Cisco SCS 4.1 – vHetNet Solution

Horacio Ruiz
Network Consulting Engineer

May 2017

Training duration

- 2-5 May, 9hs to 17hs (Flexible)
- 11hs/15.30hs Break
- 13hs lunch

Agenda

- vHetNet Introduction & Overview
- vHetNet UCS-B Architectures
- HNBGW Overview
- HeNBGW Overview
  - Variants
- HNBGW 3GPP Releases
  - Features & Capabilities
- HeNBGW 3GPP Releases
  - Features & Capabilities

Agenda II

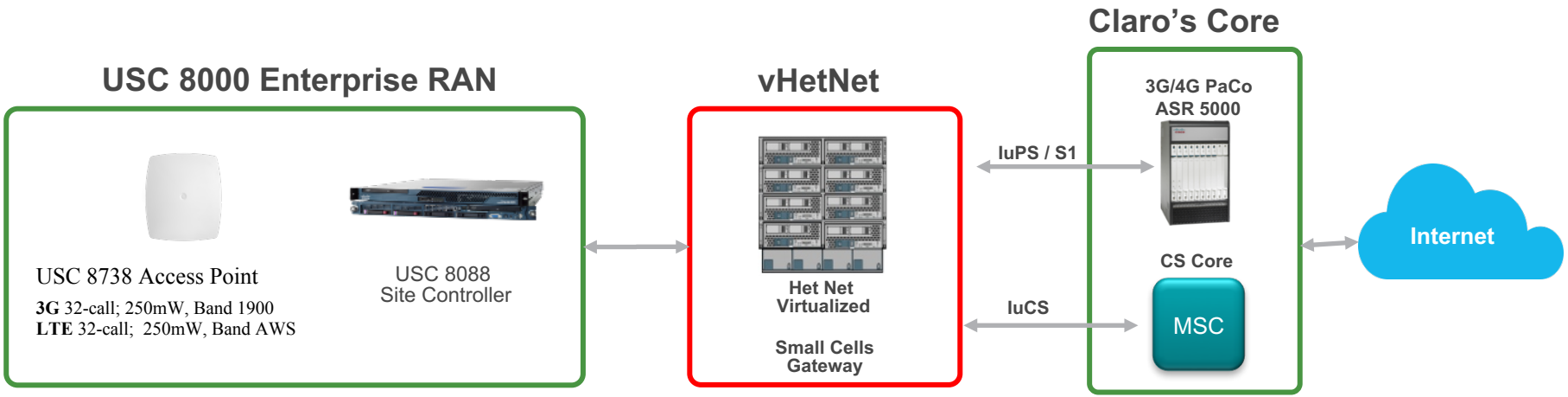
- SecGW Overview
- AAA Overview
- vCenter Architecture
- eRMS – SpiderNet

Agenda III

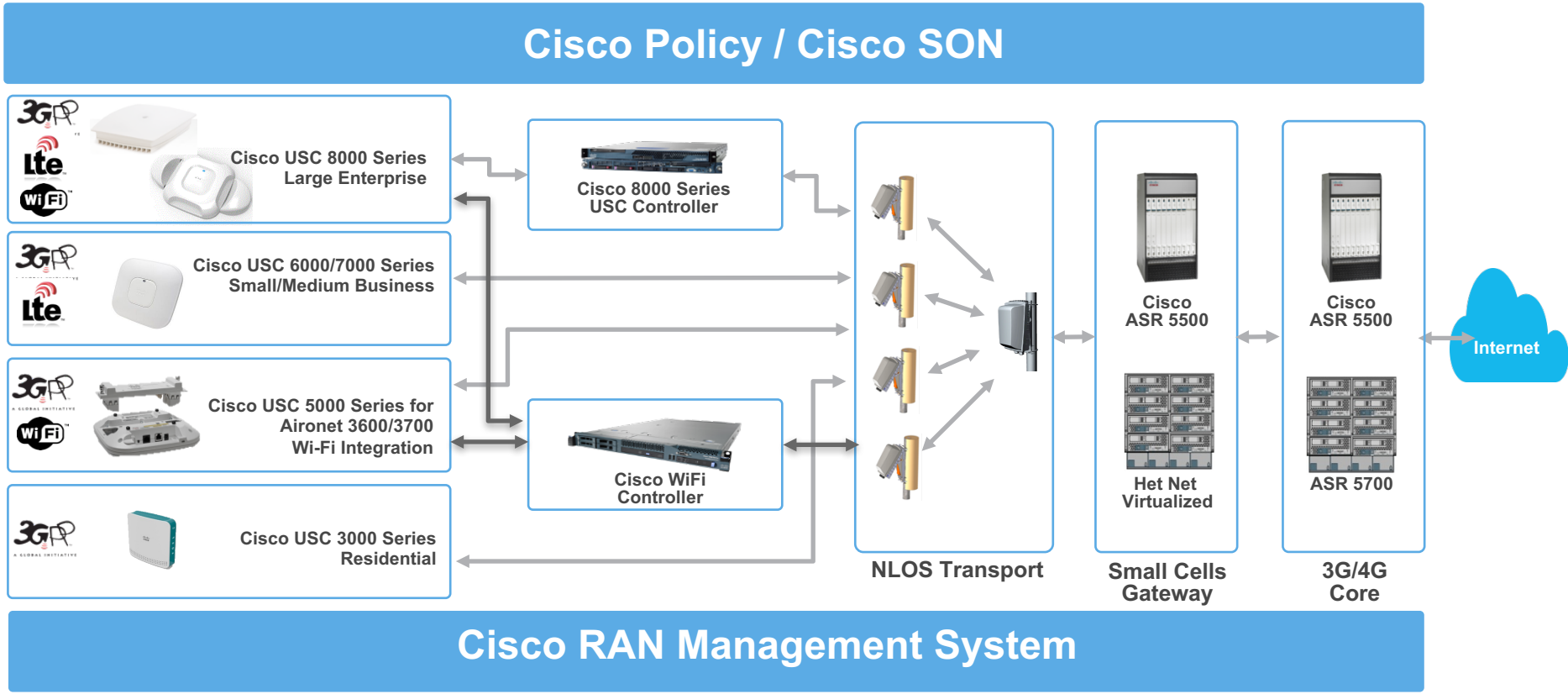
- vHetNet integration in Claro AR
  - IP Planning
  - HNBGW AMBA/MDQ
  - HNBGW CORDOBA/MENDOZA
  - HeNBGW MDQ
  - HeNBGW AMBA/CORDOBA/MENDOZA
  - eRMS (SpiderNet) Fault Management
- Security in vHetNet
- Troubleshooting
- Hands on demonstration

vHetNet Introduction & Overview

Claro Argentina Small Cells Project Scope

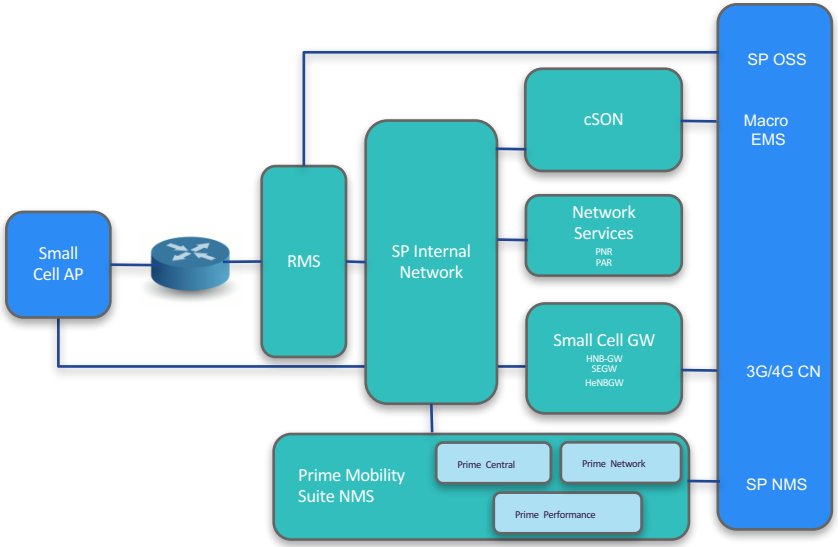


Cisco e2e Solution Components



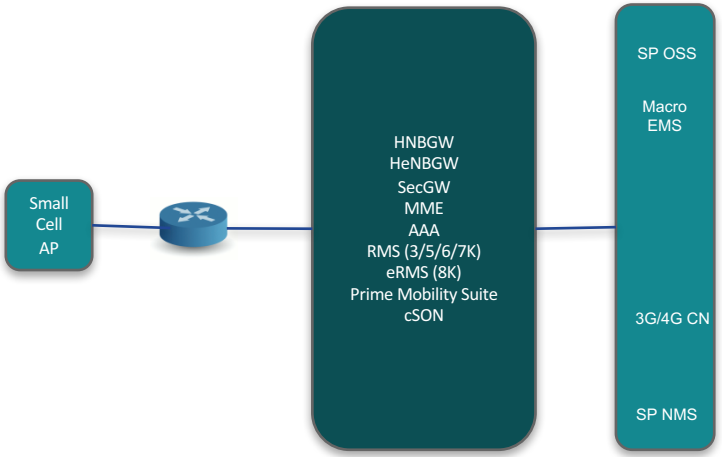
HetNet Variants

Traditional (Non-Virtualized)



- Several independent physical nodes
- Complexity in integration and verification

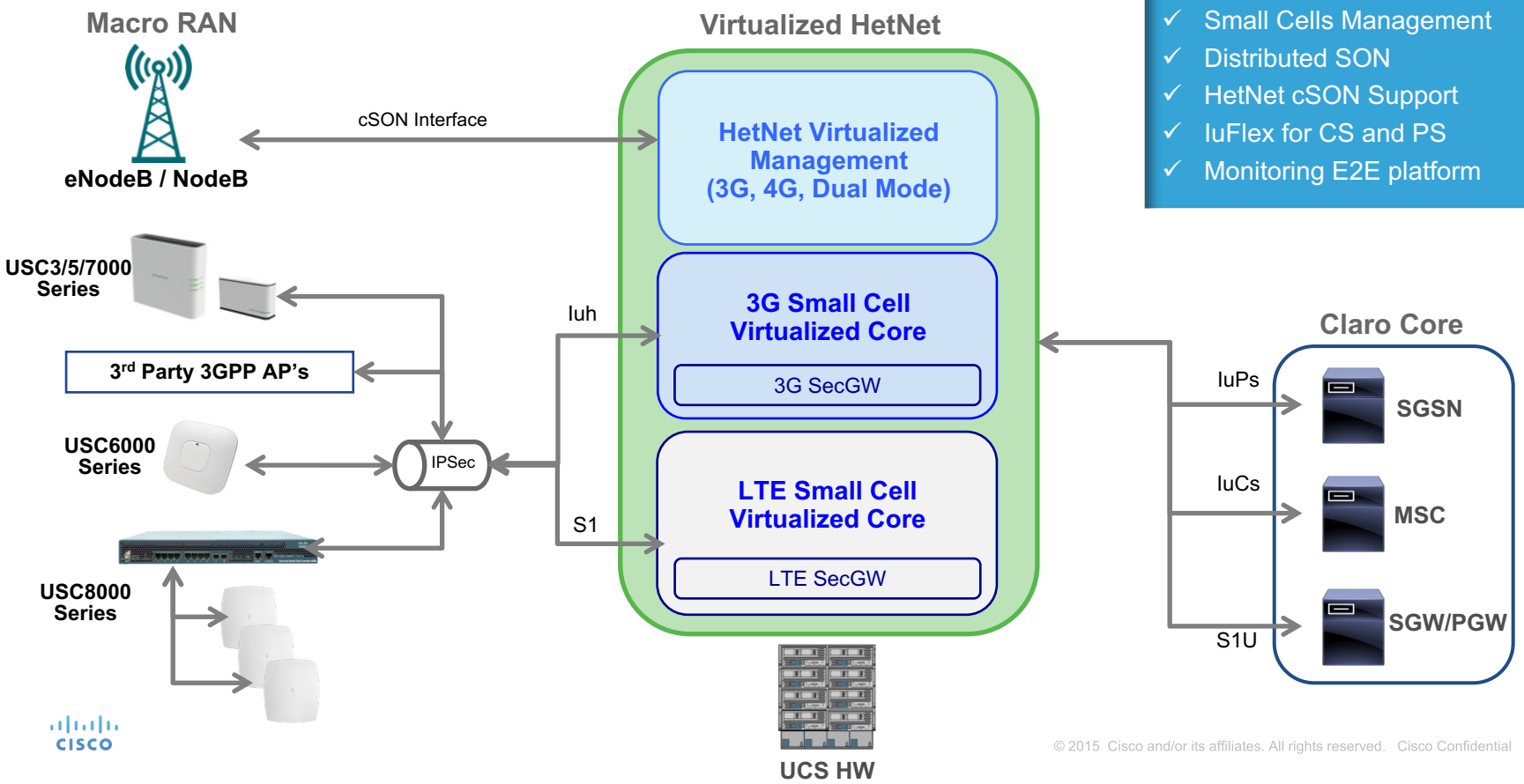
Virtualized



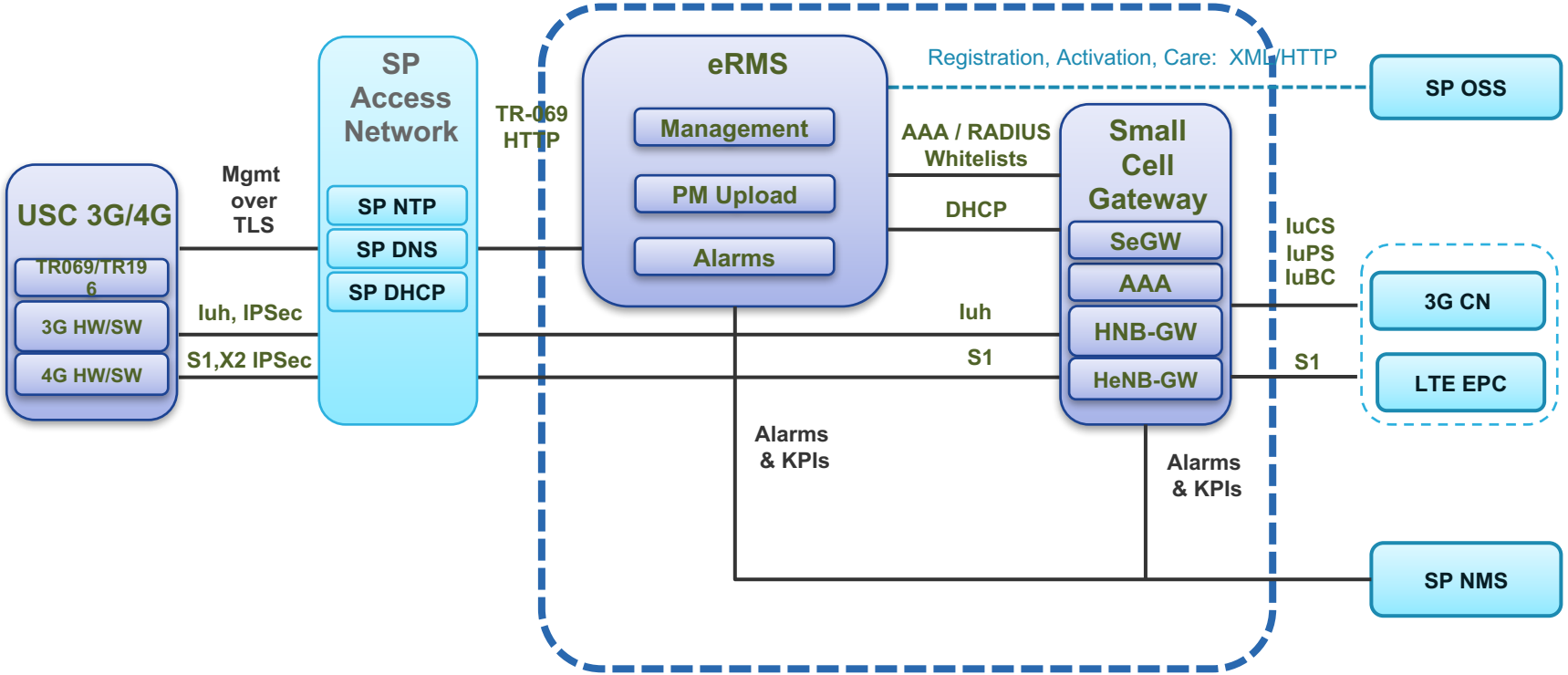
- Pre-packaged components virtualized on a single UCS B-Series Blade Server
- Orchestration via Click2Deploy
- Preconfigured hardware BoM

vHetNet All in One Virtualized Platform

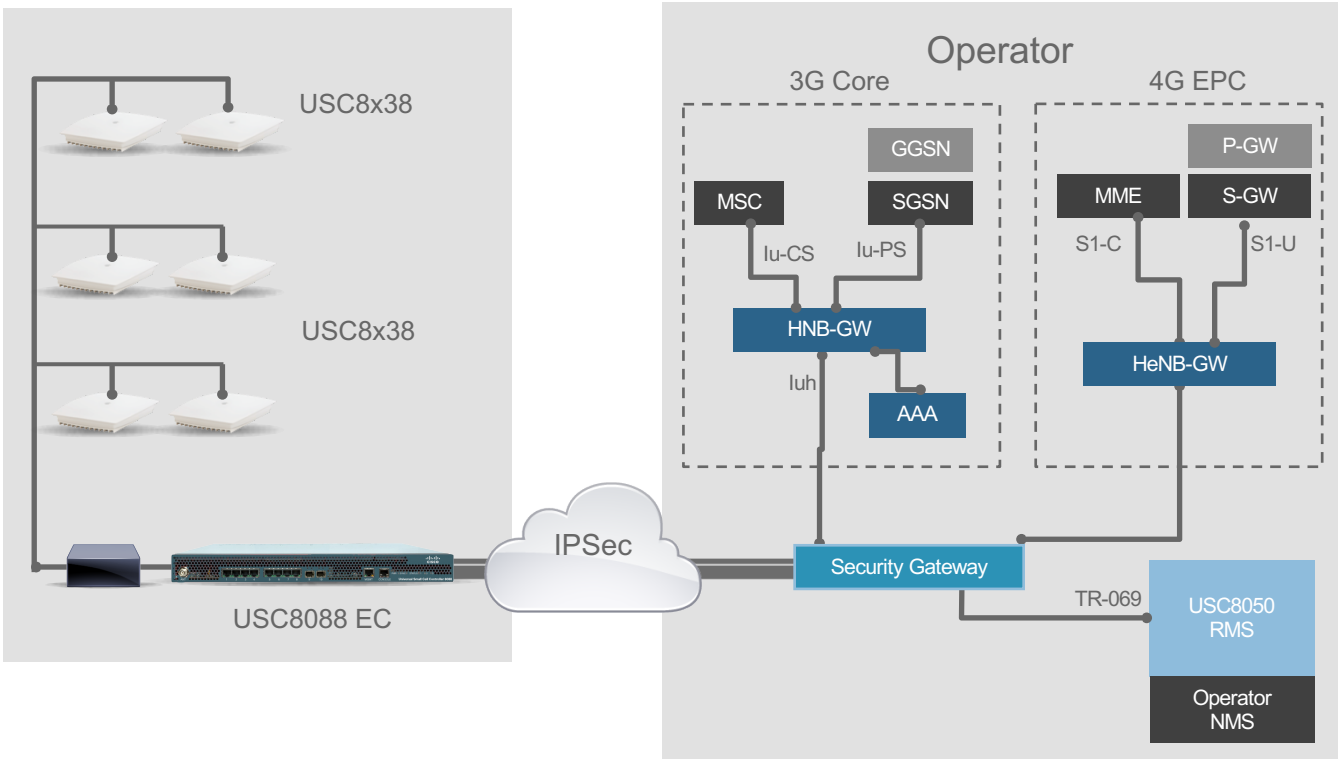
- ✓ Multi Vendor Small Cells Support
- ✓ Virtualized 3G Small Cells GW
- ✓ Virtualized LTE Small Cells GW
- ✓ Small Cells Management
- ✓ Distributed SON
- ✓ HetNet cSON Support
- ✓ IuFlex for CS and PS
- ✓ Monitoring E2E platform



vHetNet Network Architecture

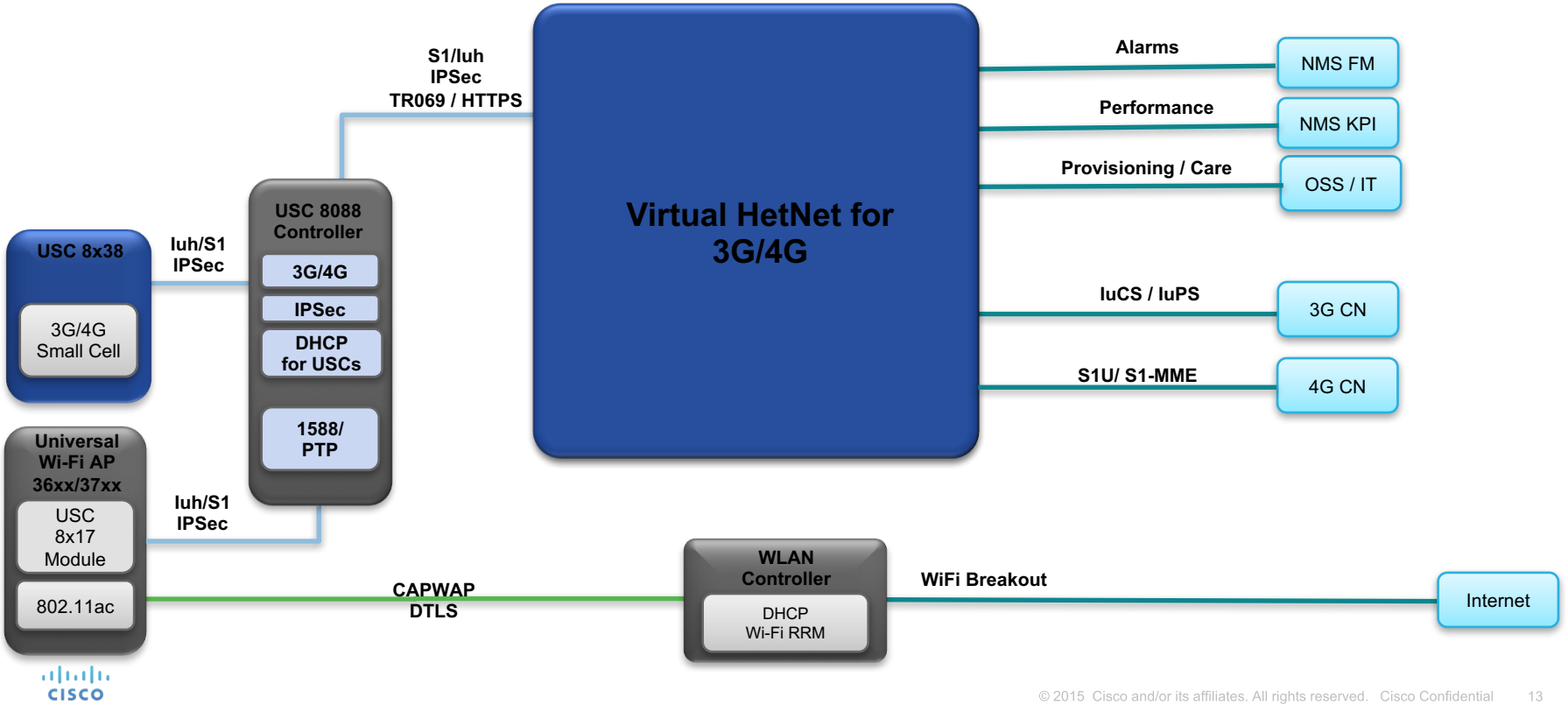


Cisco USC 8000 & vHetNet

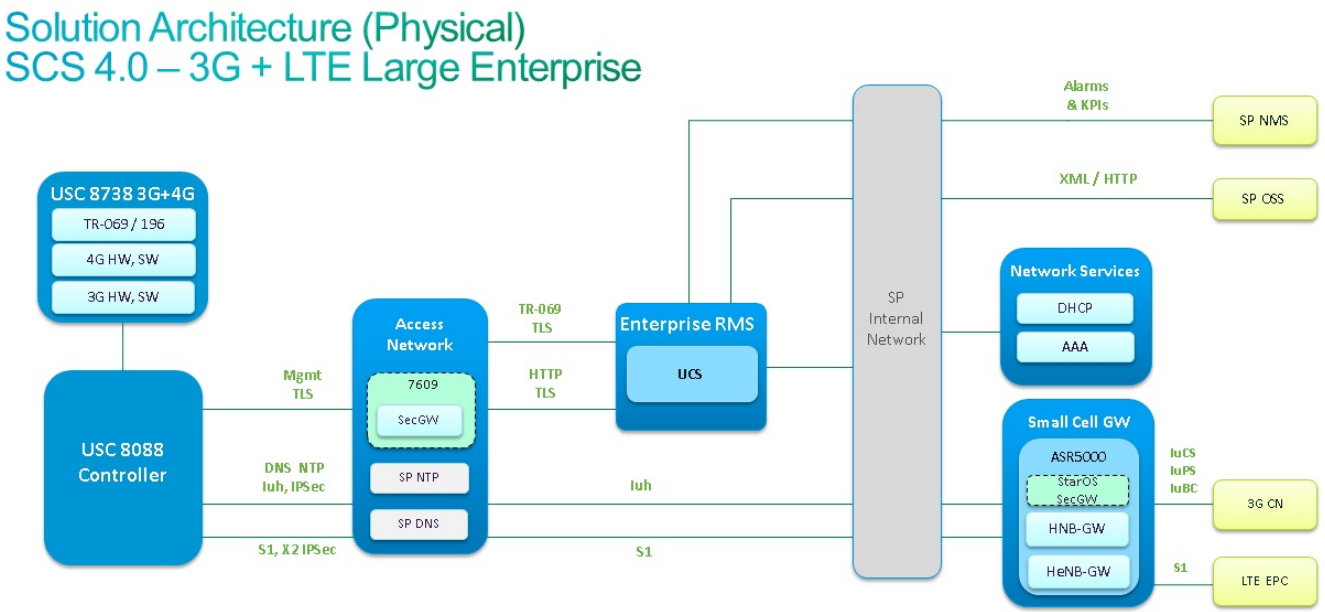


SCS 4.1 / Virtual HetNet for 3G/4G

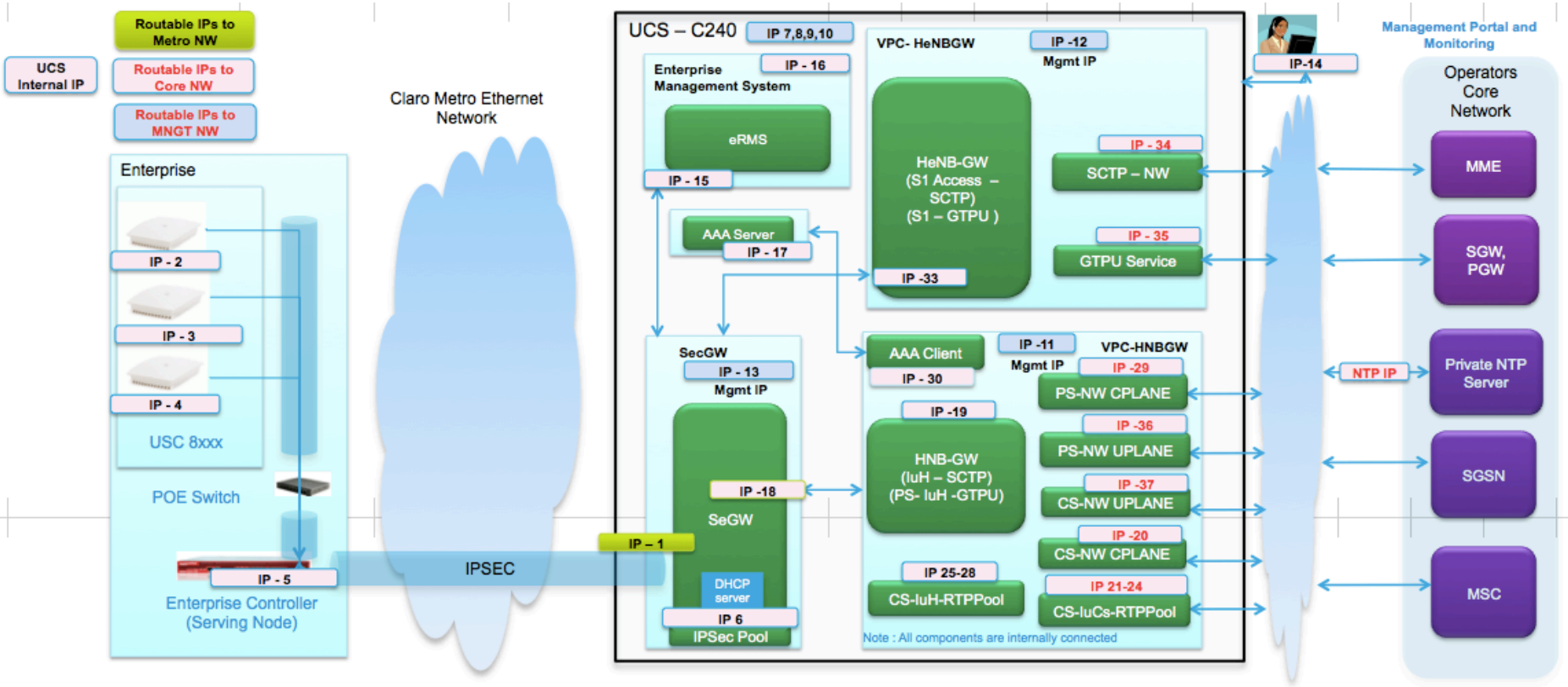
USC 8K



Architecture



vHetNet IP Requirements



H(E)NBGW Overview

- 3G+4G H(E)NB is a Multi-Mode (e)nodeB that works just as any other 3G/4G Radio Node in mobile operator's core network. 3GPP requires 3G & 4G UE traffic to be carried over from H(E)NB via Security Gateway and H(E)NB GW to the respective CN.
- H(E)NB sits at customer premises so it is essential that traffic coming to and from H(E)NB is encrypted. This is provided by secured IPSec tunnel between H(E)NB and Security Gateway(SeGW). SeGW sits in mobile operator's private network. H(E)NB-GW sits behind SeGW in private network. connects to the 3G core network using IuCS and IuPS over IP and 4G EPC over S1-AP interface.
- H(E)NB-GW also connects to a third-party FreeRadius server respectively to check the authenticity of HNB (USC Controller)

H(E)NBGW Overview II

- H(E)NB GW acts as a RNC to the 3G Core Network. MSC and SGSN connect to the H(E)NB GW on IuCS and IuPS interfaces respectively. HNB connects to the GW over the IuH Interface.
- IuCS can be connected via IP transport and it will provide Circuit Switched functionality to 3G UEs. Voice calls are setup via 12.2 kbps AMR codec
- IuPS also can be connected via IP transport and it will provide Packet Switched functionality to 3G UEs. PS user packets are carried over GTP-U path between H(E)NB GW and SGSN. Direct tunnel can be also established between H(E)NB GW and GGSN
- H(E)NB GW can be connected to multiple MSC and SGSN or core network. To route the traffic to proper MSC/SGSN, IuFlex pool can be used
- HENBGW act as eNodeB to the EPC Core Network.
- H(E)NB GW also acts as an aggregator for the S1-AP Control Plane and User Plane to the LTE EPC (specifically S1-C to MME and S1-U to SGW).

H(E)HNBGW Overview III

- ASR5000 will be provisioned with hnbgw-services and henbgw-network-services for the node to function as H(e)NBGW.
- H(e)NBGW can be connected to multiple MMEs and multiple SGWs.
- H(e)NBGW supports tracking area code (TAC) and PLMN ID used by HeNB.
- HNBGW acts as aggregator for multiple HNBs and also it can be connected to multiple CN elements. So it can be used to collect individual CN element based key performance indicators
- HNBGW is connected to Cell Broadcast Center via IuBC interface, SABP protocol over TCP connection. HNBGW receives emergency messages/alerts on IuBC interface and sends them to affected HNB over IuH interface.
- HNBGW is also connected to IP Timing Server (NTP). The HNB synchronizes its oscillator from the IP Timing server if the surrounding macro network is not available.

HeNBGW (LTE) function

- Likewise HeNBGW provides access to Small Cell users to the EPC core network and works as a gateway for HeNBs to access the core networks.
- The HeNBGW concentrates connections from a large amount of HeNBs through S1 interface and terminated the connection to existing core networks using standards-based S1-MME and S1-U network interfaces.
- The HeNB-GW appears to the MME as an eNodeB. The HeNB-GW appears to the HeNB as an MME.

HNBGW (UMTS) function

- Aggregate backhaul traffic from hundreds of thousands HNBs (Femtocells) into a single ASR5K
- Standards-based interfaces with IuH to HNB and Iu to 3GPP Core Network or IMS/SIP Network for 3GGP2 (CDMA)
- 3G Iu Connectivity – Routes traffic
  - IuCS over IP or ATM
  - IuPS over IP or ATM
- Handover support

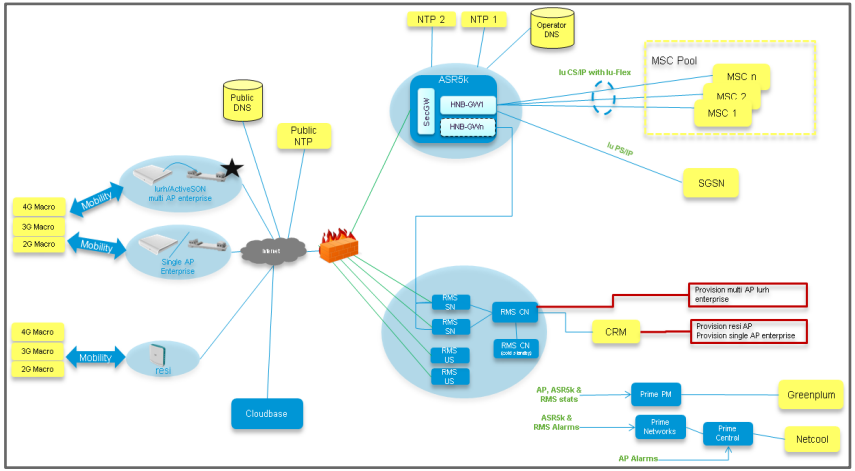
  Outgoing to Macro (2G, 3G)

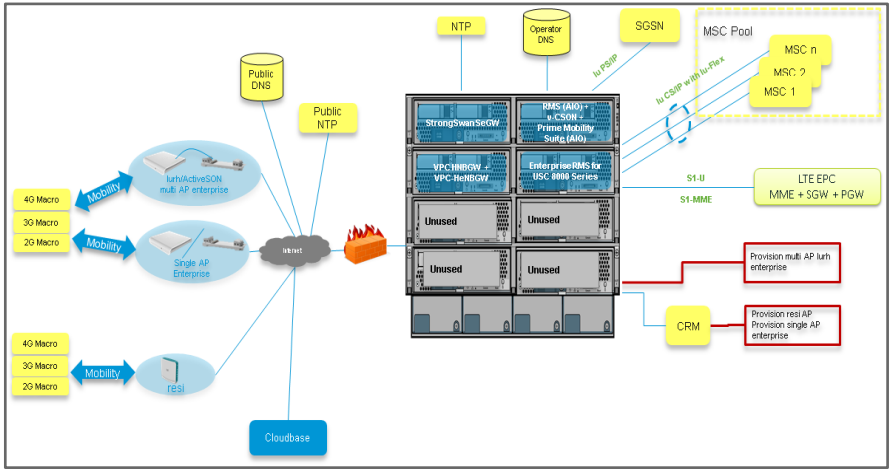
  Incoming from Macro
- Paging

vHetNet UCS-B Architectures

What is Virtualized HetNet Solution?

- HetNet Gateways and OAMP components in the conventional Small Cells Solution are virtualized into common platform.
- Radio Access and CS/PS Core Networks are not virtualized.
- Virtualization is based on VMWare vSphere and Cisco UCS platforms.



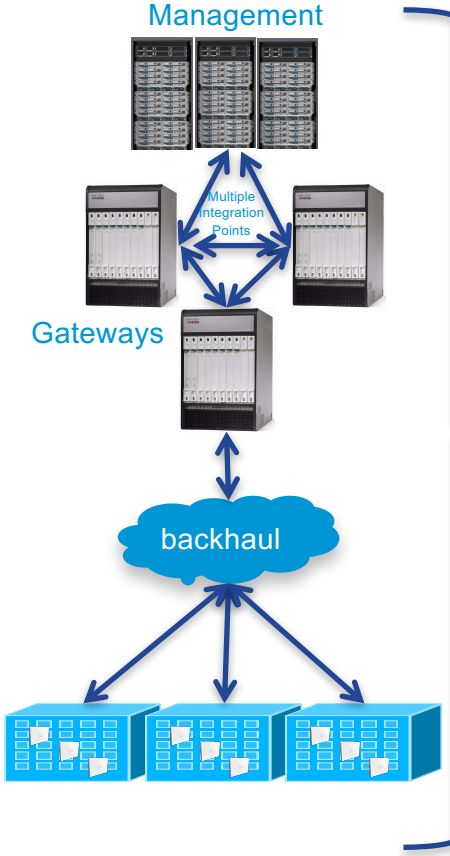


Why Virtualized HetNet Solution?

