Netmanias.com
Analyze Trends, Technologies and Market
www.netmanias.com

NMC
Consulting Group
www.nmcgroups.com

Network Architecture for LTE and Wi-Fi Interworking

August 16, 2012

Chris Yoo

+82-2-3444-5747, +82-10-3229-1852
cmyoo@netmanias.com

www.netmanias.com
www.nmcgroups.com

About NMC Consulting Group
NMC Consulting Group was founded on year 2002 and is advanced, professional network consulting company which is specialized for IP Network area like FTTH, Metro Ethernet and IP/MPLS, Service area like IPTV, IMS and CDN lastly, Wireless network area like Mobile WiMAX, LTE and Wi-Fi.

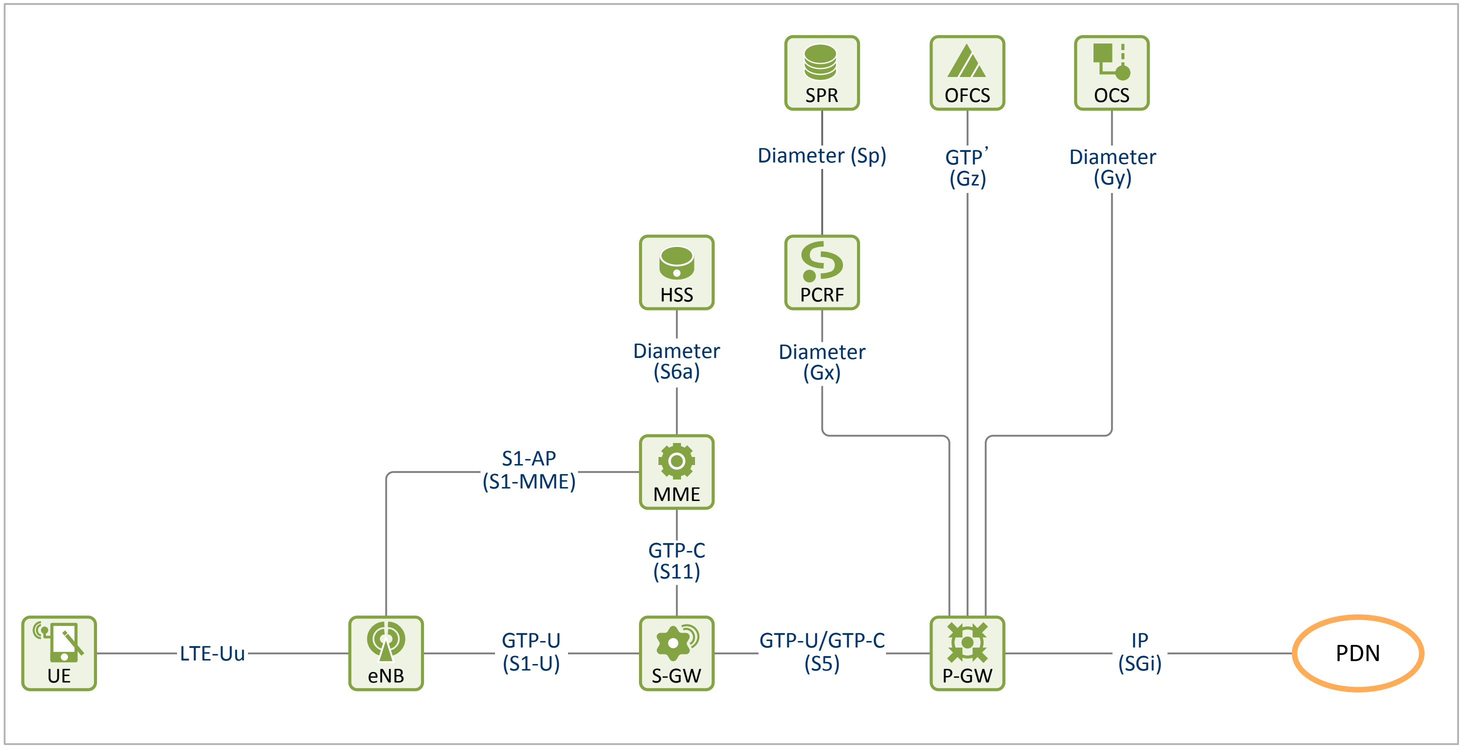
Copyright © 2002-2012 NMC Consulting Group. All rights reserved.

Table of Contents

Copyright © 2002-2012 NMC Consulting Group. All rights reserved.

LTE Overview: Network Reference Model

Related Blogs



- **LTE = E-UTRN**: eNB
- **EPC = SAE**: MME, S-GW, P-GW, HSS, PCRF, SPR, OFCS, OCS
- **EPS = LTE + EPC**

- **LTE**: Long Term Evolution
- **E-UTRAN**: Evolved-UTRAN (Universal Terrestrial Radio Access Network)
- **EPC**: Evolved Packet Core
- **SAE**: System Architecture Evolution
- **EPS**: Evolved Packet System
- **UE**: User Equipment
- **eNB**: Evolved Node B
- **S-GW**: Serving-Gateway
- **P-GW**: PDN-Gateway
- **MME**: Mobility Management Entity
- **HSS**: Home Subscriber Server
- **PCRF**: Policy and Charging Rule Function
- **SPR**: Subscriber Profile Repository
- **OFCS**: Offline Charging System
- **OCS**: Online Charging System
- **PDN**: Packet Data Network

UE

- User device which has LTE chip, antenna and USIM card (ex. Smartphone, USB modem, Router (Egg))

S-GW

- Local mobility anchor point of the data connections for inter-eNB handover and inter-3GPP handover

MME

- Main control entity for the E-UTRAN (brain of EPS)
- User authentication
- UE mobility management: UE location, UE state (ECM/EMM)

PCRF

- It makes policy decision for UE and provides PCC rules (QoS and charging rules) to P-GW

OFCS

- It manages offline charging data (CDR) per UE/per SDF, which provided by P-GW

eNB

- Base station which provides wireless connection between UE and EPC
- Encryption and integrity protected of control/data packet between UE and eNB

P-GW

- It provides PDN access for UE
- Mobility anchor point for inter S-GW handover
- IP address assignment to UE
- Online/Offline Charging
- QoS Enforcement

HSS

- Central DB holding user profile: user ID(IMSI), authentication key, QoS profile, etc
- User profile is provisioned by B/OSS when user subscription

SPR

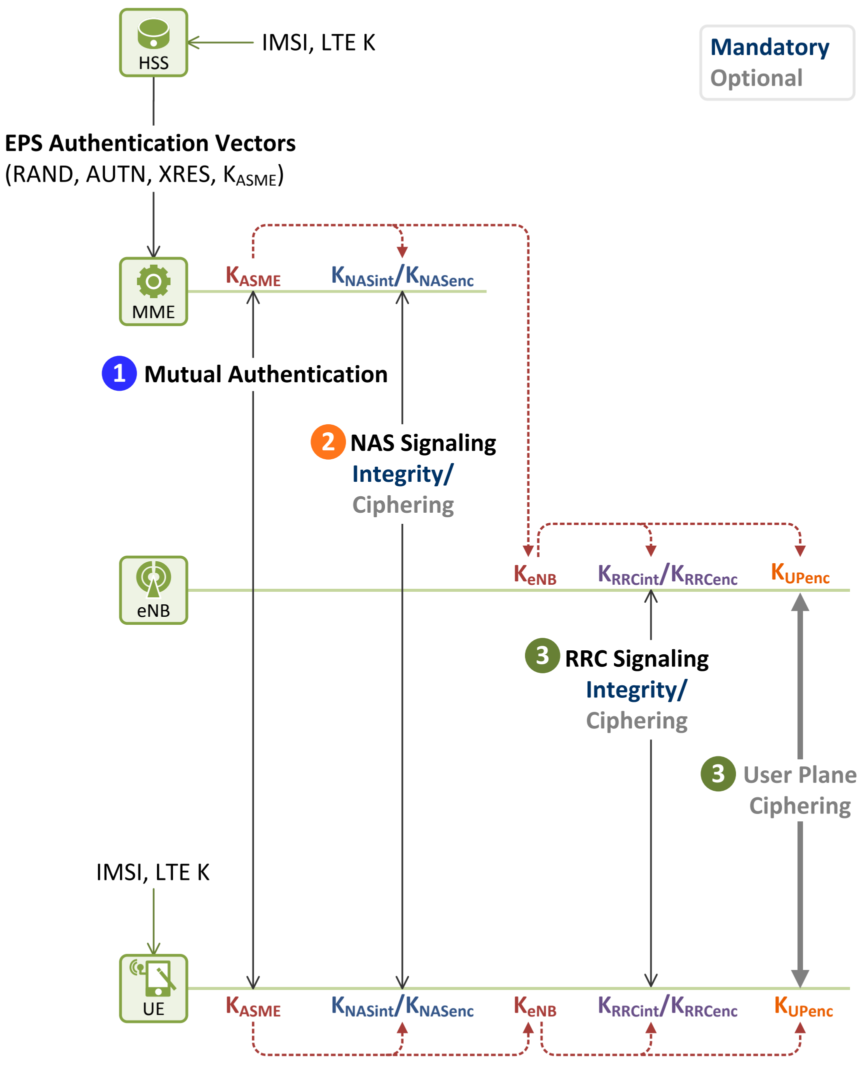
- Database for PCRF, which maintains policy and charging rule of user
- It is provisioned by B/OSS when user subscription

OCS

- It manages data volume (UL/DL bytes), time (connection time) and event based online charging data per UE/per SDF, which provided by P-GW

LTE Overview: Authentication and Security

Related Blogs



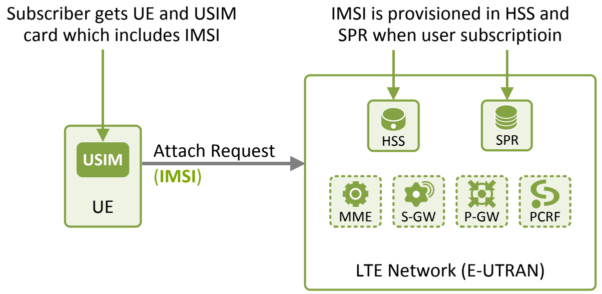
User Authentication

- User Identification: IMSI (International Mobile Subscriber Identity)
  - Global Uniqueness
  - PLMN ID (MCC + MNC) + MSIN
  - Stored at USIM (UE) and HSS (E-UTRAN)
- Authentication Key: LTE K
  - Stored at USIM (UE) and HSS (E-UTRAN)
- User Authentication Protocol: EPS-AKA
- User Authentication Process
  1. When UE requests to attach LTE network
  2. MME obtains authentication vectors (RAND, AUTN, XRES, K_{ASME}) from the HSS
  3. Mutual authentication between UE and MME
     - UE authenticates LTE network (MME)
     - MME authenticates UE

