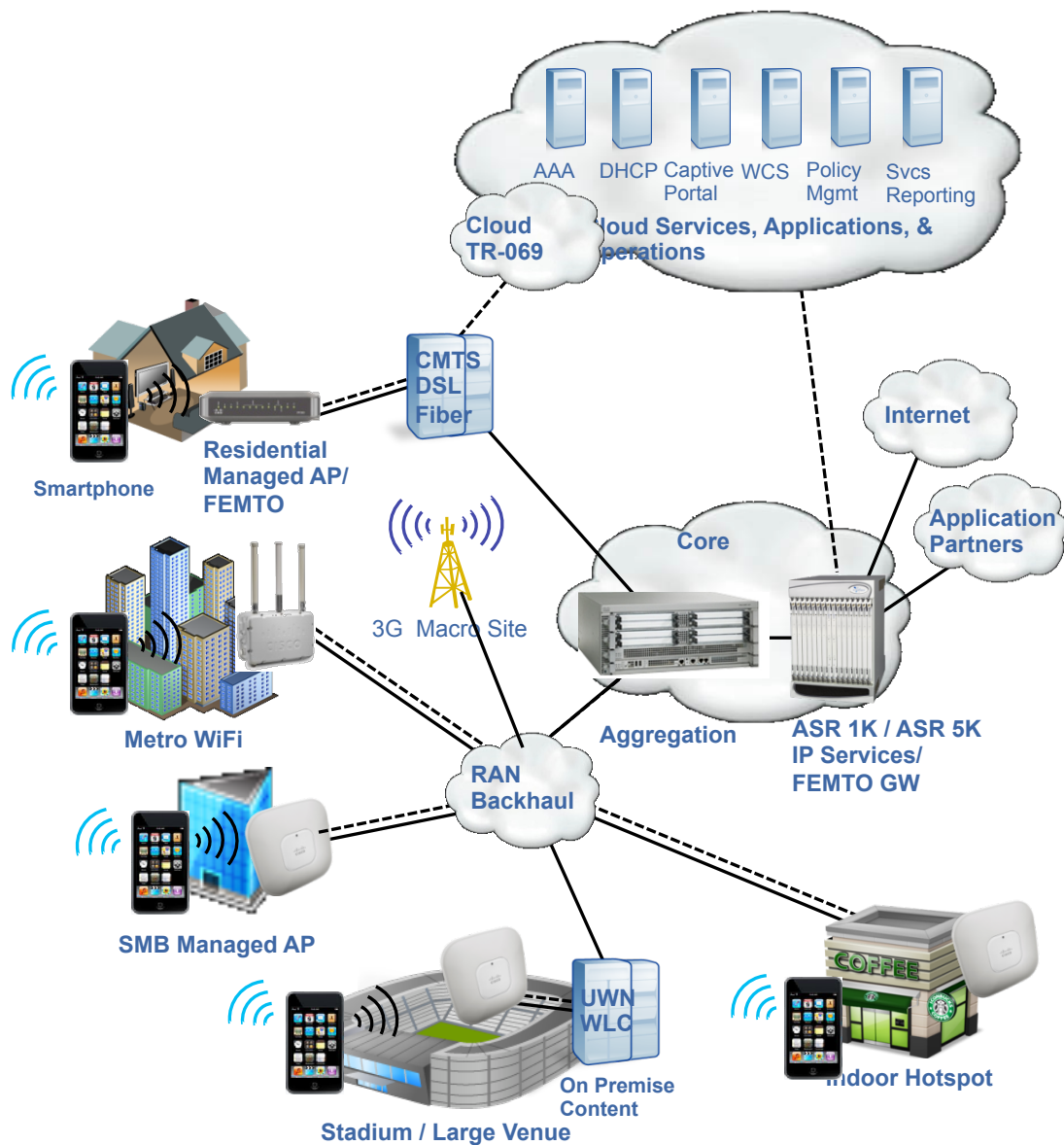
PMIPv6 – mobility из WiFi в Macro 2G/3G



Cisco SP Wi-Fi – интеграция с МРС



SP WiFi сетевая архитектура End-to-end



- Не лицензируемое радио как дополнение к 3G/4G мобильным широкополосным сетям
 - Снижение нагрузки на макро RAN
 - улучшение Indoor покрытия
 - 3G Data offload
 - Снижение TCO
- Гибкость и масштабируемость
 - Масштабируемость от Metro/indoor к Residential
 - Cloud based Operations & Services Mgmt
- Стандартизованные протоколы/ интерфейсы
 - 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

Архитектура решения с использованием контроллеров

■ Почему WiFi controller-based архитектура?