- Quick Insertion, Activation, Validation and Deployment
- Reduced HW Foot Print
- Solve Coverage and Capacity issues while minimizing OpEx & CapEx
- Fully Integrated and Validated Virtualized SCS Core and Mgmt
- Auto Install and Auto Config virtualized on UCS
- Support for all FCS and EFT Cisco Universal Small Cells (3G, LTE, Dual Mode)
- Validated and Pre-Defined Dimensioning
- Enhanced AP Troubleshooting and Monitoring Tools
- Simplified Sales Packaging
- Packages service offering with single PID

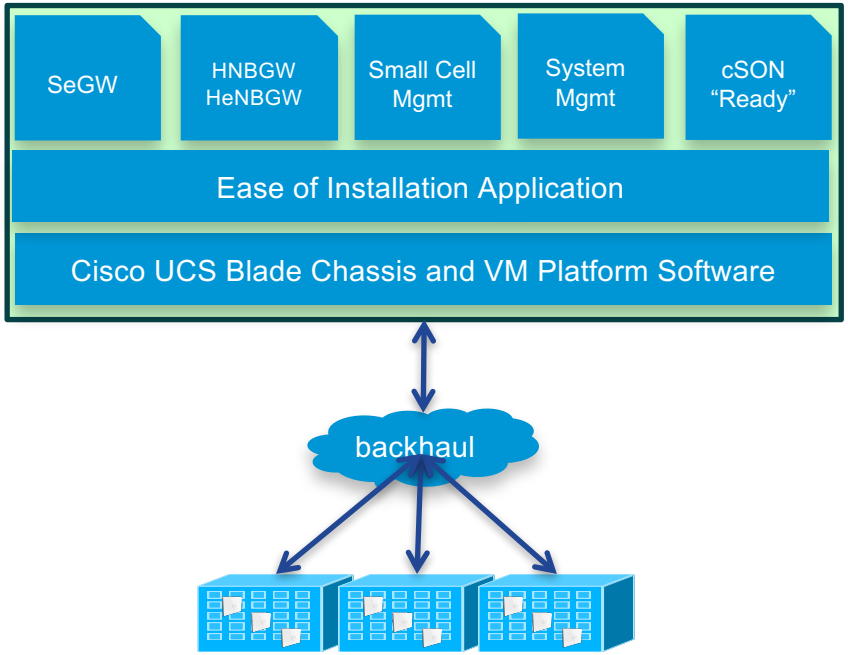
OpEx Benefits with Virtual HetNet

Traditional Model



1. Core & RF Planning
2. Equipment Hosting Site
3. Small Cell Gateway HW Procurement
4. Power Upgrades & Space
5. IP Address & Detail Core
6. AP Mgmt Design & Planning
7. AP Mgmt HW Dimensioning
8. AP Mgmt Installation & Bring up
9. Small Cell Gateway Install & Bring up
10. SecGW Design & Integration
11. NMS Installation & Configuration
12. NMS Reporting Setup
13. FAP Bring up
14. Test Calls
15. Fine Tuning
16. Scale and QoE verification
17. KPI Reporting
18. Fine Tuning
19. Go Live

Cisco vHetNet



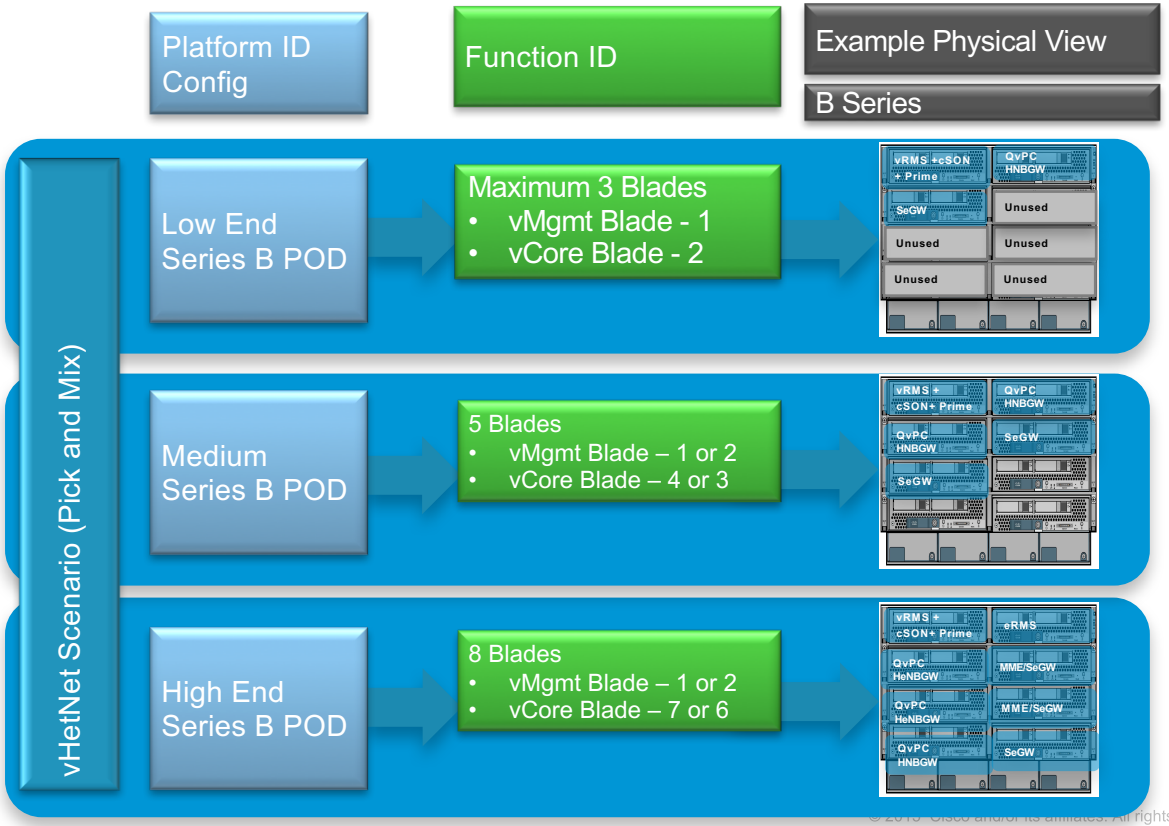
1. Order thru Single Part Number Bundle
2. Shipped as a Pre-Validated unit
3. Click to Deploy with Automated Integration Validation
4. RF Planning & Small Cell Installation and Activation
5. Test & fine Tune

Key Components

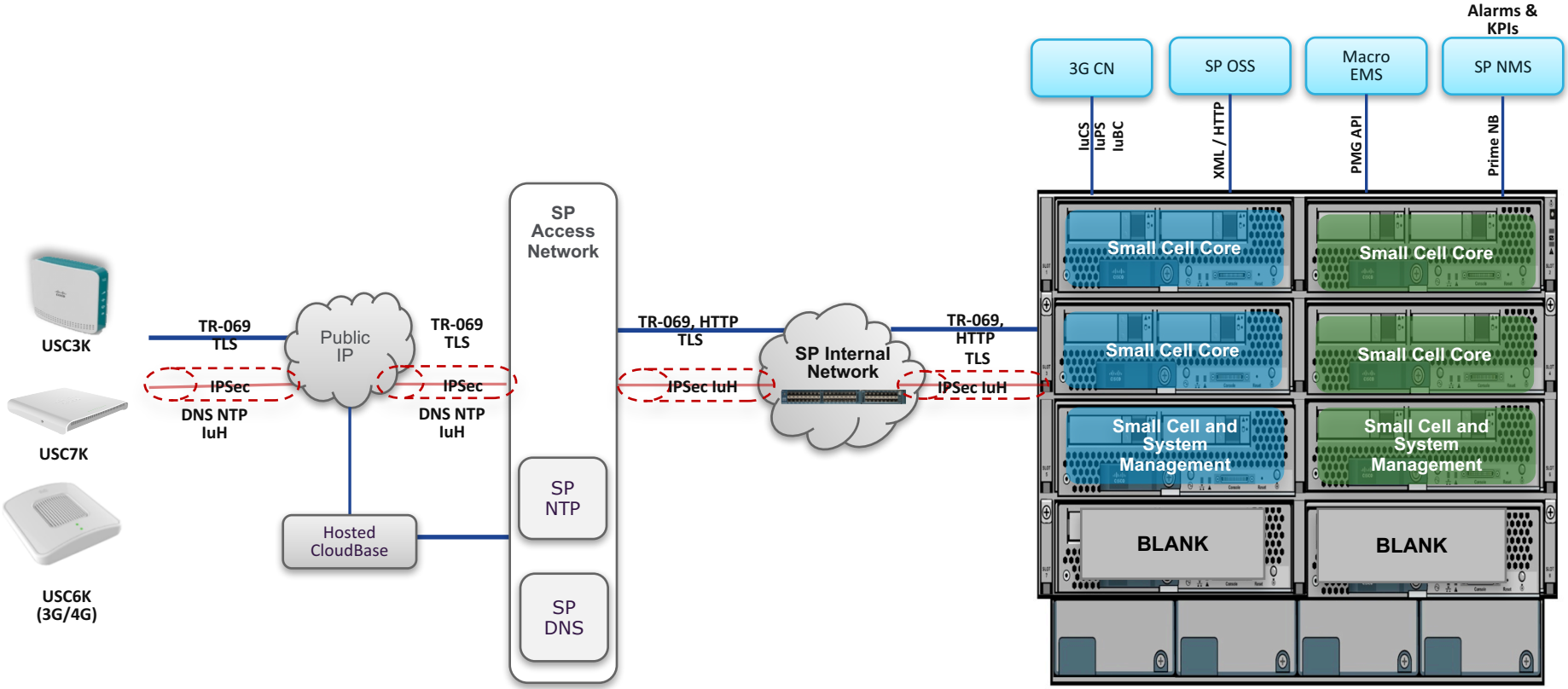
V = Virtualized
P = Physical

- Access Points:
  - 3G only: USC333x, USC5310, USC5030, USC7330, USC8338 (SCW)
  - 4G only: USC8438 (SCW)
  - 3G+4G Dual Mode: USC8738 (SCW)
- Debian Linux OS based StrongSwan Security Gateway (V)
- StarOS based HNBGW (3G) & HeNBGW (4G) (V/P)
- StarOS based MME (V/P)
- RHEL based Radio Management System (RMS) (V)
- RHEL based Prime Mobility Suite (V)
- Debian Linux OS based cSON READY (3G only) (V)
- RHEL based USC8000 Controller (SN) (P)
- RHEL based USC8000 Enterprise RMS (eRMS) (V/P)

vHetNet Solution Configuration Summary

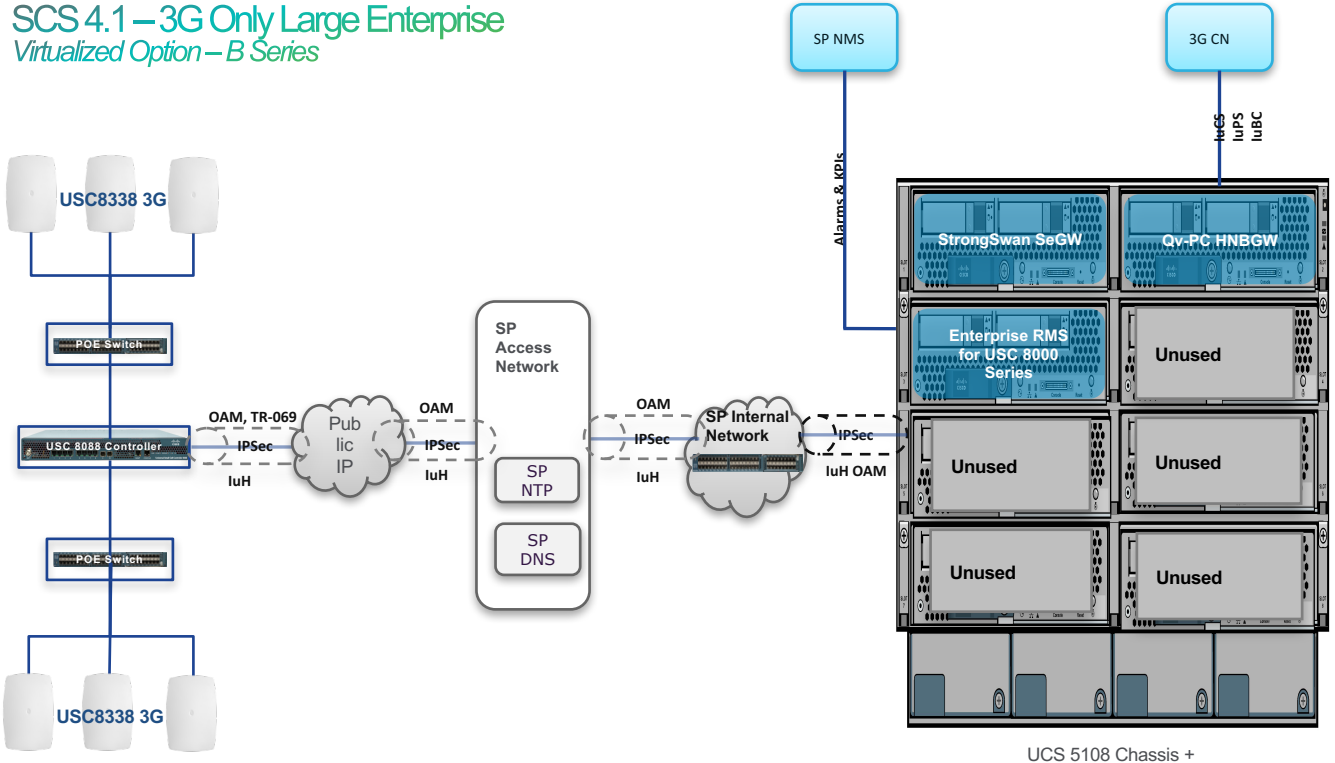


vHetNet Architecture with High Availability



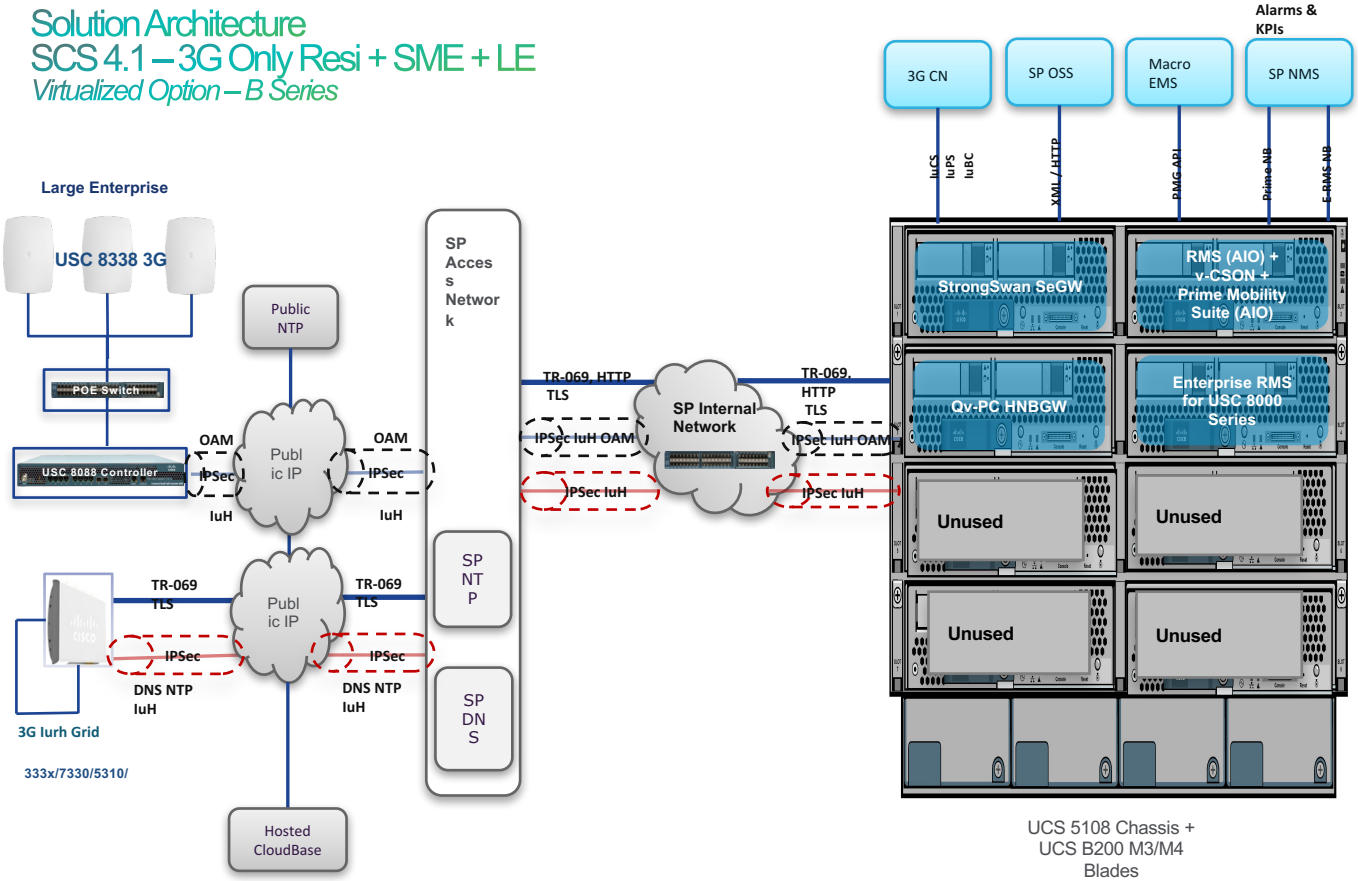
UCS 5108 Chassis + UCS B200 M4 Blades

Solution Architecture
SCS 4.1 – 3G Only Large Enterprise
Virtualized Option – B Series



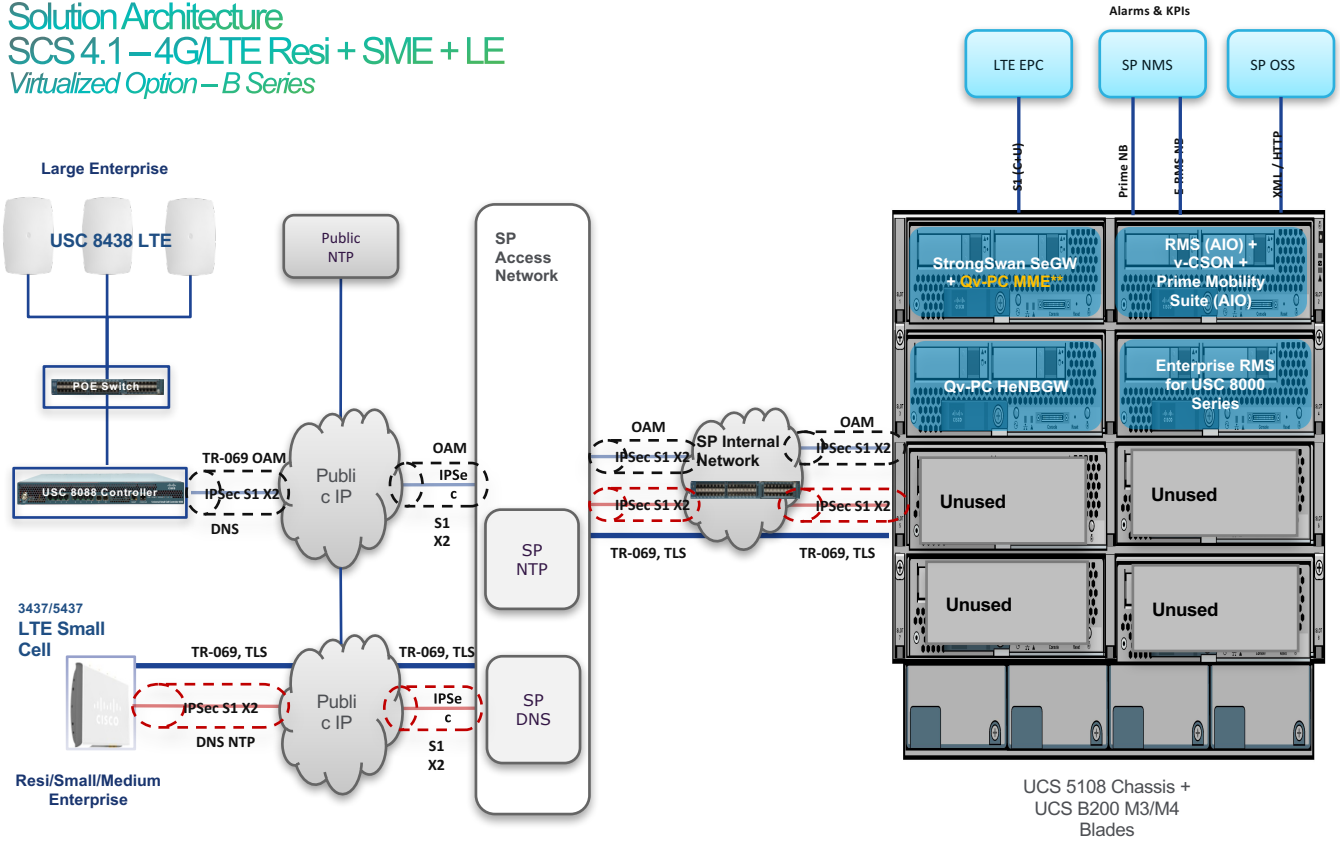
UCS 5108 Chassis +
UCS B200 M3/M4
Blades

Solution Architecture
SCS 4.1 – 3G Only Resi + SME + LE
Virtualized Option – B Series



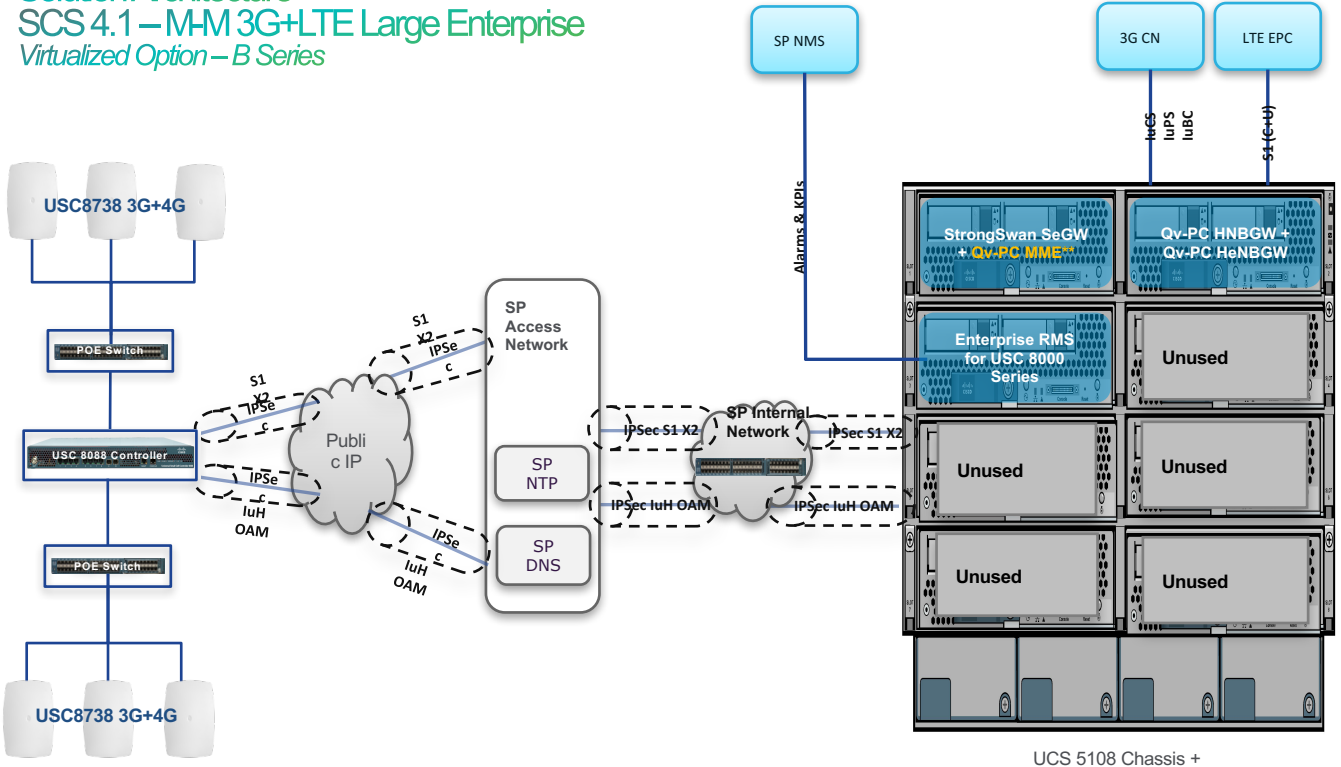
UCS 5108 Chassis +
UCS B200 M3/M4
Blades

Solution Architecture
SCS 4.1 – 4G/LTE Resi + SME + LE
Virtualized Option – B Series



** HeNBGW dimensioning is done without Qv-PC MME

Solution Architecture
SCS 4.1 – M-M 3G+LTE Large Enterprise
Virtualized Option – B Series



** HeNBGW dimensioning is done without Qv-PC MME

HNBGW Overview

Status vHetNet

- ✓ vHetNet desplegado en UCS-Blade de Claro ubicado en Torcuato
- ✓ Integrado con core Cs y Ps
- ✓ Integrado con MMEs
- ✓ Maqueta de USC 8K instalada en warehouse de Claro

Descripción

- 4 VMs desplegadas
  - AAA – Autenticación de los controllers
  - SecGW – Encargado de establecer tunel IPSEC contra los controllers
  - eRMS – Gestion de los controllers USC 8088
  - HNBGW-HeNBGW (starOS): GW de los controllers 3G(HNBGW) y 4G(HeNBGW) VM integrada al core de Claro

Principal features

- Direct tunnel HNBGW – GGSN
- Intelligent Paging
- IuFlex → Multiple MSS, SGSN, MME
- Full mobility: idle and connected-mode
- Virtualizado en HW genérico → Flexibility
- 3G/4G Support on same VM
- Multi-vendor

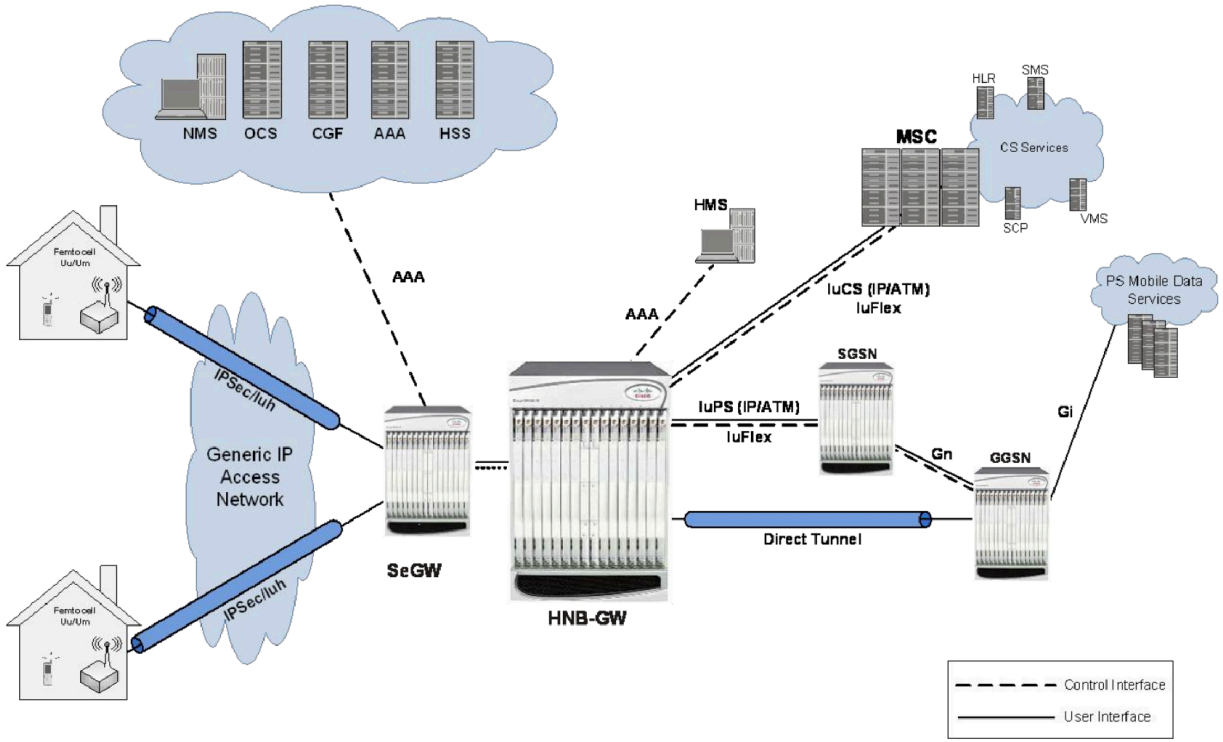
HNBGW

- The Home NodeB Gateway is the HNB network access concentrator used to connect the Home NodeBs (HNBs)/Femto Access Point (FAP) to access the UMTS network through HNB Access Network.
- Aggregates Home Node-B or Femto Access Points to a single network element and then integrates them into the Mobile Operators Voice, Data and Multimedia networks.
- The HNB-GW concentrates connections from a large amount of HNBs through IuH interface and terminates the connection to existing Core Networks (CS or PS) using standard Iu (IuCS or IuPS) interface.

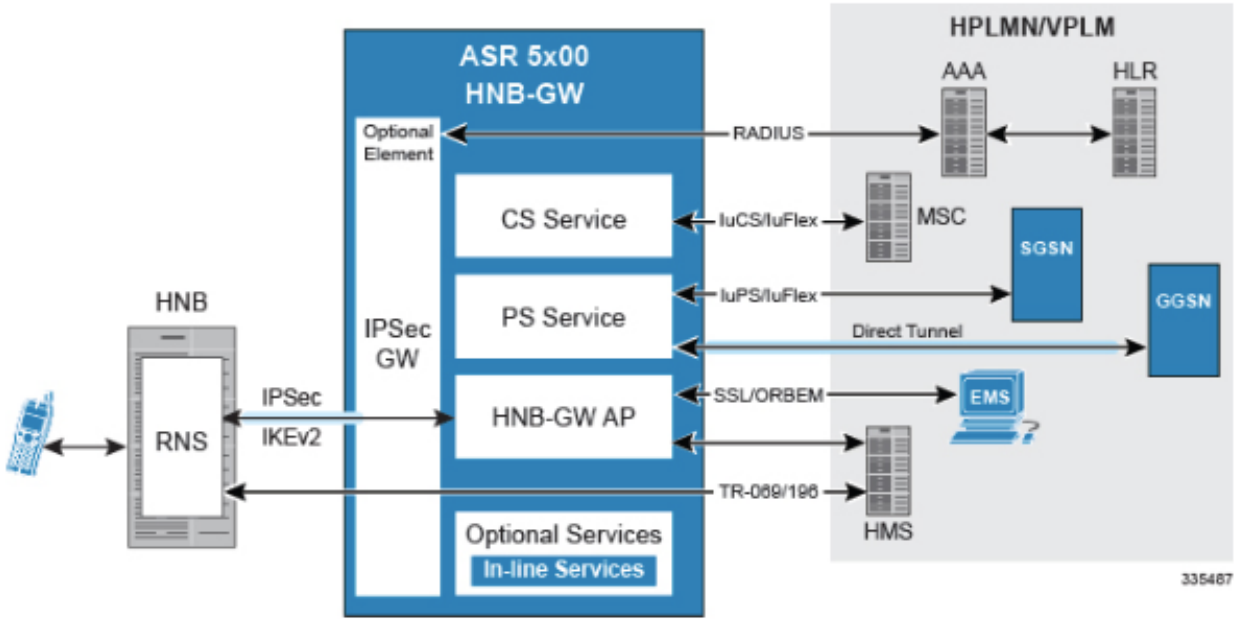
HNBGW

- In accordance with 3GPP standard, the HNB-GW provides following functions and procedures in UMTS core network:
- • HNB Registration/De-registration Function
  • UE Registration/De-registration Function for HNB • IuH User-plane Management Functions
  • IuH User-plan Transport Bearer Handling
- Iu Link Management Functions

HNBGW Architecture



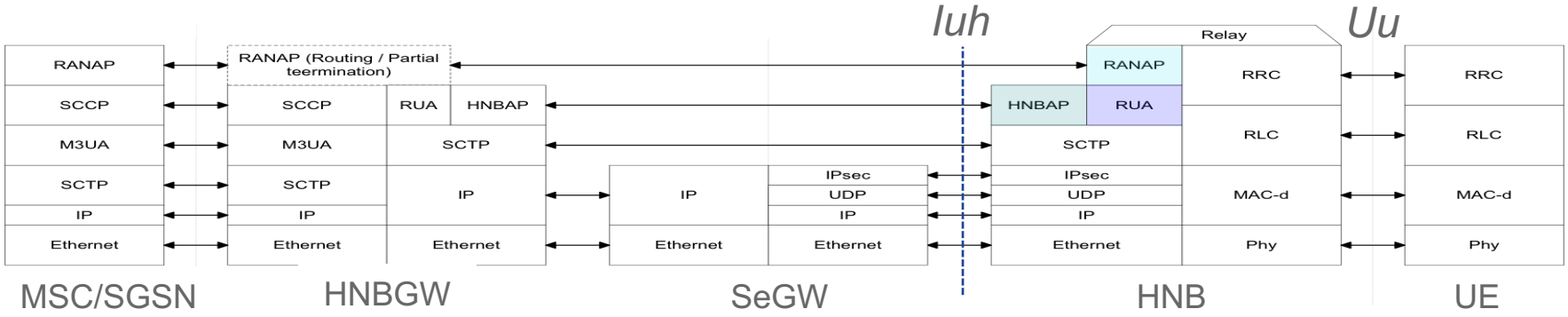
HNBGW – Interfaces & Services



Core Network Interface (Iu-CS/ Iu-PS)

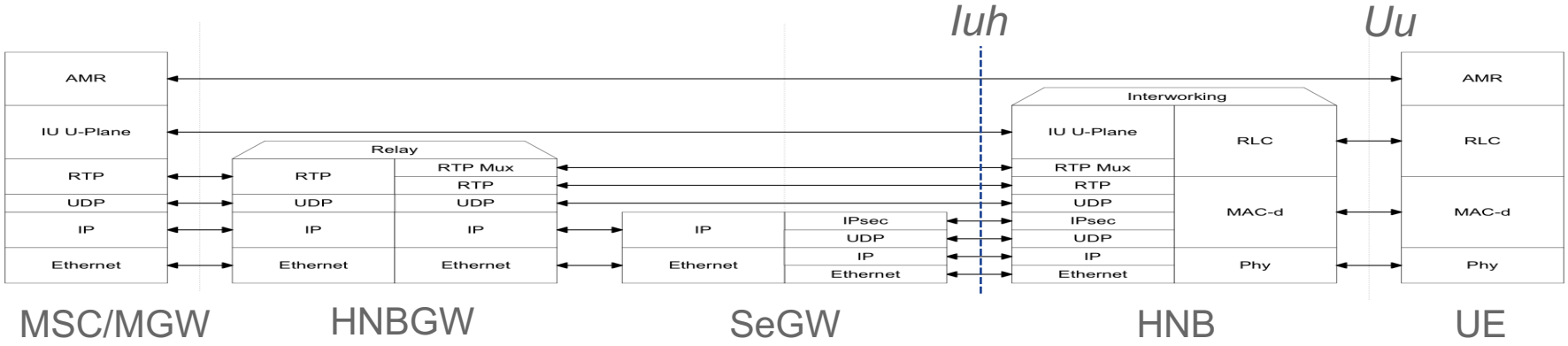
- RANAP (Radio Access Network Application Part) is used on the Iu interface to relay information between the 3GPP Radio Access Network (RAN) and the Core Network
- The communication is over IP, so SIGTRAN is the underlying protocol used to communicate between the end-points.
- The next couple of charts provide a view of the protocol stacks for control and user plane that can be used as a reference.

3G Iuh Architecture (Stacks – Control Plane)



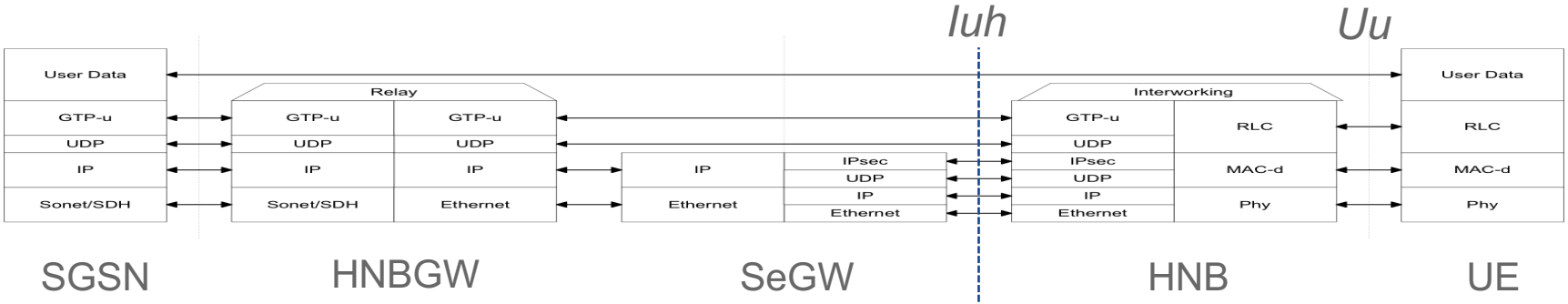
- Iu is defined in 3GPP specifications 25.410, 25.411, 25.412, 25.413, 25.414, 25.415, 25.419
- Iuh is defined in 3GPP specifications 25.467, 25.468, and 25.469
- Iuh is used to transport RANAP (Radio Access Network Application Part) signaling, CS user plane, and PS user plane traffic.
- RUA (RANAP User Adaptation – 3G TS 25.468) is an encapsulation of actual RANAP messages which the HNBGW does relay to the Core network
- HNBAP (HNB Application Part – 3G TS 25.469) terminated at the HNBGW and support a few messages related to HNB and UE registration
- In the Iuh architecture, the 3GAP (HNB) terminates RANAP (differs from the 3G macro where RANAP is on the RNC).
- *RANAP, HNBAP and RUA are good filters to use in Wireshark to see UE activity.*

3G Iuh Architecture (Stacks – CS User Plane)



- ASR5K – Provides the HNBGW (Home Node B Gateway) functions and the Security Gateway (SeGW) functions (IPSec termination)
  - In Claro Argentina project SecGW is external from starOS (StrongSwan running over Linux RedHat)
- SoftCore provides the MSC, HLR, VLR, AuC, and internal Media Gateway functions for subscriber validation/authentication, and voice call termination.
- Notice Real-time Transport Protocol (RTP) is used to carry the voice traffic. Configuration has RTP pools facing the AP (HNB) and Core network.

3G Iuh Architecture (Stacks – PS User Plane)



- ASR5K – Provides the HNBGW (Home Node B Gateway) functions and the Security Gateway (SeGW) functions (IPSec termination)
  - In Claro Argentina project SecGW is external from starOS (StrongSwan running over Linux RedHat)
- ASR5K – Provides the SGSN and GGSN for PS services (ie, terminates Iu-PS interface from HNBGW)
- GPRS Tunneling Protocol (GTP-U) is used to carry the user data within the PS domain.
- Direct Tunnel is established among HNBGW-GGSN

HeNBGW Overview

HeNBGW Introduction

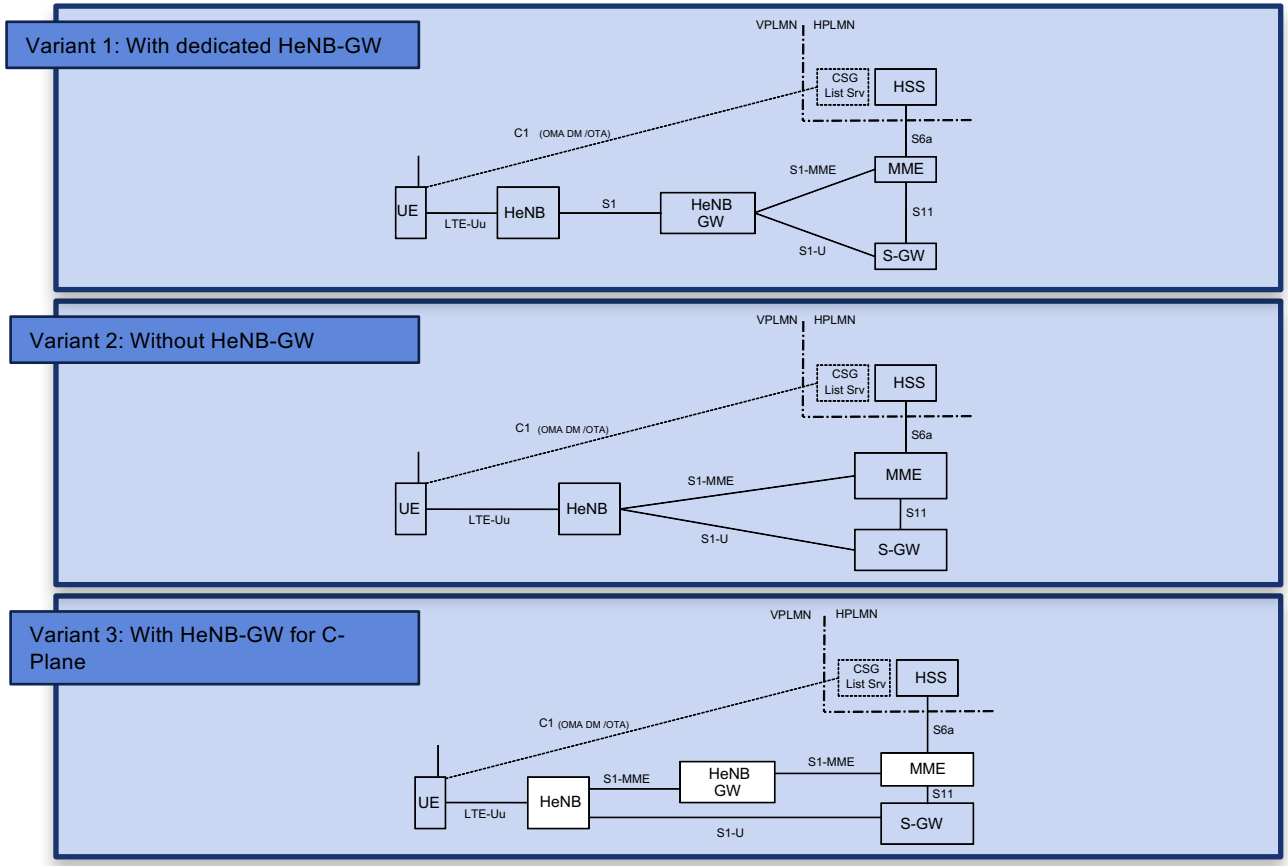
- The Home eNodeB Gateway works as a gateway for HeNBs to access the core networks. The HeNB-GW concentrates connections from a large amount of HeNBs through S1 interface and terminates the connection to existing Core Networks using standard interface.
- The Home eNodeB Gateway (HeNB-GW) has control capabilities necessary to manage large clusters of femtocells.
- It aggregates HeNBs or Femto Access Points (FAPs) to a single network element and then connects to Mobile Operators LTE core networks. The primary function of HeNB-GW is to enable simple, seamless, and highly secure access to subscribers as they roam between trusted/secure mobile networks and intrusted/insecure public networks.
- The HeNB-GW may optionally terminate the user plane towards the HeNB and towards the S-GW, and may provide a relay function for relaying User Plane data between the HeNB and the S-GW. The HeNB-GW supports NAS Node Selection Function (NNSF).

