



MAGMA

Product Specifications

February 2019



Facebook has made an effort to ensure that this documentation is accurate but does not make any representation or warranty regarding accuracy or completeness. Facebook reserves the right to update and otherwise modify the information included in this document without notice. If you find information that is incorrect or incomplete, we would appreciate your comments and suggestions.

Table of Contents

Network Management System

1. Introduction	4
1.1 Purpose	
1.2 Target Audience	
1.3 Scope	
2. Magma Architecture	5
2.1 Traditional LTE Network Architecture	
2.2 Magma based LTE Network Architecture	
2.3 Magma System Architecture	
2.4 Features	
3. Magma Access Gateway	9
3.1 Block Diagram	
3.2 Features	
3.3 Interfaces	
3.3.1 TR-069 Interface	
3.3.2 S1 Interface	
3.3.3 NAS Interface	
3.3.4 GRPC Interface with a Federated Gateway	
3.4 Subcomponents	
4. Federation Gateway	18
4.1 Block Diagram	
4.2 Features	
4.3 Interfaces	
4.3.1 S6a Interface	
4.3.2 Gx Interface	
4.3.3 Gy Interface	
4.3.4 SGs Interface	
5. Orchestrator	22
5.1 Features	
5.2 Configuration	
5.3 Monitoring	
5.4 Deployment	
6. End to End Call Flows	23
7. eNodeB Configuration and KPIs	26
7.1 eNB Configuration	
7.2 eNB KPIs	
7.3 EPC Specific Configuration	
7.4 EPC Specific KPIs	
7.5 HSS/Subscriberdb Specific Configuration	
7.6 Internal Stats and Alarms to track system performance and health	
8. Hardware Recommendations for Magma	32

1. Introduction

Magma is an open-source software platform that can help bring more people online by giving network operators an open, flexible and extendable mobile packet core. Magma enables better connectivity in the following ways:

- Allows operators to offer cellular service without vendor lock-in by providing a modern, open source core network
- Enables federation between MNOs and new infrastructure providers for sharing rural infrastructure
- Allows operators who are constrained with licensed spectrum to add capacity and reach by using Wi-Fi and CBRS
- Enables operators to manage their networks with more automation, less downtime, better predictability, and add new services and applications incrementally and with faster deployment times

Magma, coupled with the existing network infrastructure of telecommunications companies, extends mobile data services to more people. Facebook developed Magma to enhance wireless networks in order to make it easier to deploy and cheaper to maintain. In doing so, Magma will help mobile operators extend the reach of their networks.

1.1 Purpose

Purpose of this document to capture following aspects of the Magma:

- High level architecture
- Key components and features
- KPIs and configurations

1.2 Target Audience

Magma software is for providers who want to perform the following functions:

- Expand LTE coverage for mobile broadband data and voice services.
- Use Magma as a mobile packet core with their WiFi (TWAN) network to offload their cellular with a non-seamless and seamless WiFi-offload mechanism