Security for Radio Interface

- After success of mutual authentication, security for radio interface is provided based on master key (K_{ASME})
  1. Control message between UE and MME: Encrypted (optional) and Integrity Protected (mandatory)
  2. Control message between UE and eNB: Encrypted (optional) and Integrity Protected (mandatory)
  3. User data between UE and eNB: Encrypted (optional)

- **IMSI Assignment**


Subscriber gets UE and USIM card which includes IMSI
IMSI is provisioned in HSS and SPR when user subscriptioin
USIM
UE
Attach Request
(IMSI)
HSS
SPR
MME
S-GW
P-GW
PCRF
LTE Network (E-UTRAN)

- **IMSI Format**

PLMN

MCC	MNC	MSIN
3 digits	Max. 3 digits	Max. 10 digits

Max. 15 digits

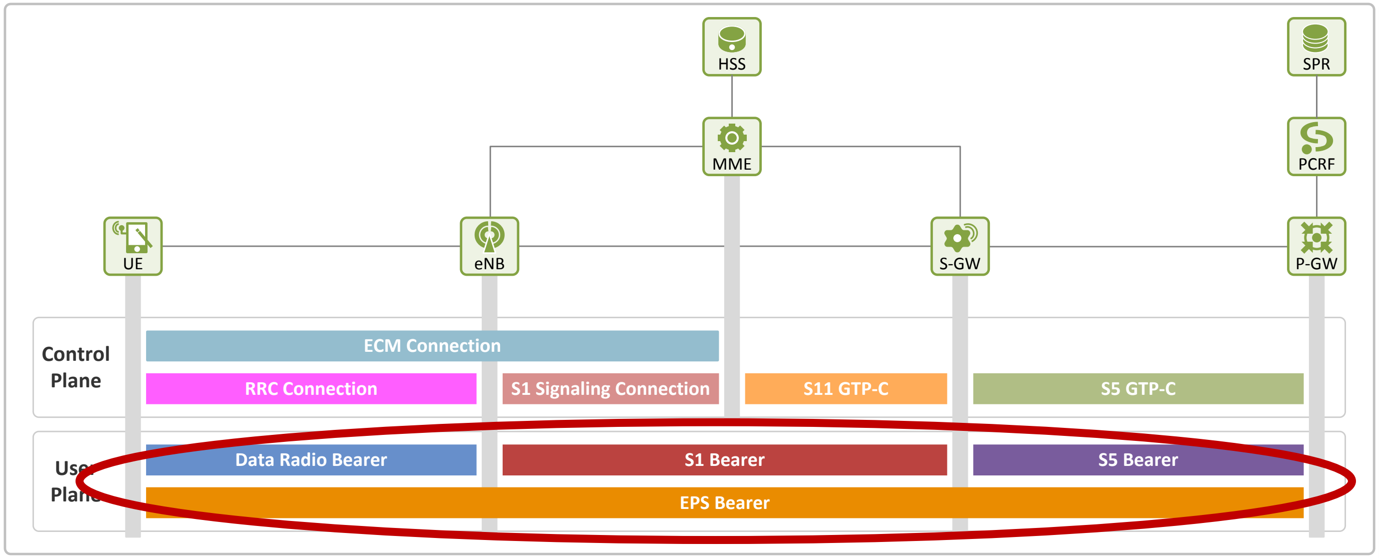
- **Example**

450	05	0123456789
Korea	SK Telecom	

Copyright © 2002-2012 NMC Consulting Group. All rights reserved.

LTE Overview: EPS Bearer

Related Blogs

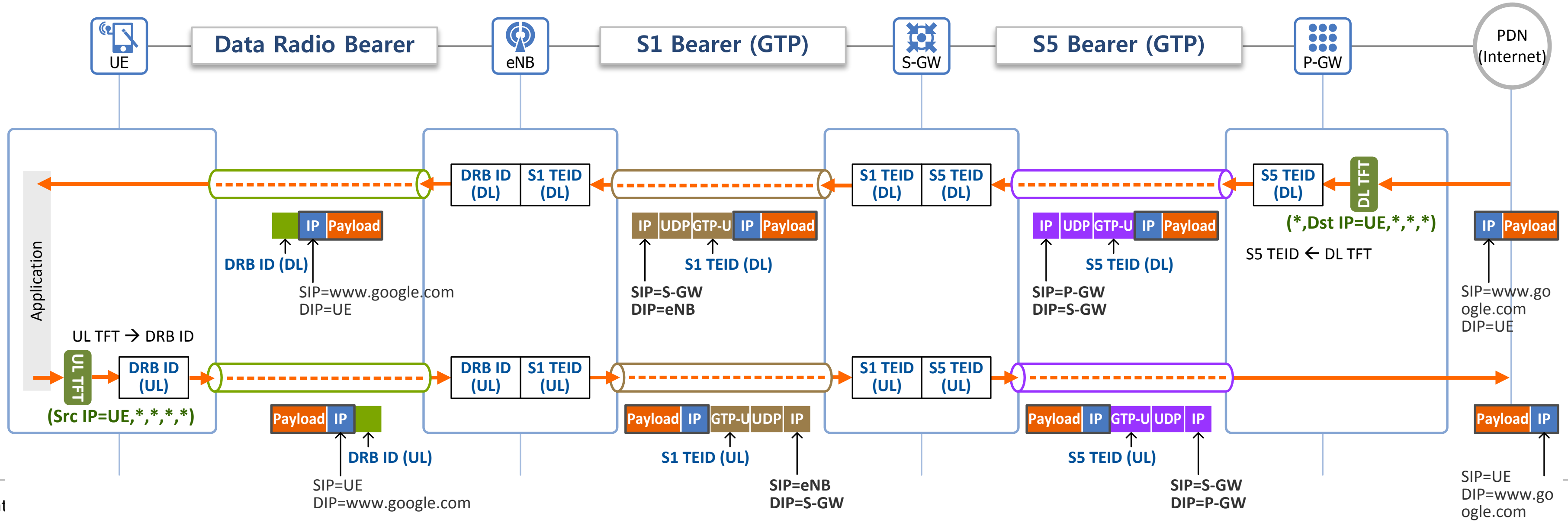


EPS Bearer

- Logical transport channel between UE and the PDN for transporting UE IP traffic
- EPS Bearer =
  Data Radio Bearer (between UE and eNB) +
  S1 Bearer (GTP tunnel between eNB and S-GW) +
  S5 Bearer (GTP tunnel between S-GW and P-GW)
- eNB can distinguish UE by DRB ID in EPS bearer
- S-GW can distinguish UE by Tunnel Endpoint ID (TEID)
- P-GW can distinguish UE by TEID or UE IP address
- At least one EPS bearer per UE, and it may also have multiple EPS bears per UE in order to provide QoS differentiation (ex. Internet bearer and VoLTE bearer)

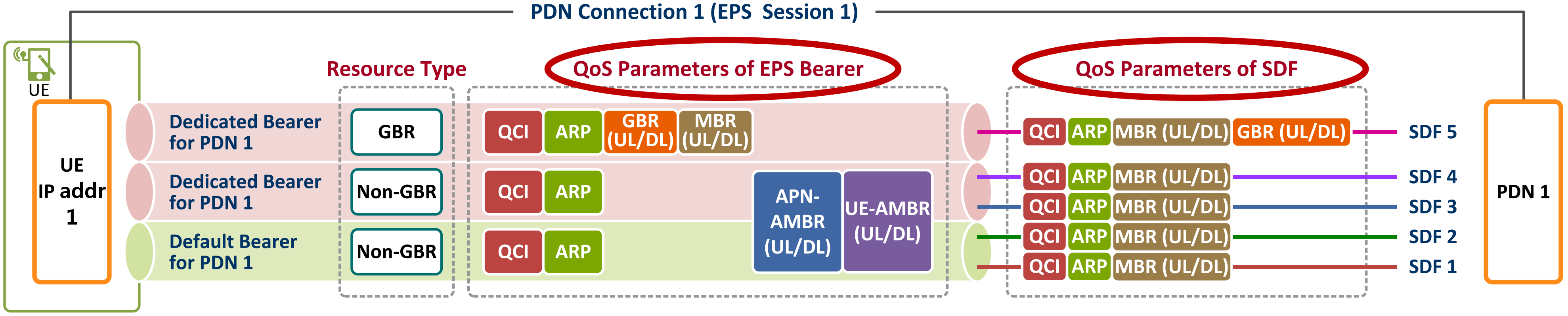
Two Types of EPS Bearer

- Default EPS Bearer
- Dedicated EPS Bearer



LTE Overview: QoS

Related Blogs



QCI: QoS Class Identifier
ARP: Allocation and Retention Priority
GBR: Guaranteed Bit Rate
MBR: Maximum Bit Rate
APN-AMBR: Access Point Name-Aggregate Maximum Bit Rate
UE-AMBR: User Equipment-Aggregate Maximum Bit Rate

■ Common QoS Parameter (Resource Type, QCI, ARP)

Resource Type

- GBR (Guaranteed Bit Rate): A certain amount of bandwidth is reserved for this bearer
- Non-GBR: It does not have a fixed (reserved) bandwidth allocated for this bearer (Best Effort)

QCI

- The class-based QoS concept (such as IP DSCP) where each EPS bearer is assigned a QCI (1 ~ 9)
- It defines packet forwarding treatment
- QoS characteristics which defines below parameters:
  - Resource Type (GBR or Non-GBR)
  - Packet Delay Budget (30ms ~ 300ms)
  - Packet Error Loss Rate (10^{-2} ~ 10^{-6})

ARP

- Priority for the allocation and retention of bearers, defined by 0 ~ 15
- Bearers with high ARP are assigned low ARP value, and vice versa (ex. VoIP emergency call service has low ARP value)
- In resource limitation situation, LTE network use the ARP to prioritize establishment and modification of bearers with a high ARP over bears with a low ARP
- It also uses ARP to decide which existed bearers to drop in case of resource limitation