HeNBGW Functions

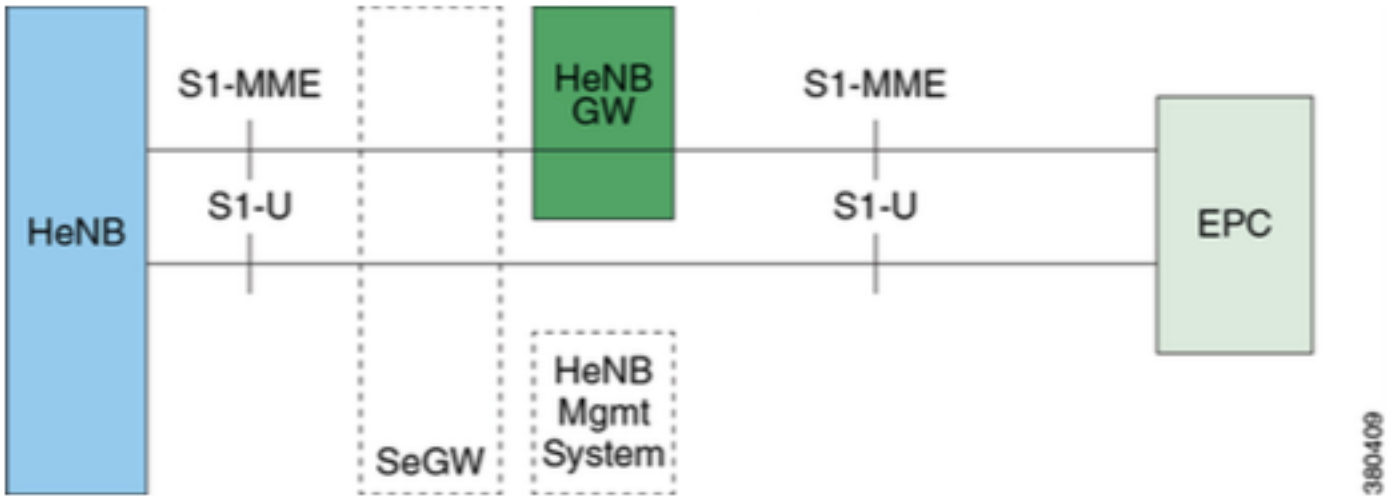
- An HeNB-GW provides standards-based S1-MME and S1-U network interfaces.
- The HeNB-GW appears to the MME as an eNodeB. The HeNB-GW appears to the HeNB as an MME.
- The S1 interface between HeNB and EPC whether the HeNB is connected to the CN/EPC via an HeNB-GW or not. The HeNB-GW connects to the EPC in a way that inbound and outbound mobility to cells served by the HeNB-GW does not necessarily require inter MME handovers.
- In accordance with 3GPP LTE standards, the HeNB-GW hosts the following functions and procedures in LTE core network:
  - Relaying UE-associated S1 application part messages between the MME serving the UE and the HeNB serving the UE.
  - Terminating non-UE associated S1 application part procedures towards the HeNB and towards the MME.
  - Optionally terminating S1-U interface with the HeNB and with the S-GW.
  - Supporting tracking area code (TAC) and PLMN ID used by the HeNB.
  - Allowing no X2 interface establishment between the HeNB-GW and other nodes.
  - Optionally performing paging optimization in case the Allowed closed subscriber group (CSG) List of the paged UE is included in the PAGING message.

HeNBGW Variants

HeNB-GW in 3GPP

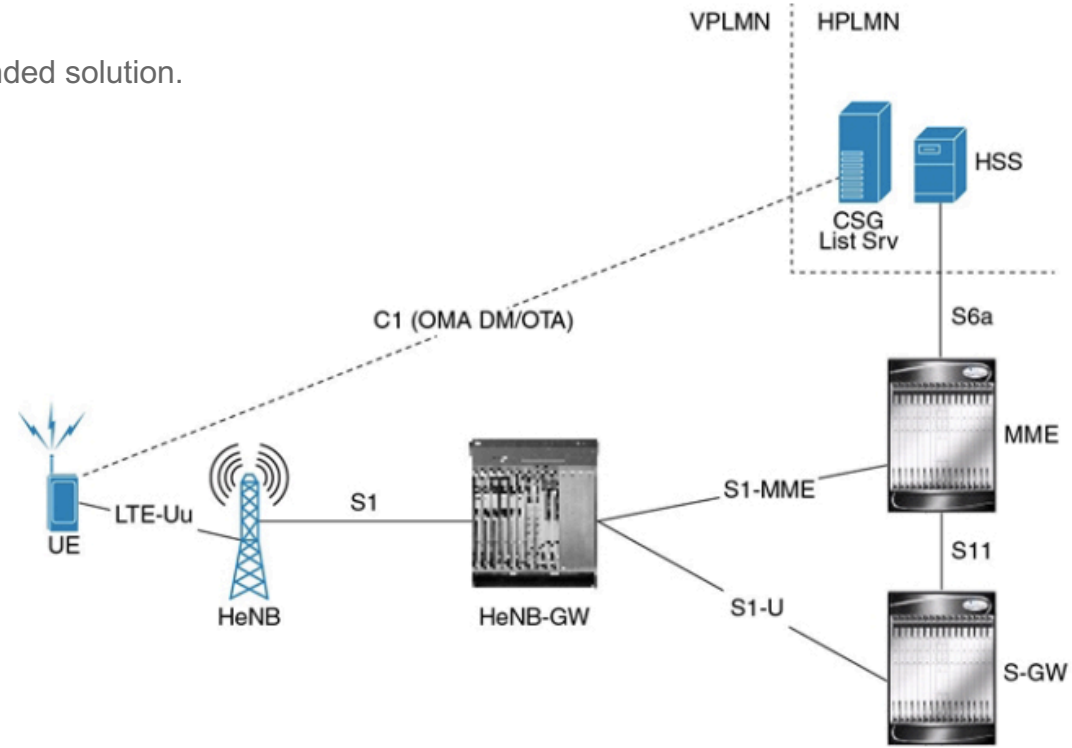


HeNBGW



HeNBGW – Variant 1

- SCS 4.1 Recommended solution.



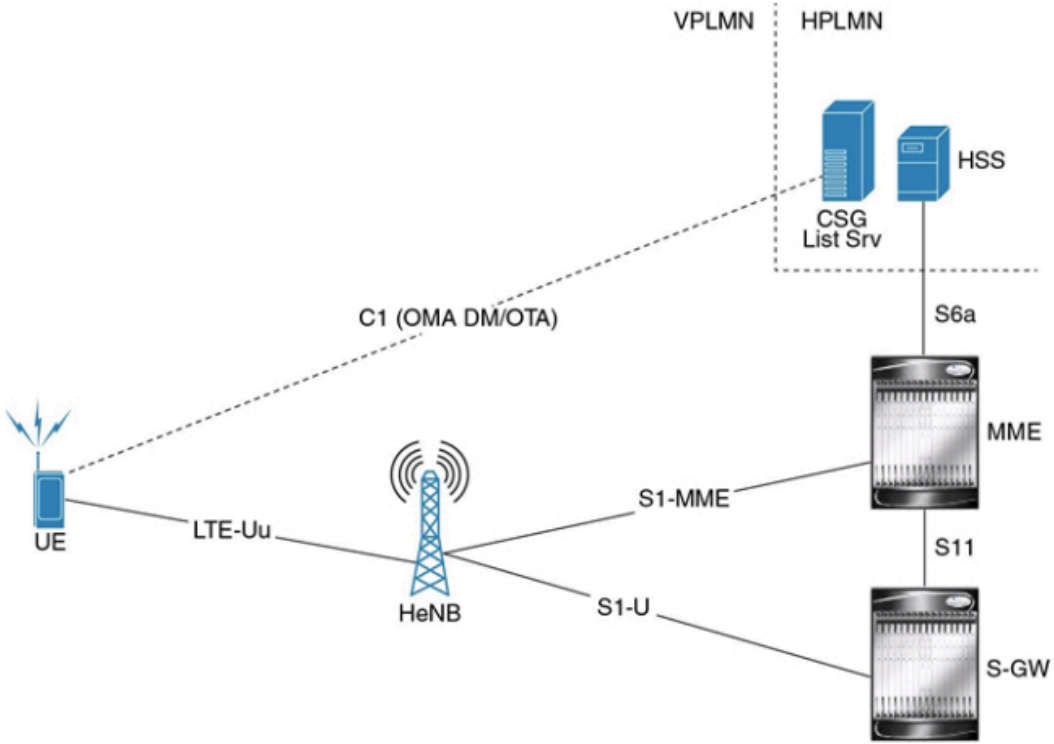
HeNBGW – Variant 1

- HeNB-GW serves as a concentrator for the C-Plane and also terminates the user plane towards the HeNB and towards the SGW (similar to 3G HNB architecture terminating both control and user plane in the Gateway)

- Provides benefits for the operators that already have a 3G HeNB solution and wish to migrate towards LTE HeNB.

- Actually deployed solution in Claro Argentina

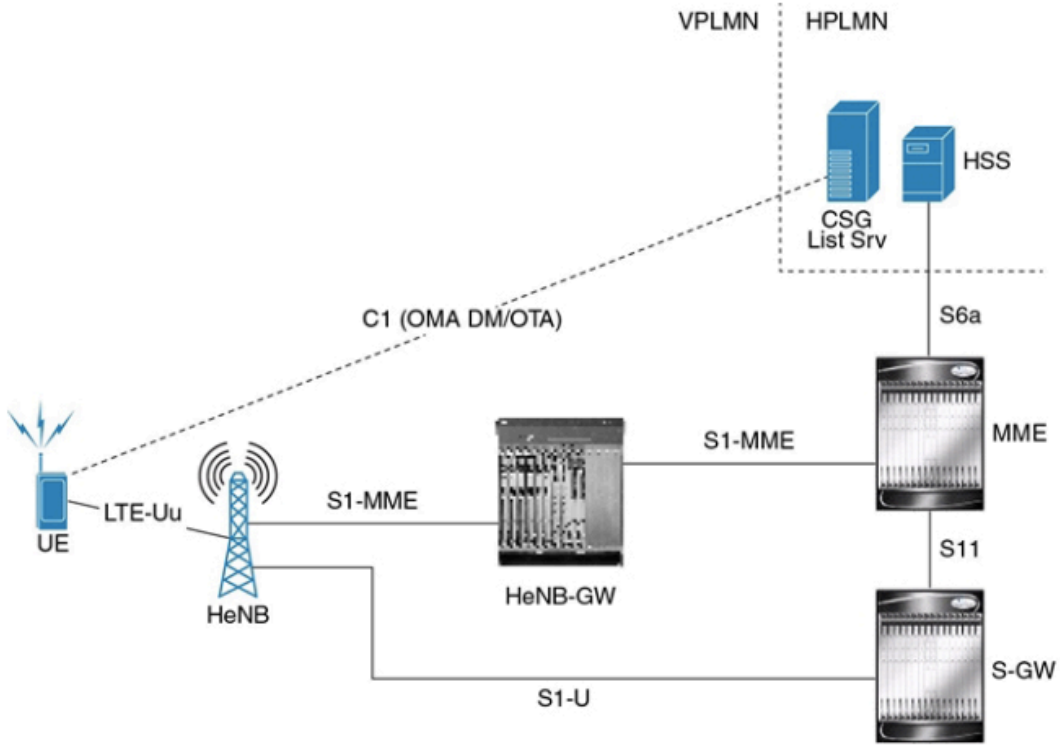
HeNBGW – Variant 2



HeNBGW – Variant 2

- The S1-U interface of HeNB is terminated in S-GW
- S1-MME interface in MME, as per eNB. The HeNB may have connection to multiple MME/S-GW, i.e. may support S1-flex.
- All HENBs are visible as a macro eNodeB in the EPC

HeNBGW – Variant 3



HeNBGW – Variant 3

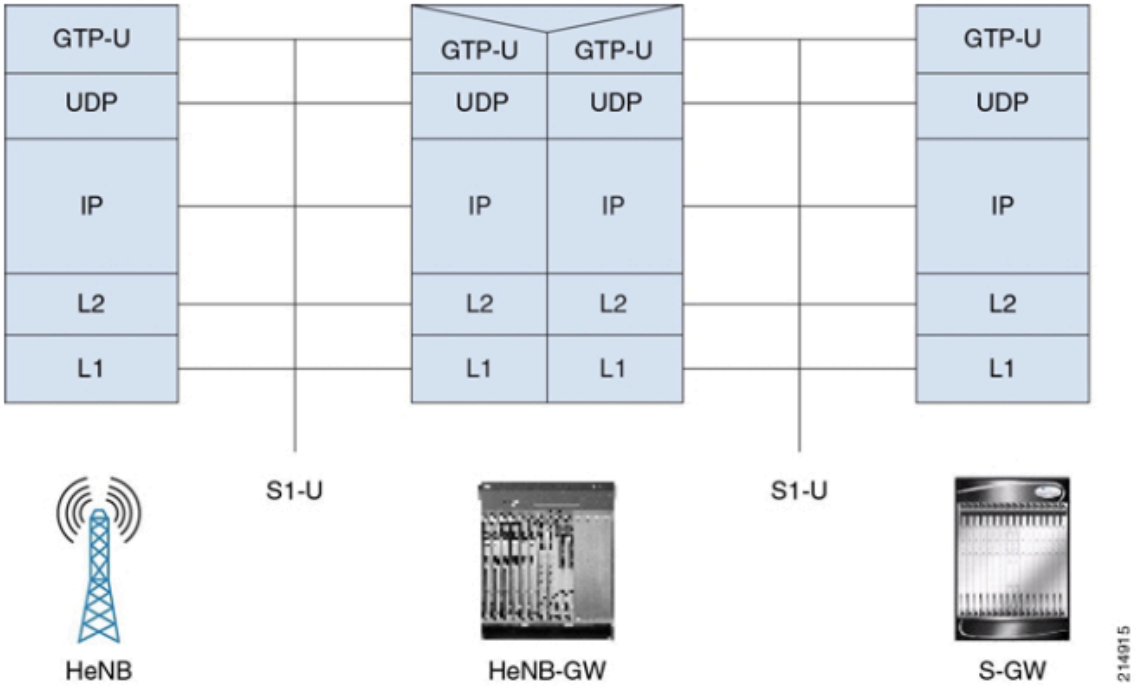
- HeNB-GW is deployed and serves as a concentrator for the C-Plane. The S1-U interface of HeNB is terminated in S-GW, as per eNB.
- A hybrid of variants 1 and 2
- Only 1 enodeBID visible in MME side (HeNBGW eNodeBId)
- Hidden the HENBs network

HeNB-GW in 3GPP

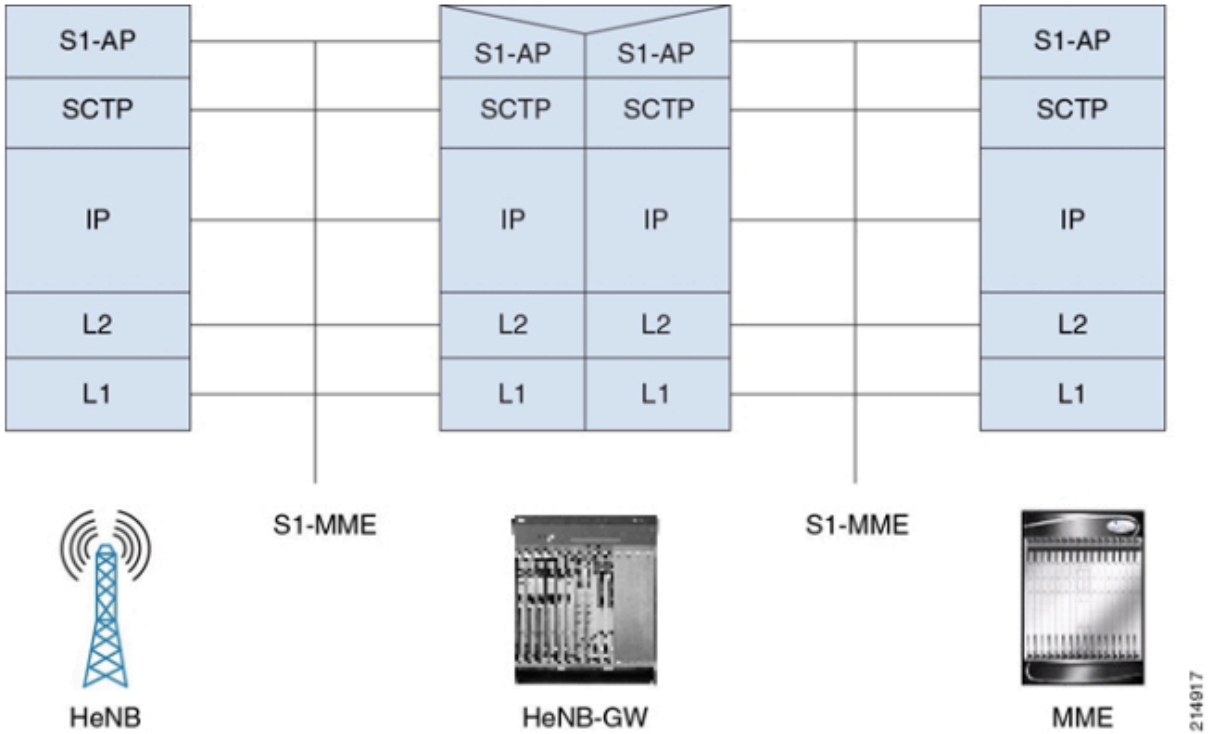
Comparison of architecture options

	Variant 1 (with HeNB GW)	Variant 2 (no HeNB GW)	Variant 3 (HeNB GW for control signaling)
Signaling overhead	Low	High	Low
No. of SCTP associations(MME load)	Small	Large	Small
SGW scalability (due to number of UDP/IP paths and GTP Echo messages)	Yes	No	No
Simpler implementation of HeNB (no need to support S1-Flex)	Yes	No	Yes
Secure architecture (ability to hide IP addresses of MME and SGW from home users)	Yes	No	Partial
Ability to offload SGW/PGW traffic (SIPTO) from the HNBGW (less need for a new network element)	Yes	No	No
Processing load due to GTP-tunnel switching at the HNB GW	High	N.A.	N.A.
Redundancy and load sharing possibilities	Low	High	Partial
Reduced Latency and system level processing	No	Yes	Partial
Need for dedicated MME/SGW for femto (and potential gateway relocations with macro-femto handovers)	No	Yes	Yes

HeNBGW Protocol Architectures S1-U



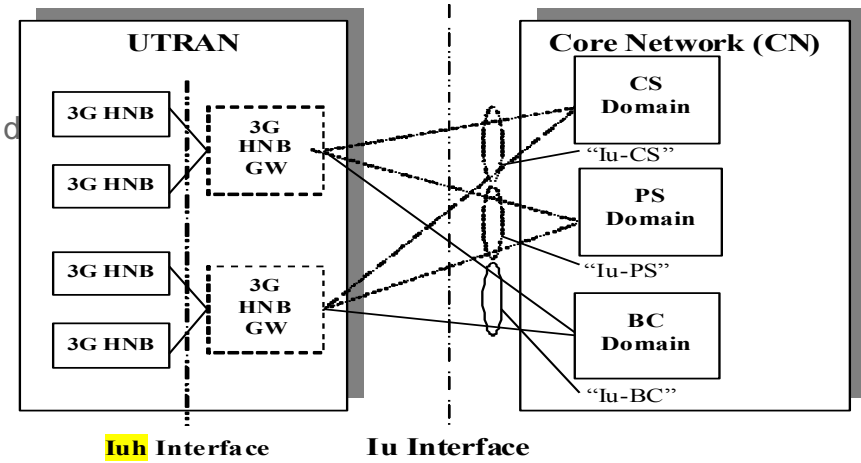
HeNBGW Protocol Architectures S1-MME



HNBGW 3GPP Releases

3GPP R8 Capabilities

- RAN-based achitecture (i.e. connecting to existing core network)
  - Iuh interface between HNB and HNB Gw (3G TS 25.467, 468, 469)
    - RTP for voice user plane (RTP multiplexing is included in R9)
    - GTP for data user plane
- Access control
  - Closed only based on Closed Subscriber Group definition
  - CSG Id is broadcasted by the HNB and part of user subscription d
- Mobility
  - Full idle mode mobility support (cell (re)selection
  - Hand-out only (femto to macro)
- Security
  - IPSec tunnel mode with IKEv2 for negotiation
  - X.509 based authentication (SIM based is optional)
- Provisioning
  - TR-069 based interface
- Management (3G TS 32.581, 582, 583, 584)
  - Standard configuration and performance management interface (XML based)



3GPP R9 & R10 focus

- HeNB architecture specification (3G TS 36.300)
  - RF aspects
  - Core Architecture (couple of options still in discussion, i.e. with or without HeNB gw)
- CSG concept finalisation
- Full Femto mobility
  - Hand-in and inter-femto (esp. Important for pico)
- Open/hybrid access mode specification
- Roaming support
- IMS-based femto architecture (postponed to R10)
  - Different options being discussed: IMS interworking in Femto or in core
- Local Breakout (postponed to R10)
  - Also know as LIPA (Local IP Access)
  - Mechanism to allow traffic to egress directly in the home environment
  - Likely to be based on local GGSN/PGW in the Femtocell

HNBGW GW

IuH Interface

- Release 9 Compliance
  - TS 25.467 3G HNB
- Architecture
- Functional Elements
  - TS 25.468 RUA
- SCTP Reliable Transfer of RANAP
  - TS 25.469 HNBAP
- HNB Registration/De-Registration
- UE Registration/De-Registration

HNBGW GW
IuCS Interface

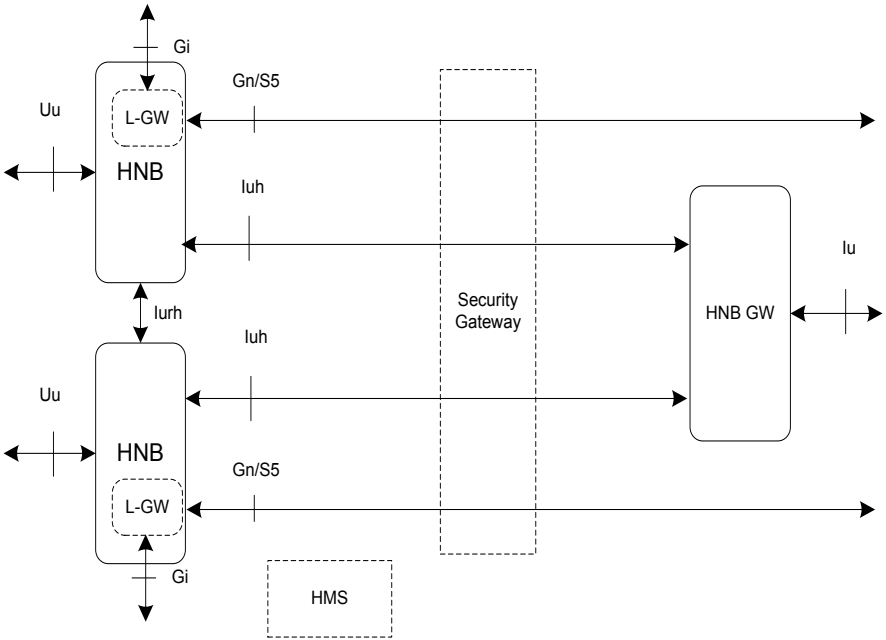
- Interfaces
  - TS 25.410 Iu Interface
  - TS 25.412 Iu Signalling Transport
  - TS 25.413 Iu RANAP Signalling
  - TS 25.414 Iu User Plane Transport & Signalling
  - TS 23.236 IuFlex
- ATM as transport media
  - Connections at OLC card

HNB-GW
IuPS Interface

- Interfaces
  - TS 25.410 Iu Interface
  - TS 25.412 Iu Signalling Transport
  - TS 25.413 Iu RANAP Signalling
  - TS 25.414 Iu User Plane Transport & Signalling
  - TS 23.060 Direct Tunnel, Gn, Gi
  - TS 23.236 IuFlex

3G HNB Reference Architecture

Refer to TS 25.467 (R10)

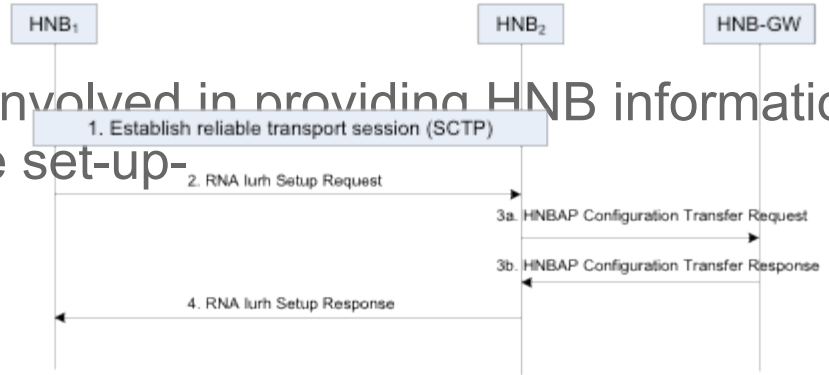


- RAN-based achitecture
  - i.e. connecting to existing 3G core network
- Multiple access control modes
  - Closed, Open, Hybrid
- Mobility
  - Full idle mode mobility support (cell (re)selection
  - Active mode mobility defined over three releases (see following slide)
- Local Breakout (LIPA/SIPTO)
  - Still under definition
- Security (38.200)
  - IPSec tunnel mode with IKEv2 for negotiation
  - X.509 based authentication (SIM based is optional and is complementary to certificate based authentication)
- Provisioning
  - TR-069 based interface
- Management (3G TS 32.581, 582, 583, 584)
  - Standard configuration and performance management interface(XML based)

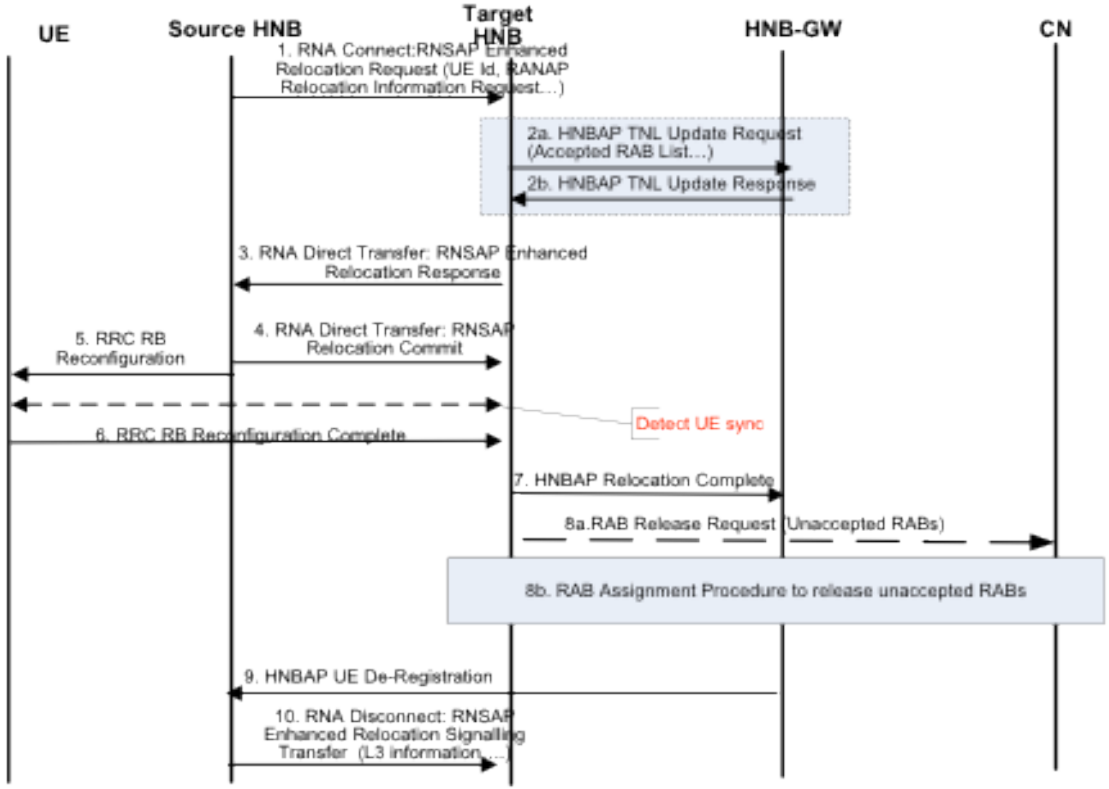
65

Iurh Interface

- two different Iurh connectivity options:
  - Direct Iurh connectivity between HNBs
  - Iurh connectivity via HNBGW serving Iurh proxy. HNBGW is transparent to RNSAP
- HNBGW involved in providing HNB information (similar as LTE X2 procedure set-up-

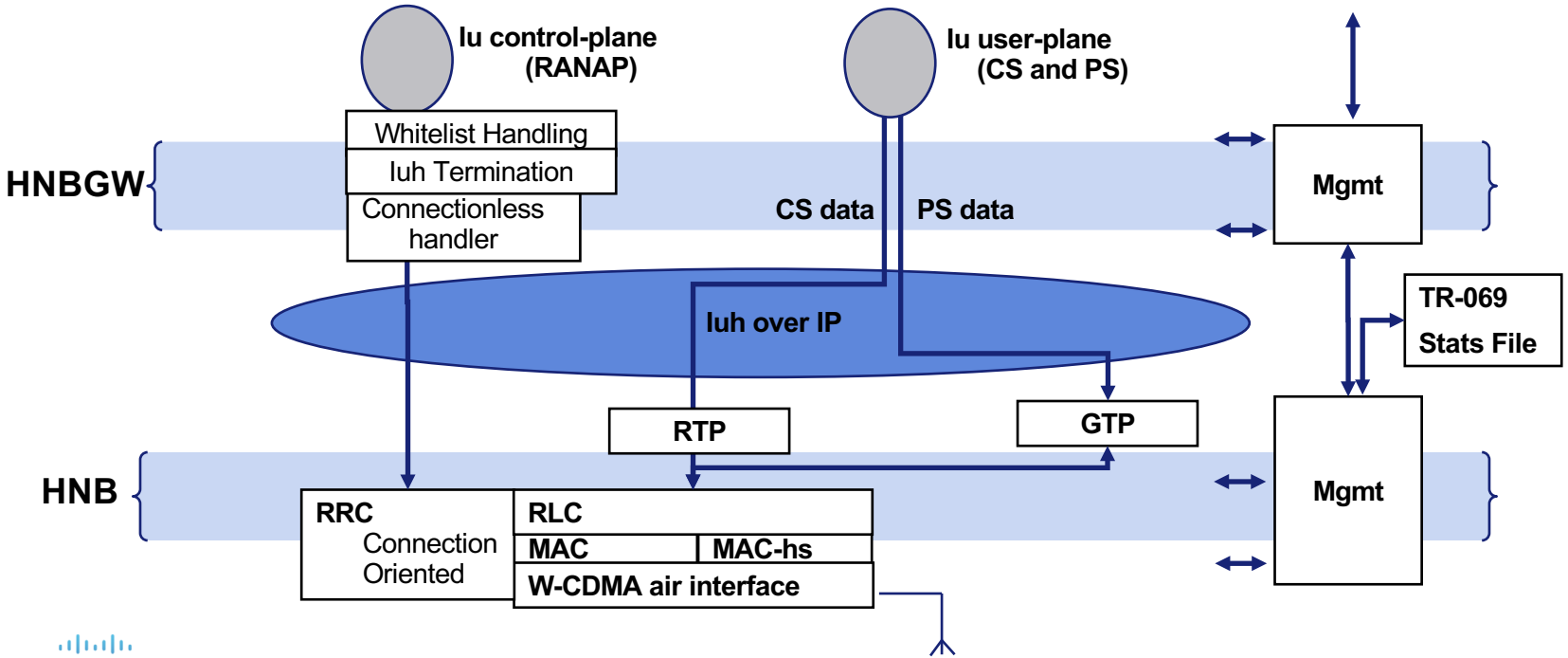


Iurh Mobility – direct HNB to HNB



3G Femtocell Functional Split

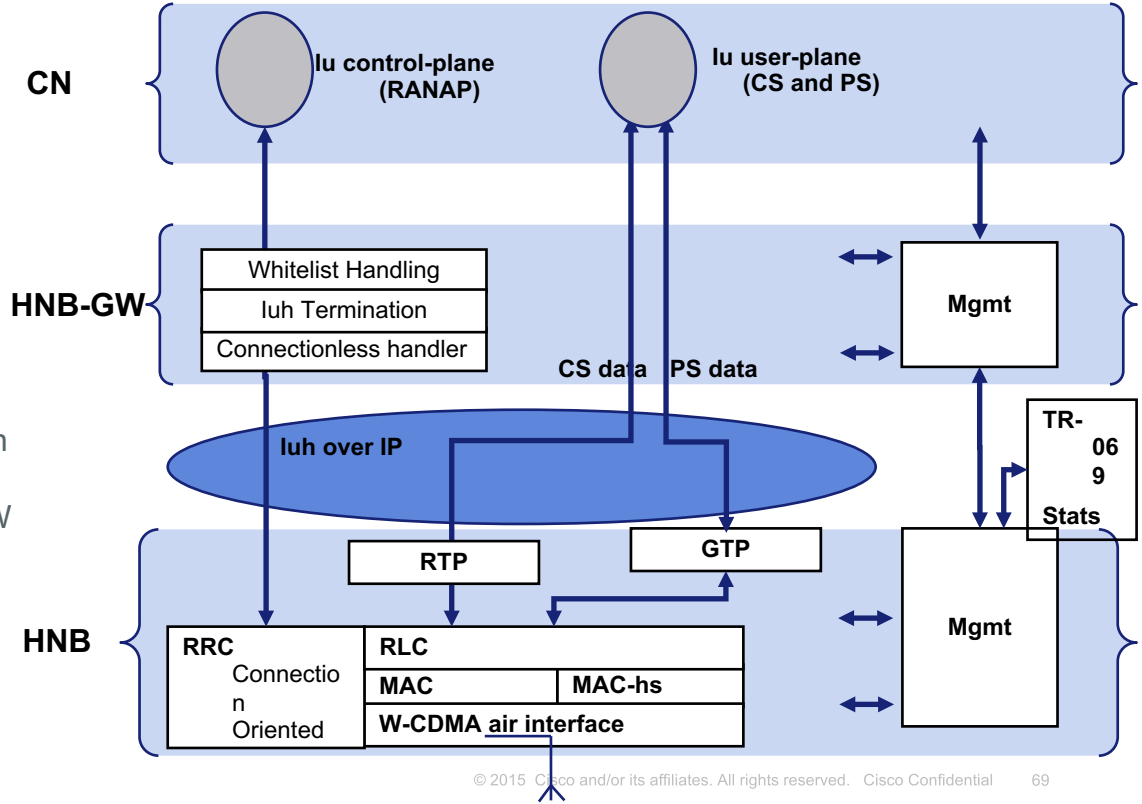
- Most 3G RNC functions are moved to the HNB
- HNBGW supports
  - HNB Aggregation (optionally includes SeGW)
  - Connectionless distribution (Paging, Hand-in filtering)
  - Iuh termination



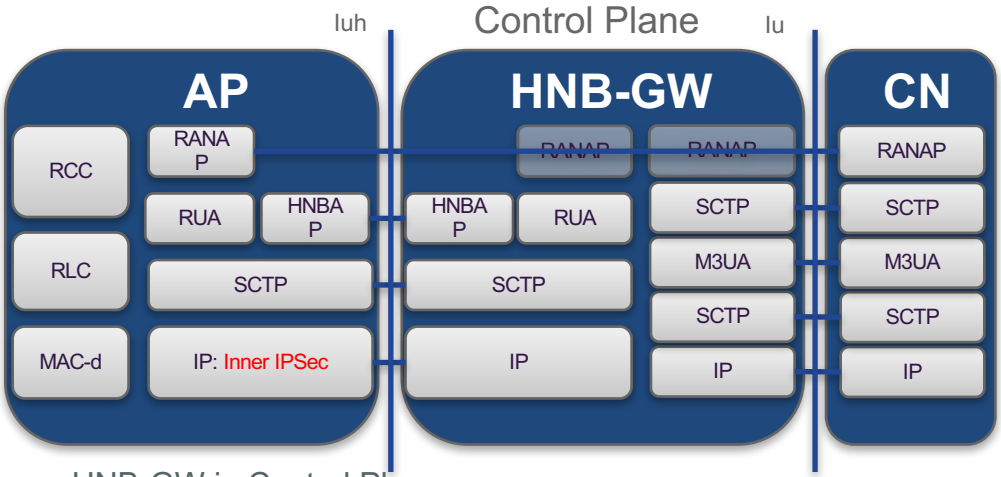
3GPP Reference Architecture (TS 25.467)

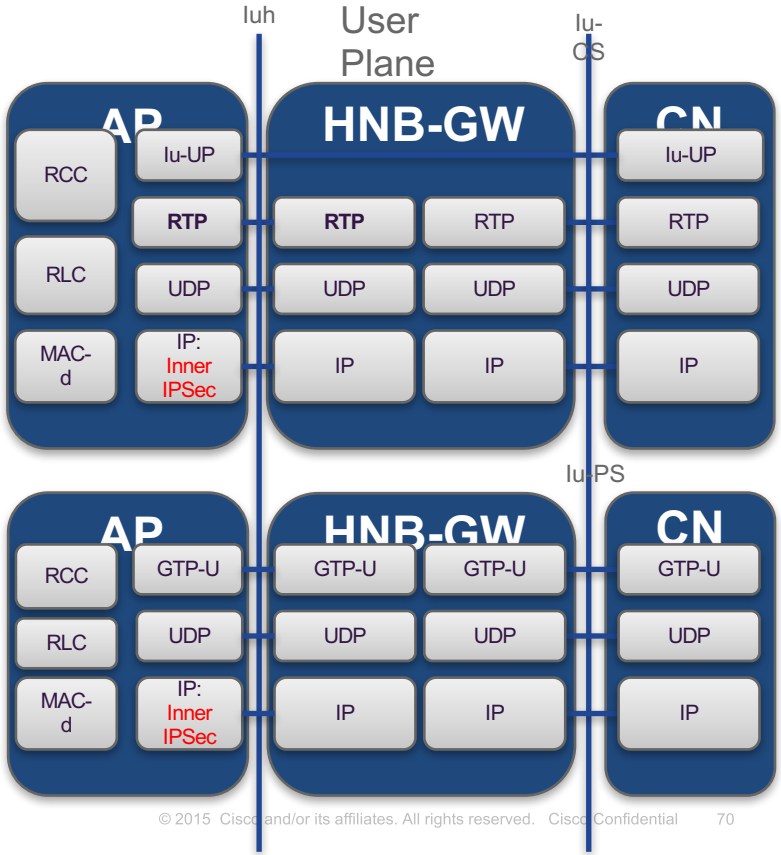
- 3GPP Femto Architecture GOALS:
  - MUST NOT impact Core Network (CN)
  - Transport over Public Internet MUST be possible
  - SUPPORT for access multivendor ecosystem

- HNB-GW appears as to CN as an RNC and serves as concentrator of HNB connections:
  - terminates Iuh from HNB
  - supports HNB and UE registration over Iuh
  - connectionless distribution (Paging, Hand-in filtering)
  - may terminate TNL for the Iurh via HNB-GW
- SecGW is defined as separate function that can be collocated with the HNB-GW:
  - authenticate HNB
  - terminate secure tunnelling for TR-069 and Iuh
- HNB incorporates most of RNC functions