- Все успешные коммерческие проекты базируются на концепции централизованного управления или централизованной агрегации RAN
- В SP Marco решении все используют Radio-network-controller (RNC) как агрегацию доступа (control plane & user plane)
- 4G LTE сеть также поддерживает централизованный контроль сигнальный и позволяет отделить его от пользовательских данных (user plane) (i.e. MME/SGW)

■ RNC (WLC) обеспечивает мобильность

- RRM (Radio Resource Management): для максимизации покрытия и пропускной способности путем: контроля «качества» RF сигнала, оценки и определения возможной интерференции, определение ресурсов (RF channels, BW, Power, ...)
- Локальная мобильность
- Одна точка взаимодействия с «чужими» сетями (e.g. foreign networks) снижение IOT & OPEX
- Детектирование типов сервиса (e.g. multicast/broadcast, voice codec optimization, ...) & (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: Архитектура WiFi “RNC”

Управление переключением (mobility) сессий между APs

Управление списком «соседних Aps» внутри/между WLC

Управление RF параметрами во время Mobile-Assisted Handoff

Быстрый & бесшовный handoff для L2 & L3 сервисов (802.11r)

LAN, MAN or WAN подключение (Layer 2 или L3 транспорт)

Нет ограничений к размеру и топологии сегментов доступа и агрегации

CleanAir технология – лидирующая в индустрии – устранение интерференции базирясь на централизованном RRM

Адаптивный wireless IPS (wIPS)

Анализ сервисов (e.g. VideoStream, VoWiFi CAC)

Multi/uni-cast admission control & media-adaptation needs central network view

Межсетевая мобильность (e.g. 3G-WiFi) via IP (e.g. PMIP)

Поддержка отдельного управления control plane & data plane

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) |
|---------------------------------------------------------------------------|--------------------------|---------------------------|
| Мобильность (layer 2 & layer 3) | ✓ | ✓ |
| Real-time Мобильность (layer 2 & layer 3) | ✓ | ✗ |
| Оптимизация пропускной способности (RRM - interference mitigation) | ✓ | ✗ |
| Сетевая безопасность и IPS (e.g. rogue AP) | ✓ | ✗ |
| Качество предоставления услуг (Context-aware voice/video optimization) | ✓ | ✗ |
| Управляемость сети и высокая масштабируемость | ✓ | ✗ |
| Более перспективное решение | ✓ | ✗ |

Одна архитектура – много приложений

- **HotZone** (стадионы, общественный транспорт, общественные места, etc)
 - Полное покрытие (централизованное управление, мобильность, CleanAir, RRM, etc)
 - Обычно, WLC размещается вместе с сервисным шлюзом(e.g. ASR1K) для учета трафика
- **HotSpot** (общественные места, etc)
 - Автономные точки доступа, размещаемые с маршрутизаторами доступа (e.g. AZR) для учета трафика и Internet offload
 - Как правило фрагментарное покрытие с ограниченными функциями мобильности
 - Control plane (централизованное управление., RRM, CleanAir, aWiPS, etc)
- **SMB** (Управляемые сервисы для малого бизнеса, etc)
 - Несколько SSID (for MSP) с сопутствующими услугами (e.g. VPLS, IP-PBX, FMC, etc)
 - Такое же покрытие как и для HotSpot
- **Домашние абоненты**
 - Непрерывные зоны покрытия -> RRM/CleanAir
 - Central or Local traffic switching (WLC)