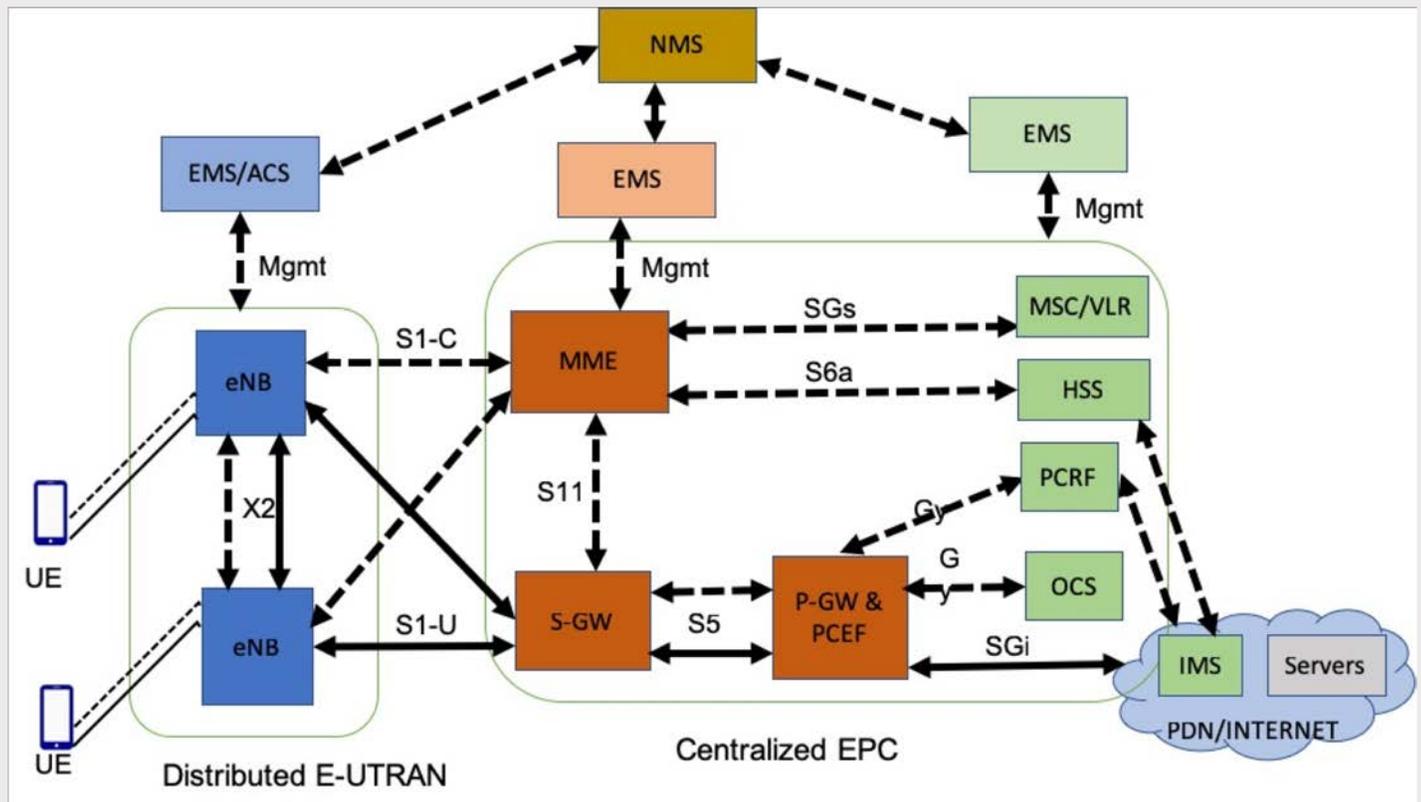
1.3 Scope

Scope of this document is limited to describe Magma's current architecture, list of features and KPIs . It does not address aspects related to development and deployment of Magma. For these aspects please refer to the other two key documents related to Magma:

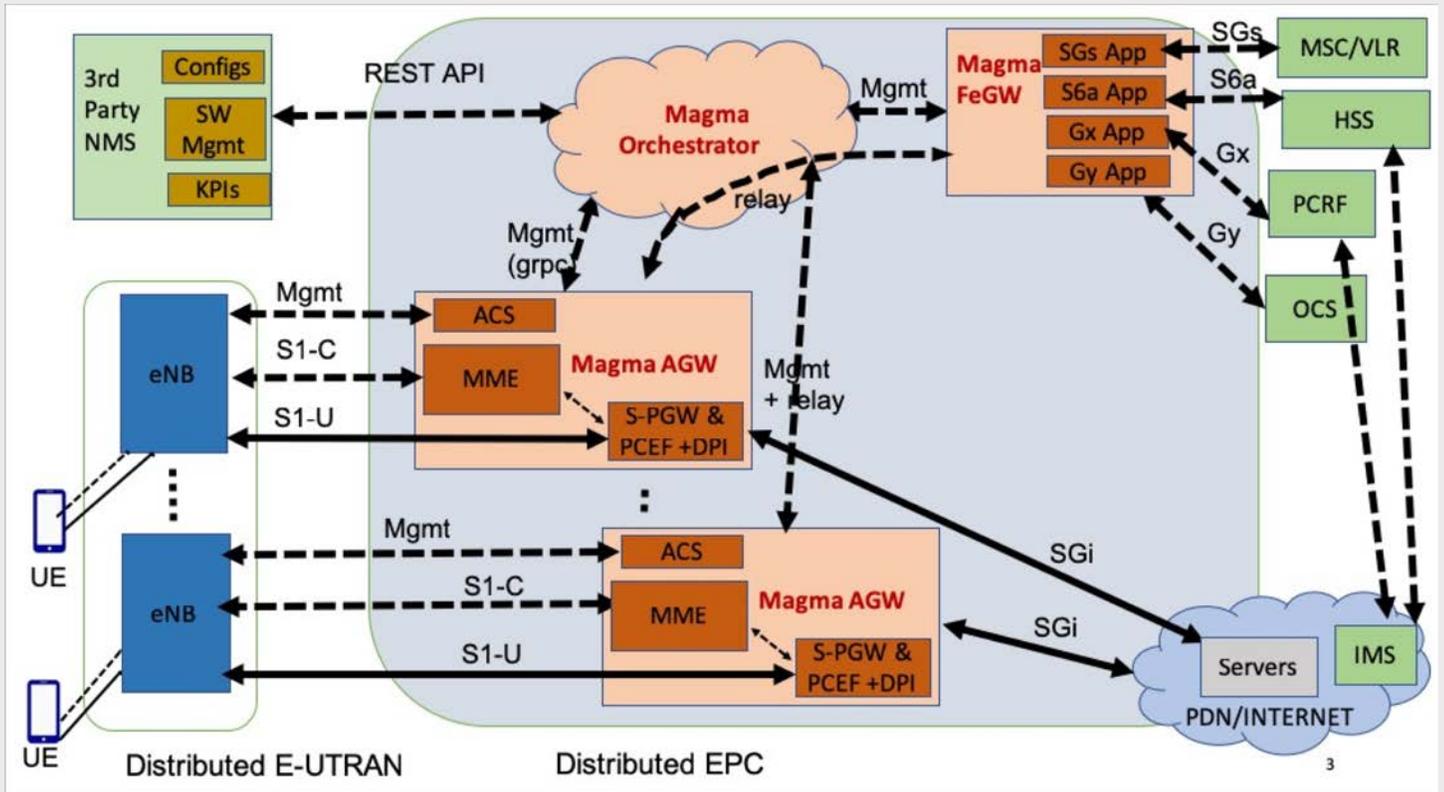
- Magma Development Guide: For developing new applications and use cases on top of Magma platform
- Magma Deployment Guide: For deploying Magma platform for supported use cases