HNB-GW impact in Control and User Plane



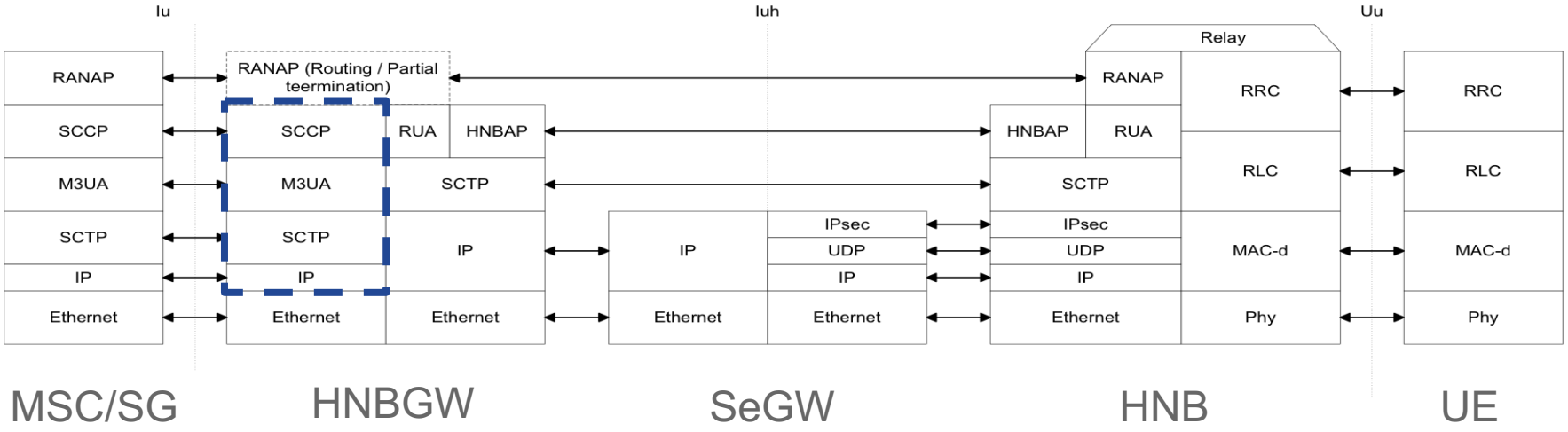


- HNB-GW in Control Plane:
  - Includes the HNBAP to control the AP and the RUA
  - RANAP is partially terminated in the HNB-GW and routed
- HNB-GW in User Plane:
  - It is completely transparent to the user data layer (not depicted in the diagram)
  - For RTP provides multiplexing capabilities that also need to be supported by the AP

Iub vs Iuh Comparison

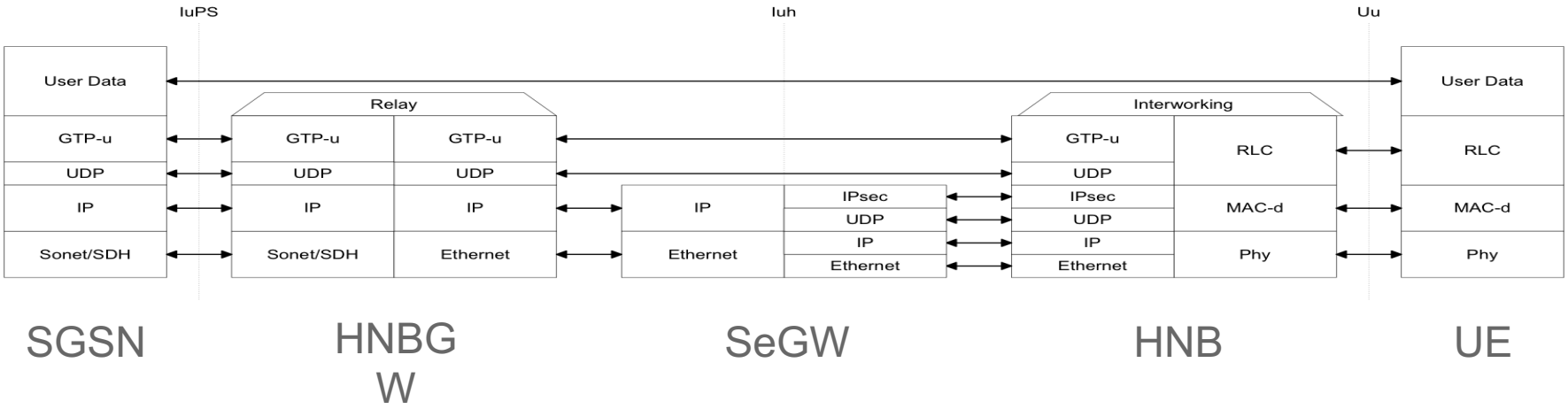
	Iub		Iuh	
Open Standard/IOT	✗	Although defined in standards, Iub is mostly proprietary hence forcing to work with macro vendor	✓	Fully standardised (Iuh/Iurh) Proven interoperability in plugfest
Backhaul tolerance	?	Split control between RNC/NodeB requires reliable backhaul	✓	Designed to work over unreliable transport (e.g. internet)
Scaling	?	Existing macro RNC can not scale beyond 100s of NodeBs; possibly requires new solution	✓	Designed to scale to 100ks of HNB based on HNBGW function
Security	✗	Relying on existing standard, nothing specific to for rogue NodeB detection and tampering	✓	E2E IPSec encryption with certificate and optionally SIM based authentication
SON/Interference/Load Balancing	✓	Can leverage existing capabilities available in the macro network	?	Requires new capabilities for self install, interference control and load balancing
Mobility	✓	Full idle and active mobility supported including Soft Handover	?	Hand-in and SC2SC requires advanced features; hard handover only
OAM/KPI integration	✓	Integration with macro allows to reuse existing KPI and OAM procedure	✗	New solution to be put in place for small cells
LTE readiness	?	Depends on actual evolution/roadmap of small cells	✓	Major parts of the architecture can be reused for LTE support
Architecture Flexibility	✗	3G only architecture	✓	Architecture allows network sharing and can integrate non-3GPP access

3G HNB Protocol Stack – Control Plane



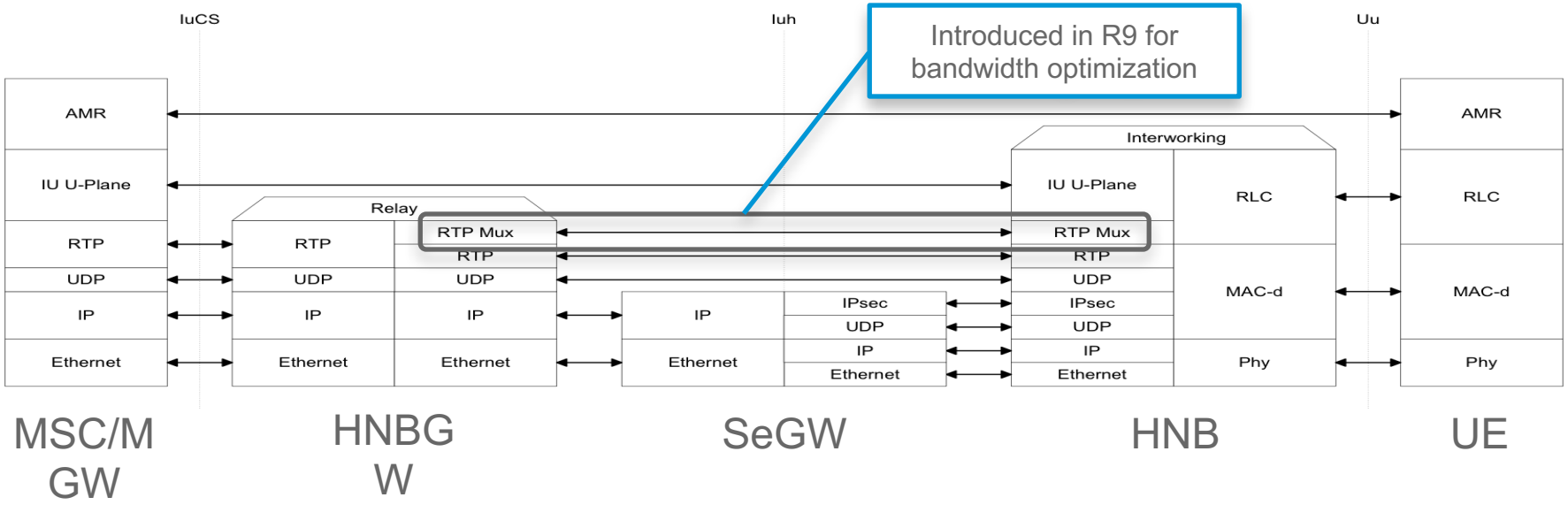
- RUA (RANAP User Adaptation – 3G TS 25.468) is a simple encapsulation of actual RANAP messages which the HNBGW does relay to the Core network
- HNBAP (HNB Application Part – 3G TS 25.469) terminated at the HNBGW and support a few messages related to HNB and UE registration
- Note there is no equivalent of Iuh in the LTE small cells architecture

3G HNB Protocol Stack – PS Bearer Plane



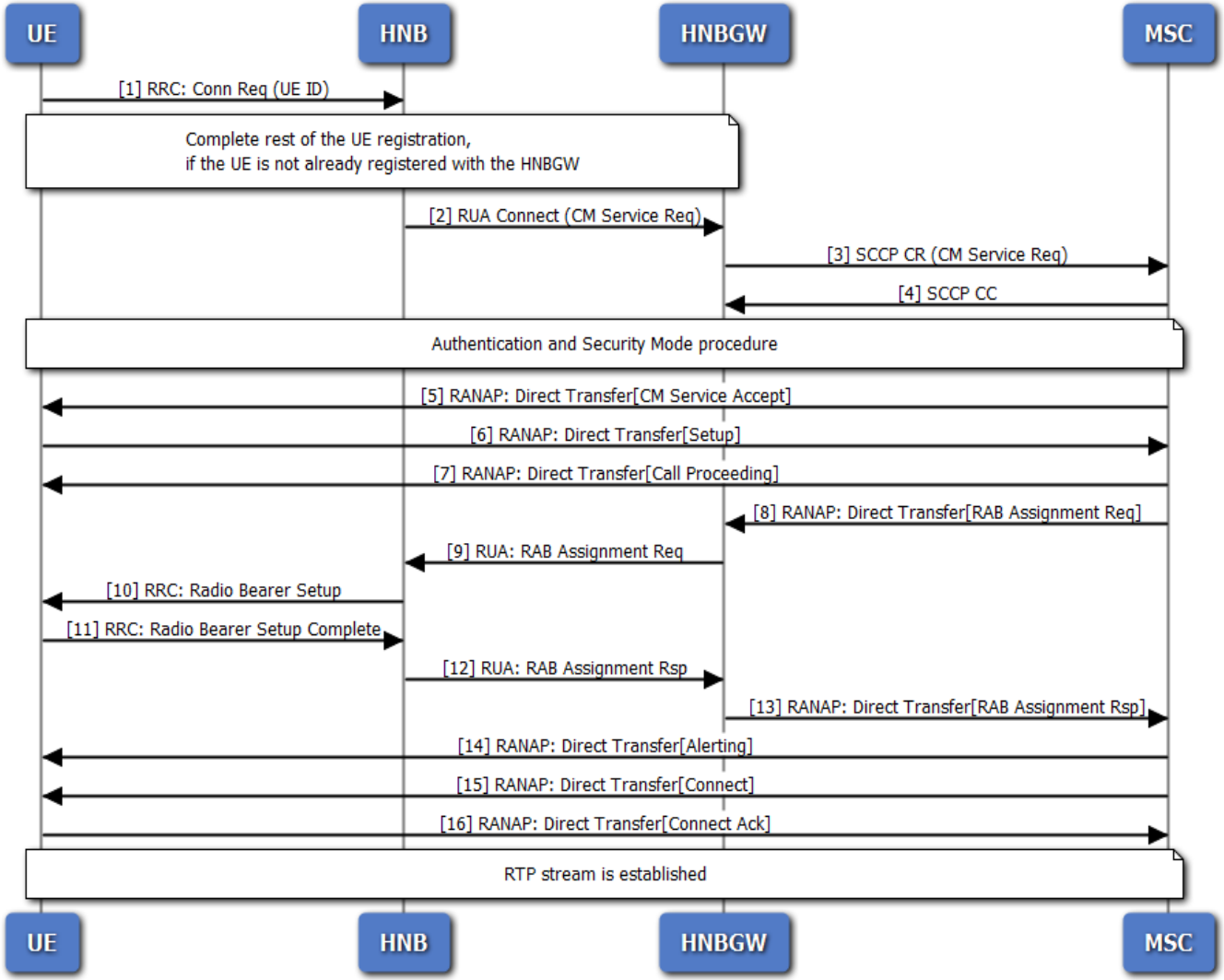
- Note GTP-u is initiated from the HNB
- Direct Tunnel can be supported with the HNBGW directly connecting to the GGSN for the PS bearer plane

3G HNB Protocol Stack – CS Bearer Plane

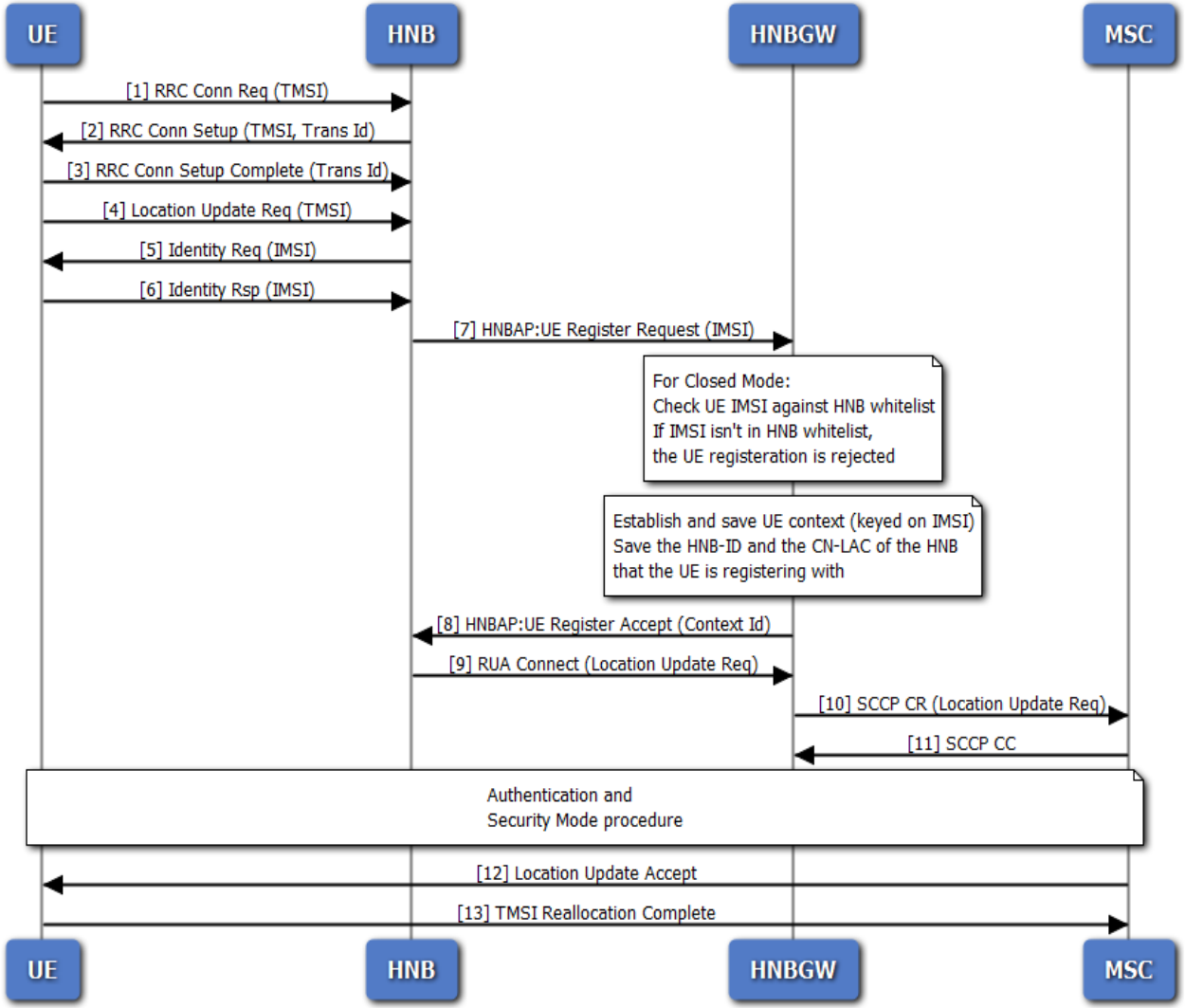


- HNB acting as RTP/RTCP proxy rewriting specific RTP parameters (e.g. sequence number)
- RTP Mux introduced in 3GPP R9 for further bandwidth optimization on the Iuh

HNB Originated CS Call Flow



UE Registration Call Flow



Features & Capabilities

IuFlex with CN

- Iu-Flex is the routing functionality for intra domain connection of HNB-GW nodes to multiple CN nodes (MSC/SGSN).
- It provides a routing mechanism and related functionality on HNB-GW to enable it to route information of different Core Network (CN) nodes with in the CS or PS domain
- Support up to 3GPP rel. 9
- HNB-GW supports Iu-Flex routing mechanism and other applications like many-to-many relation and load-sharing between CN nodes with HNB-GW and CN node pooling.

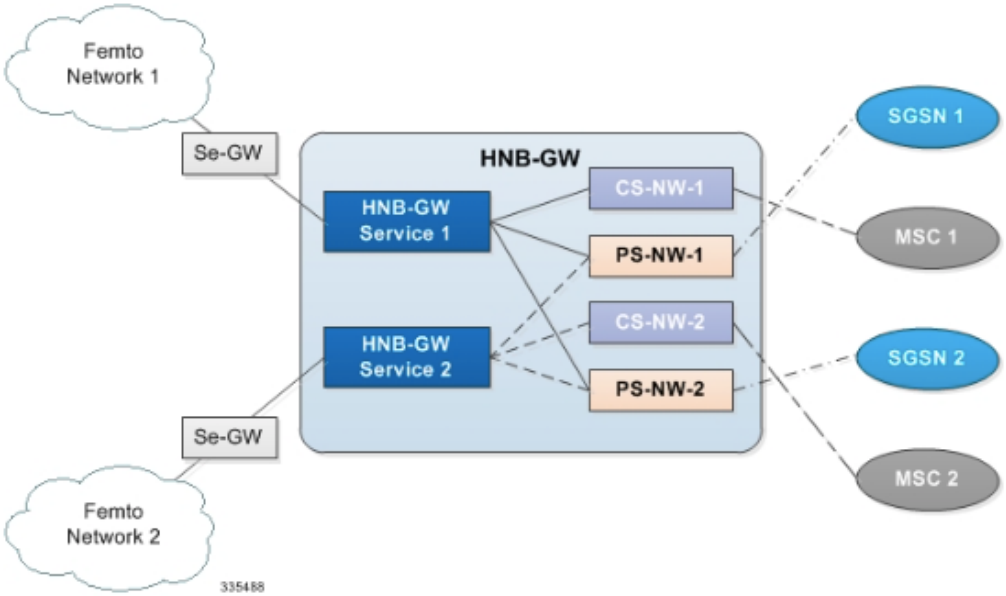
IuFlex Benefits

- Eliminates the single point of failure between an RNC/HNB-GW and a CN Node.
- Ensures geographical redundancy, as a pool can be distributed across sites.
- Minimizes subscriber impact during service, maintenance, or node additions or replacements.
- Increases overall capacity via load sharing across the MSCs/SGSNs in a pool.
- Reduces the need/frequency for inter-CN node RAUs. This substantially reduces signaling load and data transfer delays.
- Supports load redistribution with the MSC/SGSN offloading procedure

Multiple HNBGW Service Support

- A unique logical RNC represents each CS/PS network on chassis and is assigned an RNC-ID as global RNC id.
- When RUA Connect Request is received at HNB-GW, CS/PS network is selected based on values of mcc, mnc and rnc-id configured in radio network plmn of HNB-GW service and in CS/PS network.
- Multiple HNB-GW services in the same context can share the same RTP Pool
- Single GTP-U Service cannot be shared among multiple HNB-GW Services
- multiple PS networks cannot share a single GTP-U service but multiple CS networks can share the same RTP Pool and ALCAP Service.

Multiple HNBGW Service Support Architecture



Multiple MSC Selection without Iu-Flex

- HNBGW can connect to multiple MSC and SGSN through Iu-Flex or LAC mapping. This feature implements the multiple MSC selection using LAC.
- For this support the HNB-GW uses HNB's LAC, received during registration procedure in HNB_REGISTER_REQUEST message, to distribute RANAP-Initial UE message to an MSC. It maps the LAC with MSC point code and a set of LACs configured for each MSC, connected to the HNB-GW.
- In the HNBGW, to select an MSC based on the LAC the following algorithm is used:
  - If both Iu-Flex and LACs are configured for a MSC, then Iu-Flex is used to select a MSC.
  - If only Iu-Flex is configured then Iu-Flex is used for selecting MSC.
  - If only LACs are configured then MSC is selected using LAC from HNB.
  - If both Iu-Flex and LACs are not configured in the HNBGW, it selects default MSC.

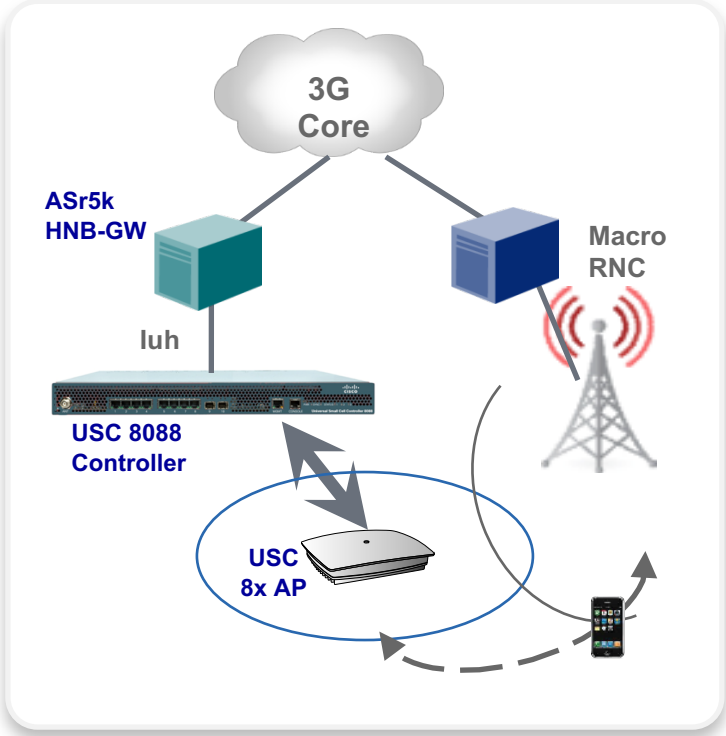
Handovers to/from 3G/2G Macro

Hand-out

- Enabled through SON neighbor list discovery
- Intra-frequency or inter-frequency hard handover from USC8x to 3G macro cell
- Inter-RAT hard handover from USC8x to GSM

Hand-in

- Intra-frequency or inter-frequency hard handover from 3G macro cell to USC8x
- Ingress PSC allocated per USC8x deployment on neighboring macro cells
- ASR5k HNB-GW forwards Hand-In requests to target USC8x



3G HNB Mobility Procedures

- Mobility Requirements
  - Active mode handover (Hand-out (femto to macro), Hand-in (macro to femto), Femto-to-Femto)
  - Hard Handover vs Soft Handover

3GPP Release	R8	R9	R10
Idle Mode reselection	Supportd(1)	Supported	Supported
Hand-out (SC to Macro)	Supported(1)	Supported	Supported
Hand-in (Macro to SC)	Can be Supported(2)	Supported(3)	Supported
SC to SC	Via CN(4)	Via CN(4)	Supported(5)

Notes:

(1) Supported based on existing 3GPP procedures, i.e. no specific mechanism required for small cells

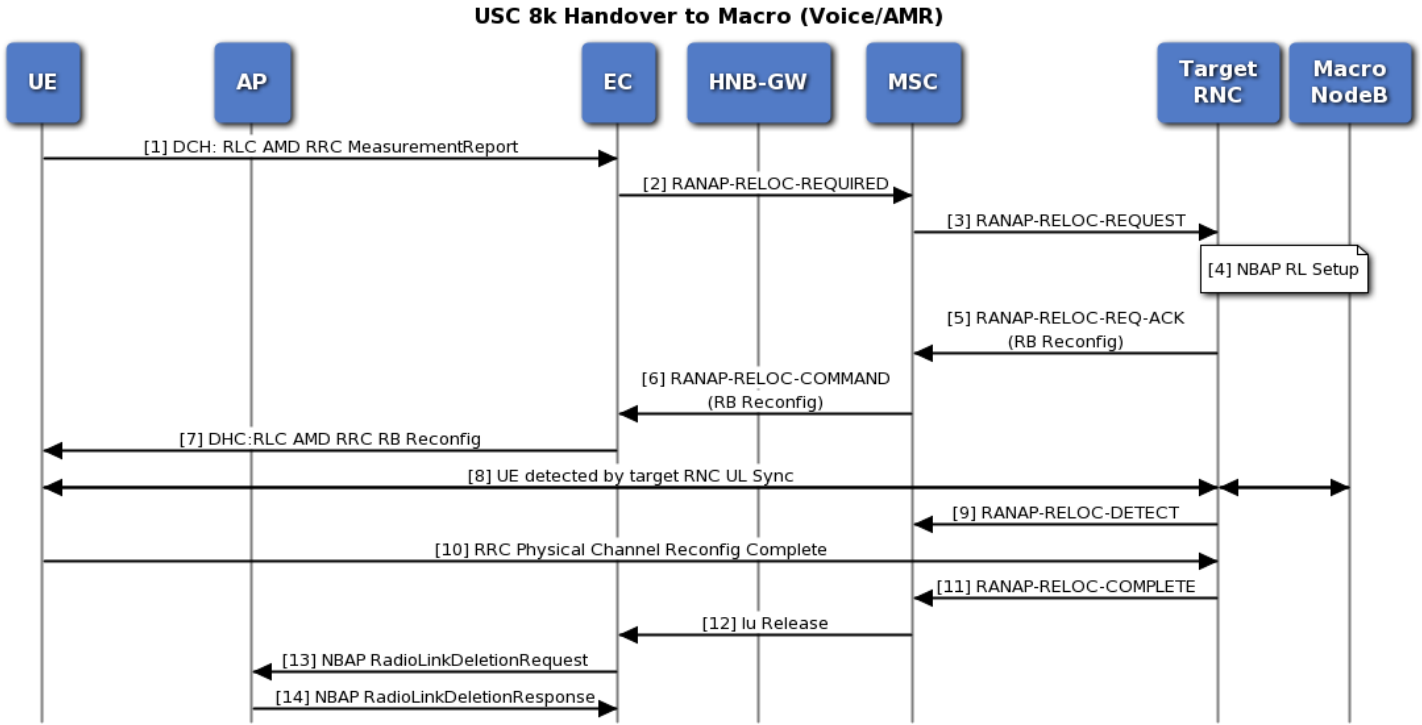
(2) Can leverage existing procedure if the small cells PSC is added as part of the macro neighbour cell list. If not, it requires PSC disambiguation capabilities in the network (e.g. IMSI filtering, time difference, relocation forking, etc.)

(3) Standard procedure introduce in 3GPP R9 requires UE to report actual Cell Id instead of PSC only; note this requires UE and macro UTRAN upgrade

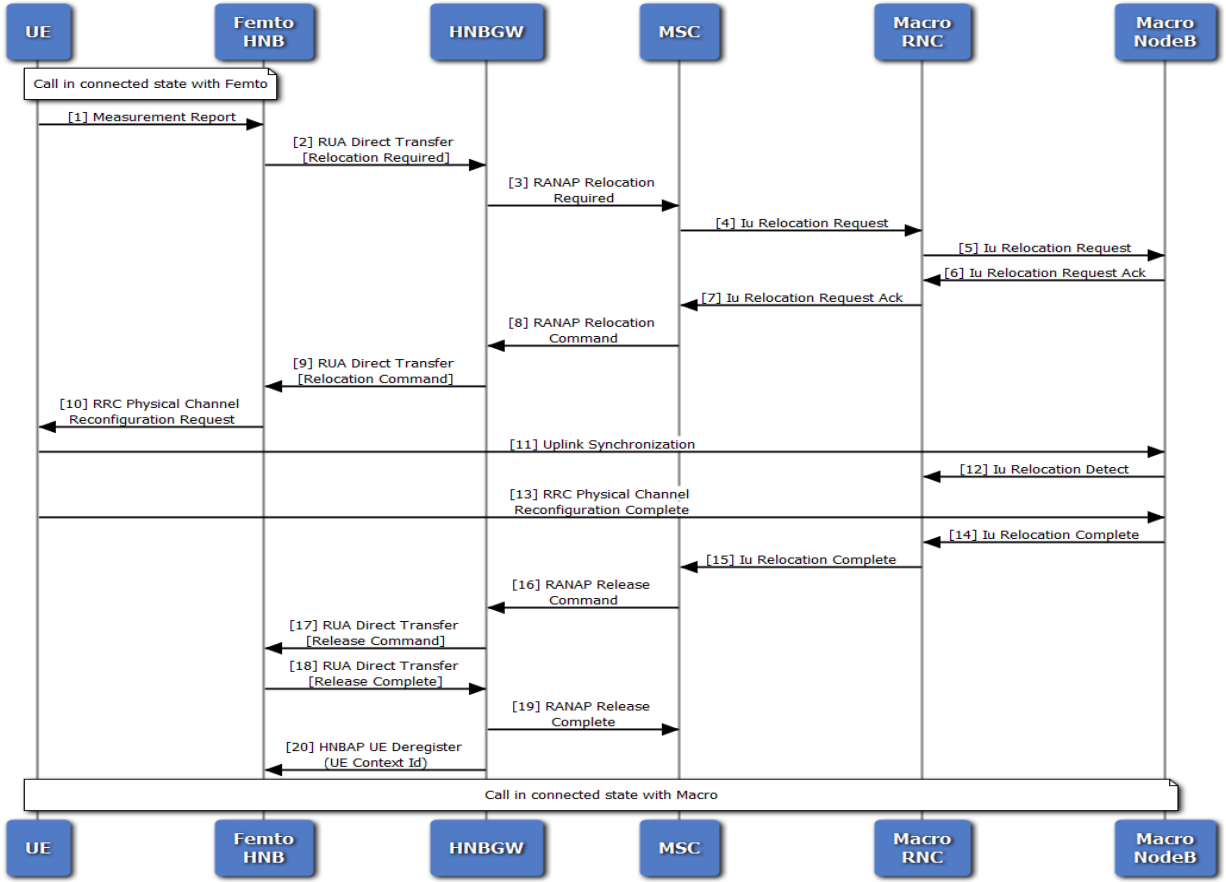
(4) Small Cells to Small Cells handover can be supported via CN based on populated Neighbour Cell List

(5) Iurh is introduced for direct SC to SC handover, i.e. preserving core network from signalling

Handout to Macro Call Flow



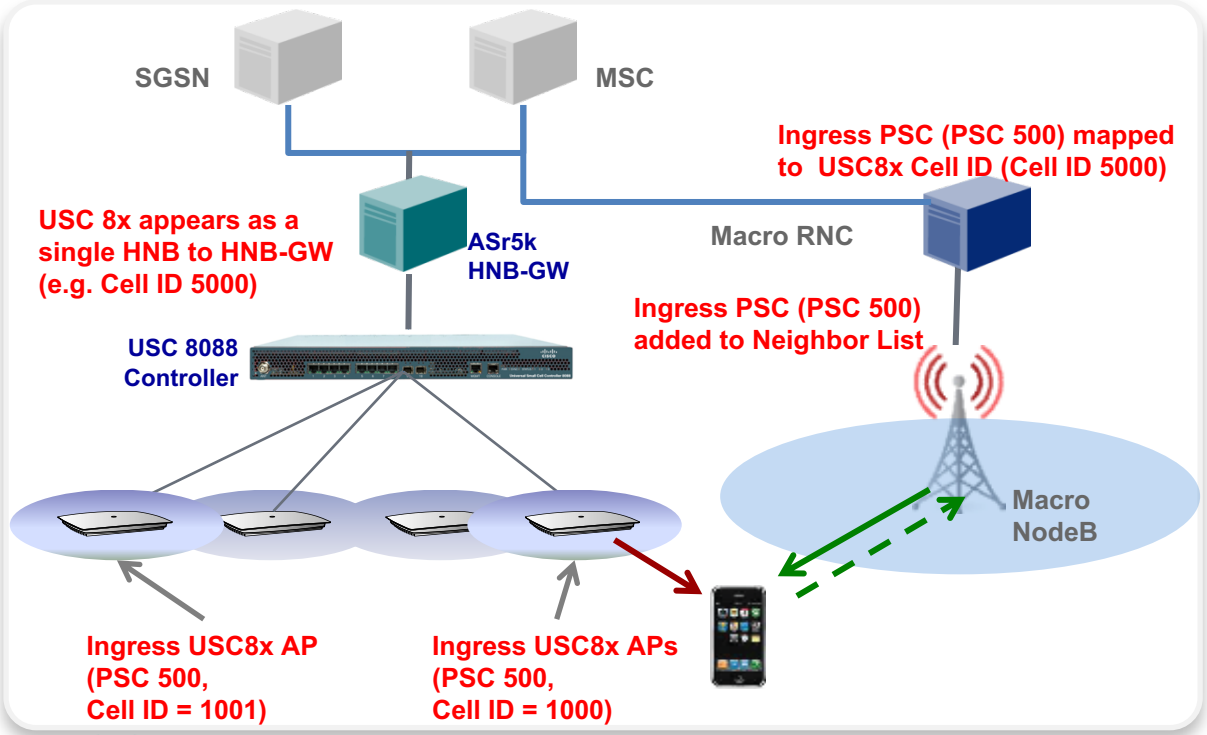
SC to Macro CS HO



Macro to Small Cell Hand-in

- Supported, but limited by Macro neighbor list size
- Known 3GPP limitations
- UEs don’t report Cell ID in 3G Measurement Reports
- Macro has to have unique Target Cell ID
- Forced to determine Target Cell based on Frequency and PSC/PCI
- Limited number of entries in Macro neighbor list
- No M2F if Multiple Small Cells share PSC/PCI within Macro sector
- Similar problem in 3G and LTE

CS Hand-in:
No change on HNB-GW and Macro Network



- UE sends a message with PSC=500 (hand-in PSC)
- Macro RNC refers to neighbor list; figures out target cell and includes target cell ID (5000) in the hand-in relocation request
- HNB-GW receives all hand-in messages
- USC8x would have registered with HNB-GW as a single HNB
- HNB-GW will forward the hand-in message to the proper USC8x
- Controller identifies which small cell the UE is handing into

Femto Access Control

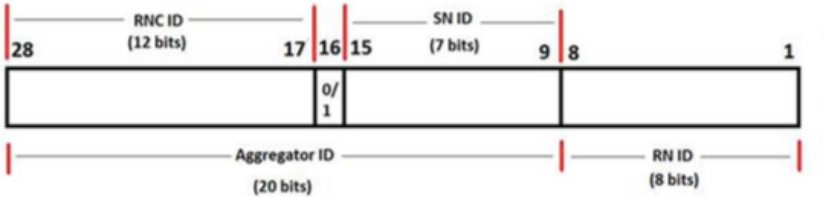
- Multiple access control modes
  - Closed access: Small Cells is restricted to a set of identified users
  - Open access: all users can access the small cells (i.e. small cells becomes an extension to macro)
  - Hybrid access: privileged access to identified set of users and open to others with restrictions
- Access control is invoked at UE registration with configurable reject methods
  - Standard Location Update Reject (barring whole LAC)
  - Option to use Authentication Failure (barring Cell only)
- Two ways to identify the users:
  - IMSI whitelist stored at HNBGW and optionally at HNB (pre-R8 UEs)
  - Closed Subscriber group (R8+ UEs)
- CSG details (see next slides)

10K UEs per HNB

- HNBGW supports registration of a maximum of 10K UEs per HNB in case of an HNB aggregator.
- Even though fewer number of HNBs need to be supported on the HNBGW, the number of UEs supported should remain the same.
- HNBGW supports simultaneous registrations from normal HNBs as well as HNB aggregators, even though different hnbgw-services are configured for each type of HNB.
- HNBGW assigns system resources appropriately for HNBs and HNB aggregators to avoid unusual behavior on HNBGW.
- No separate license is required for HNB aggregators. HNBs and HNB aggregators will be assigned the same unit of license.
- Below are the assumptions for the 10K UE support feature.
  - HNBGW assumes that an HNB aggregator can have a maximum of 10k UEs behind it. The maximum value supported for max-registered-ues-per-hnb when HNB-Aggregation is enabled is 10k.
  - One hnbgw-service can support only one kind of HNB. Therefore, if we want to support both normal HNBs and HNB aggregators, we need to use a different hnbgw-service for each.

Hand in with FAP Aggregator

- HNBGW communicates to HNBs on the IUH interface. The HNB can be a normal HNB or an HNB aggregator.
- Each HNB has a 28 bit unique Cell ID. The Cell ID comprises of the RNC ID and CID.With this feature, 1 bit (16th bit) from LSB in the Cell ID be reserved to identify whether it belongs to a normal HNB or an HNB aggregator.



- 16th Bit:
  0 - Normal HNB
  1 - HNB Aggregator

Hand in with FAP Aggregator II

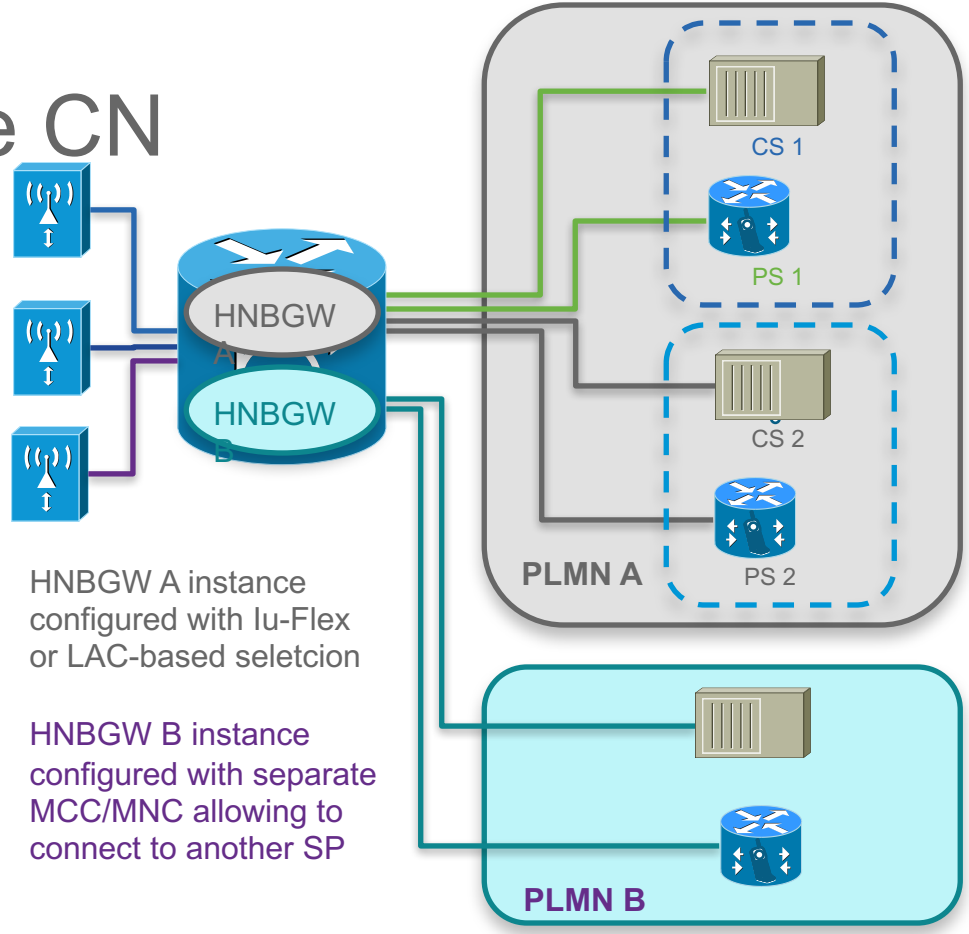
- On receiving an HNB Register request message, if HNB aggregation is enabled in the HNBGW service and if the Cell ID has the 16th bit set to 1 and if handin with aggregator feature is enabled
- HNBGW will pick the higher 20 bits of the Cell ID (from the MSB) and maintain a lookup for such HNB contexts based on the resulting integer value.
- These 20 bits carry a value which is unique for each aggregator. This combined with the remaining 8 bits gives a unique value for each individual HNB behind the aggregator.
- On receiving a Relocation Request message, HNBGW will first do a lookup using the entire 28 bit Cell ID (if there are normal HNBs too in addition to the aggregator HNBs). If this lookup fails and if the Cell ID has the 16th bit set to 1, then HNBGW will lookup using the first 20 bits in the Cell ID to find the target HNB aggregator. If this lookup is successful, it gives the HNB aggregator to which the relocation request will be forwarded. This is then further forwarded to the individual HNB by the aggregator using the remaining 8 bits.