■ QoS Parameter for GBR Bearer

GBR (UL/DL)

- Guaranteed (Reserved) bandwidth (bps) for GBR bearer

MBR (UL/DL)

- Maximum allowed bandwidth (bps) for GBR bearer
- Any traffic in excess of the MBR may be discarded

■ QoS Parameter for Non-GBR Bearer

APN-AMBR (UL/DL)

- Maximum allowed bandwidth (bps) for all non-GBR bearers associated with a specific APN

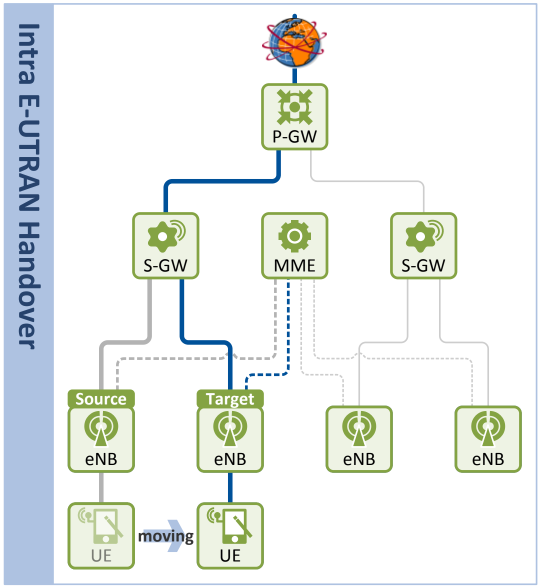
UE-AMBR (UL/DL)

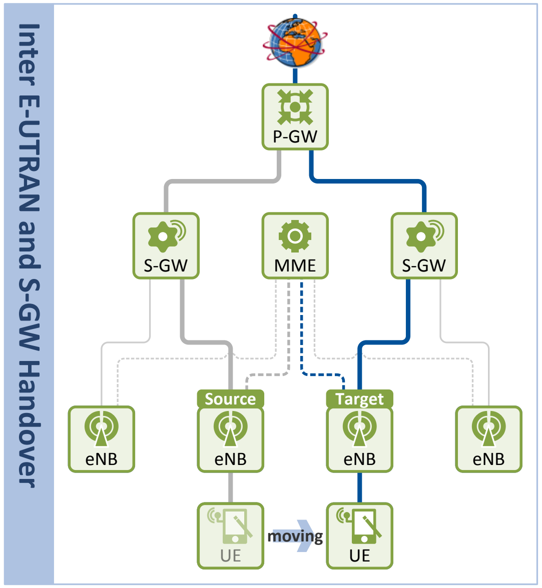
- Maximum allowed bandwidth (bps) for all non-GBR bearers of a UE

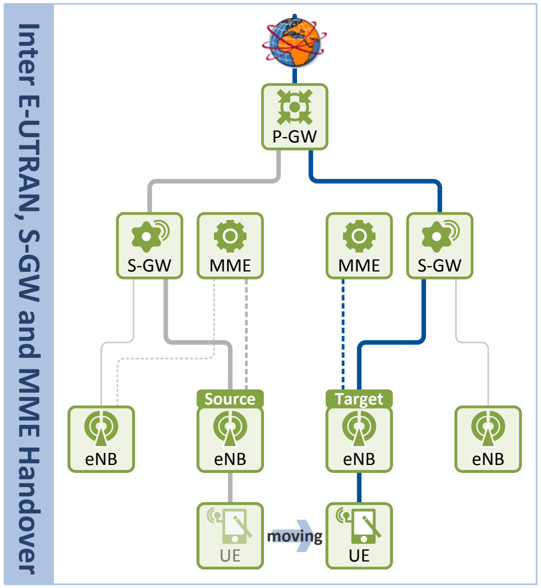
Copyright © 2002-2012 NMC Consulting Group. All rights reserved.

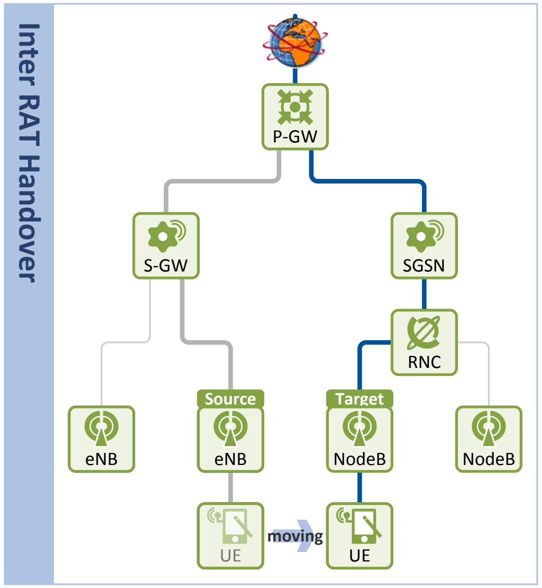
LTE Overview: Handover

Related Blogs


Intra E-UTRAN Handover


Inter E-UTRAN and S-GW Handover


Inter E-UTRAN, S-GW and MME Handover


Inter RAT Handover

Basic Requirement of Handover

- UE IP address should not be changed
- Packet loss and reordering should be minimized during handover

Handover Decision

- Handover decision is performed by serving eNB (In case of Wi-Fi, UE(STA) performs handover decision)
- Handover Decision Process
  1. UE sends Measurement Report message to serving eNB periodically (or event triggered)
  2. Measurement Report message includes
     - Radio signal strength from serving cell to UE
     - Radio signal strength from neighbor cells to UE
  3. Serving ENB decides handover based on information of Measurement Report message

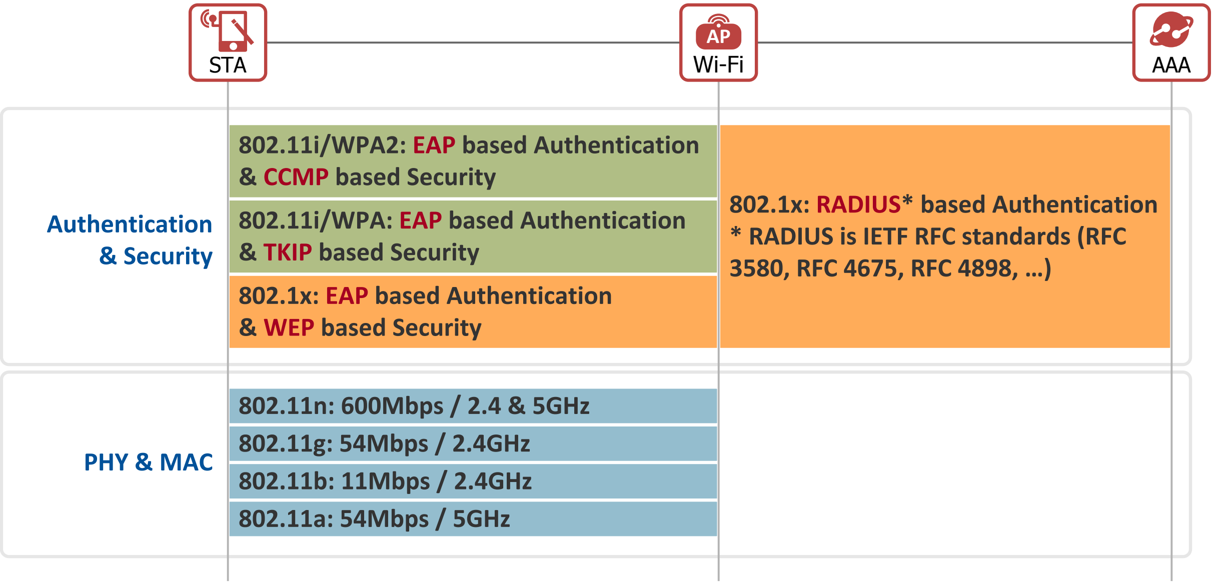
Type of Handover

- **Intra E-UTRAN**: eNB relocated, without changing MME and S-GW
- **Inter E-UTRAN and MME**: eNB and MME relocated, without changing S-GW
- **Inter E-UTRAN and S-GW**: eNB and S-GW relocated, without changing MME
- **Inter E-UTRAN and MME and S-GW**: eNB, S-GW and MME relocated
- **Inter RAT (E-UTRAN and GERAN/UTRAN)**: Handover between 3G and LTE

Copyright © 2002-2012 NMC Consulting Group. All rights reserved.

Wi-Fi Overview: Network Architecture

Related Blogs


STA
AP
Wi-Fi
AAA
Authentication & Security
802.11i/WPA2: EAP based Authentication & CCMP based Security
802.11i/WPA: EAP based Authentication & TKIP based Security
802.1x: EAP based Authentication & WEP based Security
802.1x: RADIUS* based Authentication
* RADIUS is IETF RFC standards (RFC 3580, RFC 4675, RFC 4898, …)
PHY & MAC
802.11n: 600Mbps / 2.4 & 5GHz
802.11g: 54Mbps / 2.4GHz
802.11b: 11Mbps / 2.4GHz
802.11a: 54Mbps / 5GHz

Wi-Fi Hotspot Service in Korea
: EAP based or Non Standard MAC/Web based Authentication

	SSID	Authentication
KT	ollehWiFi (secure)	EAP-AKA
	NESPOT, ollehWiFi	MAC based authentication, Web (ID/PW) based authentication
SKT	T wifi zone (secure)	EAP-AKA
	T wifi zone	MAC based authentication, Web (ID/PW) based authentication
LG U+	U+ zone (secure)	MSCHAPv2 over PEAP (Very similar with EAP-TTLS)
	FREE U+ zone	Open Access (1 hour free access after Ad. watch)

WLAN/Wi-Fi Standard

IEEE (WLAN): http://www.ieee802.org/11

- IEEE 802.11 standards define MAC and PHY layer
- "Wireless LAN (WLAN)" term is used by IEEE 802.11

Wi-Fi Alliance (Wi-Fi): http://www.wi-fi.org

- Several AP vendors came together to form a global non-profit organization with the goal of driving adoption of high-speed wireless local area networking
- "Wi-Fi" term is used by Wi-Fi Alliance

WLAN(Wireless LAN) = Wi-Fi

- The term "Wi-Fi" is used in general as a synonym for "WLAN"

Wi-Fi Network Element (Entity)

STA (Station)

- Device which has Wi-Fi chip & antenna

AP (Access Point)

- It has IEEE 802.11 Wireless LAN interface for use-facing and IEEE 802.3 Ethernet interface for network-facing port
- It provides connection between STA and IP network

AAA (Authentication, Authorization, Accounting)

- User authentication server

Authentication & Security for Radio Interface

- EAP based authentication
- User data encryption and integrity protected based on AES(CCMP)/TKIP/WEP

Copyright © 2002-2012 NMC Consulting Group. All rights reserved.