2. Magma Architecture

2.1 Traditional LTE N/W Architecture



2.2 Magma Based LTE N/W Architecture

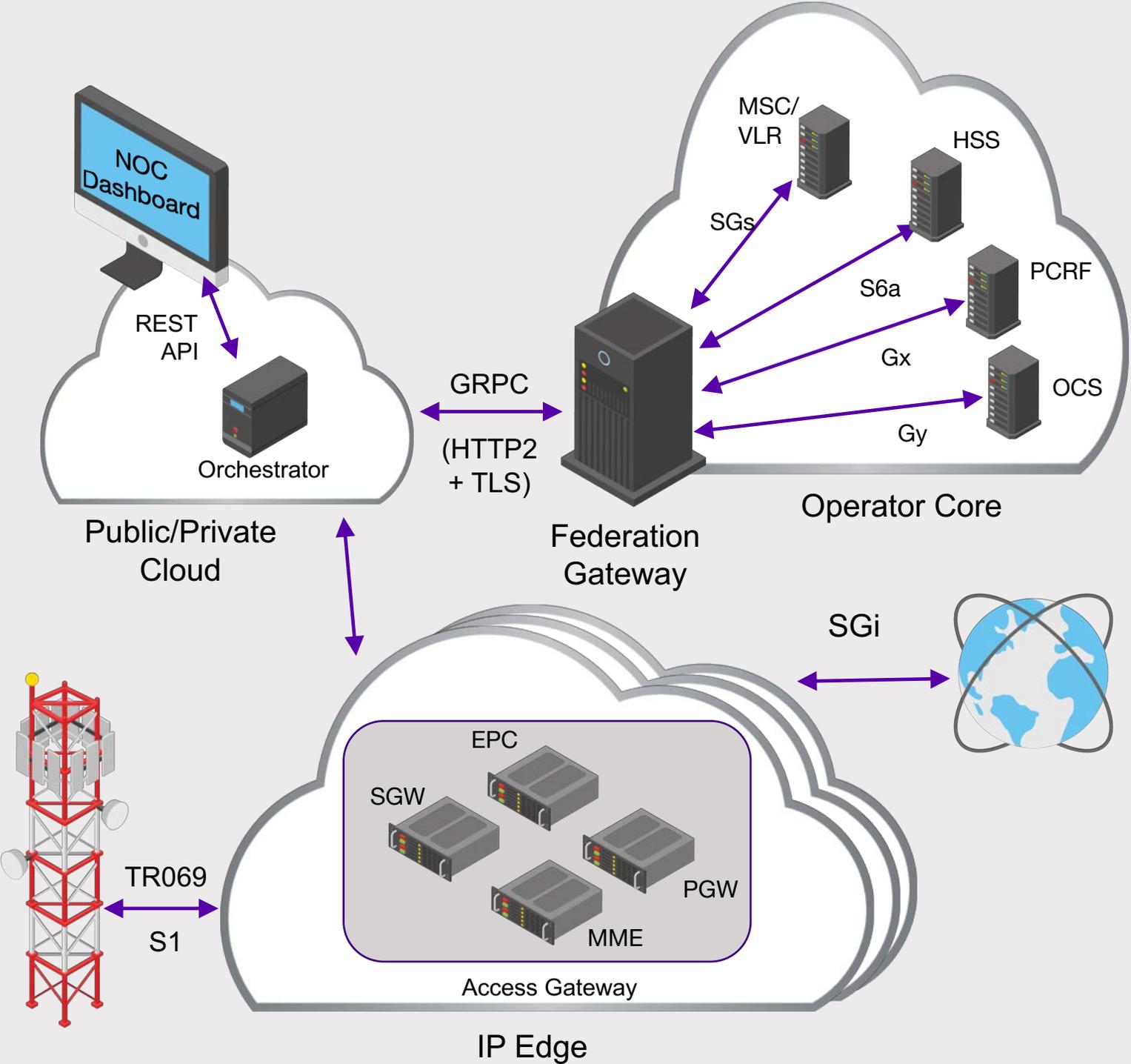


2.3 Magma System Architecture

Magma consists of following three key components as shown in the diagram on the next page:

- Access Gateway - The Access Gateway provides the mobile packet core (EPC) functionality. It is a distributed core architecture for horizontal scaling with a radio access network (RAN) like an eNodeB.
- Orchestrator - Orchestrator is a cloud service that provides a simple and consistent way to configure and monitor the wireless network securely. The Orchestrator can be hosted on a public/private cloud. The Orchestrator has 3 main functions, an NMS for configuration and basic monitoring, KPIs exposed through a REST endpoint and a secure communication channel for communication between the various gateways. Orchestrator ensures security with the use of client side certificates with SSL, a TPM key, SSH access, OpenVPN, and cloud authentication.
- Federation Gateway - The Federation Gateway integrates the MNO core network with Magma by using standard 3GPP interfaces to existing MNO components. It acts as a proxy between the Magma

AGW and the operator's network and facilitates core functions, such as authentication, data plans, policy enforcement, and charging to stay uniform between an existing MNO network and the expanded network with Magma.