Small Cells Network Sharing

- Objective: deploy a single small cells layer which can then be connected to multiple CN instances within a single PLMN or belonging to two different PLMNs
- Applicable to 3G UMTS networks, specific capabilities have been defined
  - Iu-Flex as defined in 3G TS 23.236
  - MOCN (Multiple Operator Core Network) as defined in 3G TS 23.251
- Both solutions not specifically defined for small cells but principle can be applied
- Two specific cases
  1. Supporting UEs allowing to use specific information for selection

Network Sharing Connecting to multiple CN

- Single HNBGW can be connected to multiple CN core elements belonging to the same or multiple operators
- Benefits
  - Signaling optimization as small cells can be connected to the CN nodes serving the surrounding macro
  - Load sharing of CN
- HNBGW supported following features
  - Standard Iu-Flex (per 23.236)
  - LAC-based CN selection
  - Multiple HNBGW instance that can then connect to multiple CN node (from single or different MSP)
- Future support for MOCN allowing single femto to be connected to multi PLMN
  - Selection based on received IMSI

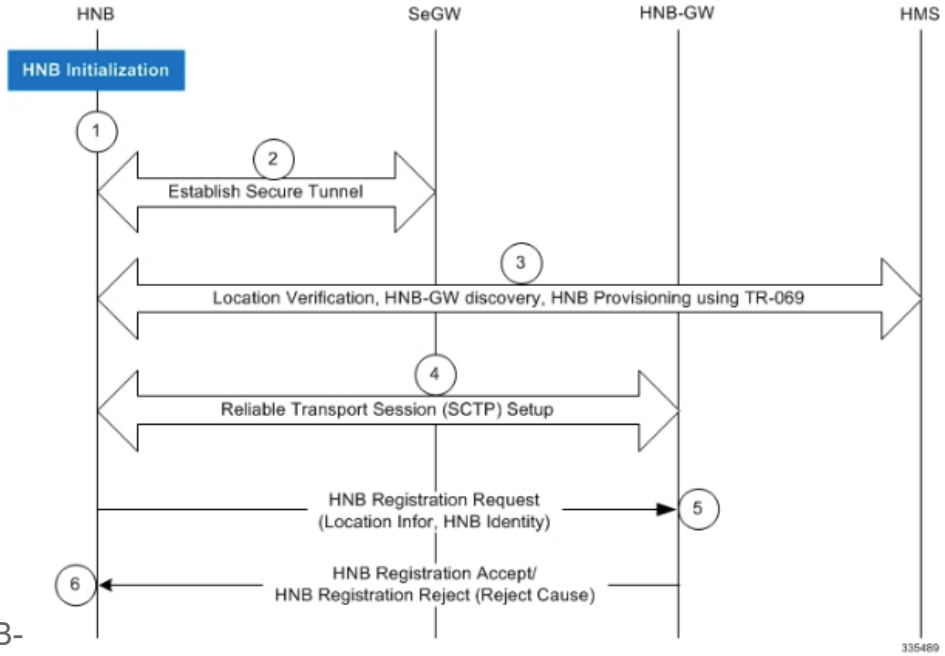


HNBGW A instance configured with Iu-Flex or LAC-based seletcion

HNBGW B instance configured with separate MCC/MNC allowing to connect to another SP

HNB Registration Procedure

- **1** HNB initialization
- **2** A secure tunnel is established from the HNB to the Security Gateway.
- **3** Location verification shall be performed by the HMS based on information sent by the HNB (e.g. macro neighbor cell scans, global navigational satellite system type of information etc.).
- **4** Reliable transport setup (SCTP) completed and the HNB sets up a SCTP transport session to a well-defined port on the serving HNB-GW. HNB Registration procedure started.
- **5** The HNB attempts to register with the serving HNB-GW using a HNB-REGISTER-REQUEST message.
- **6** The HNB-GW uses the information from the HNB-REGISTER-REQUEST message to perform access control of the HNB



Paging Procedure

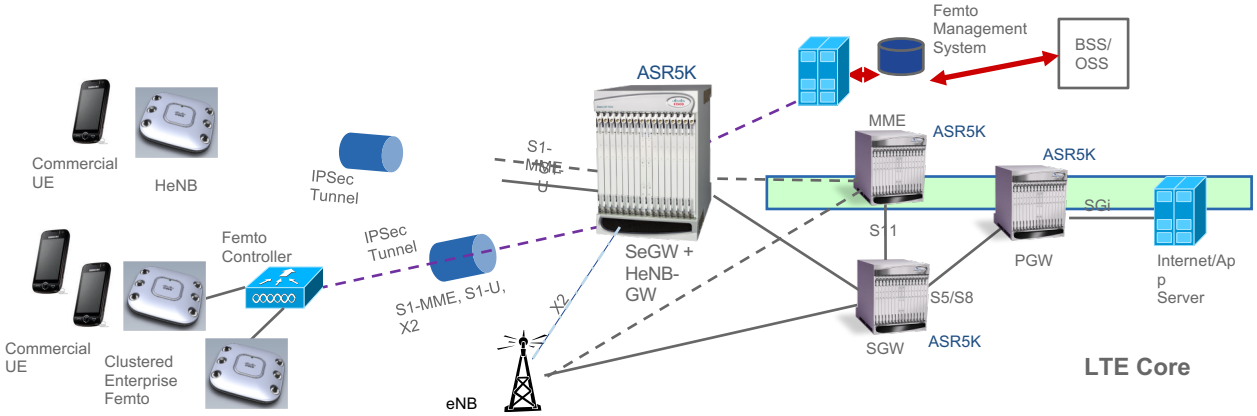
- **1** HNB-GW receives Paging from SGSN/MSC. HNB-GW finds out if any UE is registered with that IMSI.
- **2** If a UE is registered then HNB-GW sends the Paging message to the HNB through which the UE is
- registered.
- **3** If no registered UE is found then HNB-GW finds out the list of HNBs which have IMSI received in the
- message in their respective Whitelist.
- **4** If one or more HNBs were found, and Paging message contained LAI, then HNB-GW compares the HNB's
- PLMN-ID and LAC values against LAI received in the Paging. The HNB which do not have matching
- values is dropped from this list.
- **5** If one or more HNBs were found, and Paging message contained RAI, then HNB-GW compares the HNB's
- PLMN-ID, LAC and RAC values against RAI received in the Paging. The HNB which do not have
- matching values is dropped from this list.

SRNS Procedure

- **1** HNB-GW receives Relocation-Request from SGSN/MSC in case subscriber moves from Macrocell to Femtocell in a connected mode.
- **2** If the request does not contain IMSI (i.e. for an emergency call), HNB-GW sends Relocation-Request-Reject with an appropriate cause.
- **3** . If the request contains IMSI, HNB-GW finds the list of registered HNBs which have this IMSI in their white-list. If there is no such HNB found, HNB-GW sends Relocation-Request-Reject with appropriate cause.
- **4** If there is only one such HNB found which has this IMSI in its white-list, HNB-GW sends Relocation-Request to this HNB.
- **5** If there are more than one such HNBs found which have this IMSI in their whitelist, then HNBGW looks for Home-HNB for this IMSI. If there are more than one Home-HNB found then HNB-GW sends Relocation-Request-Reject with appropriate cause.
- **6** If there are multiple HNBs registered which have this IMSI in their whitelist but only one Home-HNB found, HNBGW sends Relocation-Request to this HNB.

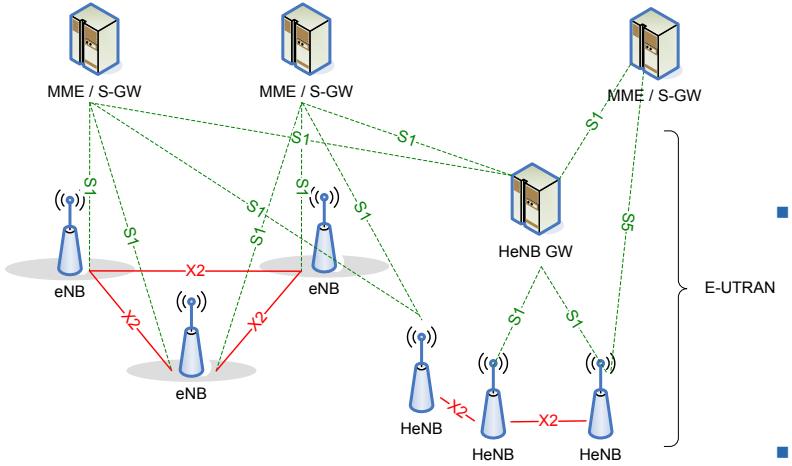
HeNBGW 3GPP Releases

HeNB-GW Architecture



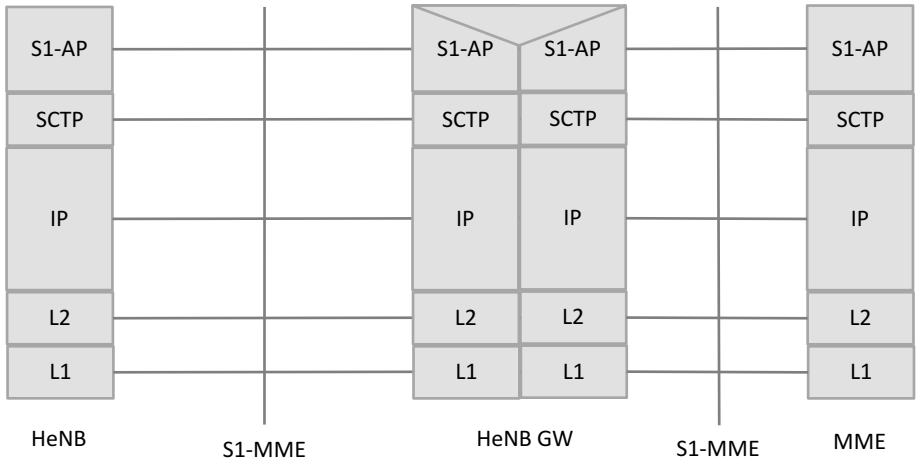
- 4G LTE Small Cells are part of LTE overall deployment plan
- LTE femto/small cells from all major operators increasing
  - SMB, Public Access and Enterprise deployments

Femto LTE HeNB Architecture (3GPP TS 36.300 and 23.830)



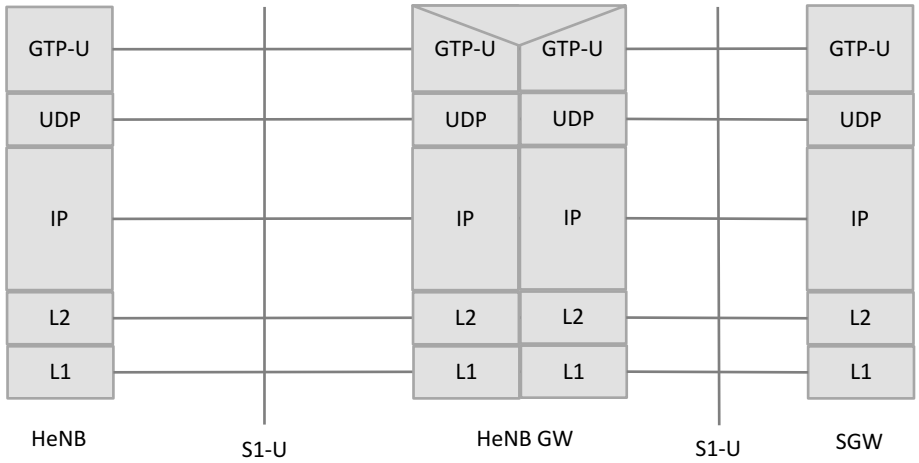
- HeNB is similar to eNB functions but different deployment requirements due to RF interference, volume, cost, PnP etc.
- No X2 support initially but introduced in R10 for
  - Inter-HeNB mobility
  - Inter-HeNB and inter-eNB SON features (eICIC, etc.)
- HeNBGW as X2 proxy for scaling (planning phase)
- Security Gateway is required

Protocol stacks for S1 control plane (S1-MME)



- The HeNB GW appears to the MME as an eNB
- The HeNB GW appears to the HeNB as an MME
- The S1-MME interface between the HeNB and the MME is the same whether the HeNB is connected to the MME via a HeNB GW or not
- There is an SCTP connection between each HeNB and the HeNB-GW
- There is an SCTP connection between the HeNB-GW and each MME

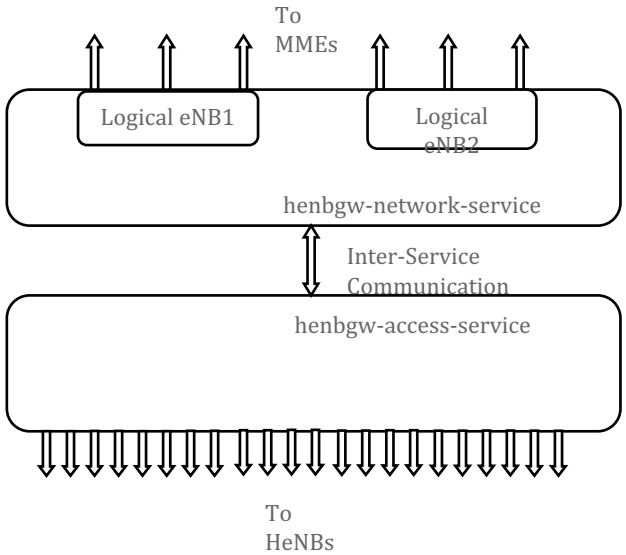
Protocol stacks for S1 user plane (S1-U)



- The HeNB GW appears to the SGW as a eNodeB GTP endpoint
- The HeNB GW appears to the HeNB as a SGW GTP endpoint
- The S1-U interface between the HeNB and the SGW is the same whether the HeNB is connected to the SGW via a HeNB GW or not

Features & Capabilities

HeNB-GW Internal Architecture



- henbgw-access-service
  - Handles the interface towards the HeNBs
  - Handles the interface towards the SGW as well
    - To support S1-U relay functionality, ingress and egress GTPU services are associated to the access service
- henbgw-network-service
  - Handles the interfaces towards the MMEs
  - Supports configuration of multiple logical eNodeBs
  - The Logical eNodeB concept allows for the HeNB-GW, to present itself as one or more eNodeBs towards the MME
- One to One association between a henbgw-access-service and a henbgw-network-service to handle S1-MME messages between the HeNBs and MMEs

HeNBGW Services in starOS

- **HeNB-GW Access Service**:
  - The configuration of this service controls the functionality of S1-MME interface between HeNB-GW and the HeNBs.
    This service is bound to a local SCTP end-point address (IP address) to listen the incoming SCTP associations from HeNBs.
- ◦**HeNB-GW Network Service**:
  - The configuration of this service controls the functionality of S1-MME interface between HeNB-GW and MME. One-to-one mapping is maintained between the HeNB-GW Access service and HeNB-GW Network service.
  - It is the HeNB-GW Network service where enabling of logical eNodeBs is configured within the HeNB-GW.
  - The Logical eNodeB configuration can be used to support load balancing among different TAI Lists.
  - Each Logical eNodeB can connect up to 8 MMEs from the MME pool and therefore 64 connections are possible to be established between HeNB-GW and MME.

HeNBGW Access Service

- A minimum of the following critical parameters must be configured in an access service to move the service to started state:
- • SCTP bind address
  • SCTP bind port
  • MME group id and PLMN ID
  • HENBGW Network service
  • GTPU services if S1U is enabled
- A maximum of 16 HENBGW Access services in the same or different VPN contexts can be configured.
- There will be a single instance of HENBGW Network service. All the access services share all the logical ENodeB's configured in the HENBGW Network service. The logical ENodeB will be selected based on the TAI sent by the HENB.

Multi HeNBGW Access Service & QoS

- Upto 16 Henbgw Access services in the same or different VPN contexts can be configured. Each Henbgw Access service will have a unique SCTP IP address and port combination.
- Each HENBGW Access service have a provision to configure a DSCP value per QCI value. Separate values can be specified in uplink and downlink direction. This DSCP value shall be applied to GTPU packets of eRABs with the given QCI value.
- GTPU packets of eRABs coming from or sent to HENBs registering with a particular HENBGW Access service are treated as per the DSCP configuration of that HENBGW Access service.
- In scenarios where HENBGW does not know the QCI value for a particular eRAB, a configurable default DSCP value is used. Also configurable pass through mode is available where the DSCP marking will be unaltered by the HENBGW before relaying the packet to the other side.

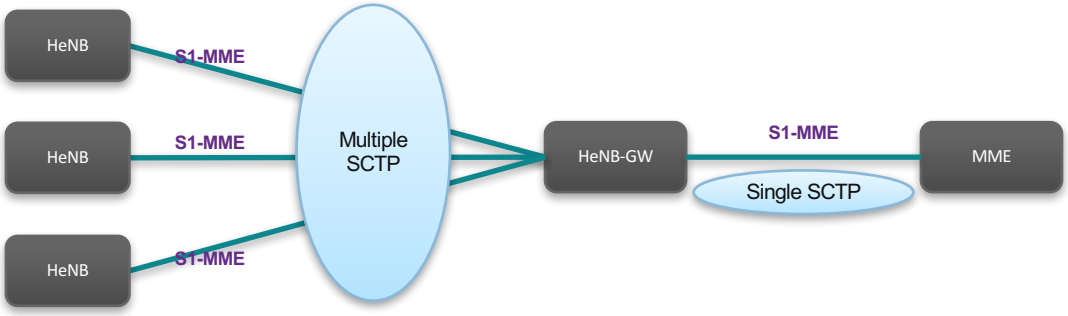
HeNB-GW Functions

- HeNB-GW supports the concept of Logical eNodeBs
  - Maximum of 8 Logical eNodeBs
- Support TAC and PLMN ID used by the HeNB
  - Each Logical eNodeB supports 256 TAIs, and a total of 2048 TAIs per HeNB-GW
- Relay UE-associated S1 application part messages between the MME serving the UE and the HeNB serving the UE
- Terminate non-UE associated S1-AP procedures towards the HeNB and towards the MME
- Supports S1-flex towards a maximum of 64 MMEs
- Terminating S1-U interface with the HeNB and with the S-GW
  - One S1-U GTP tunnel endpoint toward each SGW

MME Pooling

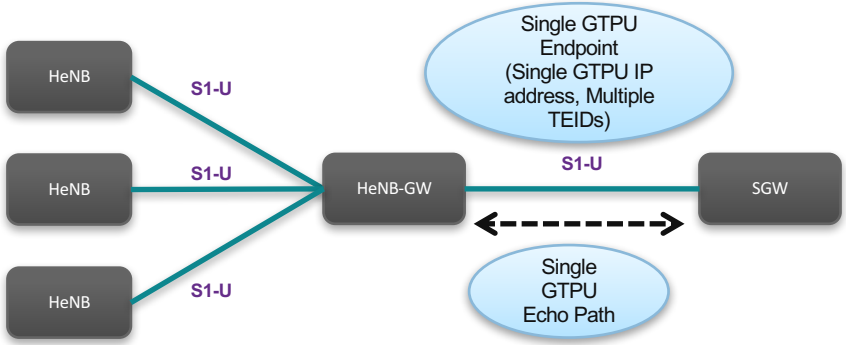
- IuFlex supported to connect to multiple MMEs
- HeNBGW supports 32 MMEs max per MME pool.

S1-MME Aggregation



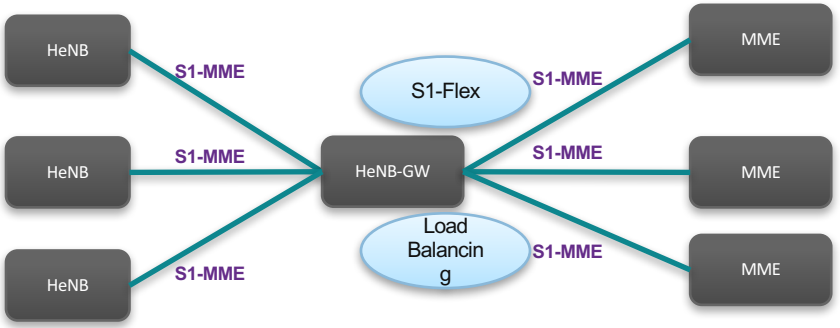
- Single SCTP connection towards each MME
- One SCTP connection per HeNB from the HeNBGW
- Hides HeNB SCTP connections from MME
  - Reduces number of SCTP connections to be handled
  - Reduces SCTP capacity load on MME
  - Reduces SCTP heartbeat load on MME
  - Eliminates maintenance of a large number of SCTP associations as well as the frequent establishment and release of the SCTP associations

S1-U Aggregation



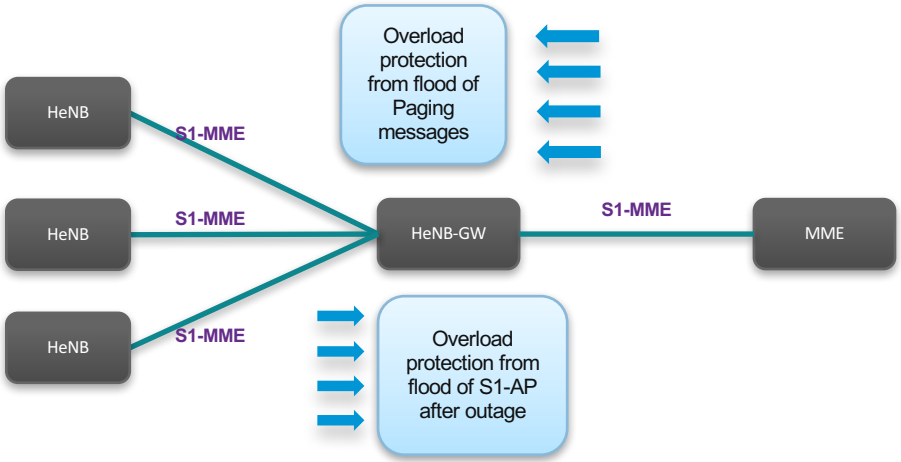
- Single GTPU end point towards SGW reduces
  - GTPU Endpoint capacity load on SGW
  - GTPU Path handling
  - GTPU echo handling load on SGW
  - Single GTP Peer per SGW

S1-Flex and MME Load balancing



- S1-Flex support (MME Pool) at HeNB-GW eliminates need of HeNBs to support S1 flex
- HeNB-GW performs NAS Node Selection Function (NNSF)
  - Based on the TAI and GUMMEI/S-TMSI info in S1AP message selects the MME from the configured MME pool
- HeNB-GW supports MME Load Balancing using the Relative MME Capacity information in S1AP setup response.

Overload protection



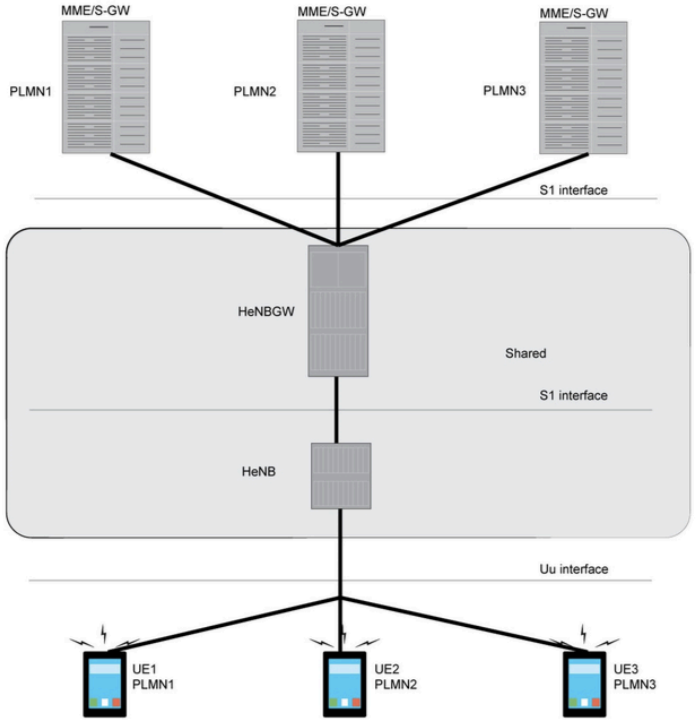
- Overload control mechanism at HeNB-GW protects MME from the flood of S1 messages during large HeNB outage / link failure scenarios
- HeNB-side overload control on HeNB-GW to account for flood of S1 messages
  - Mechanism triggered based on the Rate of S1 messages
  - Also based on the configurable CPU/Memory usage threshold on HeNB-GW
- MME-side overload control on HeNB-GW to account for flood of paging messages
  - Based on configurable paging rate
- HeNB-GW supports standard OVERLOAD START/STOP mechanism from MME
  - Overload Start / Stop message from MME processed at the HeNB-GW without fan-out to HeNBs

Paging Optimization on HeNB-GW

- Three Step Paging Optimization:
  - Stage 1: Page last known HeNB
  - Stage 2: Page HeNBs in last known Enterprise Grid
  - Stage 3: Page HeNBs in TAI
- Optimized paging also supported with CSG-ID and TAC
- Results in faster HeNB paging and call termination
- Hides HeNB paging complexity from MME

MOCN in HeNBGW

- One HENB can handle more than one core network operator.
- In this scenario HENB broadcasts a list of PLMN Ids to UE's.
- UE's supporting MOCN functionality decode the broadcast system information sent by HENB and are able to select a core network operator as the serving operator within a shared network.
- Needed unique TAC pero PLMN



HeNB-GW Key Benefits - 1

- Standard Compliance enabling multi-vendor deployment (Small Cells and macro)
  - Standard S1 interfaces (S1-MME and S1-U) to any MME/SGW and any small cell
- S1-MME Aggregation and Optimizations
  - - Single S1-AP/SCTP association towards MME for HeNB layer
  - - MME pool support (S1-flex) eliminating need HeNBs to support S1 flex
  - - Hiding some specific events to MME (e.g. intra-HeNBGW/MME S1-based HO)
  - - HeNB-GW can avoid overloading of MME in case of massive failure of HeNB
- S1-U Aggregation and Optimizations
  - - Topology hiding between HeNB and SGW (GTP-U scalability)
- X2 Optimizations (Relay/proxy function)
  - - X2 aggregator function (i.e. single point of contact) towards macro eNB
  - - X2 HeNB clustering support for inter-HeNB and eNB-to-HeNB traffic
  - - SON support and further optimizations over X2 interface.
- Paging Optimization
- NNSF (NAS Node Selection Function) support for Neutral Host and MOCN (future)

HeNB-GW Key Benefits - 2

- Security
  - - Optional support for integrated SeGW for untrusted broadband backhaul
  - - Secure Architecture: Topology hiding of MME/SGW to the HeNB
  - - Common Security Gateway for Multi-radio CPE (3G, 4G LTE, WiFi)
- High Performance and Scalability based on Cisco ASR5000 and ASR5500
- Simultaneous access for Multi-Radio (3G and 4G LTE) Femto/Small Cell (co-located HNBGW & HeNBGW on the same ASR5K platform)
- Integrated functions
  - - Optional support for MME/SGW/PGW on the same ASR5K platform
  - - WiFi aggregation capabilities
- Zero touch Provisioning and SON Support.
- Application API support such as Location/Presence API (future)

LTE Mobility:
Handovers to/from Macro eNBs

Hand-in

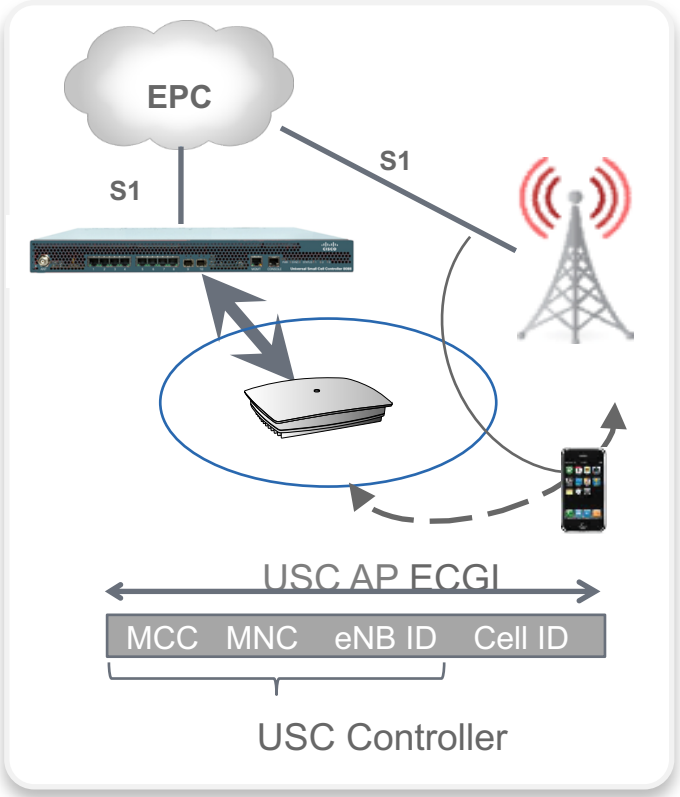
- S1-based handover from macro eNB to USC8088
- USC8x EC maps handover request to USC8x AP

Hand-out

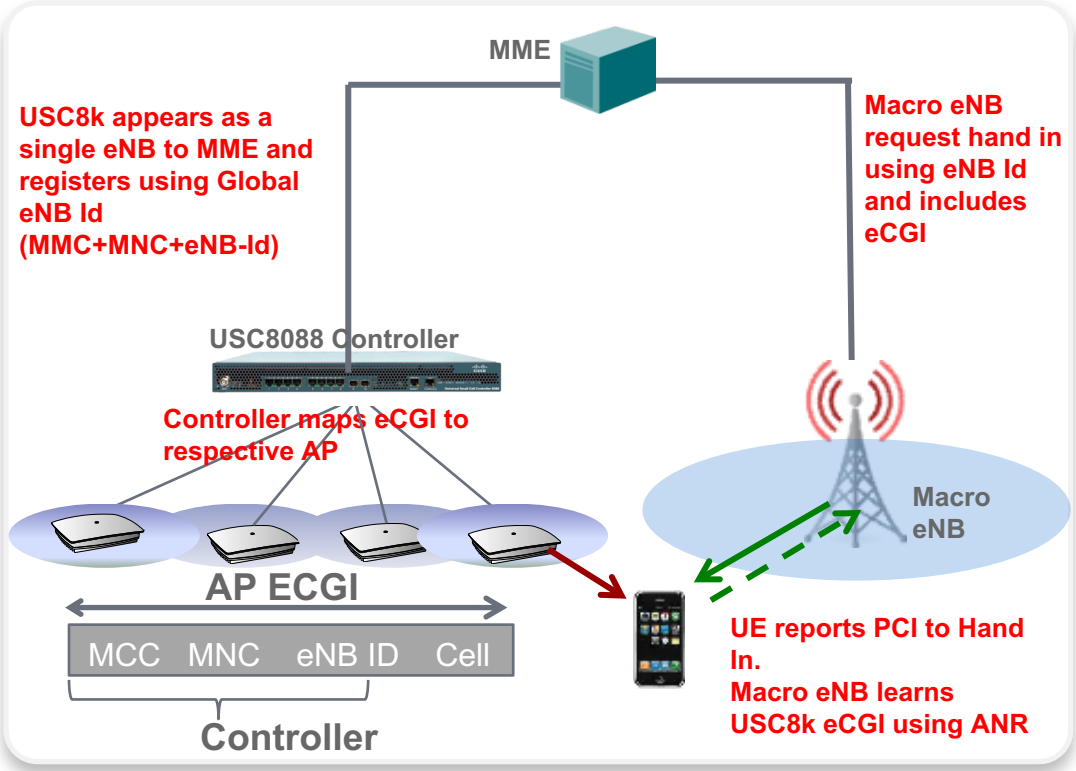
- S1-based handover from USC8088 to macro eNB
- USC8088 maintains PCI-to-ECGI mapping, provides NRTs

Architecture benefits

- Add small cells inside buildings without provisioning new eNBs at MME
- Easy to support X2-based handovers in partnership with macro eNB vendors



LTE Hand-in using ANR



- Controller registers to MME using Global eNB-id and appears as a single eNodeB
- UE sends a measurement report with small cell PCI
- Macro eNB will request for ANR and learns eCGI
- Macro eNB request S1 Handover using Global eNB-Id and includes eCGI
- MME will forward the hand-in message to the proper Controller using Global eNB-id.
- Controller identifies which AP the UE is handing into

SecGW Overview

SecGW In General

- Security Gateway is important element to protect Smallcell network. It provides network layer security for message exchange between H(E)NB and H(E)NB GW. All H(E)NBs will be authenticated with SeGW, before they talk to H(E)NB GW.
- For X.509 based authentication, if multiple Certificate Authorities have issued H(E)NB certificates then SeGW also supports multiple trust anchors. If SubCA issues H(E)NB certificate, instead of root CA, then authentication for Chain of Certificate is also supported.
- Once encryption algorithm and DH keys are exchanged, both end will start encapsulating the payloads. One of the proposed algorithms can be chosen for Encryption and Integrity keys. Establishing child SAs can renegotiate these keys periodically.
- Independent of traffic, whether signaling or bearer, and number of UEs per H(E)NB, a single IPSec tunnel is established per H(E)NB. This tunnel stays up all the time, i.e. till H(E)NB is rebooted. H(E)NB runs periodical heartbeats with SeGW to mark its presence, also known as Dead Peer Detection.
- Once H(E)NB is authenticated, an IP address will be assigned so that it(H(E)NB) can talk to protected network, i.e. H(E)NB GW and CN.

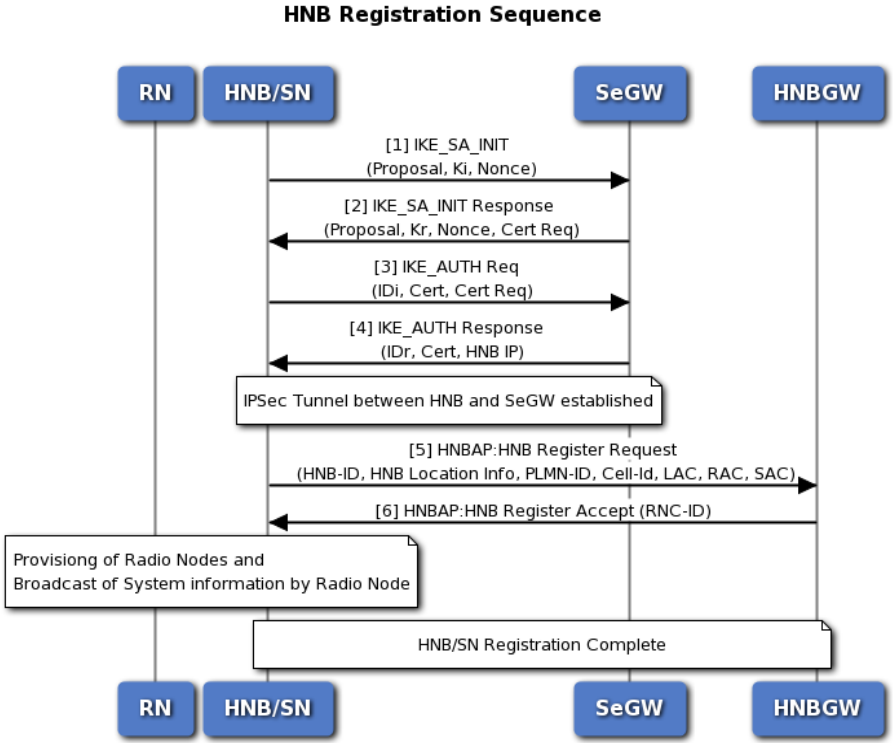
SeCGW UMTS

- Basic function of this entity are:
  - Authentication of HNB
  - Providing access to HMS and HNB-GW
- This entity terminates the secure tunnelling for IuH and TR-069 between HNB and HNB-GW and HMS respectively.
- In Claro Argentina SecGW is based on StrongSwan running over Linux RedHat

SecGW LTE

- The Security Gateway is an logical function on HeNB-GW in the LTE femtocell network deployment, however it is specified as a requirement in the Femtocell LTE network architecture.
- It may be implemented either as a separate physical entity or co-located with an existing entity. The SeGW secures the communication from/to the HeNBs.
- Basic function of this entity are:
  • Authentication of HeNBs
  • Termination of encrypted IPsec data connection from the femtocells • Providing access to HeMS and HeNB-GW
- The SeGW holds capability of implementing a Denial of Service (DoS) shield to protect the EPC (S-GW and MME) by detecting and then filtering out the attack traffic while maintaining the QoS (Quality of Service) of useful traffic. In our implementation, it is an optional element which is situated on HeNB-GW.

Ipsec tunnel establishment



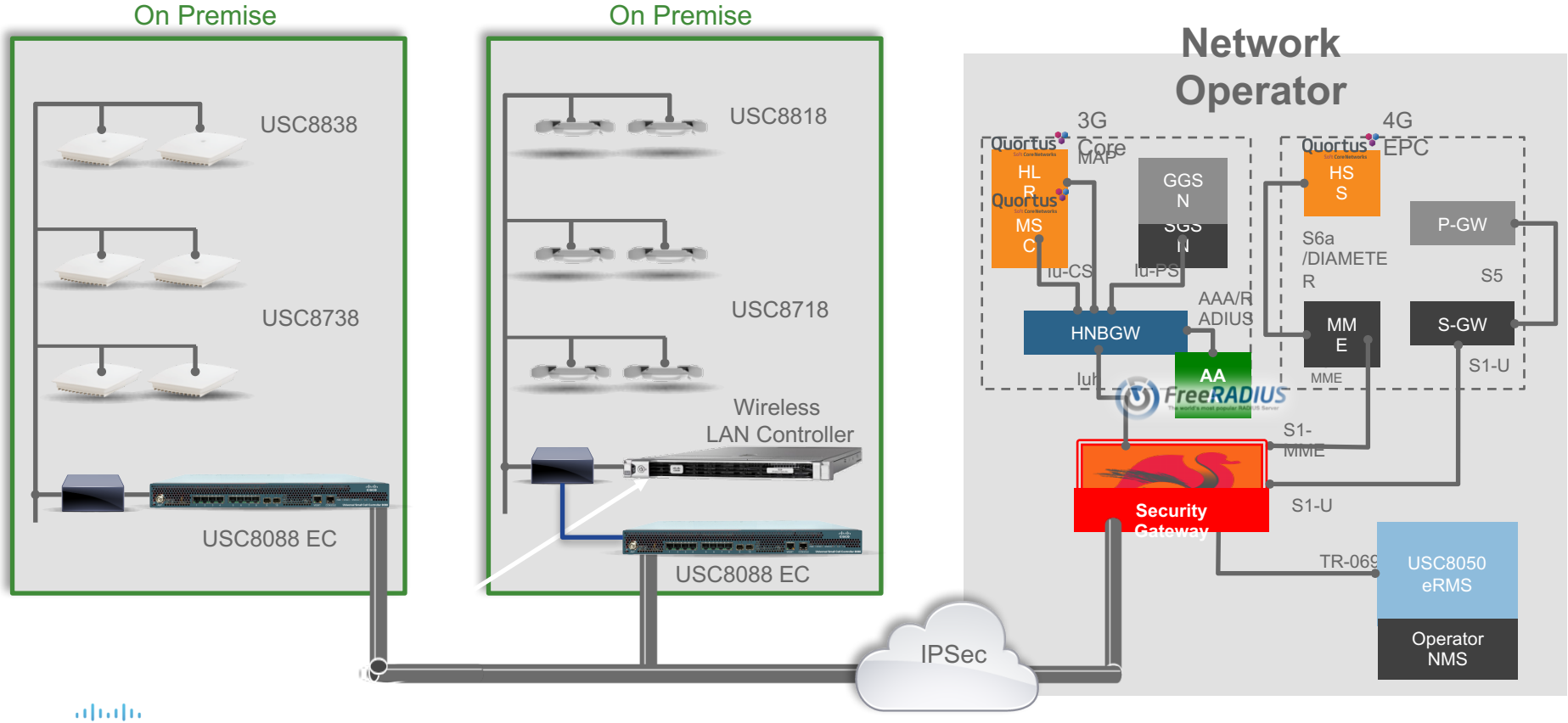
StrongSwan Security Gateway

An open-source IPSec-based VPN solution for Linux and other UNIX-based operating systems.