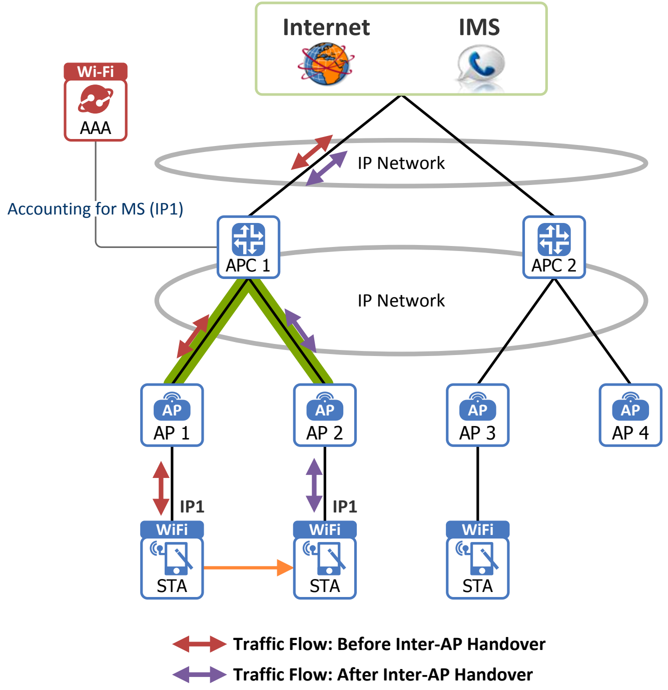
Wi-Fi Overview: Handover (Vendor Specific Solution)

Wi-Fi Handover

- AP Controller (APC, or Wireless LAN Controller(WLC)) will be required to support Inter-AP handover
- Major AP/APC providers such as Aruba, Avaya, Meru support vendor specific protocol between AP and APC (CAPWAP[RFC 5415, 5416] driven by Cisco, but other vendors still support their own methods http://community.arubanetworks.com/aruba/attachments/aruba/115/422/1/CAPWAP+Position.pdf)

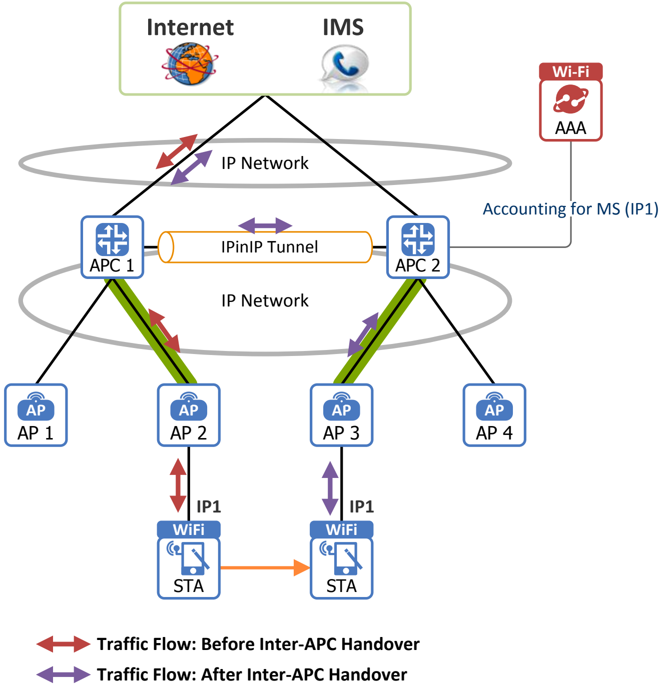
■ Example: Handover Solution of the Meru Networks

Wi-Fi Inter-AP Handover



- STA can't recognize Inter-AP handover, which means that BSSID (AP MAC) is not changed
- STA IP address (IP1) is not changed
- Accounting Data from APC1
- Handover Time: 3ms

Wi-Fi Inter-APC Handover



- STA IP address (IP1) is not changed
- IPinIP Tunnel between APCs
- Accounting Data from APC2
- Handover Time: 200ms ~ 2s (802.11 HO standard)

Copyright © 2002-2012 NMC Consulting Group. All rights reserved.

Comparison

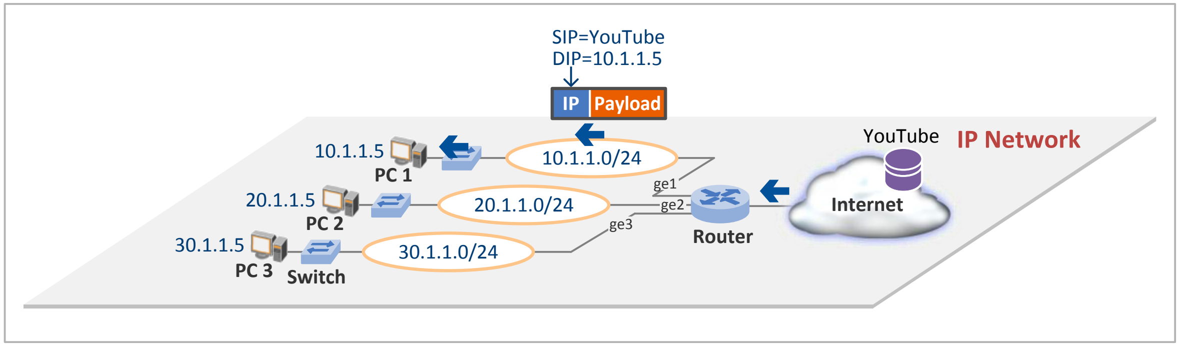
	LTE	Wi-Fi
Standard	• 3GPP	• IEEE 802.11/Wi-Fi Alliance
Standard Entity	• UE • LTE (E-UTRAN): eNB • EPC (SAE): S-GW, P-GW, MME, HSS, PCRF, SPR, OCS, OFCS	• STA, AP, AP Controller(optional), AAA
User Authentication	• EPS-AKA	EAP based Authentication (Standard) • EAP-AKA/SIM • EAP-TLS • EAP-TTLS, etc Web based Authentication (WBA) • ID/PW MAC based Authentication (Non Standard) • STA MAC
Security for User Data	• Encryption	EAP based Authentication • Encryption/Integrity Protected Web/MAC based Authentication • None
QoS Support	• Supported	• Supported (WMM), but not guaranteed
Handover (User Mobility) Support	• Supported	• Supported, but vendor specific methods • AP Controller required • Packet Loss during handover
Tunneling Protocol	• GTP	• Vendor Specific
Frequency Interference	• None	• Big issue (ISM band)
Frequency Band	• KT: 1.8GHz • SKT: 800MHz, 1.8GHz • LG U+: 800MHz, 2.1GHz	• 2.4GHz/5GHz

Copyright © 2002-2012 NMC Consulting Group. All rights reserved.

Tunneling Technology for Mobile Network

Related Blogs

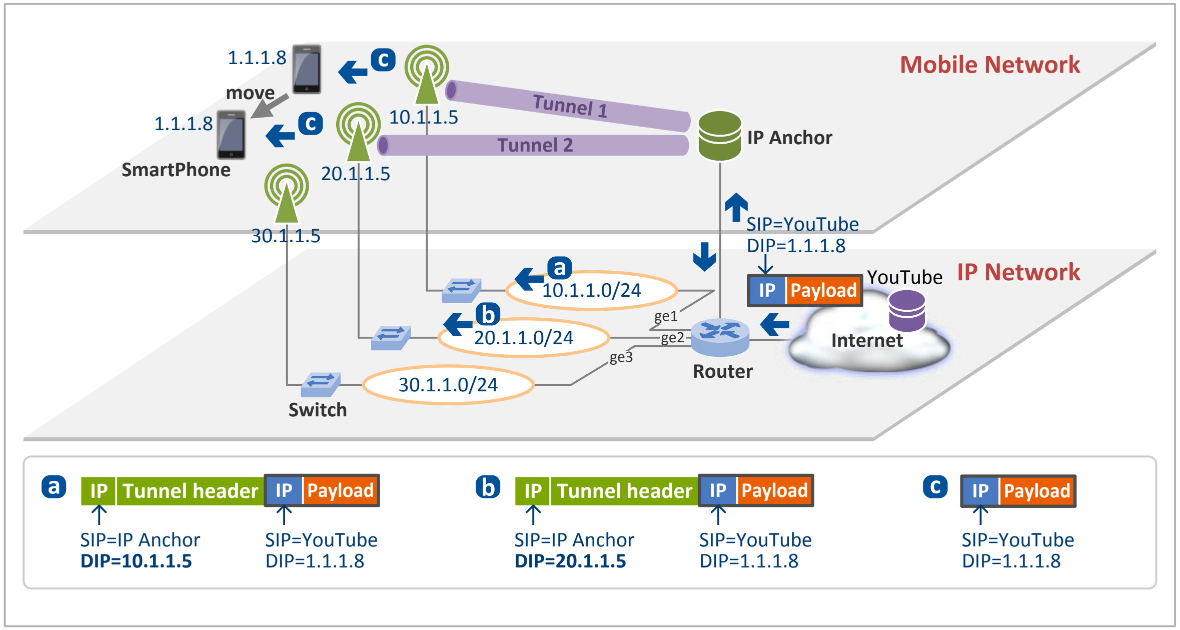
Wired Access Network (FTTH, DSL, Ethernet, HFC, etc)



User Mobility in Wired Network

- If user moves to another location without changing IP address in wired access network, communication will be broken because IP routing network can not recognize user mobility

Wireless/Mobile Access Network (3G, LTE, WiMAX, Wi-Fi, etc)



User Mobility in Wireless/Mobile Network

- The key requirement of user mobility is “User IP address should not be changed”
- IP Anchor should be existed in wireless/mobile network for supporting user mobility (3G: GGSN, LTE: P-GW, WiMAX: ASN-GW, Wi-Fi: AP Controller)
- Downstream traffic delivered process
  1. IP Anchor advertises user IP address prefix to IP routing network via OSPF, IS-IS or BGP
  2. IP Anchor receives IP packet destined to user over the Internet
  3. IP Anchor encapsulates the user IP packet with ‘Tunnel header’ and forwards the resulting outer IP packet to the Base Station(BS)
  4. So, IP routing network between BS and IP Anchor has no chance to see user IP address, which means that IP routing network does not require to concern about user mobility