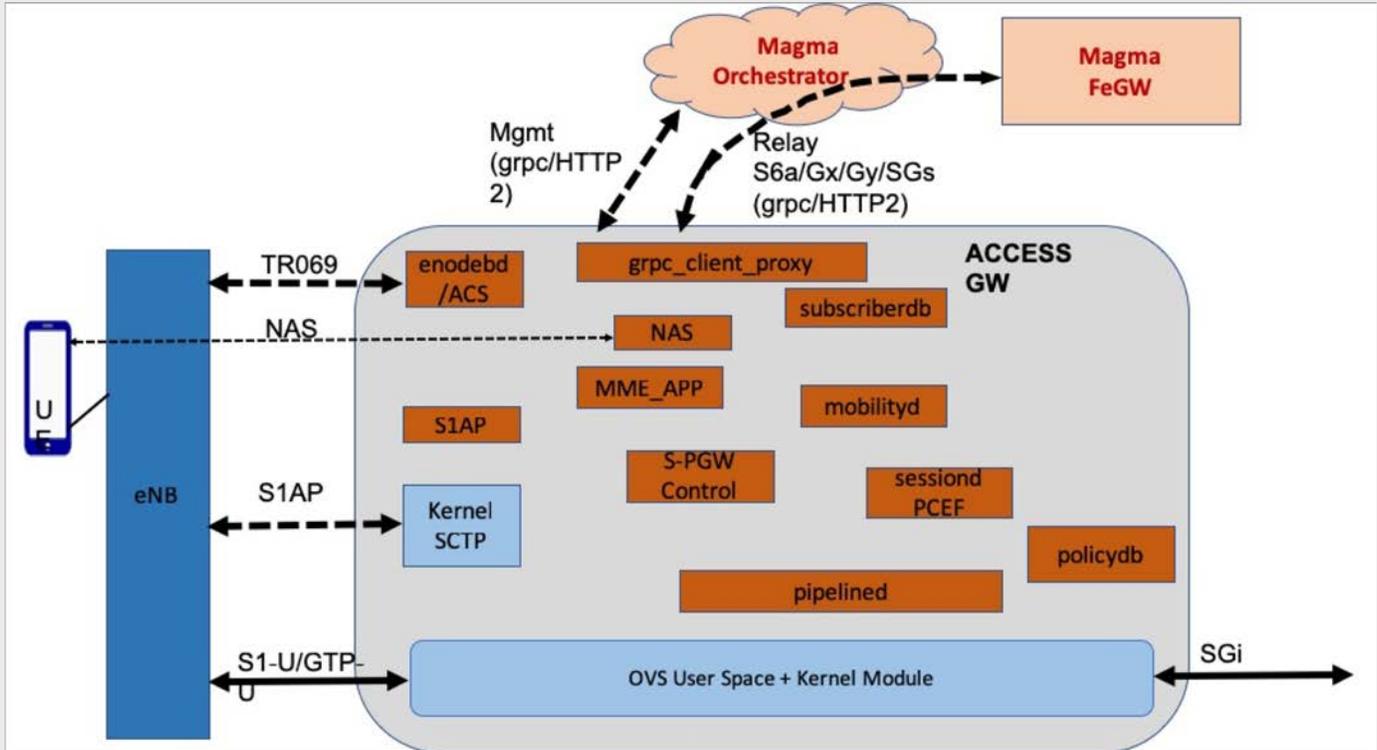
2.4 System Level Features

Magma provides the following system level features:

- Network Management Software
 - Configuration (includes eNodeB configuration)
 - Key Performance Indicators (KPI) data metrics
 - User-Interface to manage the network
- LTE mobile broadband data service
 - Cellular CS - Voice Service through CSFB to overlay 2G/3G network
 - CS - SMS Service over LTE network through interworking with 2G/3G MSC
 - Cellular PS - Voice Service (VoLTE) through interworking with IMS
 - PS-SMS Services via interworking with IMS
- Charging Policy and QoS Policy enforcement with PCRF
 - Installation and activation of static and dynamic PCC rules
 - Usage monitoring status updates
- Credit Management/Online charging with OCS
 - Session based Charging with Unit Reservation (SCUR)
 - Centralized rating and Centralized Unit determination
 - Volume based Grants
- Non-Seamless WiFi-Offload (NSWO)
 - Authentication and authorization for 4G subscribers to use WiFi TWAN with LBO at TWAN
 - Credit management for WiFi Subscribers via interworking with OCS

3. Magma Access Gateway

3.1 Block Diagram



3.2 Features and Functionalities

Access Gateway provides the mobile evolved packet core (EPC) functionality. It contains MME, unified S-GW & P-GW, PCEF as some of the key components. The features below are also supported with Magma access gateway.