WiFi точки доступа



11abg

11n

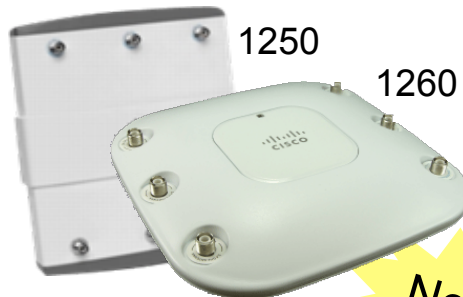
11n + CleanAir



Ruggedized



1240



1250

1260

New



3500e

New

Carpeted



1140



1040

New



3500i

New

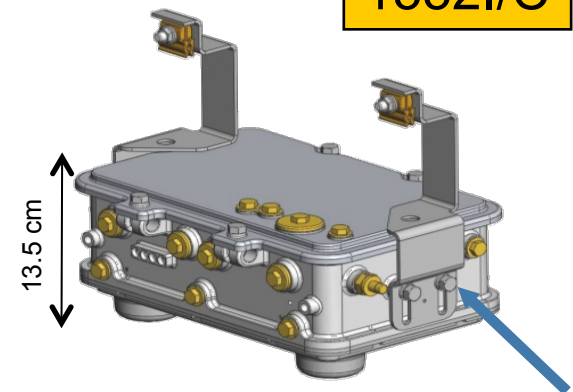
1550 Точка доступа – модельный ряд

- 1552: Dual-Band (2.4 & 5 GHz), 4 Models
- 40 MHz BW channel support, Data rates ≤ 300 Mbps
- DOCSIS 3.0 (8x4) / (304 x108) Mbps or EuroDOCSIS 3.0 (4x4) / (152 x 108) Mbps Cable Modem
- MIMO (2X3), 2 SS (Spatial Streams)
- Dual band, omni-directional antennas
 - 3 Stick antennas, 4 dBi (2.4 GHz), 7 dBi (5 GHz)
 - 3 element array, Low Profile, Single Radom, 2 dBi (2.4 GHz), 4 dBi (5 GHz)
- CleanAir 2.4 GHz Spectrum Intelligence
- ClientLink Legacy Beam Forming
- Universal Access for 5GHz clients

1552E/H



1552I/C



Cisco 5500 Series Wireless Controller



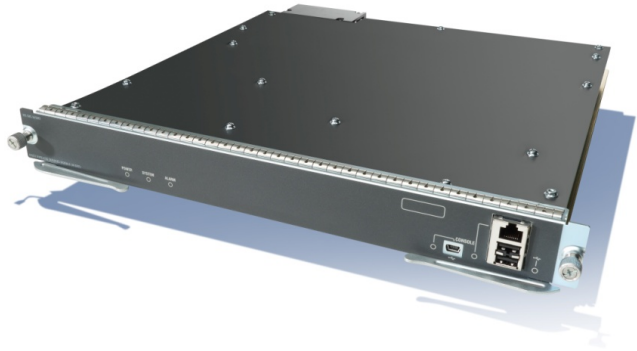
| | |
|---------------------------|----------------------|
| Кол-во точек доступа | 12 - 500 |
| Кол-во абонентов | 7,000 |
| Form-factor | 1 RU |
| Кол-во и типы интерфейсов | 8x 1GE ports, LAG |
| Лицензирование | 25,50,100,250 |
| Потребляемая мощность | 125W |

Преимущества:

- Высокая производительность
- Безопасность
- Снижение OPEX
- Обновление 500 APs
- Поддержка медиа приложений (multicast)

Cisco Wireless Services Module 2

Модуль для Catalyst 6500 Chassis



Преимущества:

- Высокая производительность
- Безопасность
- Снижение OPEX
- Обновление 500 APs
- Поддержка медиа приложений (multicast)
- Высокая масштабируемость решения

| | |
|----------------------------------|-----------------------------|
| Кол-во течек доступа | 100-500 |
| Кол-во абонентов | 10,000 |
| Масштабируемость на уровне шасси | 3,500 APs 70,000 Clients |
| Типы интерфейсов | 10 GE |
| Лицензирование | 100, 200 |

Cisco Flex 7500 Series Cloud Controller








| | |
|------------------------|-------------------|
| Кол-во точек доступа | 300 - 2,000 |
| Кол-во абонентов | 20,000 |
| Branches | 500 |
| Access Points / Branch | 50 |
| Режим работы | FlexConnect |
| Form Factor | 1 RU |
| Типы интерфейсов | 2x 10GE |
| Лицензирование | 100, 200, 500, 1K |