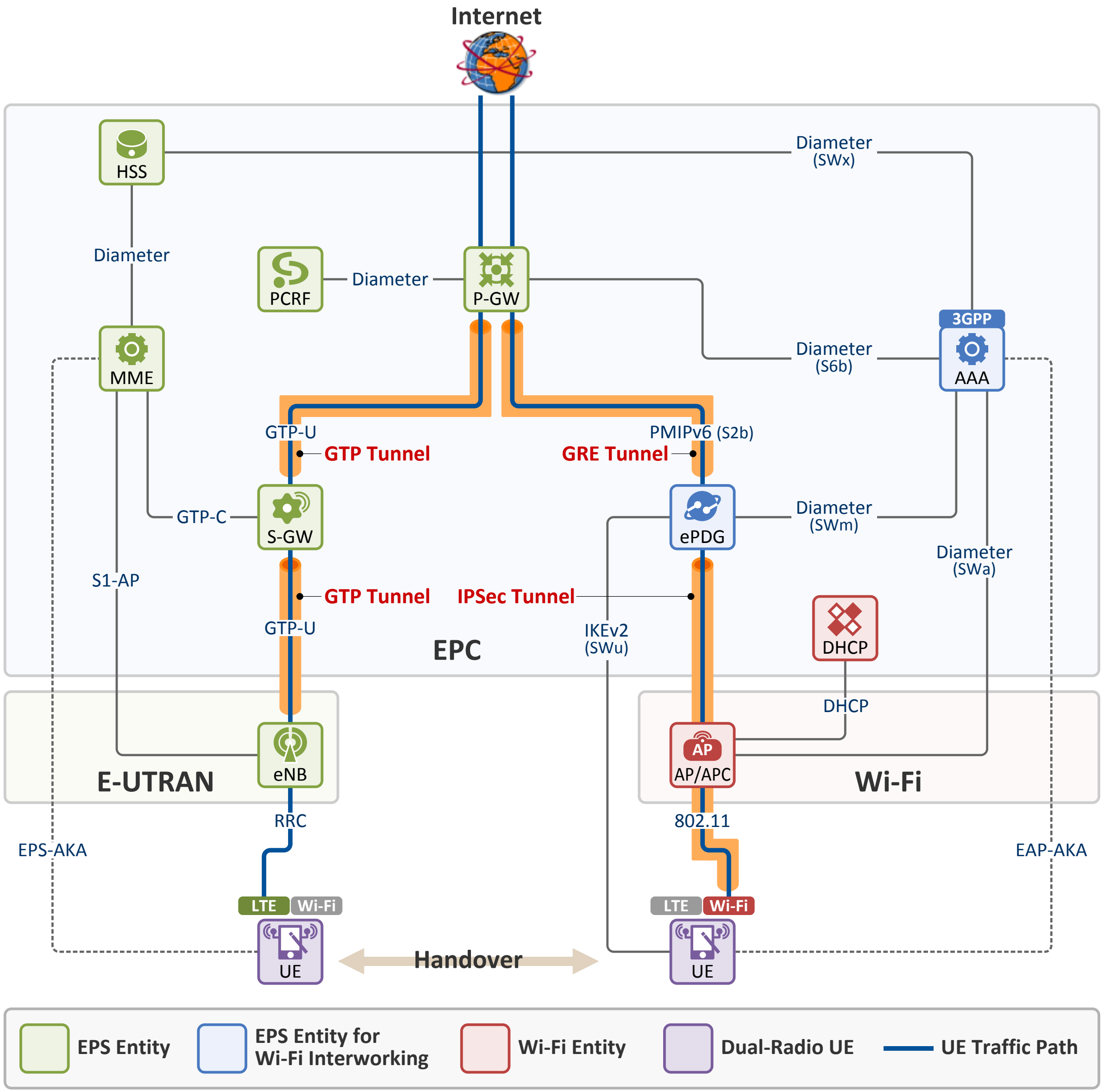
Tunneling Protocol in Wireless/Mobile Network

- 3G/LTE (standardized by 3GPP)
  - eNB ~ S-GW: GTP Tunnel (3GPP)
  - S-GW ~ P-GW: GTP Tunnel (3GPP)
- WiMAX (standardized by WiMAX Forum)
  - BS ~ ASN-GW: GRE Tunnel (RFC 1702)
  - ASN-GW ~ HA: IPinIP Tunnel (RFC 2003)
- Wi-Fi (standardized by IEEE/Wi-Fi Alliance)
  - AP ~ AP Controller: Vendor Specific Tunnel

Copyright © 2002-2012 NMC Consulting Group. All rights reserved.

LTE and Wi-Fi Interworking: (1) Network Reference Model

Related Blogs

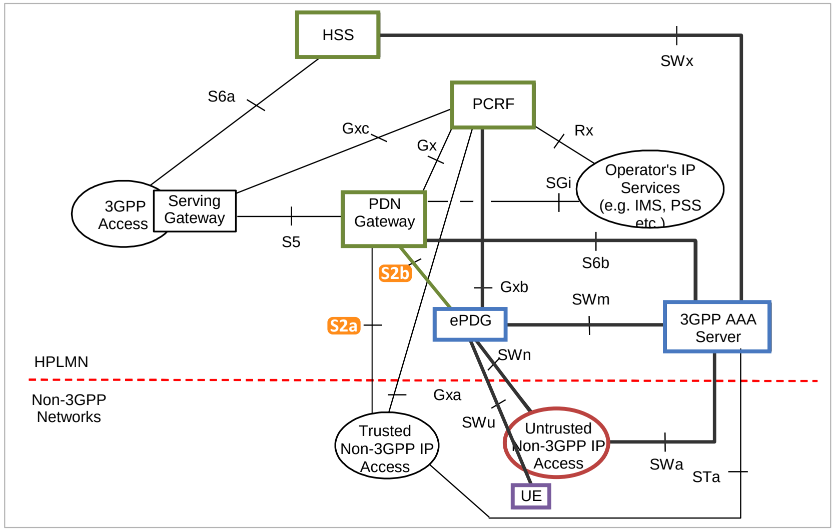


Mobile Data Offloading

- Data offloading is the use of complementary network technologies for delivering data originally targeted for cellular networks. The main complementary network technologies used for the mobile data offloading are Wi-Fi, Femtocell
- “Let’s use cheaper Wi-Fi access instead of expensive cellular (LTE) network!”

Trust & Untrust Access Network

- Simply put, this is really an indicator on if the 3GPP operator trust the security of the non-3GPP access network
- If non-3GPP access network supports trust security level from the 3GPP core (EPC) viewpoint, it is interworked with S2a interface, otherwise S2b interface is used
  - Example of Trust network: WiMAX
  - Example of Untrust network: WLAN(Wi-Fi) in a public café

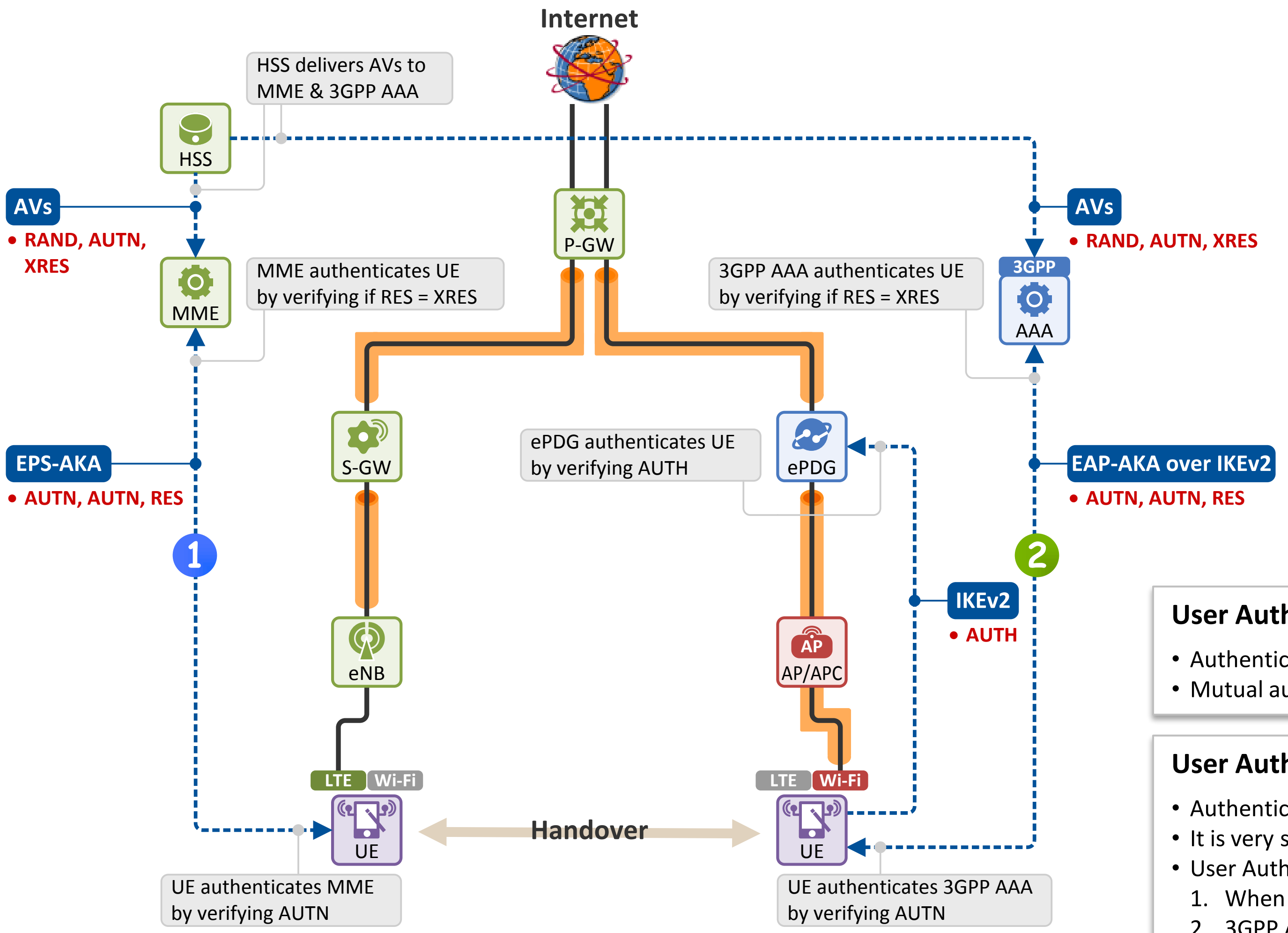


3GPP TS 23.402 Figure 4.2.2-1: Non-Roaming Architecture within EPS using S5, S2a, S2b

Copyright © 2002-2012 NMC Consulting Group. All rights reserved.