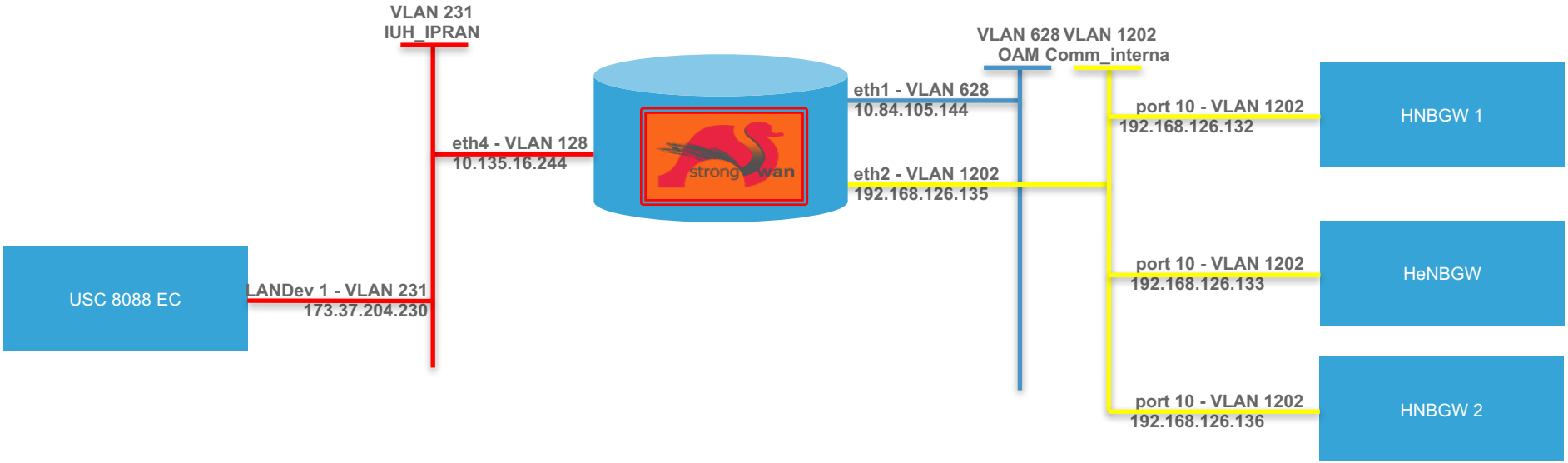
Key Exchange Protocols:

- IKEv1
- IKEv2
- Act as DHCP server for H(E)NB (assigns an internal IP for communication with VMs)

Cisco USC 8000 Series Deployment Reference



StrongSwan SeGW Interfaces & Connections



AAA Overview

FreeRadius AAA Server

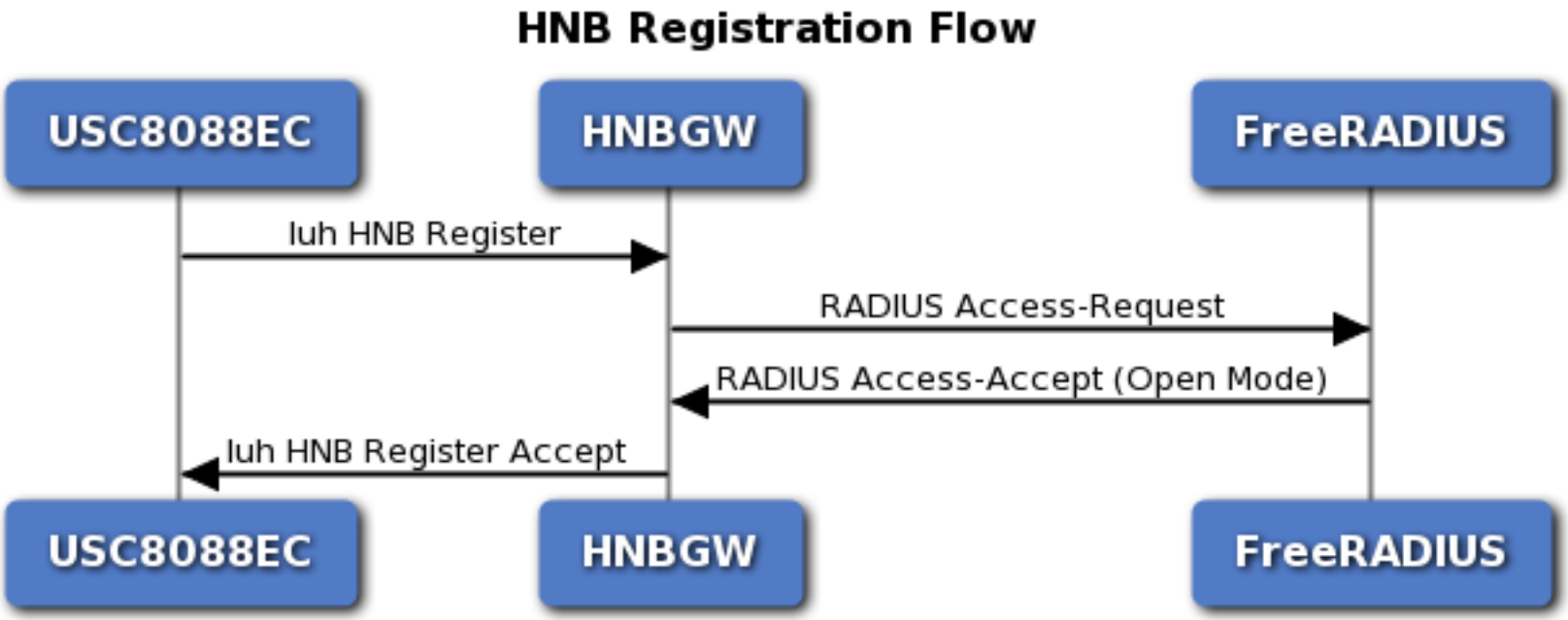
- Most widely deployed RADIUS server in the world.
- Supplies the AAA needs of many Fortune-500 companies and Tier 1 ISPs.
- Widely used in the academic community.
- Fast, feature-rich, modular, and scalable.

*Used as a workaround: unable to disable AAA authentication in HNBGW

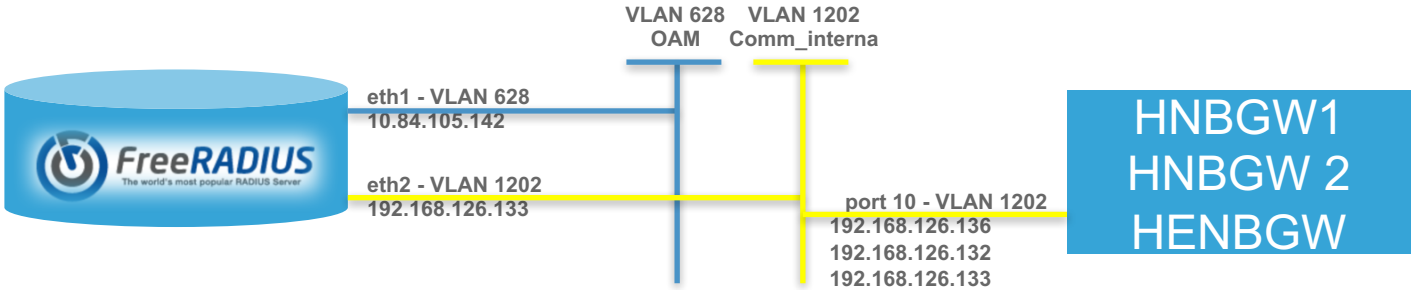
AAA

- FreeRadius used as RADIUS server only for H(E)NB authentication
- Not allowed for external use
- Low usage
  - During new SN provissioning
  - After SN restart

Cisco USC 8000 - FreeRADIUS



FreeRADIUS Interfaces & Connections



Only O&M and internal communication (RADIUS) with HNBGW

vCenter Architecture

vHetNet : Virtualization of Small cell gateways and OAM

Small cell HetNet virtualisation involves integrating the small cell HetNet gateways and OAMP components as virtual machines running on a common hardware platform. This common hardware platform uses Cisco UCS components.

This release supports the virtualisation of the following HetNet components onto this common hardware platform:

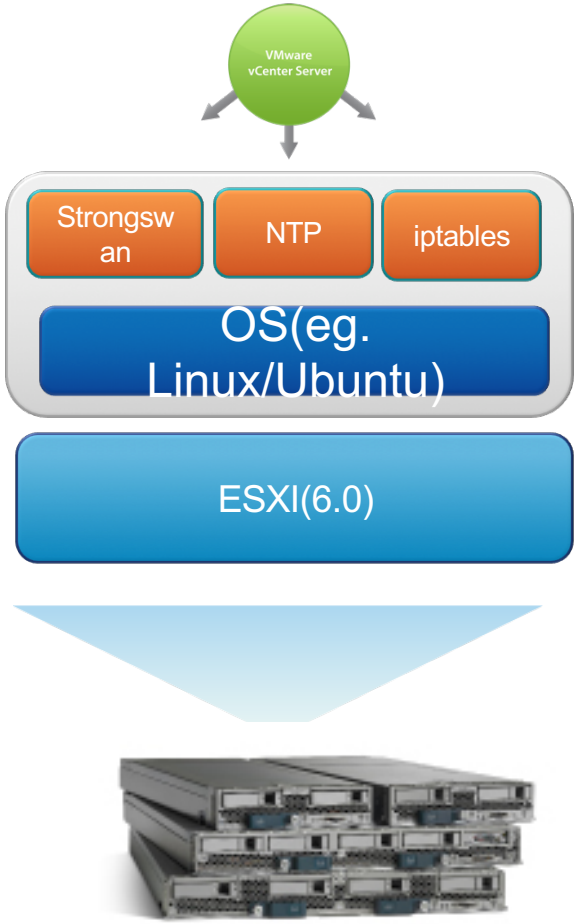
SeGW
H(E)NB-GW
eRMS
AAA
C2D –Click 2 Deploy – Internal tool from Cisco to quickly deploy vHetNet

vCenter Management

- vCenter manages all the ESXi hosts that are being used for vHetNet.

- vCenter IP is part of CIQ and customer has to make sure that these IPs are well protected by enabling proper firewall rules and should be from a secured vLAN of Operator Network.

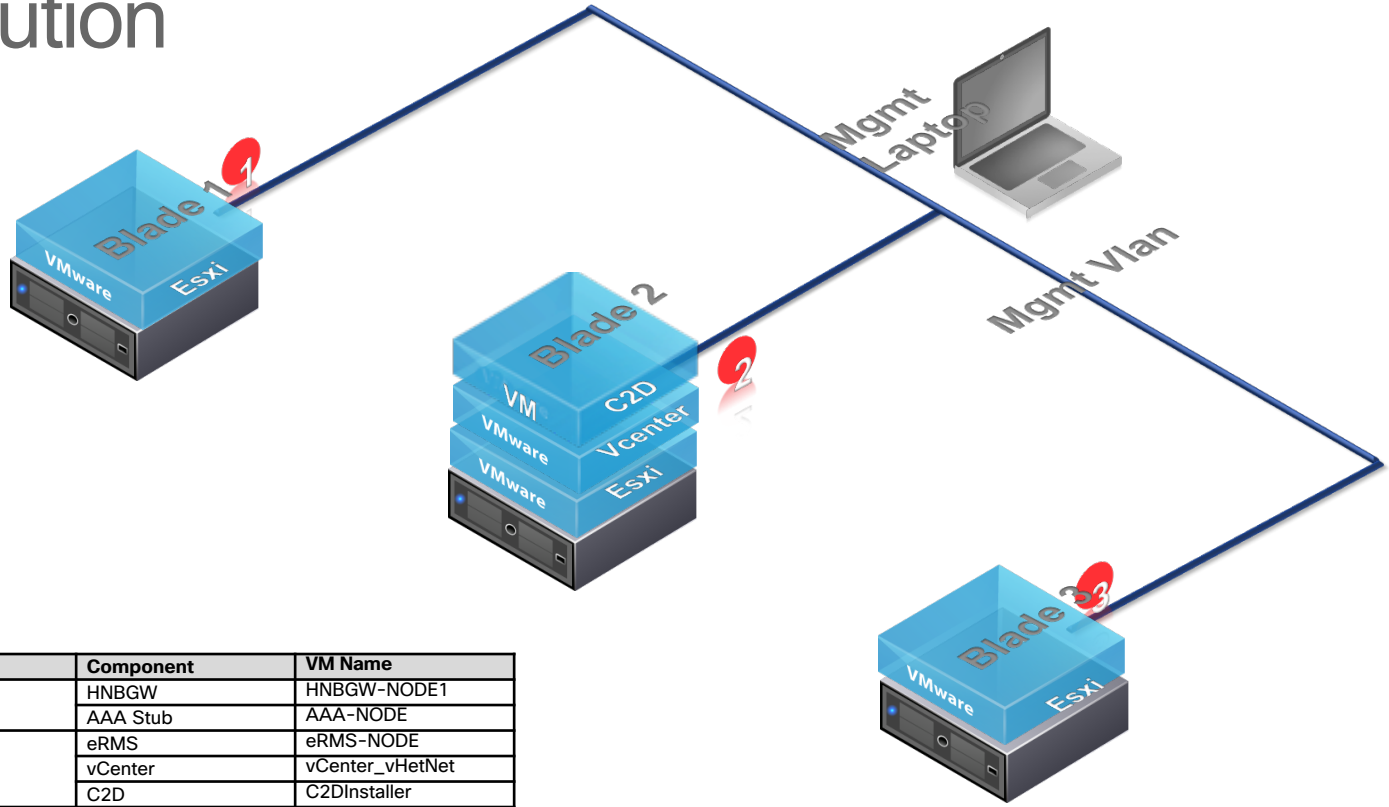
vMware Architecture



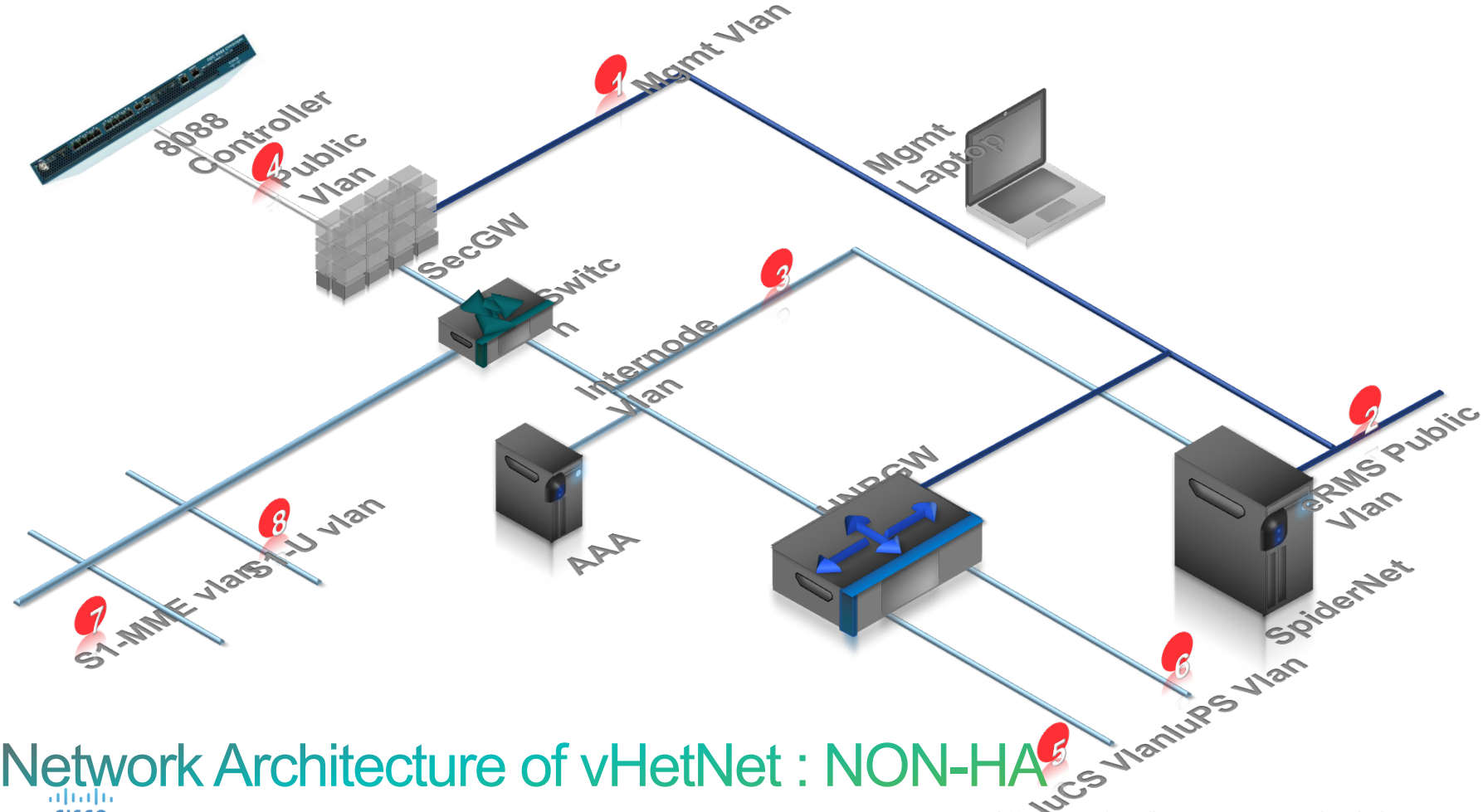
Prerequisite: UCS Configuration details

- UCS requires server port and uplink ports to be configured.
- UCS requires vlan configuration on uplink ports.
- UCS requires MAC pool for the network.
- UCS requires Pool of IPs on Mgmt(native) vlan as KVM ip pool for remote monitor access.
- UCS requires the service profile associated with blades for bootup with above defined pools.

vMware Distribution

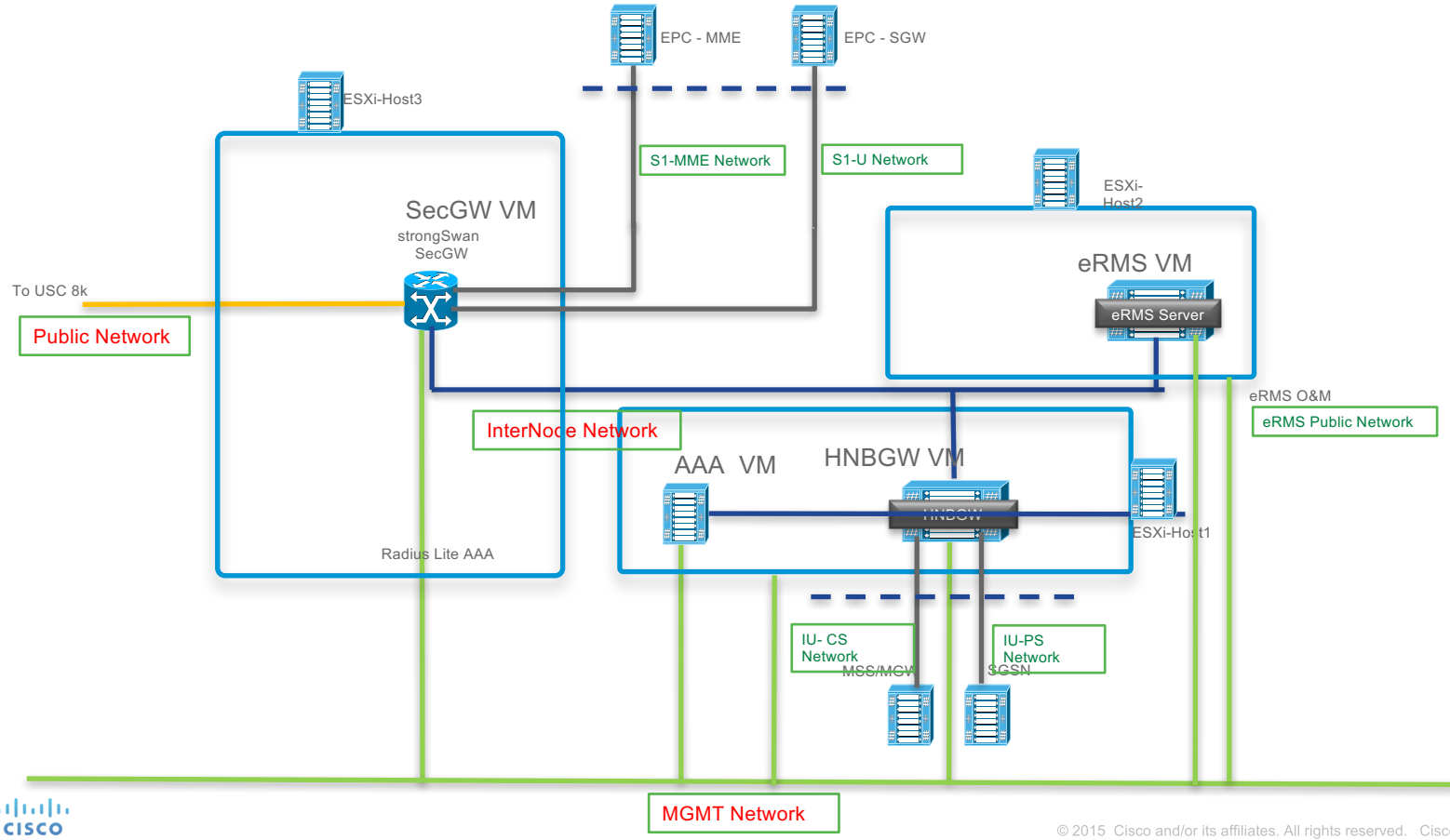


Blade	Component	VM Name
1	HNBGW	HNBGW-NODE1
	AAA Stub	AAA-NODE
2	eRMS	eRMS-NODE
	vCenter	vCenter_vHetNet
	C2D	C2DInstaller
3	SeGW	SEGW-NODE1



Network Architecture of vHetNet : NON-HA

vHetNet Network

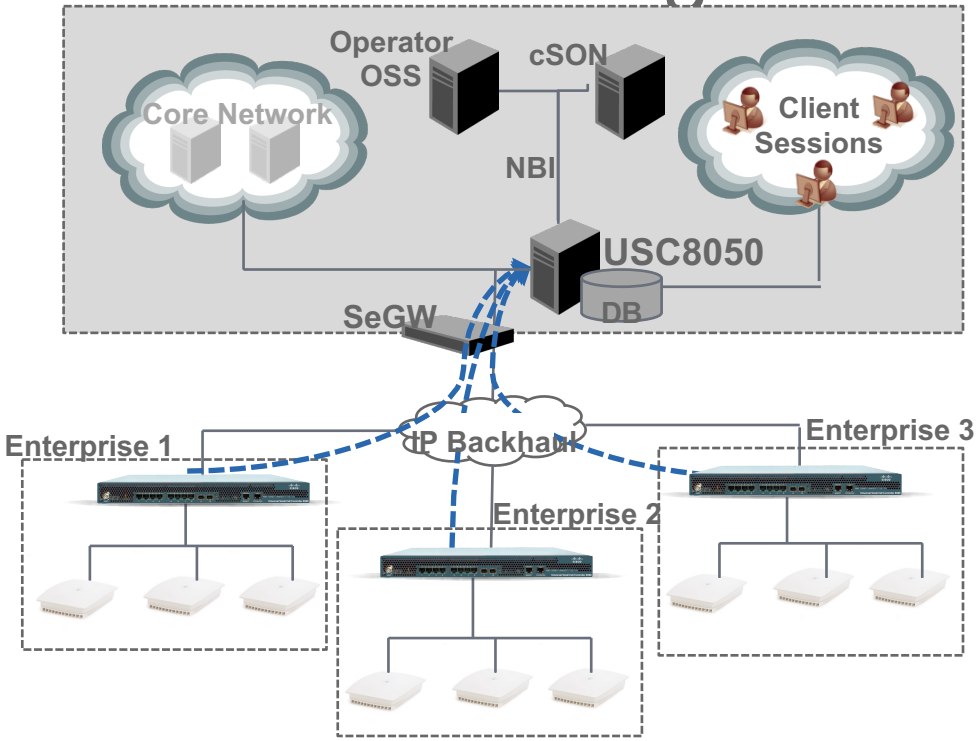


eRMS - SpiderNet

Management Related References

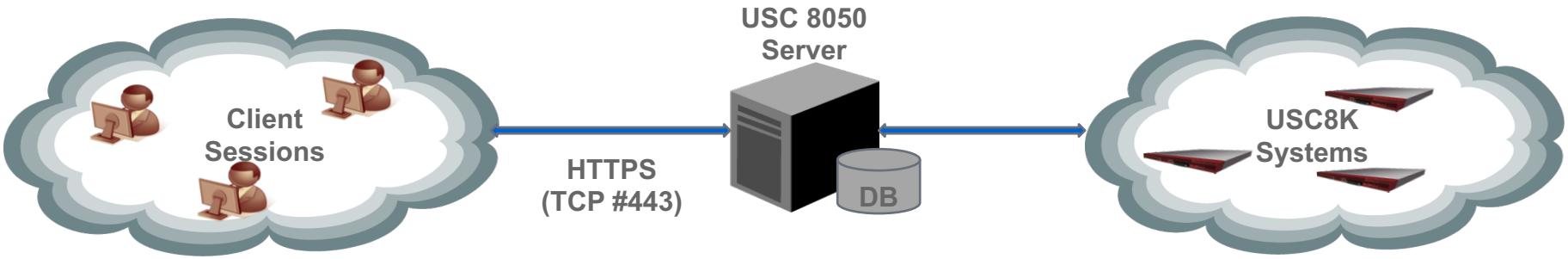
Title	OAM relevance
8000 Series OS Data Model Reference Guide	details about the objects and parameters that comprise the system configuration and operational state
8000 Series OS Faults, Conditions, and Events Reference Guide	details about all alarms, conditions, and events in the system
8000 Series Performance Measurements for Dual-Mode Small Cell Solution	PM counters and KPIs that monitor the health and state of the small cell solution
8050 eRMS Installation and Administration Guide	installing the 8050 management server and client and using it to remotely manage small cell deployments
8050 eRMS NBI Integration Guide	integrating the 8050 management system into operator's OSSs
8000 Series Call Performance Event Reporting Guide	detailed about CPER including the file format, reported events, and event parameters

USC8050 Management System Overview



- GUI based centralized management system dedicated for USC8000 series
- NBI to operator's network management and SON systems
- Features
  - Configuration management
  - Bulk provisioning (templates)
  - Scheduled operations (upgrades, backups)
  - User access control and audit trails
  - Fault management and correlation
  - Inventory Management
  - NBI for alarms to OSS
  - NBI for PM counters and KPIs
  - KPI Threshold crossing alerts
  - KPI Reports, emails

Platform Requirements



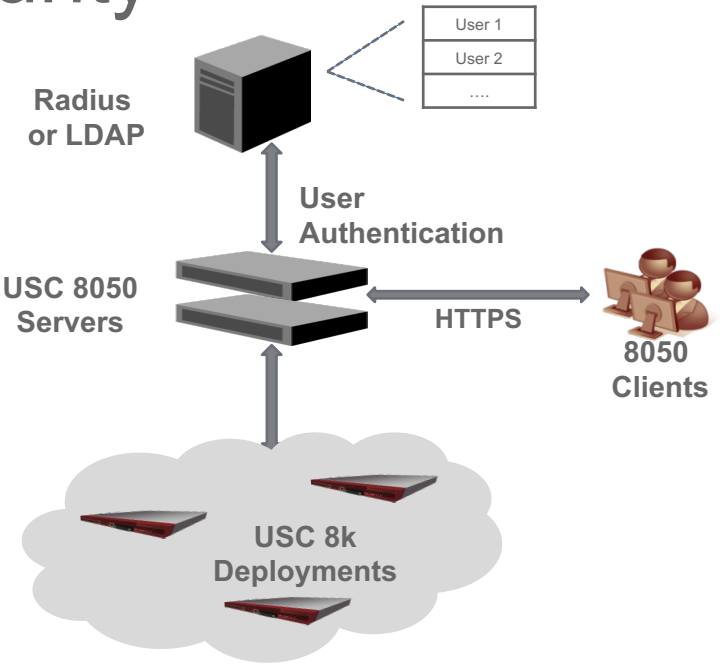
Client
Java Applet (in browser)
or
Java Desktop Application (Windows/Linux)

Server License
Per server / up to 400 Controllers

Minimum Server Requirements
Intel Xeon 6-core 64-bit
CPU 2.4 GHz or equivalent
16GB RAM
1 TB free disk space
O/S:
RedHat Enterprise Linux Server (RHEL 6.4)
or Linux CentOS 5.8 (or later)
Database:
MySQL Classic Edition

User Management and Security

- **User Management**
  - Add/modify/delete users and user profiles
  - Profile based - restrict users to specific workstations/views/actions
  - View connected users
  - Strict password control (min length / characters / expiry)
  - Allow/restrict multiple /shared logins
  - Lock/logoff users
- **Security**
  - Located in Operator core, behind SeGW
  - Authenticated and encrypted client-server sessions
  - Audit trail logging with filtering. Export to CSV.
  - User authentication (username/password) locally by 8050 option for external Radius / LDAP servers (with auto-fallback to 8050)

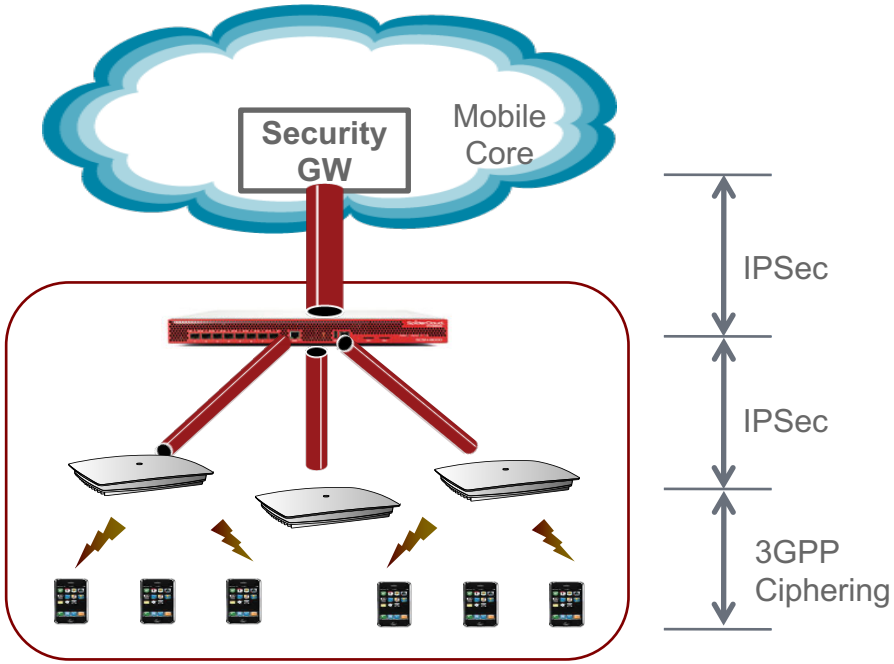


Northbound Interfaces Summary

- Fault Management:
  - Alarm correlation with suppression/forwarding to OSS via SNMP traps
  - Periodic alarm synchronization / heartbeat (keep alive)
- Inventory Management:
  - Scheduled CSV exports
- Performance Management:
  - Performance data stored in XML files on the 8050
  - XML files can be periodically pulled by OSS
- Configuration Management:
  - periodic configuration backup in XML file of all Controllers to OSS
  - RESTful API for provisioning (from SCS5.0)

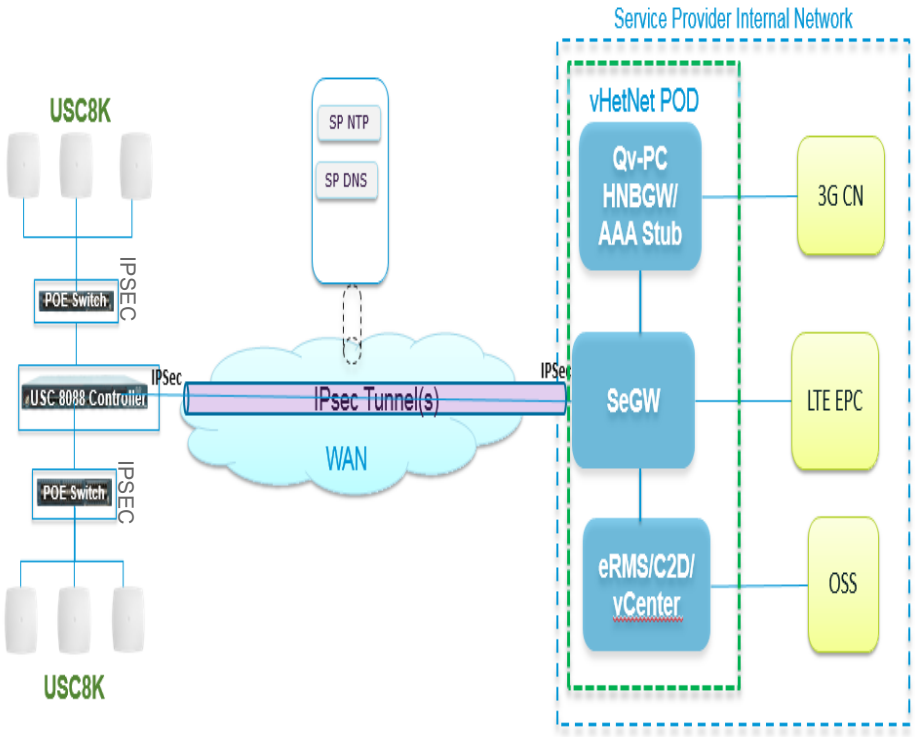
Security in vHetNet

Security



- Certificate based authentication between UC/APs and UC/SeGW
- Factory provisioned X.509 certs
- Secure boot
- Encrypted file system
- APs not allowed to radiate without connection to core
- Radio interface ciphering (Kasumi, snow-3G)
- Vulnerability system testing by independent lab

vHetNet Security Architecture Summary



vHetNet system supports the following authentication mechanisms:

- Interface between the controller and the security gateway.
  - Certificate-based authentication between USC8088 Controller – SeGW
  - IPSEC Encryption
  - Factory provisioned X.509 certs through secure CA channel
- Interface between the controller and eRMS over IPSEC Tunnel
  - Certificate-based authentication (X.509 RSA based) between USC8088 Controller – eRMS
- IPSEC &TLS Encryption
- Certificate Replacement/Renewal

Vulnerability Testing on each vHetNet component (Application plus OS) in the Cisco LAB

vHetNet Security-IPSEC Tunnel

- IPSec tunnel used to secure communications between the small cell controller and the vHetNet SP network.
- Single IPSEC tunnel is configured for 3G and 4G.
- Only IPv4 IPSEC is supported between USC Controller and SeGW.
- Uses certificate based authentication for IPSEC establishment.
- IPSec ESP used for authentication and encryption.
- IKE establishes the keys used by ESP to authenticate the communication end points, verify integrity and by ESP to encrypt and decrypt data.

Strongswan used for IPSec tunneling and High Availability

Authentication Mechanisms
- X.509 RSA certificate-based

Security Protocols
- IPSec ESP Tunnel Mode (RFC 2406)
- IKEv2 (RFC 4306) for Certificate/key exchange

Default IKEv2 Algorithms and Parameters
- Encryption algorithm: AES-CBC
- Integrity algorithm: HMAC-SHA1-96
- Diffie-Hellman group:2048
- Re-key interval: 24 hours

Default ESP (IPSec Algorithms and Parameters)
- Encryption algorithm: AES-CBC
- Integrity algorithm:HMAC-SHA1-96
- Re-key interval : 24 hours

Certificates

SeGW:

- SN ROOT and Intermediate Certificates are copied in SeGW VM.
  - These Certificates are part of the Image itself.

- USC8088 Controller:

  - SeGW ROOT Cert has to be copied to SN as part of post deployment steps.
    - Mentioned in C2D Deployment Guide .

SeGW Security

- Traffic from different entity is separated by different Ethernet interface.
  - Interface towardsUSC8088 EC will accept only ESP/ISKMP packets on Port 500 from USC8088 EC
  - Traffic between USC8088 EC and SeGW will secured by IPSec tunneling
  - Interface towards HNBGW, SGW, MME will forward/receive respective traffic
  - Other PORTS are closed by IPTables
- Management Interface will allow SSH, ICMP, DNS and NTP packets
- Root access is disabled from vCenter and Remote machine.
- Root shell access is disabled inside the machine
- Tripwire is installed for monitoring file system
- Unused network services like ftp, telnet disabled/removed in the system
- ASLR and X-Space protection is enabled
- Log rotation is enabled. 4 weeks logs are kept
- Minimal and required packages are installed in the system
- System is up to date with all security fixes from Ubuntu at time of release

Mutual Authentication

Cisco USC supports **IKEv2** to mutually authenticate the H(e)NB and the SeGW according to 3GPP TS 33.320 V9.0.0:

a. **Mandatory certificate** authentication:
   - The certificate binds the USC identity (serial number) to its unique public/private key locked and protected by the Root of Trust.
   - The FQDN in the Idr must fully match the FQDN in the certificate

b. **Optional EAP-AKA** authentication:
   - If the operator policy mandates EAP-AKA, the USC performs certificate authentication followed immediately by EAP-AKA authentication during the same IKEv2 exchange.

EAP-AKA - Extensible Authentication Protocol - Authentication and Key Agreement

IPSec Tunnel

- The **H(E)NB** supports IPSec ESP Tunnel via IKEv2:
  - IKEv2 profile algorithms:
    - Confidentiality: ENCR_AES_CBC, with fixed key length 128 bits, according to RFC 3602
    - Pseudo-Random Function: PRF_HMAC_SHA1, with a key length of 160 bits, according to RFC 2104 and 2404
    - Integrity: AUTH_HMAC_SHA1_96 according to RFC 2404, AES-XCBC-MAC-96
  - ESP algorithms:
    - Integrity: AUTH_HMAC_SHA1_96 as per RFC 2404, AES-XCBC-MAC-96
    - Confidentiality: AES-CBC-128.
- If the IPSec tunnel is lost, the **H(E)NB** stops providing service until the IPsec tunnel is re-established

HNBGW Security

- HNBGW VM is within secured vLAN of operator Network and behind SeGW(Trusted Boundary)

- HNBGW StarOS, which is a hardened version of the debian Linux OS. Cisco uses industry best practices in order to harden the product against attacks.