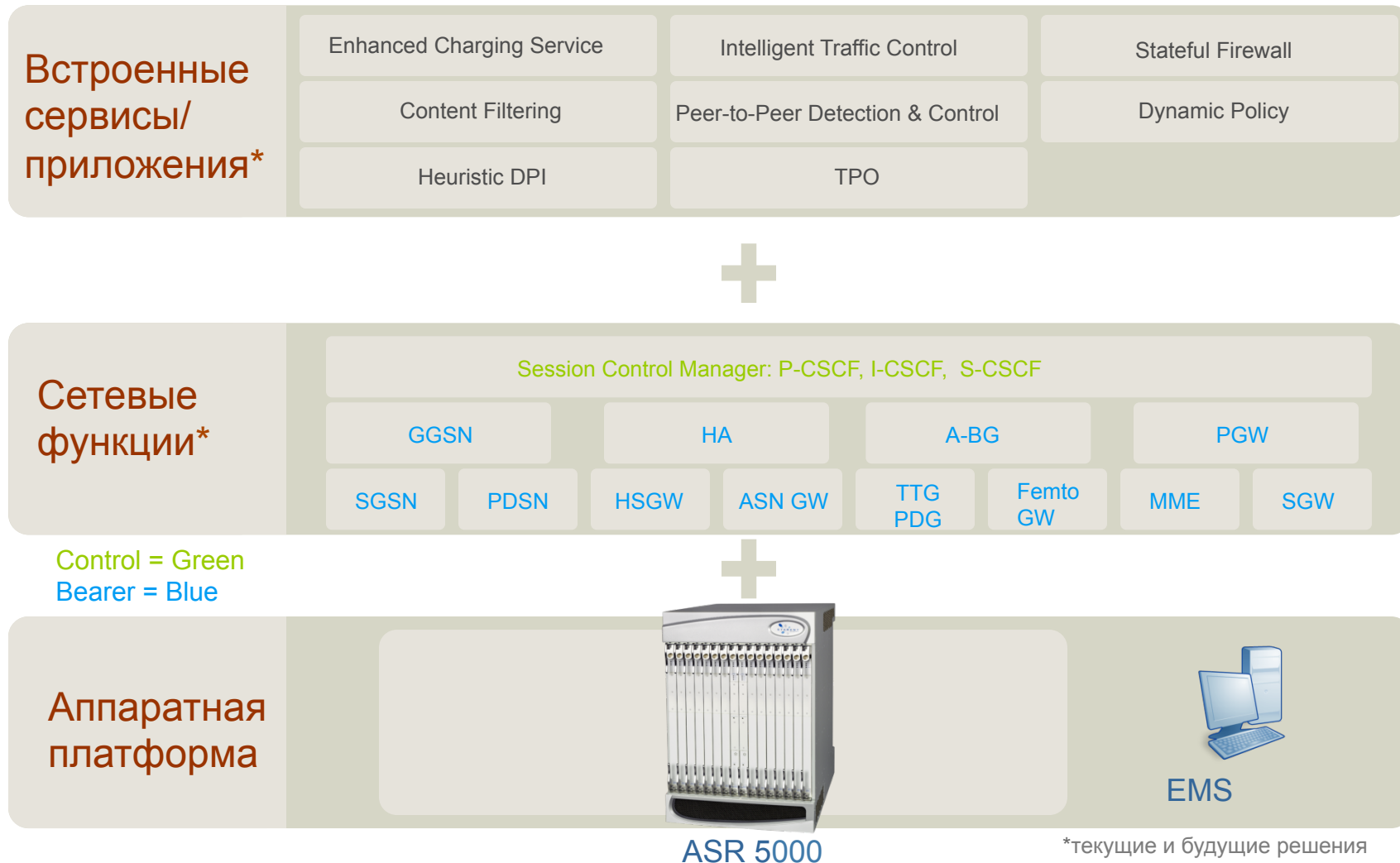
Competitive Differentiation

- Подключение AP через WAN
- Толерантность к высоким задержкам
- Безопасность
- 802.1x based port authentication
- Voice support
- Voice CAC

ASR 1000 решение для ISG/MAG/LAG

| | ASR1001 | ASR 1002 | ASR 1004 | ASR 1006 | ASR 1013 |
|-----------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| |  |  |  |  |  |
| SPA Slots | 1-slot | 3-slot | 8-slot | 12-slot | 24-slot |
| ESP Slots | Integrated | Integrated | 1 | 2 | 2 |
| SIP slots | Integrated | Integrated | 2 | 3 | 6 |
| IOS Redundancy | Software | Software | Software | Hardware | Hardware |
| Built-in GE | 4 | 4 | N/A | N/A | N/A |
| Height | 1.75" (1RU) | 3.5" (2RU) | 7" (4RU) | 10.5" (6RU) | 22.7" (13RU) |
| Bandwidth | 2.5 to 5 Gbps | 5 to 10 Gbps | 10 to 40 Gbps 40 Gbps as of 3.2S | 10 to 40 Gbps | 40+ Gbps |
| Maximum output Power | 400W | 470W | 765W | 1275W | 3200W |
| Airflow | Front to back | Front to back | Front to back | Front to back | Front to back |
| Integrated I/O Daughtercard | 1 | | | | |

ASR 5000 Решение для операторов мобильной связи



Cisco Wi-Fi решение для операторов связи



Hotspot нового поколения – HotSpot 2.0

Роуминг, Авторизация, Монетизация



Надежность
Решение
операторского
класса

Простота
Упрощение
процедуры выбора
сети и авторизации

Безопасность
Расширение
способов
авторизации с
шифрования

**Новые
источники
дохода**
Дополнительные
сервисы

HotSpot 2.0 vs. Обычный WiFi клиент

Ручной режим установки:

- Включить устройство или разблокировать телефон;
- Выбрать WiFi SSID;
- Открыть Web browser для Web-auth;
- Username/password;
- Выбрать роуминг план;
- Доступ в Интернет



Автоматический режим установки:

- Включить устройство или разблокировать телефон;
- Автоматический процесс выбора SSID и метода авторизации.

Cisco Expo 2011



Спасибо!

Просим Вас оценить эту лекцию.
Ваше мнение очень важно для нас.

Онлайн-анкеты: www.ceq.com.ua

innovate *together*