LTE and Wi-Fi Interworking: (2) Authentication and Security

Related Blogs


Internet
HSS delivers AVs to MME & 3GPP AAA
HSS
AVs
• RAND, AUTN, XRES
MME
MME authenticates UE by verifying if RES = XRES
P-GW
3GPP AAA authenticates UE by verifying if RES = XRES
AVs
• RAND, AUTN, XRES
3GPP
AAA
S-GW
ePDG authenticates UE by verifying AUTH
ePDG
EPS-AKA
• AUTN, AUTN, RES
EAP-AKA over IKEv2
• AUTN, AUTN, RES
1
2
IKEv2
• AUTH
eNB
AP
AP/APC
LTE
Wi-Fi
LTE
Wi-Fi
UE
Handover
UE
UE authenticates MME by verifying AUTN
UE authenticates 3GPP AAA by verifying AUTN

User Authentication for LTE access 1

- Authentication Protocol: EPS-AKA (USIM based)
- Mutual authentication between UE and MME

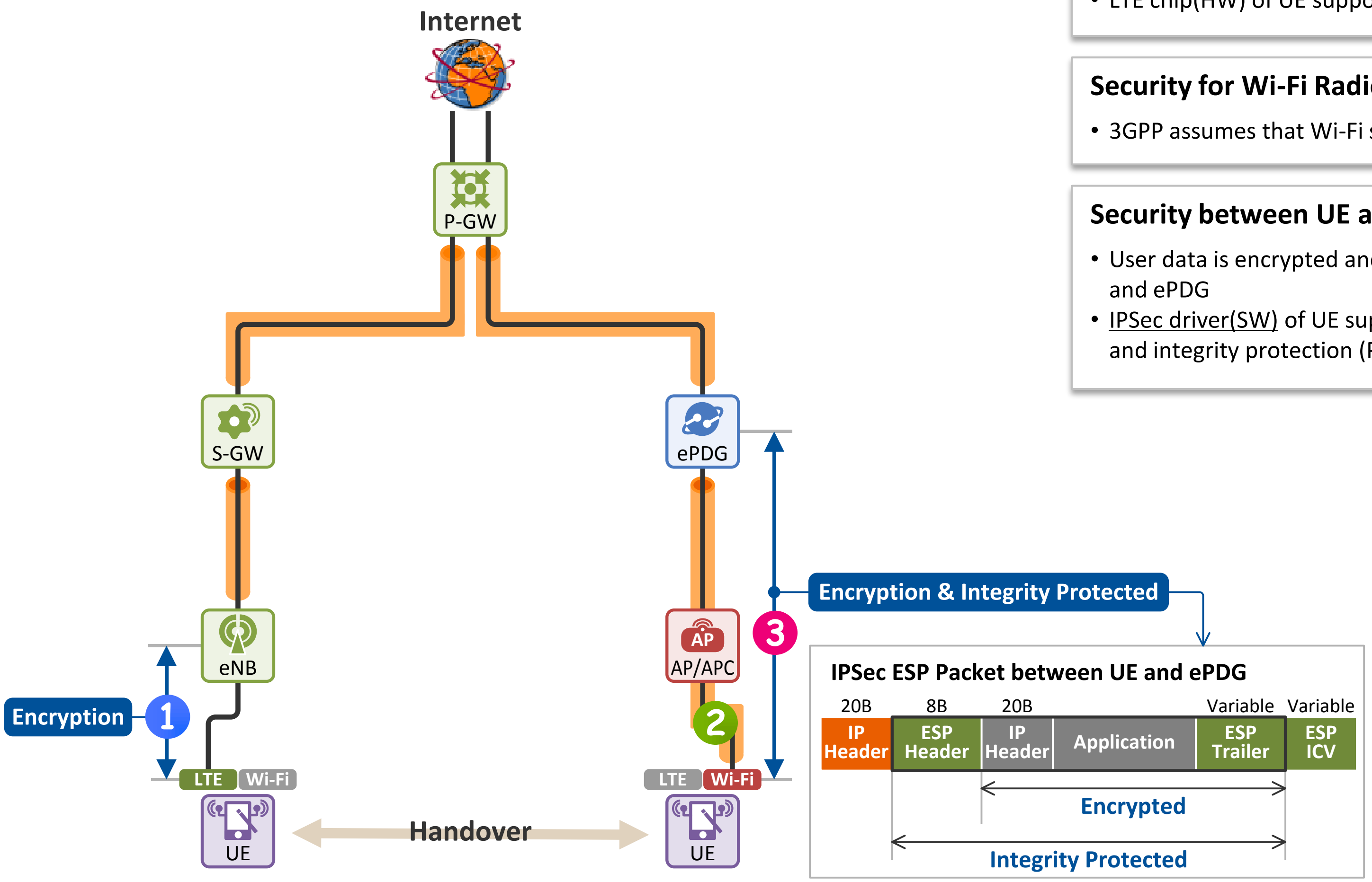
User Authentication for ePDG access 2

- Authentication Protocol: EAP-AKA ove IKEv2 (USIM based)
- It is very similar with EPS-AKA in LTE network
- User Authentication Process
  1. When UE requests to connect with ePDG
  2. 3GPP AAA obtains authentication vectors (RAND, AUTN, XRES) from the HSS
  3. Mutual authentication between UE and 3GPP AAA
     - UE authenticates 3GPP AAA
     - 3GPP AAA authenticates UE

Copyright © 2002-2012 NMC Consulting Group. All rights reserved.

LTE and Wi-Fi Interworking: (2) Authentication and Security (cont)

Related Blogs



IPSec ESP Packet between UE and ePDG

20B	8B	20B		Variable	Variable
IP Header	ESP Header	IP Header	Application	ESP Trailer	ESP ICV

Security for LTE Radio Interface 1

- User data is encrypted between UE and eNB
- LTE chip(HW) of UE supports data encryption/decryption

Security for Wi-Fi Radio Interface 2

- 3GPP assumes that Wi-Fi security is not enabled (supported)

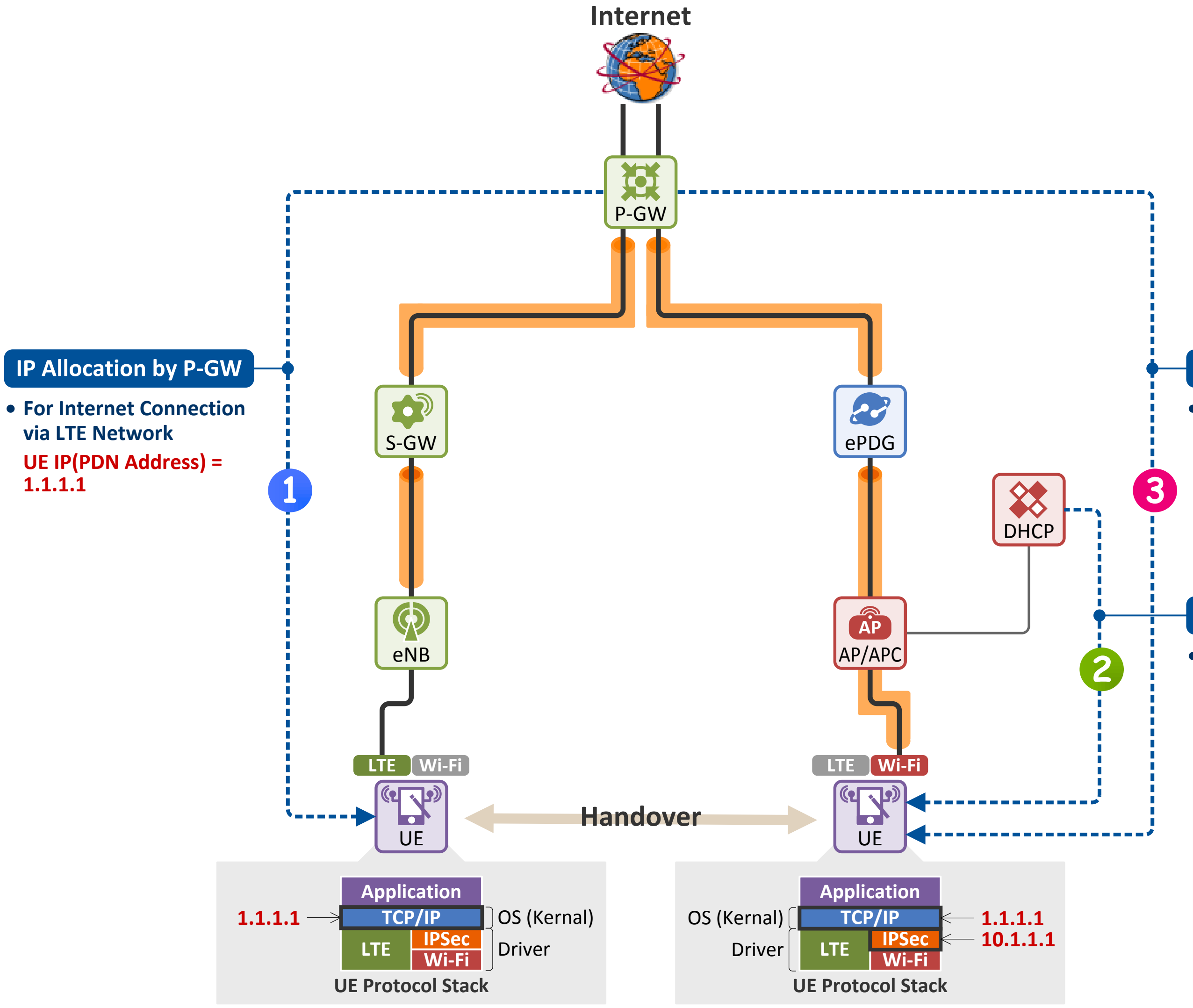
Security between UE and ePDG 3

- User data is encrypted and integrity protected between UE and ePDG
- IPSec driver(SW) of UE supports data encryption/decryption and integrity protection (Performance issue?)