- Security mechanisms implemented include the use of a hardened Debian Red Hat Linux OS, which ensures that only explicitly required services are enabled e.g. ftp and tftp cannot be enabled on any context other than the local context telnet and ssh can be configured on any context but normally they are only enabled in the local context. If not configured, the packets are dropped

AAA Stub Security

- AAA is Internal function used by HNBGW, not accessible or configurable by operator.
- Needed to support HNB-GW operation and always returns “success”* to HNB-GW queries.
- This Component is not used externally to the vHetNet Box

  - AAA VM is with secured vLAN of Operator Network.
  - 1812 port for radius opened on internode interface and other ports are closed by IPTables. Internode interface receive packets only from HNBGW.
  - SSH, NTP, DNS ports are opened on management interface and other ports are closed by IPTables
  - AAA uses radiuslited server which is provided by MITG.
  - Root access is disabled from vCenter and Remote machine
  - Root shell access is disabled inside the machine
  - Tripwire is installed for monitoring filesystem
  - Unused network services like ftp, telnet disabled/removed in the system
  - ASLR and X-Space protection is enabled.
  - Log rotation is enabled. 4 weeks logs are kept
  - Minimal and required packages are installed in the system
  - System is up to date with all security fixes from RHEL
  - SELinux is enabled

eRMS Security

- eRMS VM is with secured vLAN of operator Network and behind SeGW(Trusted Boundary). All Service Node traffic will be secured by IPSec tunnel.
- Firewall is enabled
  - Port 8080, 8443, 7543 for TR069, Port 514, 50514 for syslog , Port 161, 162, 8161, 8162, 9162 for SNMP and Port 21, 22 for file transfer opened towards service node by IP Tables
  - Port 2223 (CLI), 443, 9443 (Web Interface) opened towards eRMS client by Iptables
  - Port 112, 12345, 44532, 22345, 3306 for MySQL opened for eRMS Redundancy(Based on the Reference to the eRMS Administration R5.1 Guide section 2.1.4)
  - DNS(53)and NTP(123) port also opened
  - Port 8112 (eRMS Redundancy Multicast UDP) and 9161(SNMP)
  - All other ports are closed.
- Root access is disabled from vCenter and Remote machine
- Root shell access is disabled inside the machine.
- Tripwire is installed for monitoring filesystem.
- Unused network services like ftp, telnet disabled/removed in the system
- ASLR and X-Space protection is enabled
- Log rotation is enabled. 4 weeks logs are kept
- Minimal and required packages are installed in the system
- System is up to date with all security fixes from RHEL

eRMS Security

- Located in Operator core, behind SeGW
- Authenticated and encrypted client-server sessions
- Audit trail logging with filtering. Export to CSV.
- User authentication (username/password) locally by USC8050 eRMS
- option for external Radius / LDAP servers (with auto-fallback to USC8050 eRMS)

Open Ports

Component	Open port	Function/Purpose	Interface
C2D	22	SSH	C2D MGMT Network
	8443	HTTPS	HTTPS Interface
SeGW	22	SSH	SeGW MGMT Network
	500	ESP/ISAKMP packets)	ERAN to SeGW(IPSEC)
	4500	MobIKE support	ERAN to SeGW(IPSEC)
AAA	22	SSH	AAA MGMT Network
	1812	RADIUS	INTER-NODE Network
eRMS	443	eRMS Client	HTTPS Interface
	22	SSH	eRMS MGMT Network
	3306	eRMS redundancy /MySQL	eRMS MGMT Network
	44532	eRMS redundancy Database fast path	eRMS MGMT Network
	12345	eRMS redundancy Keep Alive	eRMS MGMT Network
	22345	eRMS redundancy synchronization	eRMS MGMT Network
	9443	eRMS client	HTTPS Interface
	8112	eRMSRedundancy multicast UDP(running as non root user)	eRMS MGMT Network

Note: MGMT Network interface - secured vLAN of Operator Network

Open Ports

Component	Open port	Function/Purpose	Interface
eRMS	8080	TR069	ERAN to eRMS
	514	Syslog	ERAN to eRMS
	162	SNMP	ERAN to eRMS
	22	SCP	ERAN to eRMS
	21	FTP	ERAN to eRMS
	8443	TR069	ERAN to eRMS
	8161	SNMP agent(Running as non root user)	ERAN to eRMS
	8162	TRAP service((Running as non root user)	ERAN to eRMS
	9161	SNMP	ERAN to eRMS
	9162	SNMP	ERAN to eRMS
	161	SNMP	ERAN to eRMS
	7543	TR069	ERAN to eRMS
	112	eRMS redundancy	eRMS MGMT Network
	123	NTP	ERAN to eRMS
	53	DNS	ERAN to eRMS
	50514	Syslog((Running as non root user)	ERAN to eRMS

Note: ERAN to eRMS traffic is wrapped inside IPSec from controller- SeGW, and on the internal internode network from SeGW to eRMS

vHetNet integration Claro AR

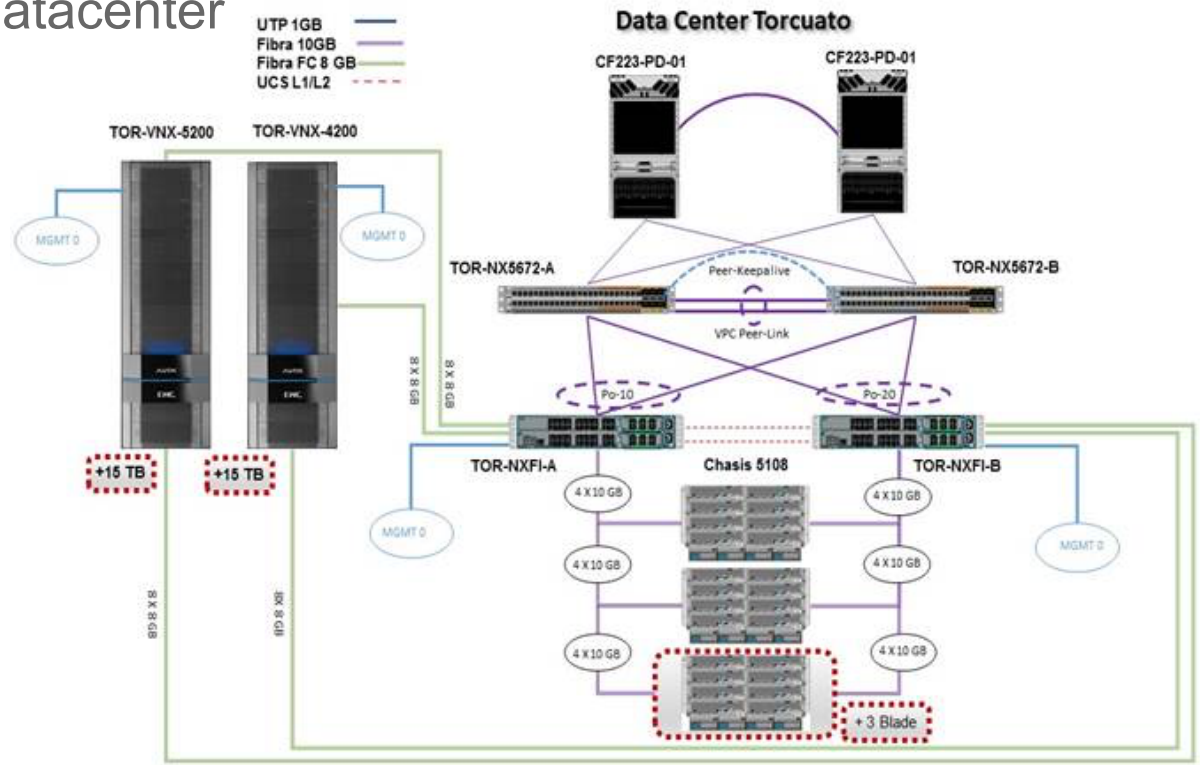
vHetNet Deployment

- 4 VMs deployed
  - SecGW
  - AAA
  - eRMS (SpiderNet)
  - starOS – H(E)NBGW

  - Deployment in Claro´s UCS-B located in Don Torcuato

Physical location of vHetNet

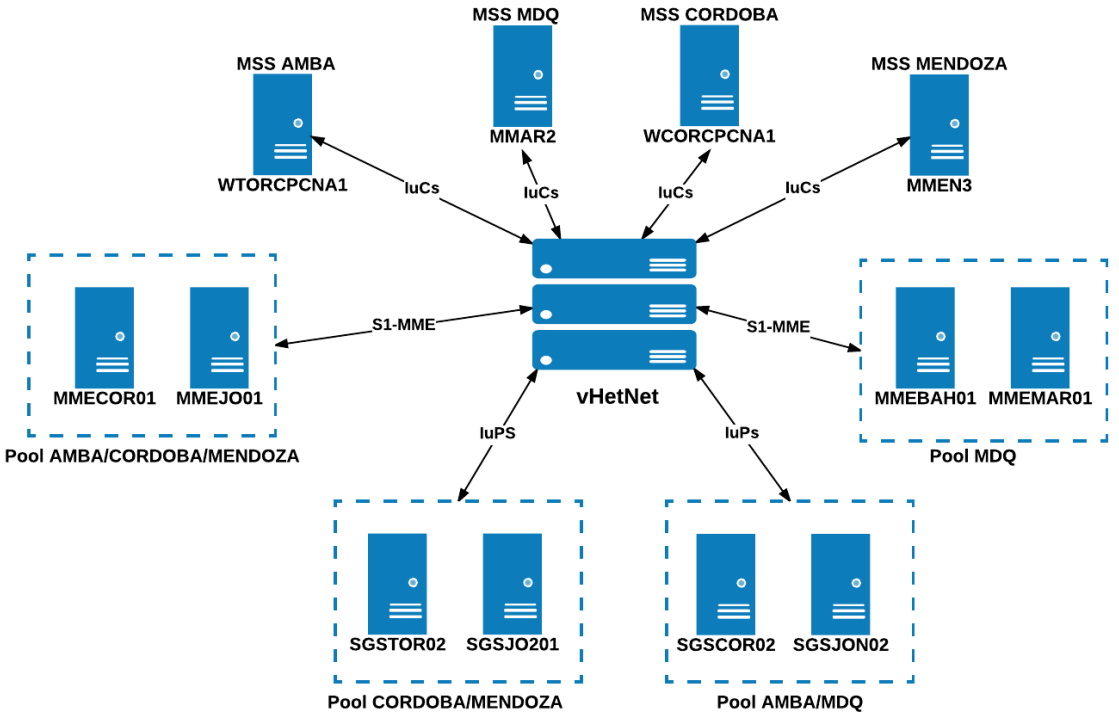
vHetNet was installed in the cluster N2A08 of UCS 5108 located in Don Torcuato Datacenter



vHetNet integration

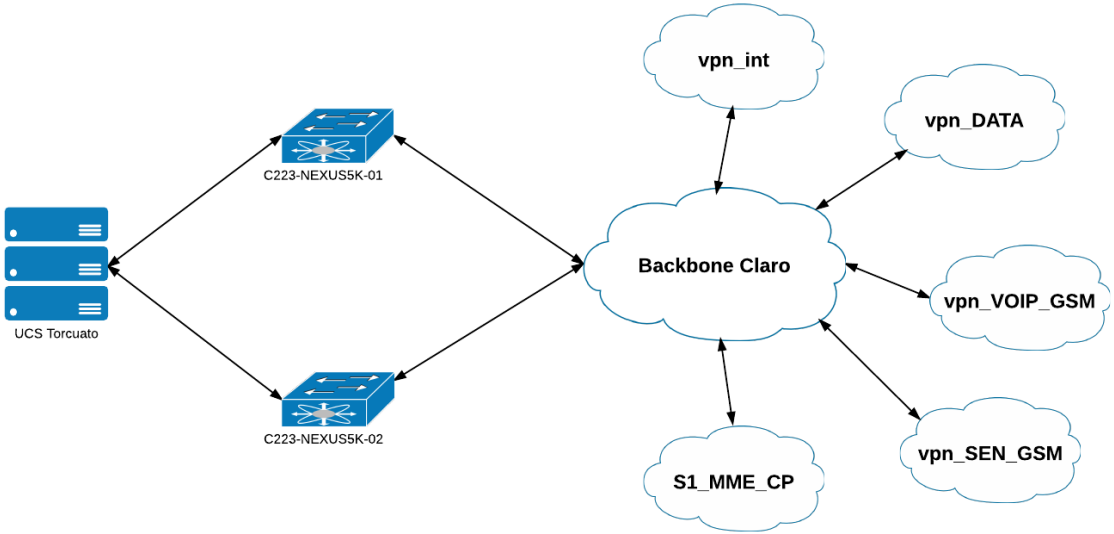
Actually integrated with 4 different pools in 3G/4G:

- AMBA
- MDQ
- CORDOBA
- MENDOZA



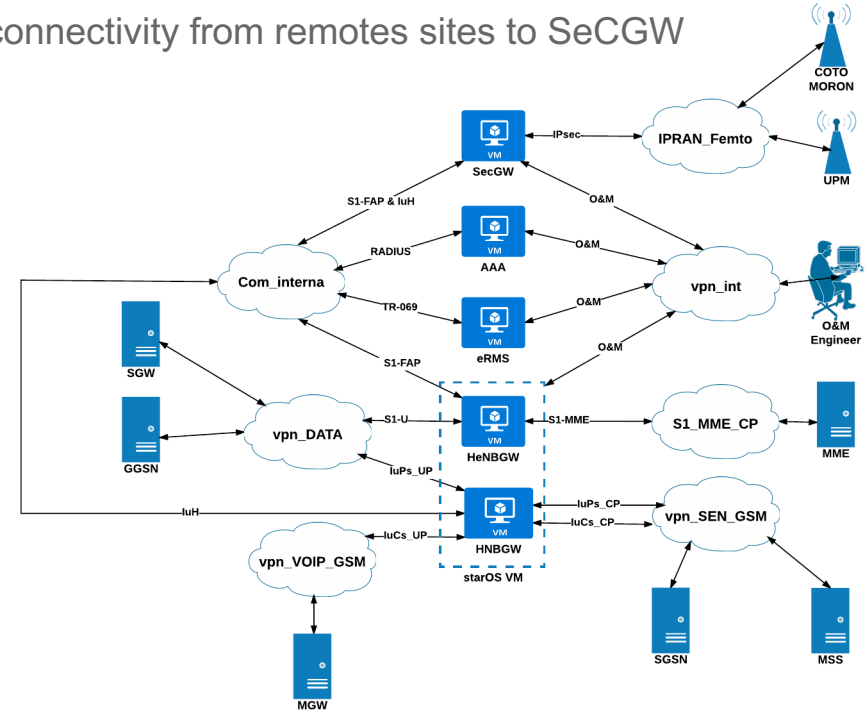
Connectivity with Claro´s CN

- 3G/4G VRFs names



VMs & VRFs Connectivity

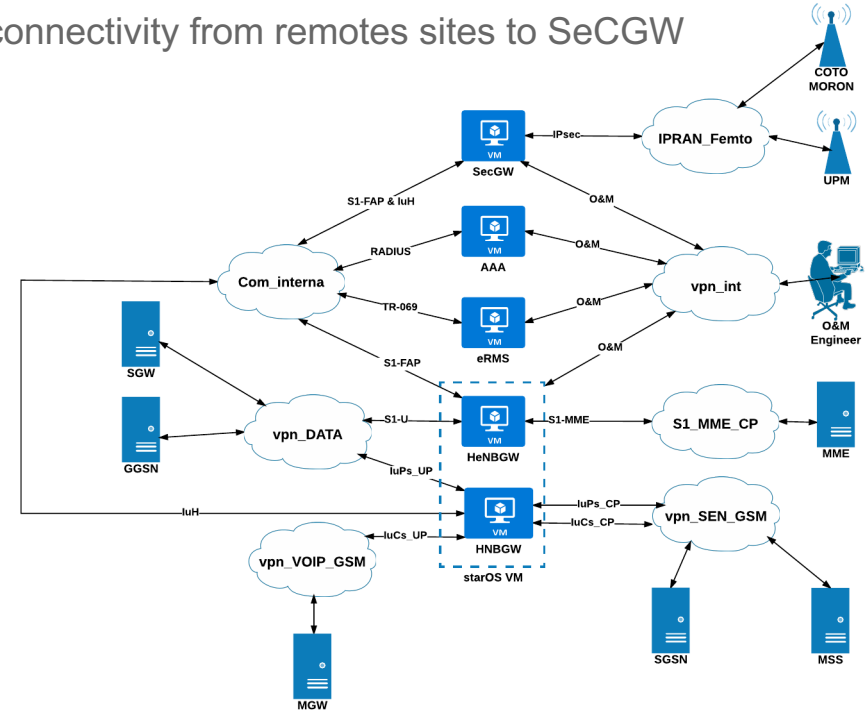
- VRF IPRAN_Femto created for this project
  - Provides IPRAN connectivity from remotes sites to SeCGW



IP Planning

VMs & VRFs Connectivity

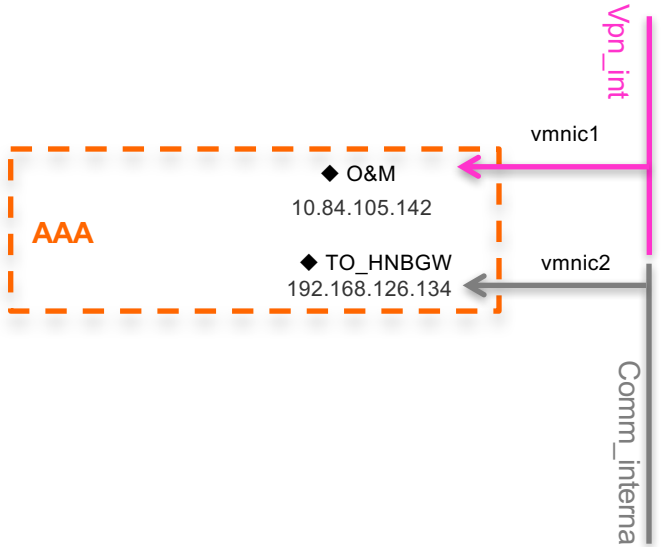
- VRF IPRAN_Femto created for this project
  - Provides IPRAN connectivity from remotes sites to SeCGW



AAA IP Details

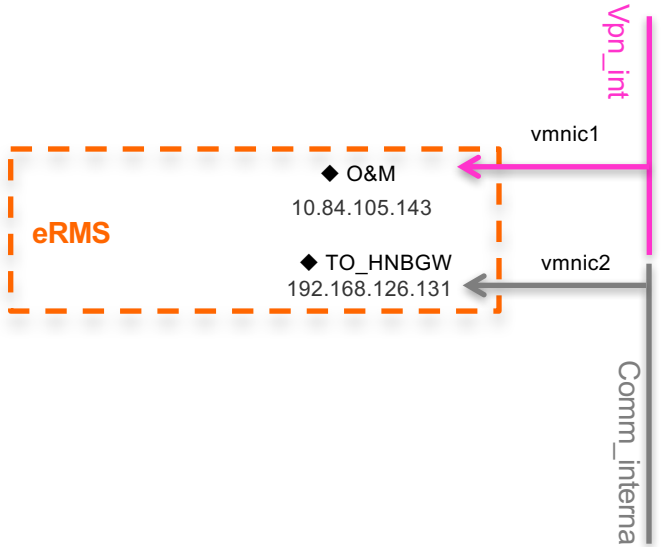
- AAA only for internal use of HNBGW during USC 8088 authentication

VM	IP	MASK	DF GW	VRF	VLAN
AAA	10.84.105.142	255.255.255.0	10.84.105.1	vpn_int	628
AAA	192.168.126.134	255.255.255.128	192.168.126.129	Comm_interna	



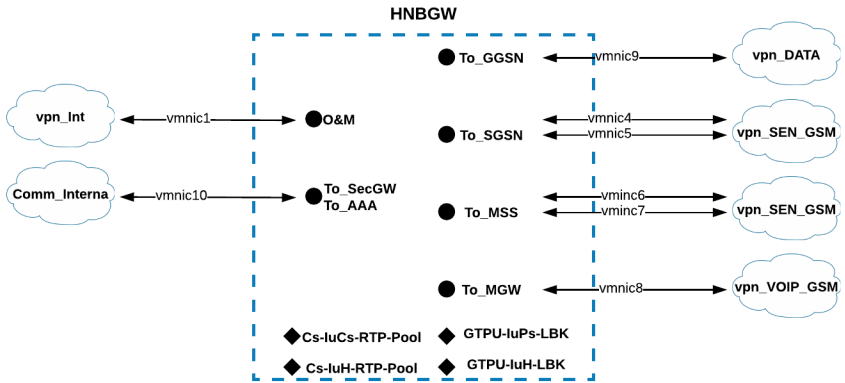
eRMS IP Details

VM	IP	MASK	DF GW	VLAN
eRMS	10.84.105.143	255.255.255.0	10.84.105.1	628
eRMS	192.168.126.131	255.255.255.128	192.168.126.129	



HNBGW Interfaces & IPs

- IuCs/IuPs control plane with redundancy ports

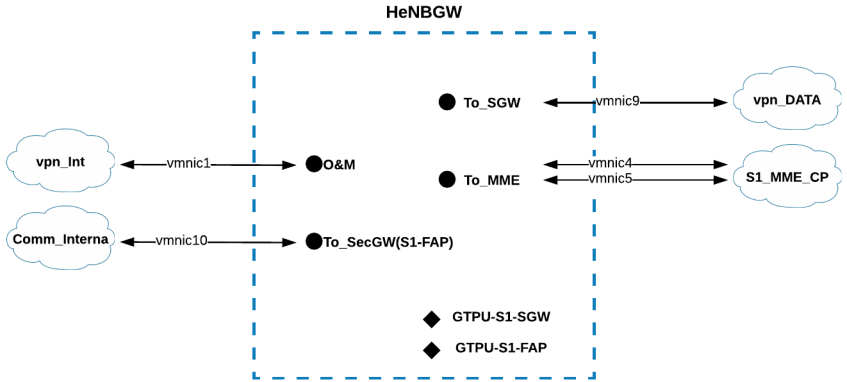


	Tipo IP	IP	MASK	DF GW	VLAN
AMBA/MDQ	Comm interna	192.168.126.132	255.255.255.128	192.168.126.129	
	IuPs_UP	10.128.29.116	255.255.255.240	10.128.29.113	232
	IuPs_CP1	10.114.26.196	255.255.255.240	10.114.26.193	238
	IuPs_CP2	10.114.96.212	255.255.255.240	10.114.96.209	239
	IuCs_CP1	10.114.96.228	255.255.255.240	10.114.96.225	240
	IuCs_CP2	10.114.96.244	255.255.255.240	10.114.96.241	241
CORDOBA/MENDOZA	IuPs_CP1	10.114.26.197	255.255.255.240	10.114.26.193	238
	IuPs_CP2	10.114.96.213	255.255.255.240	10.114.96.209	239
	IuCs_CP1	10.114.96.229	255.255.255.240	10.114.96.225	240
	IuCs_CP2	10.114.96.245	255.255.255.240	10.114.96.241	241
	IuPs_UP	10.128.29.117	255.255.255.240	10.128.29.113	232
	Comm interna	192.168.126.136	255.255.255.128	192.168.126.129	
TODAS	O&M	10.84.105.145	255.255.255.0	10.84.105.1	628
	IuCs User Plane	10.120.76.228	255.255.255.240	10.120.76.225	243
	RTP Pool_IuCs	10.120.112.224	255.255.255.224		
	RTP Pool_IuH	192.168.126.160	255.255.255.224		

HeNBGW Interfaces & IPs

- IuCs/IuPs control plane with redundancy ports

Región	Tipo IP	IP	MASK	DF GW	VLAN
AMBA/CORDOBA/ MENDOZA	S1-MME	10.139.252.228	255.255.255.240	10.139.252.225	236
MDQ	S1-MME	10.139.252.229	255.255.255.240	10.139.252.225	236
Todas	Comm interna	192.168.126.133	255.255.255.128	192.168.126.129	
Todas	S1-U	10.128.29.212	255.255.255.240	10.128.29.209	234



HNBGW Pool integration details

- 4 regions
- 2 hnbgw-service
  - Hnbgw-service
  - Hnbgw-service-cordoba
- Shared RTP pools in 4 regions
- SGSN pools are shared across regions, based on that following configuration of hnbgw was decided:
  - HNBGW 1: AMBA/MDQ: shares same hnbgw service, IuCs, IuPs & IuH IPs
  - HNBGW 2: CORDOBA/MENDOZA: shares same hnbgw service, IuCs, IuPs & IuH IPs

HeNBGW Pool integration details

- 4 regions
- 2 hnbgw-service
  - Hnbgw-service
  - Hnbgw-service-cordoba
- Shared RTP pools in 4 regions
- SGSN pools are shared across regions, based on that following configuration of hnbgw was decided:
  - HNBGW 1: AMBA/MDQ: shares same hnbgw service, IuCs, IuPs & IuH IPs
  - HNBGW 2: CORDOBA/MENDOZA: shares same hnbgw service, IuCs, IuPs & IuH IPs

HNBGW Engineering Rules

- A maximum of 16 HNB-GW service can be configured on a system which is further limited to a maximum of 256 services (regardless of type) can be configured per system.
- A maximum of 16 CS-network instances can be configured on system for HNB-GW network function but multiple HNB-GW services can be associated with the same CS-network instance.
- A maximum of 16 PS-network instances can be configured on system for HNB-GW network function but multiple HNB-GW services can be associated with the same PS-network instance.
- A particular HNB-GW service can be associated with more than one CS/PS network entity.
- A maximum of 12 HNB-SCCP-network instance can be configured on system for HNB-GW network function.
- A maximum of 1 RNC id can be configured in a Radio Network PLMN.
- A maximum of 1 SeGW IP address can be associated with an HNB-GW service.

IuCs Interface Rules

- An IuCS interface is created once the IP address of a logical interface is bound to an ASP-IP defined in the SS7-RD-instance which is defined in SCCP Network instance which is defined in CS Network configuration based on destination point-code.
- The logical interface(s) that will be used to facilitate the IuCS interface(s) must be configured within the egress context.
- CS Network services must be configured within the local context.
- Multiple MSCs (maximum 25) can be configured through IuCS interfaces within the HNB-GW service instance.

IuPs Interface Rules

- An IuPS interface is created once the IP address of a logical interface is bound to a PS Network service.
- The logical interface(s) that will be used to facilitate the IuPS interface(s) must be configured within the egress context.
- PS Network services must be configured within the local context at the system level.
- • Multiple SGSNs (maximum 25) can be configured through IuPS interfaces within the HNB-GW service

HNBGW AMBA/MDQ

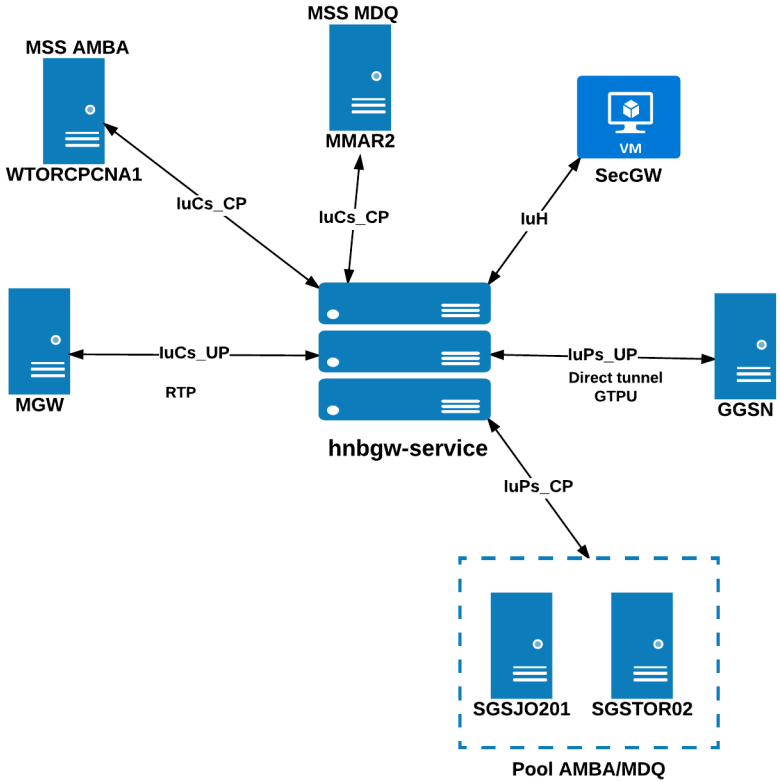
Integration with Claro´s Core

- HNBGW Service serving AMBA & MDQ
- Individual LAC/RAC per region
- Different MSS per region
- Same pool of SGSN

Region	RNC ID	LAC	RAC
AMBA	391	17169	87
MDQ	391	14188	78

HNBGW Interfaces

- IuPs_CP: IuFlex 2 SGSNs
  - SGSJO201 & SGSTOR02
- IuPS_UP: Direct Tunnel
- WTORCPCNA1 - AMBA MSS
- MMAR2 – MDQ MSS



IuPs AMBA/MDQ

- Shared SGSN pool
  - SGSJO201 & SGSTOR02
  - 10 SCTP associations for each SGSN impleme
- IuPS_UP: Direct Tunnel

Primary FEMTO IP Address	Secondary FEMTO IP Address	Primary SGSN IP Address	Secondary SGSN IP Address	SGSN
10.114.26.196	10.114.96.212	10.112.110.66	10.112.110.98	SGSTOR02-PGI3
10.114.26.196	10.114.96.212	10.112.110.99	10.112.110.67	
10.114.26.196	10.114.96.212	10.112.110.68	10.112.110.100	
10.114.26.196	10.114.96.212	10.112.110.101	10.112.110.69	
10.114.26.196	10.114.96.212	10.112.110.70	10.112.110.102	
10.114.26.196	10.114.96.212	10.112.110.103	10.112.110.71	
10.114.26.196	10.114.96.212	10.112.110.72	10.112.110.104	
10.114.26.196	10.114.96.212	10.112.110.105	10.112.110.73	
10.114.26.196	10.114.96.212	10.112.110.74	10.112.110.106	
10.114.26.196	10.114.96.212	10.112.110.107	10.112.110.75	
10.114.26.196	10.114.96.212	10.112.80.66	10.112.80.98	SGSJO201-PGI3
10.114.26.196	10.114.96.212	10.112.80.99	10.112.80.67	
10.114.26.196	10.114.96.212	10.112.80.68	10.112.80.100	
10.114.26.196	10.114.96.212	10.112.80.101	10.112.80.69	
10.114.26.196	10.114.96.212	10.112.80.70	10.112.80.102	
10.114.26.196	10.114.96.212	10.112.80.103	10.112.80.71	
10.114.26.196	10.114.96.212	10.112.80.72	10.112.80.104	
10.114.26.196	10.114.96.212	10.112.80.105	10.112.80.73	
10.114.26.196	10.114.96.212	10.112.80.74	10.112.80.106	
10.114.26.196	10.114.96.212	10.112.80.107	10.112.80.75	

IuCs AMBA

- WTORCPCNA1 acting as MSS
- 4 SCTP associations implemented

Primary FEMTO IP Address	Secondary FEMTO IP Address	Primary MGW CLUSTER IP Address	Secondary MGW CLUSTER IP Address
10.114.96.228	10.114.96.244	10.112.40.17	10.112.40.49
10.114.96.228	10.114.96.244	10.112.40.81	10.112.40.113
10.114.96.228	10.114.96.244	10.112.40.8	10.112.40.40
10.114.96.228	10.114.96.244	10.112.40.72	10.112.40.104

IuCs MDQ

- MSS is MMAR2
- 2 SCTP associations implemented

Primary FEMTO IP Address	Secondary FEMTO IP Address	Primary MGW CLUSTER IP Address	Secondary MGW CLUSTER IP Address
10.114.96.228	10.114.96.244	10.112.200.109	10.112.200.45
10.114.96.228	10.114.96.244	10.112.200.42	10.112.200.106

HNBGW CORDOBA/MENDOZA

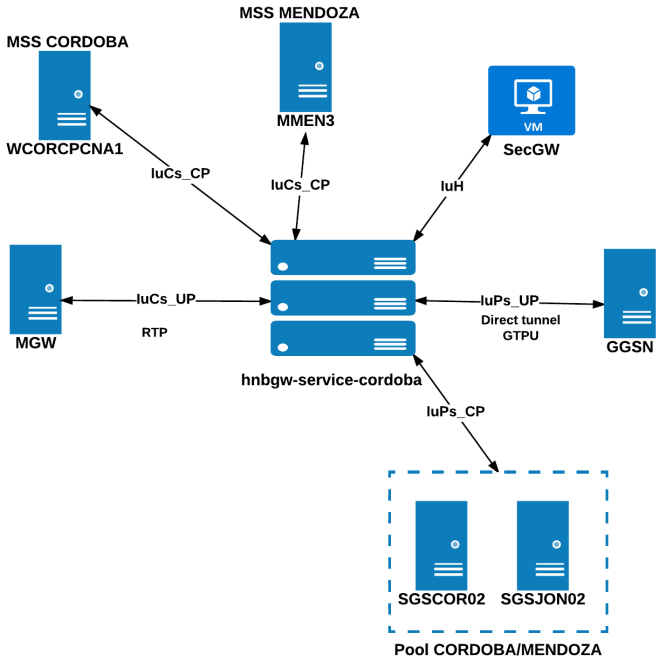
Integration with Claro´s Core

- HNBGW Service serving CORDOBA & MENDOZA
- Individual LAC/RAC per region
- Different MSS per region
- Same pool of SGSN

Region	RNC ID	LAC	RAC
CORDOBA	397	11189	80
MENDOZA	397	16288	82

HNBGW Interfaces

- IuPs_CP: IuFlex 2 SGSNs
  - SGSCOR02 & SGSJON02
- IuPS_UP: Direct Tunnel
- WCORCPCNA1- CORDOBA MSS
- MMEN– MENDOZA MSS



IuPs CORDOBA/MENDOZA

- Shared SGSN pool
  - SGSCOR02 & SGSJON02
  - 10 SCTP associations for each SGSN implemented
- IuPS_UP: Direct Tunnel

Primary FEMTO IP Address	Secondary FEMTO IP Address	Primary SGSN IP Address	Secondary SGSN IP Address	SGSN
10.114.26.197	10.114.96.213	10.112.142.12	10.112.142.44	SGSCOR02
10.114.26.197	10.114.96.213	10.112.142.13	10.112.142.45	
10.114.26.197	10.114.96.213	10.112.142.14	10.112.142.46	
10.114.26.197	10.114.96.213	10.112.142.15	10.112.142.47	
10.114.26.197	10.114.96.213	10.112.142.16	10.112.142.48	
10.114.26.197	10.114.96.213	10.112.142.17	10.112.142.49	
10.114.26.197	10.114.96.213	10.112.142.18	10.112.142.50	
10.114.26.197	10.114.96.213	10.112.142.19	10.112.142.51	
10.114.26.197	10.114.96.213	10.112.142.20	10.112.142.52	
10.114.26.197	10.114.96.213	10.112.142.21	10.112.142.53	
10.114.26.197	10.114.96.213	10.112.70.140	10.112.70.204	SGSJON02
10.114.26.197	10.114.96.213	10.112.70.141	10.112.70.205	
10.114.26.197	10.114.96.213	10.112.70.142	10.112.70.206	
10.114.26.197	10.114.96.213	10.112.70.143	10.112.70.207	
10.114.26.197	10.114.96.213	10.112.70.144	10.112.70.208	
10.114.26.197	10.114.96.213	10.112.70.145	10.112.70.209	
10.114.26.197	10.114.96.213	10.112.70.146	10.112.70.210	
10.114.26.197	10.114.96.213	10.112.70.147	10.112.70.211	
10.114.26.197	10.114.96.213	10.112.70.148	10.112.70.212	
10.114.26.197	10.114.96.213	10.112.70.149	10.112.70.213	

IuCs CORDOBA

- WCORCPCNA1 acting as MSS
- 4 SCTP associations implemented

Primary FEMTO IP Address	Secondary FEMTO IP Address	Primary MGW CLUSTER IP Address	Secondary MGW CLUSTER IP Address
10.114.96.229	10.114.96.245	10.114.7.5	10.114.7.37
10.114.96.229	10.114.96.245	10.114.7.9	10.114.7.41
10.114.96.229	10.114.96.245	10.114.13.112	10.114.13.144
10.114.96.229	10.114.96.245	10.114.13.105	10.114.13.137

IuCs MENDOZA

- MSS is MMEN3
- 2 SCTP associations implemented

Primary FEMTO IP Address	Secondary FEMTO IP Address	Primary MGW CLUSTER IP Address	Secondary MGW CLUSTER IP Address
10.114.96.229	10.114.96.245	10.114.14.10	10.114.14.2
10.114.96.229	10.114.96.245	10.114.14.3	10.114.14.11

HeNBGW Architecture

Integration with Claro´s Core

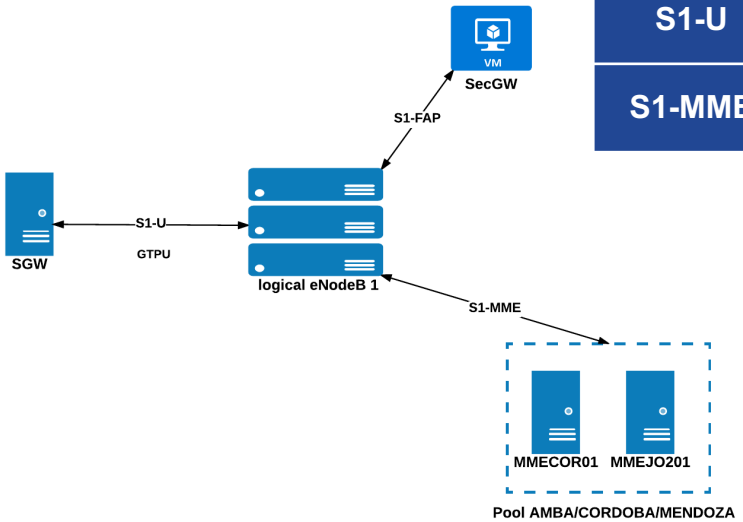
- Based on Claro´s 4G core architecture the following configuration has been implemented:
  - 2 logical eNodeBs, same hengw-service:
    - Logical eNodeB 1: MDQ
    - Logical eNodeB 2: AMBA-CORDOBA-MENDOZA

- MME Pool dedicated for MDQ
- Shared S1-U (GTPU) among regions AMBA/MDQ/CORDOBA/MENDOZA

- TAC-LAC mapping done at MME levels with corresponding TAC-LAC assigned per region

HeNBGW AMBA/CORDOBA/MENDOZA

IP Planning



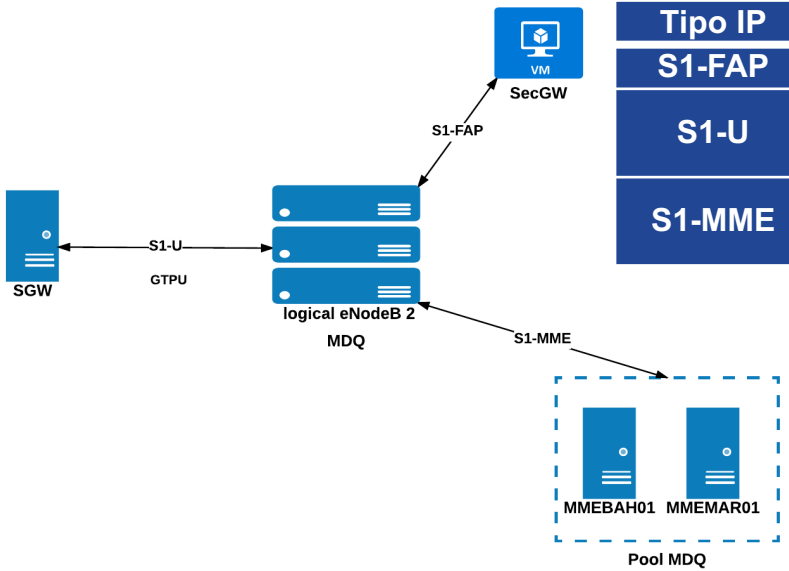
Tipo IP	IP	MASK	DF GW	VRF	VLAN
S1-FAP	192.168.126.133	255.255.255.128	192.168.126.129		
S1-U	10.128.29.212	255.255.255.240	10.128.29.209	vpn_DATA	234
S1-MME	10.139.252.228	255.255.255.240	10.139.252.225	S1_MME_CP	236

REGION	MME	IP
AMBA/CORDOBA/MENDOZA	MMECOR01	10.113.220.60
AMBA/CORDOBA/MENDOZA	MMEJO201	10.113.231.84

Region	TAC
AMBA	46169
CORDOBA	41189
MENDOZA	46288

HeNBGW MDQ

IP Planning



Tipo IP	IP	MASK	DF GW	VRF	VLAN
S1-FAP	192.168.126.133	255.255.255.128	192.168.126.129		
S1-U	10.128.29.212	255.255.255.240	10.128.29.209	vpn_DATA	234
S1-MME	10.139.252.229	255.255.255.240	10.139.252.225	S1_MME_CP	236

REGION	MME	IP
MDQ	MMEBAH01	10.113.231.172
MDQ	MMEMAR01	10.114.35.4

Region	TAC
MDQ	44188

eRMS(SpiderNet) Fault Management

Fault Mangenement

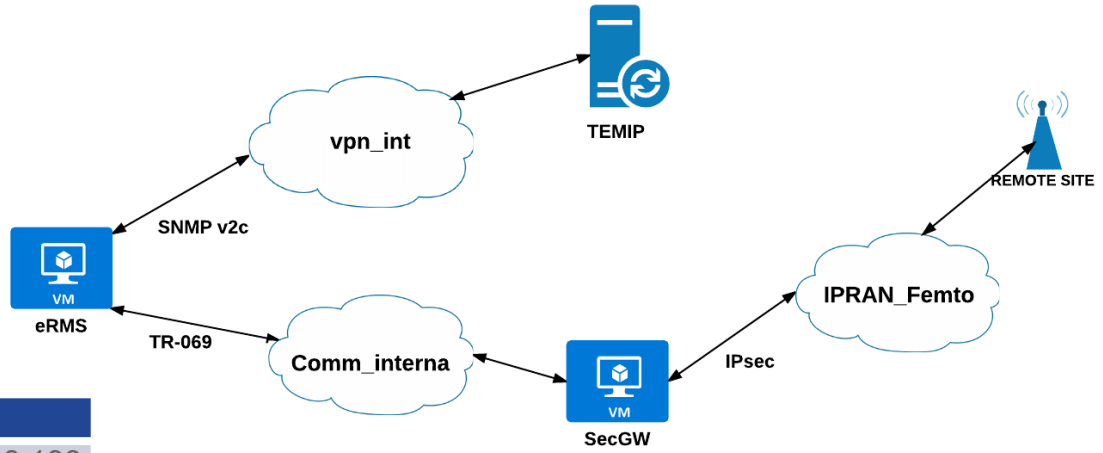
- Fault management and Small Cell monitoring is a key challenge for the service provider managing their Small cell networks
- Fault management refers to eRMS generated alarms, such as connection loss to a managed services node, alarms generated by individual services nodes and their managed cells.
- eRMS(SpiderNet) has been integrated with Claro´s TEMIP.
- Successfully tested different alarms raises in TEMIP with the AM created based on the specific MIBs.
-

Protocols

- eRMS(SpiderNet) uses the following fault management protocols:
- **SNMP:** Services nodes send SNMPv2c and SNMPv3 trap and inform messages to the eRMS server.
- **TR-069:** used by eRMS- Serving Node tosynchronize current alarms
- eRMS displays alarms and events based upon four sources:
  - SNMP traps sent by services nodes
  - The current alarm table contained in the services node data model
  - Internal alarms and events generated by internal modules of the eRMS server
  - Syslog events