Copyright © 2002-2012 NMC Consulting Group. All rights reserved.

LTE and Wi-Fi Interworking: (3) IP Allocation

Related Blogs



IP Allocation by P-GW

- **For Internet Connection via LTE Network**

UE IP(PDN Address) = 1.1.1.1

IP Allocation by P-GW

- **For Internet Connection via Wi-Fi Network**

UE IP(WLAN UE's Remote IP) = 1.1.1.1

IP Allocation by DHCP

- **For ePDG Connection via Wi-Fi Nework**

UE IP(WLAN UE's Local IP) = 10.1.1.1

Which entity allocates UE IP address? 1 3

- P-GW allocates UE IP address in both case that UE attaches to LTE and Wi-Fi network
- User packet is routing with this address in the Internet
- UE IP address is not changed even if access network is changed (LTE to Wi-Fi, and Wi-Fi to LTE)

Another IP address for accessing Wi-Fi network 2

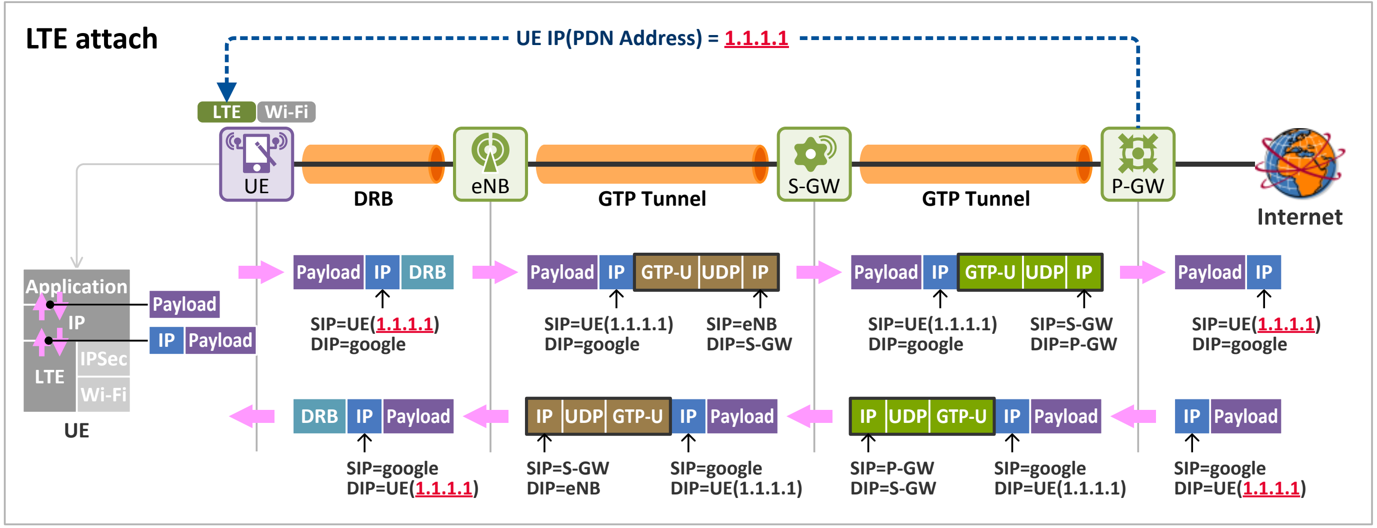
- Wi-Fi AP or External DHCP server allocates Outer IP address in Wi-Fi access network for IPSec Tunneling between UE and ePDG
- This outer IP address can be changed during Wi-Fi handover. So, MOBIKE should be supported in UE and ePDG
- So, Two IP addresses are required when UE accesses to Wi-Fi network
  - **WLAN UE's Local IP**: Outer IP address which allocated by AP/DHCP server
  - **WLAN UE's Remote IP**: Inner IP address which allocated by P-GW

Copyright © 2002-2012 NMC Consulting Group. All rights reserved.

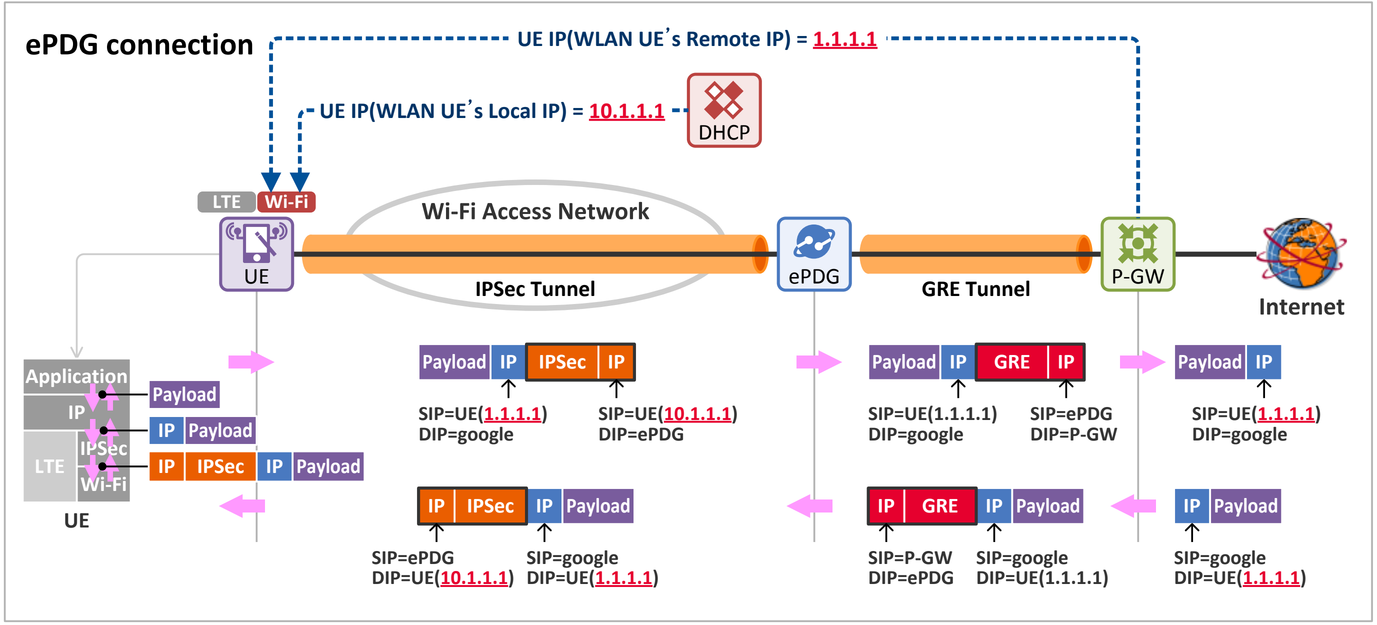
LTE and Wi-Fi Interworking: (3) IP Allocation (cont)

Related Blogs

- Example of IP address usage



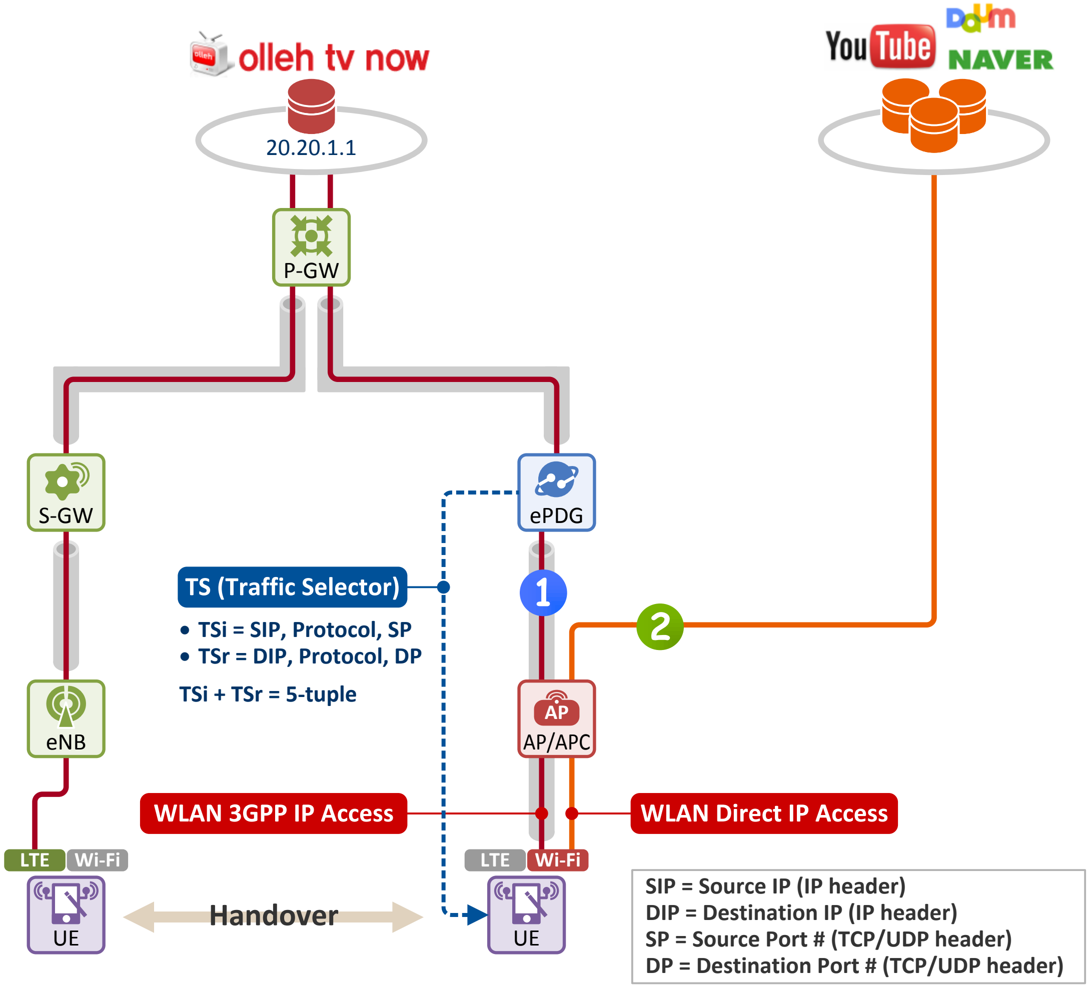
LTE attach



ePDG connection

Copyright © 2002-2012 NMC Consulting Group. All rights reserved.

LTE and Wi-Fi Interworking: (4) Traffic Selector



TS (Traffic Selector)

- TSi = SIP, Protocol, SP
- TSr = DIP, Protocol, DP

TSi + TSr = 5-tuple

SIP = Source IP (IP header)
DIP = Destination IP (IP header)
SP = Source Port # (TCP/UDP header)
DP = Destination Port # (TCP/UDP header)

WLAN 3GPP IP Access

1

- User Traffic Path: UE – Wi-Fi AP – ePDG – P-GW – Internet
- Traffic is passed through the 3GPP core, which means that it can support handover between LTE and Wi-Fi
- Use Case: Operator Service (example: KT olleh TV now). Operator can provide differentiated service (e.g., heterogeneous handover) to their subscriber

WLAN Direct IP Access

2

- User Traffic Path: UE – Wi-Fi AP – Internet
- Traffic is not passed through the 3GPP core, which means that it can not support handover between LTE and Wi-Fi
- Use Case: OTT service (example: YouTube)

Traffic Selector

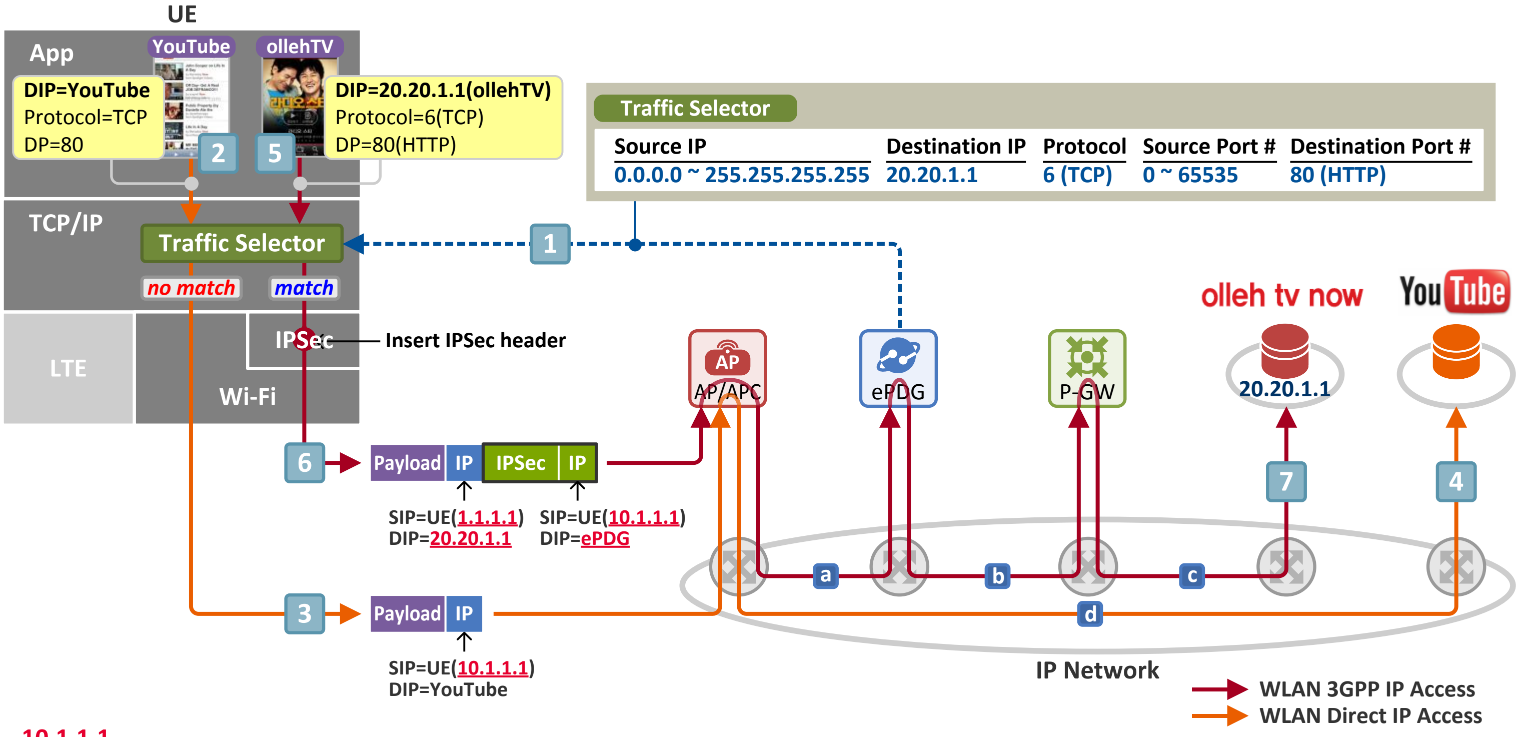
- Traffic Selector can be used to distinguish between WLAN 3GPP IP Access and WLAN Direct IP Access
- UE gets Traffic Selector from the ePDG during the IKEv2 procedure
- Traffic Selector consists of TSi and TSr:

  - TSi = Source IP Address(SIP) range,
    Protocol range,
    Source Port Number(SP) range
  - TSr = Destination IP Address(DIP) range, → Server Identification
    Protocol range (same as TSi, → TCP or UDP
    Destination Port Number(DP) range → Service Identification
- Tsi + TSr = 5-tuple
- Based on 5-tuple, UE (IPSec driver) can determine whether application traffic (IP flow) is served by WLAN 3GPP IP Access or WLAN Direct IP Access

Copyright © 2002-2012 NMC Consulting Group. All rights reserved.

LTE and Wi-Fi Interworking: (4) Traffic Selector (cont)

Related Blogs



Traffic Selector

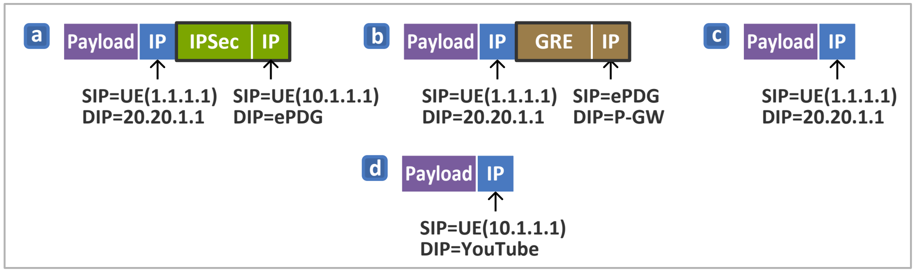
Source IP	Destination IP	Protocol	Source Port #	Destination Port #
0.0.0.0 ~ 255.255.255.255	20.20.1.1	6 (TCP)	0 ~ 65535	80 (HTTP)

10.1.1.1

- WLAN UE’s Local IP Address
- Allocated by AP/DHCP Server in Wi-Fi Network
- IPSec Tunnel Outer Source IP in case of WLAN 3GPP IP Access
- Source IP in case of WLAN Direct IP Access

1.1.1.1

- WLAN UE’s Remote IP Address
- Allocated by P-GW
- IPSec Tunnel Inner Source IP in case of WLAN 3GPP IP Access



Copyright © 2002-2012 NMC Consulting Group. All rights reserved.

Status of KT, SKT & LG U+ and UE Requirements

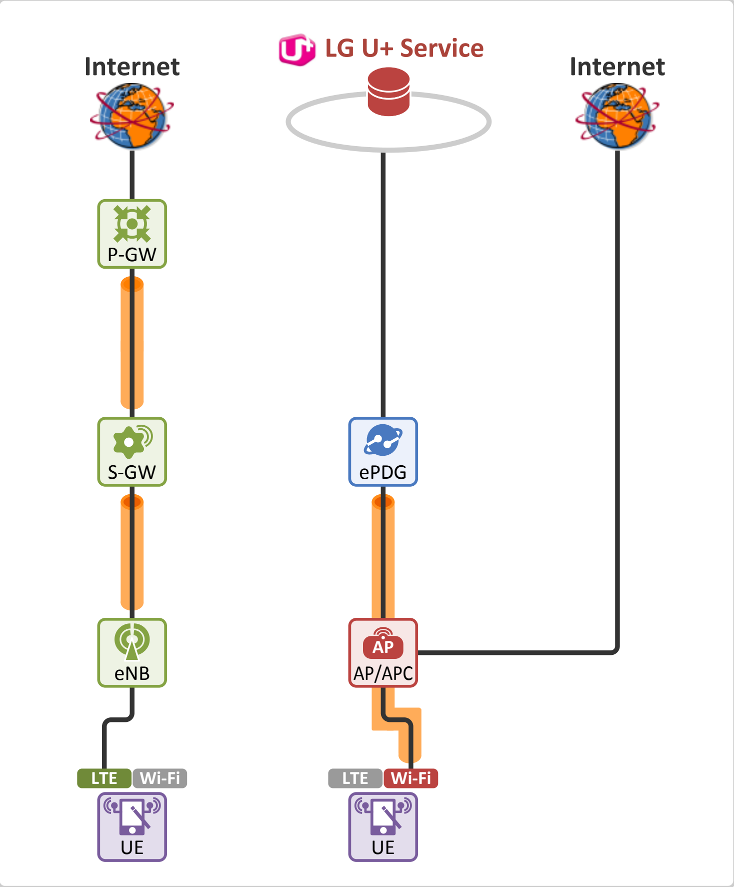
- KT, SKT: No plan
- LG U+: Deploy ePDG from Insprit (http://www.in-sprit.com/kr/content/main/index.php), but do not service yet

LG U+: The Purpose of ePDG Deployment

- Provides security when subscriber accesses LG U+ service via Wi-Fi network
- At this moment, there's no interworking (no PMIPv6/GTE tunnel) between P-GW and ePDG which means that it does not support handover between LTE and Wi-Fi

UE Software Requirement for LTE/Wi-Fi Interworking

- IPSec(MOBIKE) driver (Kernel Layer) is required
- Handover Manager (Kernel Layer) is required: Handover decision by monitoring LTE and Wi-Fi signal strength
- Big Issue: Apple willing to support "IPSec and Handover Manager" in iPhone/iPad???



Copyright © 2002-2012 NMC Consulting Group. All rights reserved.