Integration with TEMIP

- eRMS (SpiderNet) actually integrated with Claro TEMIP
- Successfully tested differnet alarms



Tipo IP	IP
O&M eRMS	192.168.126.133
TEMIP	10.92.50.194

Troubleshooting in vHetNet

Topics Covered

- Licensing
- HNB-GW Configuration
- Show commands
- Debug Commands

Config -HNBGW

```
  context HNBGW
    ip pool IPSEC-1 10.116.170.0 255.255.255.0 group-name IPSEC public 0 policy allow-
static-allocation
    ip pool IPSEC-2 10.116.171.0 255.255.255.0 group-name IPSEC public 0 policy allow-
static-allocation
    ip pool IPSEC-3 10.116.172.0 255.255.255.0 group-name IPSEC public 0 policy allow-
static-allocation
    ip pool IPSEC-4 10.116.172.0 255.255.255.0 group-name IPSEC public 0 policy allow-
static-allocation
    ipsec transform-set IPSEC
    #exit
    ikev2-ikesa transform-set IKE
    #exit
    crypto template SECURITY ikev2-dynamic
      authentication local certificate
      authentication remote certificate
      ikev2-ikesa transform-set list IKE
      keepalive interval 30 timeout 40 num-retry 3
      payload segwsa match childsa match ipv4
        ip-address-alloc dynamic
        ipsec transform-set list IPSEC
      #exit
      certificate asr5k
      ca-certificate list ca-cert-name client
    #exit
    interface 17/2-Iuh-1
      ip address 10.10.65.129/27
    #exit
    interface 17/2-Iuh-2
      ip address 10.10.65.161/27
    #exit
    interface 17/4-RMS-1
      ip address 10.10.65.68/27
    #exit
    interface Iuh_GTPU_Loopback loopback
      ip address 10.10.65.193 255.255.255.255
    #exit
    interface Iuh_Loopback loopback
      ip address 10.10.65.194 255.255.255.255
    #exit
    interface SeGW_Loopback loopback
      ip address 190.238.35.254 255.255.255.255
    #exit
    subscriber default
      dhcp service CNR context HNBGW
      ip address pool name IPSEC
    exit
    aaa group default
      radius attribute nas-ip-address address 10.10.65.68
      radius server xxx.xxx.xxx.xxx encrypted key
+A38zcu3rlekd8814cl004m2pn2m12wcj5nakja813a341unxdaz85 port 1812
    #exit
    gtpp group default
    #exit
    gtpu-service HNB_GTPU
      bind ipv4-address 10.10.65.193
    exit
    dhcp-service CNR
      dhcp client-identifier ike-id
      dhcp server xxx.xxx.xxx.xxx
      lease-time 7200
      no dhcp chaddr-validate
      dhcp server selection-algorithm round-robin
      dhcp server port 61610
      bind address 10.10.65.68
    #exit
    hnbgw-service hnbgw1
      sctp bind address 10.10.65.194
      sctp bind port 29169
      associate gtpu-service HNB_GTPU
      sctp sack-frequency 5
      sctp sack-period 5
      no ue registration-timeout
      hnb-access-mode mismatch-action accept-aaa-value
      radio-network-plmn mcc 716 mnc 06
        rnc-id 18
      security-gateway bind address 190.238.35.254 crypto-template SECURITY context HNBGW
    #exit
    ip route 0.0.0.0 0.0.0.0 xxx.xxx.xxx.xxx 17/1-Iuh-1
    ip route 0.0.0.0 0.0.0.0 xxx.xxx.xxx.xxx 17/1-Iuh-2
    ip igmp profile default
    #exit
```

Config Iu & IuPS

```
context Iu
    #exit
    subscriber default
    exit
    aaa group default
    #exit
    gtpp group default
    #exit
    alcap-service al1
      associate ss7-routing-domain 1
      self-point-code 14621
      aal2-route endpoint default aal2-node nod
      aal2-node node1
        point-code 14399
        aal2-path-id 1
        aal2-path-id 2
          aal2-path-id 3
          aal2-path-id 4
          aal2-path-id 5
          aal2-path-id 6
          aal2-path-id 7
          aal2-path-id 8
          aal2-path-id 9
          aal2-path-id 10
          aal2-path-id 11
          aal2-path-id 12
          aal2-path-id 13
          aal2-path-id 14
          aal2-path-id 15
          aal2-path-id 16
```

```
context IuPS
    interface 17/1-IUPS-1
      ip address 10.10.65.225/27
    #exit
    interface IuPS_CP_Loopback1 loopback
      ip address 10.10.219.129 255.255.255.255
    #exit
    interface IuPS_CP_Loopback2 loopback
      ip address 10.10.219.130 255.255.255.255
    #exit
    interface IuPS_UP_Loopback1 loopback
      ip address 190.238.35.252 255.255.255.255
    #exit
    interface IuPS_UP_Loopback2 loopback
      ip address 190.238.35.253 255.255.255.255
    #exit
    subscriber default
    exit
    aaa group default
    #exit
    gtpp group default
    #exit
    gtpu-service gtpu_ps1
      echo-interval 60
      max-retransmissions 10
      bind ipv4-address 190.238.35.252
    exit
    gtpu-service gtpu_ps2
      echo-interval 60
      max-retransmissions 10
      bind ipv4-address 190.238.35.253
    exit
    ip route 0.0.0.0 0.0.0.0 xxx.xxx.xxx.xxx 17/1-IUPS-1
    ip igmp profile default
    #exit
```

Config - Global

```
ss7-routing-domain 1 variant itu
    ssf reserved
    linkset id 1
      self-point-code 14621
      adjacent-point-code 14399
      link id 1 link-type atm-broadband
        priority 0
        signaling-link-code 0
        arbitration active
      #exit
      link id 2 link-type atm-broadband
        priority 0
        signaling-link-code 1
        arbitration active
      #exit
    #exit
    route destination-point-code 14399 linkset-id 1
    route destination-point-code 14392 linkset-id 1
#exit
ss7-routing-domain 10 variant itu
    ssf reserved
    routing-context 1
    asp instance 1
      end-point port 2934
      end-point address 10.10.219.129 context IuPS
      end-point bind
    #exit
    asp instance 2
      end-point port 2935
      end-point address 10.10.219.130 context IuPS
      end-point bind
    #exit
    peer-server id 1
      name SGSN-SI02
      mode loadshare
      routing-context 1
      self-point-code 14600
      psp instance 1
        psp-mode server
        exchange-mode single-ended
        routing-context discard-inbound suppress-outbound
        timeout sctp-heart-beat 300
        end-point port 2934
        end-point address 10.10.236.90
        associate asp instance 1
      #exit
      psp instance 2
        psp-mode server
        exchange-mode single-ended
        routing-context discard-inbound suppress-outbound
        timeout sctp-heart-beat 300
        end-point port 2935
        end-point address 10.10.236.91
        associate asp instance 2
      #exit
#exit
sccp-network 10 variant itu
    self-point-code 14621
    associate ss7-routing-domain 10
    destination dpc 14600 name SGSN-SI02
    destination dpc 14600 version ITU96
    destination dpc 14600 ssn 142
#exit
sccp-network 1 variant itu
    self-point-code 14621
    associate ss7-routing-domain 1
    destination dpc 14392 name MSC
    destination dpc 14392 version ITU96
    destination dpc 14392 ssn 142
#exit
ps-network ps1
    associate sccp-network 10
    sgsn point-code 14600
    no sgsn deadtime
    global-rnc-id mcc 716 mnc 06 id 18
    associate gtpu-service gtpu_ps1 context-name IuPS
    associate gtpu-service gtpu_ps2 context-name IuPS
#exit
cs-network cs1
    associate sccp-network 1
    associate alcap-service all context Iu
    msc point-code 14392
    no msc deadtime
    ranap reset hnbgw-initiated
    global-rnc-id mcc 716 mnc 06 id 18
#exit
hnbgw-global
    paging open-hnb hnb-where-ue-registered fallback always
#exit
```

Config – Port/Binding

```
port ethernet 17/1
    preferred slot 17
    no shutdown
    vlan XXX
      no shutdown
      bind interface 17/1-IUPS-1 IuPS
    #exit
  #exit
  port ethernet 17/2
    preferred slot 17
    no shutdown
    vlan XXX
      no shutdown
      bind interface 17/2-Iuh-1 HNBGW
    #exit
    vlan XXX
      no shutdown
      bind interface 17/2-Iuh-2 HNBGW
    #exit
  #exit
  port ethernet 17/3
    preferred slot 17
    shutdown
  #exit
  port ethernet 17/4
    preferred slot 17
    no shutdown
    vlan XXX
      no shutdown
      bind interface 17/4-RMS-1 HNBGW
    #exit
  #exit
  port atm 19/1
    no shutdown
    pvc vpi 1 vci 34 type aal5
      no shutdown
      bind link ss7-routing-domain 1 linkset-id 1 link-id 1
    #exit
    pvc vpi 1 vci 35 type aal5
      no shutdown
      bind link ss7-routing-domain 1 linkset-id 1 link-id 2
    #exit
    pvc vpi 1 vci 40 type aal2 cps-payload-size 45
      no shutdown
      bind alcap-service al1 context Iu aal2-node node1 aal2-path 1
    #exit
    pvc vpi 1 vci 41 type aal2 cps-payload-size 45
      no shutdown
      bind alcap-service al1 context Iu aal2-node node1 aal2-path 2
    #exit
    pvc vpi 1 vci 42 type aal2 cps-payload-size 45
      no shutdown
      bind alcap-service al1 context Iu aal2-node node1 aal2-path 3
```

HNB-GW Services

- show service all

```
ContextID   ServiceID   ContextName   ServiceName   State         MaxSessions   Type
---------   ---------   -----------   -----------   ----------    -----------   ----
2           1           HNBGW         HNB_GTPU      Started       0             gtpu
2           2           HNBGW         CNR           Started       0             dhcp
2           3           HNBGW         HNBGW         Started       460000        hnbgw
3           4           IU            IuPS                  Started       0             gtpu
```

Show Commands for HNB-GW

HNB-GW Commands:

- show hnbgw sessions full all
- show hnbgw disconnect-reasons
- show hnbgw counters
- show hnbgw statistics
- show hnbgw sessions summary
- show hnbgw sessmgr all memory statistics (hidden CLI)
- show hnbgw sessmgr all internal statistics (hidden CLI)
- show demux-mgr statistics hnbmgr full

Debug logging for HNB

Debug logging

- ASR-5K# logging filter active facility hnbmgr level debug
- ASR-5K# logging filter active facility hnb-gw level debug
- ASR-5K# logging filter active facility sessmgr level debug
- ASR-5K# logging filter active facility aaamgr level debug
- ASR-5K# logging filter active facility radius-auth level debug
- ASR-5K# logging active

Monitor Protocol

- ASR-5K# mon pro
- Options –72 (HNBAP) , 73(RUA) and 56 (RANAP

Show Commands for HNB-GW IU-CS and IU-PS

- show cs-network all
- show ps-network all
- show ss7-routing-domain all
- show sccp-network all
- show ss7-routing-domain 1 m3ua status peer-server all
- show sccp-network 1 status all
- show ss7-routing-domain 1 sctp asp all status gen
- show subscribers hnbgw-only full imsi <IMSI>
- show subscribers hnbgw-service <Service_Name>

Debug logging for IU-CS and IU-PS Setup

Debug logging

- ASR-5K# logging filter active facility sctp level debug
- ASR-5K# logging filter active facility m3ua level debug
- ASR-5K# logging filter active facility sccp level debug
- ASR-5K# logging filter active facility linkmgr level
- ASR-5K#logging active

Mon Protocol

- ASR-5K# mon pro

Mon-sub/Protocol Examples

```
Monday October 06 2014
INBOUND>>>>>  20:30:19:671 Eventid:122903(3)
IKEv2 Rx PDU, from 172.242.94.115:4500 to 208.245.34.96:4500 (304)
+ IKE Header Processed-Dump, HBO (Length: 28 (0x1C) bytes)
   Initiator SPI  (U64): 0xDF491F78606B81F4
   Responder SPI  (U64): 0x0000000000000000
   Next Payload   (U08): SA/33 (0x21)
   Major Version  (U04): 2
   Minor Version  (U04): 0
   XCHG Type      (U08): IKE_SA_INIT/34 (0x22)
   Reserved       (U03): 0
   Initiator Flag (U01): Initiator/1 (0x01)
   Version Flag   (U01): 0
   Response Flag  (U01): 0
   Reserved       (U02): 0
   MSGID          (U32): 0
   Length         (U32): 304 (0x130) bytes
+ SA Payload Processed-Dump, HBO (Length: 48 (0x30) bytes)
   Next Payload   (U08): KE/34 (0x22)
   Critical       (U01): 0
   Reserved       (U07): 0
   Payload Length (U16): 48 (0x30) bytes
   Proposal Substructure:
    Last               (U08): Yes/0 (0x00)
    Reserved           (U08): 0
    Proposal Length    (U16): 44 (0x2C) bytes
    Proposal Number    (U08): 1
    Protocol ID        (U08): IKE/1 (0x01)
    SPI Size           (U08): 0 (0x0) bytes
    Number of Transforms (U08): 4
    Transform Header #1
     Last              (U08): No/3 (0x03)
     Reserved          (U08): 0
     Transform Length  (U16): 12 (0xC) bytes
     Transform Type    (U08): ENCR/1 (0x01)
     Reserved          (U08): 0
     Transform ID      (U16): ENCR_AES_CBC/12 (0x000C)
     Attribute
      Attribute AF     (U01): 1
      Attribute Type   (U15): IKEV2_TS_ATTRIBUTE_TYPE_KEY_LENGTH/14
(0x0E)
      Attribute Value  (U16): 128 (0x0080)
    Transform Header #2
```

```
-------------------------------------------------------------------------------
Incoming Call:
-------------------------------------------------------------------------------
 MSID/IMSI  :                    Callid     : 08588930
 IMEI       : n/a                MSISDN     : n/a
 Username   : n/a                SessionType : ggsn-pdp-type-ipv6
 Status     : Active             Service Name: awn_hnbgw
 Src Context : femto_source_1    Dest Context: femto_source_1
-------------------------------------------------------------------------------

Thursday December 04 2014
INBOUND>>>>>  21:21:46:998 Eventid:152001(18)

===> RANAP User Adaption (RUA) (103 bytes)
 RUA PDU
 | 0... .... | Ext bit : 0
 | .00. .... | Choice index : Initiating Message (0)
  Procedure Code : id-Connect (1)
  Criticality
   | 01.. .... | Ignore (1)
  Connect Value :
   | .110 0011 | Length Determinant : 99
   Value :
    Connect
     | 0... .... | Ext bit : 0
     Bit map :
      | .0.. .... | Connect Extensions : Not present
     Connect IEs
      IEs Count : 5
       IE : 1
        Protocol IE ID : CN Domain Indicator (7)
        Criticality
         | 00.. .... | Reject (0)
        CN Domain Indicator Value :
         | .000 0001 | Length Determinant : 1
         Value :
          | 0... .... | cs-domain (0)
       IE : 2
        Protocol IE ID : Context ID (3)
        Criticality
         | 00.. .... | Reject (0)
        Context ID Value :
         | .000 0011 | Length Determinant : 3
         Value :
          | 0000 0000 | + 16 bits : 0x000020
```

Config/Monsub Attachments

Mon-protocol sample

```
Monday October 06 2014
INBOUND>>>>>  20:30:19:671 Eventid:122903(3)
IKEv2 Rx PDU, from 172.242.94.115:4500 to 208.245.34.96:4500 (304)
+ IKE Header Processed-Dump, HBO (Length: 28 (0x1C) bytes)
   Initiator SPI  (U64): 0xDF491F78606B81F4
   Responder SPI  (U64): 0x0000000000000000
   Next Payload   (U08): SA/33 (0x21)
   Major Version  (U04): 2
   Minor Version  (U04): 0
   XCHG Type      (U08): IKE_SA_INIT/34 (0x22)
   Reserved       (U03): 0
   Initiator Flag (U01): Initiator/1 (0x01)
   Version Flag   (U01): 0
   Response Flag  (U01): 0
   Reserved       (U02): 0
   MSGID          (U32): 0
   Length         (U32): 304 (0x130) bytes
+ SA Payload Processed-Dump, HBO (Length: 48 (0x30) bytes)
   Next Payload   (U08): KE/34 (0x22)
   Critical       (U01): 0
   Reserved       (U07): 0
   Payload Length (U16): 48 (0x30) bytes
   Proposal Substructure:
    Last               (U08): Yes/0 (0x00)
    Reserved           (U08): 0
    Proposal Length    (U16): 44 (0x2C) bytes
    Proposal Number    (U08): 1
    Protocol ID        (U08): IKE/1 (0x01)
    SPI Size           (U08): 0 (0x0) bytes
    Number of Transforms (U08): 4
    Transform Header #1
     Last               (U08): No/3 (0x03)
     Reserved           (U08): 0
     Transform Length   (U16): 12 (0xC) bytes
     Transform Type     (U08): ENCR/1 (0x01)
     Reserved           (U08): 0
     Transform ID       (U16): ENCR_AES_CBC/12 (0x000C)
     Attribute
      Attribute AF      (U01): 1
      Attribute Type    (U15): IKEV2_TS_ATTRIBUTE_TYPE_KEY_LENGTH/14
(0x0E)
      Attribute Value   (U16): 128 (0x0080)
    Transform Header #2
```

Mon-sub sample

```
-----------------------------------------------------------------------
Incoming Call:
-----------------------------------------------------------------------
 MSID/IMSI   :                       Callid     : 08588930
 IMEI        : n/a                  MSISDN     : n/a
 Username    : n/a                     SessionType : ggsn-pdp-type-ipv6
 Status      : Active                 Service Name: awn_hnbgw
 Src Context : femto_source_1          Dest Context: femto_source_1
-----------------------------------------------------------------------

Thursday December 04 2014
INBOUND>>>>>  21:21:46:998 Eventid:152001(18)

===> RANAP User Adaption (RUA) (103 bytes)
  RUA PDU
  | 0... .... | Ext bit : 0
  | .00. .... | Choice index : Initiating Message (0)
   Procedure Code : id-Connect (1)
   Criticality
    | 01.. .... | Ignore (1)
   Connect Value :
    | .110 0011 | Length Determinant : 99
    Value :
     Connect
      | 0... .... | Ext bit : 0
      Bit map :
       | .0.. .... | Connect Extensions : Not present
      Connect IEs
       IEs Count : 5
        IE : 1
         Protocol IE ID : CN Domain Indicator (7)
         Criticality
          | 00.. .... | Reject (0)
         CN Domain Indicator Value :
          | .000 0001 | Length Determinant : 1
          Value :
           | 0... .... | cs-domain (0)
        IE : 2
         Protocol IE ID : Context ID (3)
         Criticality
          | 00.. .... | Reject (0)
         Context ID Value :
          | .000 0011 | Length Determinant : 3
          Value :
           | 0000 0000 | + 16 bits : 0x000020
```

Config sample

```
[local]HNBGW-POD# show config
config
  logging filter runtime facility all level trace critical-info
  logging disable eventid 10171
  logging disable eventid 10800
  no logging console
  license key "\
VER=1|DOI=1432184386|DOE=1448081986|ISS=1|NUM=78514|CMT=Atlanta_Sug
arl\
oaf_Lab_-_AT&T_Provisioning_Femto_#2|LSG=10000|FIS=Y|FR4=Y|FSR=Y|FID=Y\
|FI6=Y|FLI=Y|FCA=Y|FAA=Y|FSG=Y|HIL=XT2|FAP=Y|FGT=Y|LHN=250000|LHR=10
00\
000|FMX=Y|LIP=250000|LIU=11000|SIG=MC4CFQCb0nqqwv+0VqnIU8bBCJEUQBQ
5gAI\
VAMKRXSp1e41GH76kr67cs7iqlXRH"
  system hostname HNBGW-POD
  autoconfirm
  clock timezone us-central
  cli configuration-monitor
  orbem
    ssl-certificate string "-----BEGIN CERTIFICATE-----\n\
MIIELDCCA5WgAwIBAgIBATANBgkqhkiG9w0BAQQFADCBsTELMAkGA1UEBhMCV
VMx\n\
FjAUBgNVBAgTDU1hc3NhY2h1c2V0dHMxEjAQBgNVBAcTCVRld2tzYnVyeTEeMBw
G\n\
A1UEChMVU3RhcmVudCBOZXR3b3JrcyBJbmMuMSIwIAYDVQQLExlFbGVtZW50IE1
h\n\
bmFnZW1lbnQgU3lzdGVtMQ4wDAYDVQQDEwVPUkJFTTEiMCAGCSqGSIb3DQEJAR
YT\n\
b3JiZW1AbnVsaW5raW5jLmNvbTAeFw0wMjA5MDYxMjE5MTNaFw0yMjA5MDEx
MjE5\n\
MTNaMIGxMQswCQYDVQQGEwJVUzEWMBQGA1UECBMNTWFzc2FjaHVzZXR0czES
MBAG\n\
A1UEBxMJVGV3a3NidXJ5MR4wHAYDVQQKExVTdGFyZW50IE5ldHdvcmtzIEluYy4x
\n\
IjAgBgNVBAsTGUVsZW1lbnQgTWFuYWdlbWVudCBTeXN0ZW0xDjAMBgNVBAMTB
U9S\n\
QkVNMSIwIAYJKoZIhvcNAQkBFhNvcmJlbUBudWxpbmtpbmMuY29tMIGfMA0GCSq
G\n\
SIb3DQEBAQUAA4GNADCBiQKBgQC6Dh79iaK/zZG/Kwme2XS6G8/n3/+sac6huxI1
\n\
WNyammyYZKZpXTjHUlS92fvn0UUM4tFjN4XoqveSiqy3IqUhnVKS3+0L7s9beanQ\
n\
UJuR9MdLy9Ho7qh720wpN4isqN7YfGLoqGslLQjhS8z6ZT0ZUhyusY0rE6yHTV23\n
\
```

Logging Facilites - HeNBGW

- The following logging facilities can be used for troubleshooting HENB-GW:
- • henbgw
  • henbgwdemux
  • henbgwmgr
  • henbapp
  • gtpumgr
  • egtpu
  • ipsec
  • ikev2
  • sessmgr
  • henbgw-sctp-acs • henbgw-sctp-nw

Hands On Demonstration

Backup

CBS support

3GPP Warning Systems

The following warning solutions are considered:

- **ETWS** (Earthquake Tsunami Warning System).
- **PWS:** Generic warning service.
- **CMAS**: US warning system.
- **EU-Alert**: EU warning system.

Standards	
ETWS:	3GPP TS 22.168
PWS:	3GPP TS 22.268
CMAS:	ATIS-0700010
EU-Alert:	ETSI TS 102 900

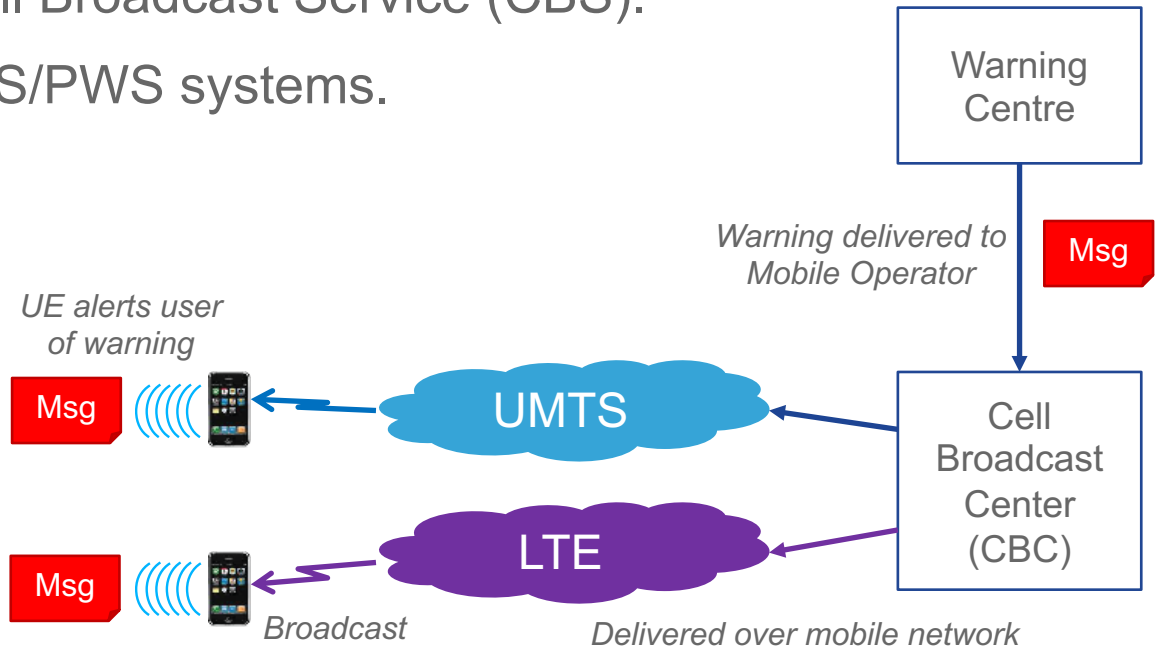
USC 8k Support	
ETWS:	No
PWS:	Partial
CMAS:	Yes
EU-Alert:	Yes

ETWS vs PWS

- **ETWS** (3GPP Rel 8):
  - Targeted at rapid delivery of a single urgent warning.
  - Primary Alert: 2 bytes of critical information delivered < 4s.
  - Secondary Alert: additional warning information that may take longer to be delivered.
- **PWS** (3GPP Rel 9):
  - Generic warning and broadcast information service.
  - Supports broadcast of multiple concurrent warnings.
- CMAS and EU-Alert carried by the PWS service.

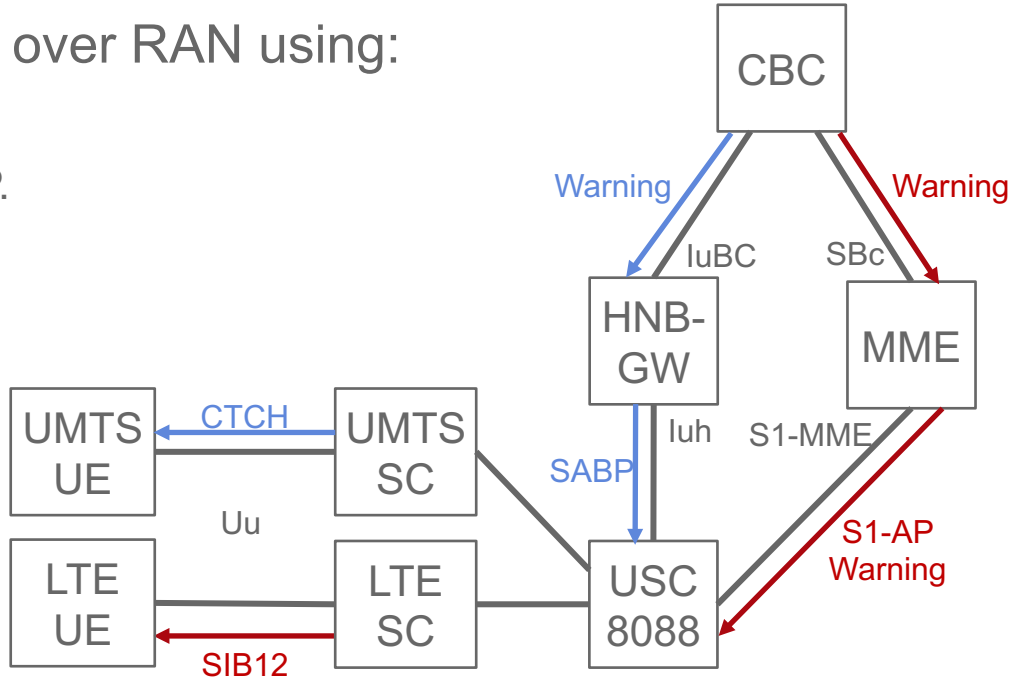
Warning System Architecture (General)

- UMTS: Carried by Cell Broadcast Service (CBS).
- LTE: Carried by ETWS/PWS systems.



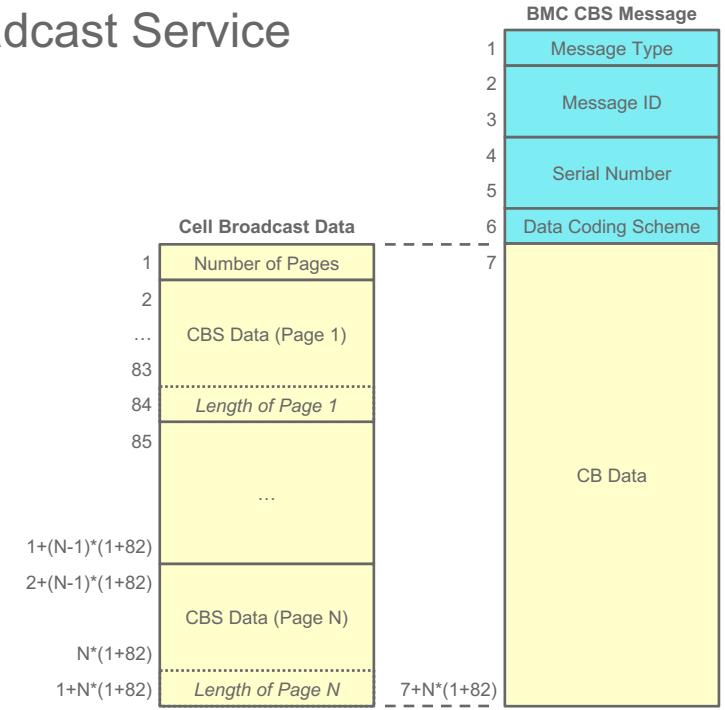
Supporting Warnings in the RAN

- Warnings messages delivered over RAN using:
  - UMTS: CBS service.
    - Delivered over IuBC using SABP.
    - Broadcast on CTCH.
  - LTE: PWS service.
    - Delivered over S1-AP.
    - Broadcast in SIB12.



Warning Message Support

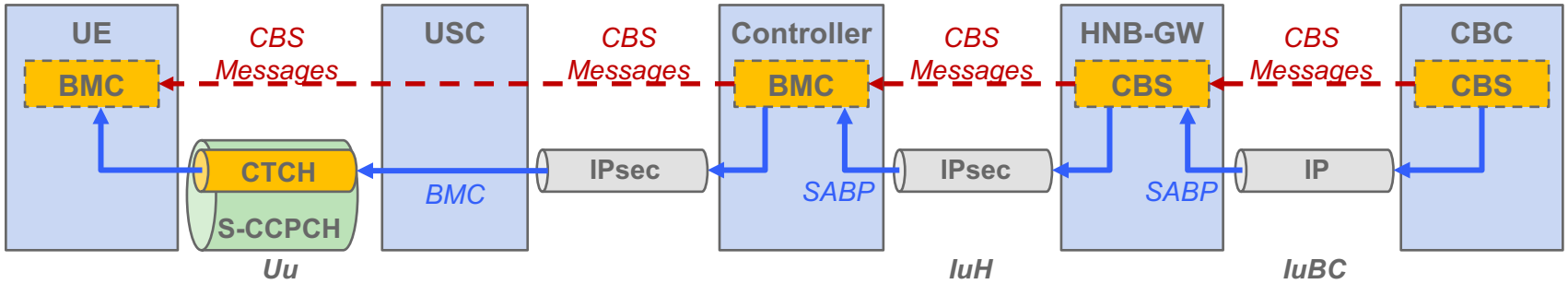
- Warning carried over mobile network in Cell Broadcast Service format.
  - Similar to SMS: 3GPP TS 23.038.
  - Warning carried as one or more pages (max 15).
  - Page is 82 octets (93x 7-bit chars).
- CMAS warnings:
  - currently 90 characters in size (1 page).
  - FEMA will increase this to 360 characters.
- SCOS 5.1 only supports 1 page messages.
- Message content is transparent to the RAN.



CBS in UMTS

CBS Principles

- HNB-GW provides IuBC interface to CBC.
  - HNB-GW distributes/consolidates SABP messages.
- SABP carried over Iuh using SCTP.
- CBS messages broadcast over the air interface in the CTCH.

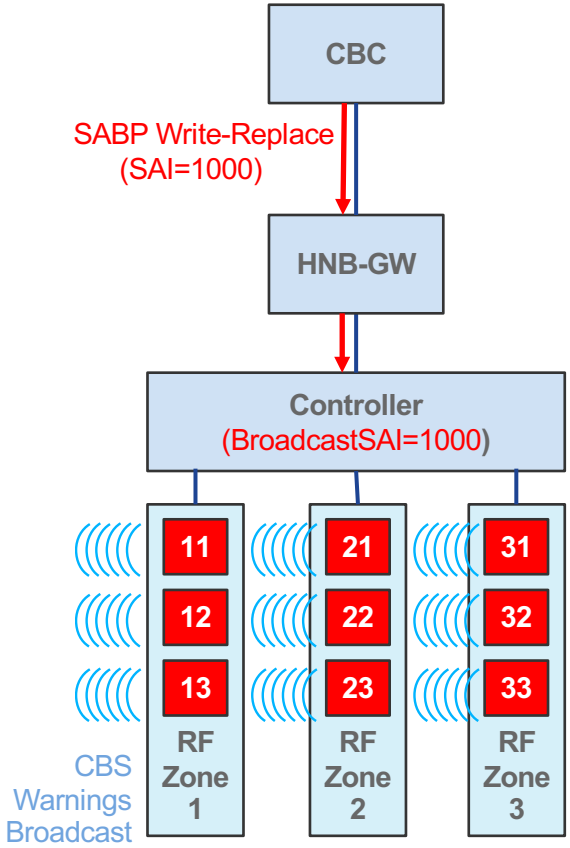


UMTS CBS Support

- Controller appears as a single “cell” to the CBC.
  - Identified through its configured “Broadcast-SAI”.
  - Centralized controller zone based warnings are not supported.
- SABP Restart sent when controller/HNB-GW starts.
  - Warnings not retained through controller or HNB-GW reboot (“data lost”).
- Active warnings can be cancelled or replaced.
- 4 concurrent warnings can be sent.
- New CBS messages scheduled as soon as possible (<2s typical).

UMTS CBS Warning Identities

- Controller assigned its own SAI.
  - “Service Area for Broadcast”.
- Configured by:
  - Data model.
  - HeNB-GW through HNBAP.
- CBC sends warning to this SAI.
- Controller broadcasts warnings to all active cells.
- Newly activated cells also broadcast on-going warnings.



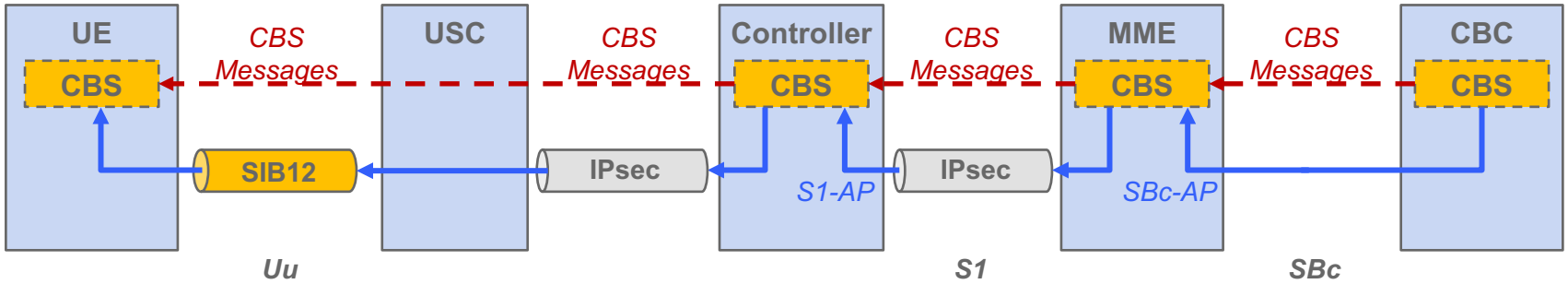
HNB-GW Aspects

- HNB-GW acts as an SABP relay.
- HNB-GW combines controller SABP responses into a single SABP message to the CBC.
  - HNB-GW waits for configurable period (1 – 300s, default: 10s).
- If HNB-GW restarts it sends an SABP Restart on behalf of all its controllers (data lost).
- IuBC interface:
  - Single IPv4 address and TCP (CBC initiated session).
  - TCP heartbeats detect IuBC connection loss and trigger alarm.

CBS in LTE

PWS Principles

- CBC sends warnings to MME using SBc interface (3GPP TS 29.168).
- MME sends warnings to controller over S1 using S1-AP.
- Warning messages broadcast over the air interface in SIB12.

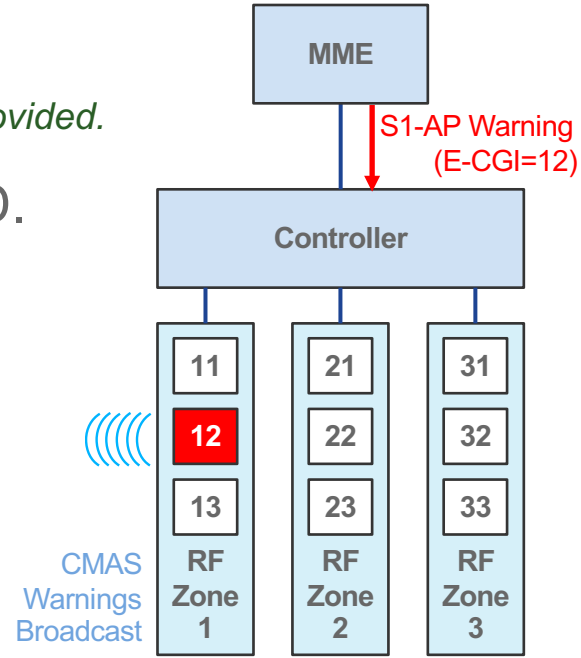


PWS Support

- SIB12 transmitted every 1.28s (fixed).
- Active warnings can be cancelled or replaced.
- 2 concurrent warnings can be sent.
- Warnings scheduled immediately (<1.28s).
- Controller reboot does not retain warnings.
- Warning Area List:
  - Size: 2000 E-CGI, 2500 TAI, 3000 EAID.

LTE Warning Area Identity Handling

- All cell identities supported:
  - E-CGI, TAC, EAID, *All** ** no Warning Area List IE is provided.*
- Warning broadcast in all cells with configured ID.
  - E-CGI & TAC match on a per-cell basis
  - EAID common for all cells under the controller.
  - A newly activated cell matching warning ID also broadcasts ongoing warning
- S1-AP response messages list E-CGI of all cells broadcasting warning



Warning Type

- The USC 8k supports either CMAS or EU-Alert warnings.
- Warning type selected using the following DM parameter:
  - *FAPService.{i}.CellConfig.LTE.EPC.PWS*
- There is no difference in the handling of these two different types of warning by the RAN.

Note: if used, the Emergency Area ID of all cells under the controller can be configured by the parameter:

- *FAPService.{i}.CellConfig.LTE.EPC.EAID*

Provisioning

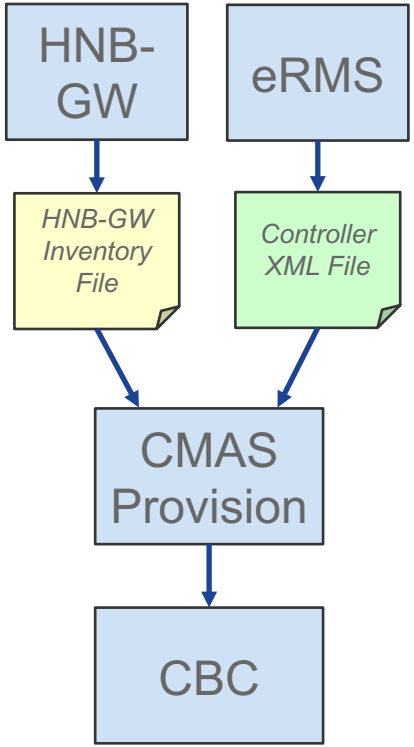
Provisioning Requirements

- Warnings are normally targeted at a geographical area.
- The CBC needs to map a geographical area to a set of UMTS and LTE cells.
- The customer network can periodically extract data from the USC 8k deployment to build these mapping tables.

CMAS Provisioning

- Daily provisioning information from 2 sources:
  - **HNB-GW**: Provides it's inventory file.
  - **eRMS**: Database parameters for controller and cells.
- The following information is available:

HNB-GW	UMTS Controller	LTE Cell
• HNB-GW ID • IuBC IP Address • Controller RNC ID	• CGI • RNC-ID • BroadcastSAC • Lat/Long • In service	• E-CGI • TAI • Lat/Long • Cell radius * • Cell enabled



** Actually horizontal position uncertainty*