- **Security**
 - NAS keys generation and integrity protection and encryption of NAS signaling
 - Support for NAS Integrity protection algorithms - Null, Snow3G and AES
 - Support for NAS encryption/decryption algorithms- Null
 - eNB key generation and distribution to eNB to manage AS security
 - Permanent identity protection via temporary identity allocation for the subscriber
- **Subscriber supported features**
 - LTE Subscriber Registration for both EPS and Non-EPS services (CS voice and CS-SMS)
 - LTE Subscriber mutual authentication via EPS-AKA mechanism
 - LTE Subscriber authorization

- IP address allocation to the subscriber
- Pull the subscriber profiles (APN, Subscribed QoS etc) from HSS during registration
- Update the current serving MME id for the subscriber to HSS.
- Get the charging policy and QoS policy (PCC Rules and Rating groups) from PCRF for the subscriber and enforce the same on data flows.
- Get the allowed data grant from the OCS for different rating groups for the subscriber and enforce the same on data flows.
- Mobile broadband data service over default EPS bearer and enforcement of charging and QoS policy at flow level.
- Managing the transition of subscribers between connected and idle state
- Handle service request from subscribers to move the subscribers to connected state to handle outgoing signaling/data
- Page subscribers to move the subscribers to a connected state to handle incoming signaling/data
- Track the inactive subscribers and de-registers inactive subscribers from the system.
- Support subscriber initiated de-registration request
- Support HSS initiated subscriber de-registration request
- **Voice over LTE supported features**
 - VoLTE - PDN connection toward IMS to support VoLTE
 - VoLTE - Support for multiple EPS bearers (default and dedicated EPS bearer) within one PDN connection to support VoLTE
 - VoLTE and Data - Multiple PDN/APN connections to support VoLTE and Internet services simultaneously
- **Supports QCI to DSCP mapping for GBR bearers** (QC1 bearer for VoLTE)
- **CSFB** - Supports NAS, S1AP, and SGs procedures to support CSFB for incoming and outgoing CS call and CS-SMS

3.3 Interfaces and Procedures

3.3.1 TR-069

Magma currently supports management of eNodeB devices that use TR-069 as management interface. This is used for both provisioning the eNodeB and collecting the performance metrics.

- Device Data model : TR-181 and TR-098
- Information Data model : TR-196

The following RPC methods are supported and used by AGW.

RPC Methods Supported by ACS	CPE's RPC Methods used by ACS
Inform	GetParameterValues
GetRPCMethods	SetParameterValues
TransferComplete	AddObject(part of objects)
	DeleteObject(part of objects)
	Reboot
	Download

3.3.2 S1 Interface

Magma supports 3GPP compliant S1AP over SCTP and GTP over UDP protocols to support c-plane and u-plane interfaces, respectively with eNodeBs.

The following S1AP Procedures are currently supported:

S1AP Procedures	Message Names
S1 Setup	S1 Setup Request
	S1 Setup Response
	S1 Setup Failure
Initial UE Message	Initial UE Message
Initial Context Setup	Initial Context Setup Request
	Initial Context Setup Response
	Initial Context Setup Failure
Downlink NAS Transport	Downlink NAS Transport
Uplink NAS Transport	Uplink NAS Transport
UE Context Release	UE Context Release Command
	UE Context Release Request
	UE Context Release Complete
UE context Modification	UE context Modification Request
	UE context Modification Response
	UE context Modification Failure
UE Capability Info Indication	UE Capability Info Indication
NAS non delivery indication	NAS non delivery indication

S1AP Procedures	Message Names
Reset- eNB initiated	Reset Request
	Reset Ack
Paging	Paging for CS domain
	Paging for PS domain
E-RAB Setup	E-RAB Setup Request
	E-RAB Setup Response
E-RAB Release	E-RAB Release Request
	E-RAB Release Response

3.3.4 NAS

The following NAS Procedures are currently supported:

NAS Procedures	Message Names
Attach	Attach Request
	Attach Accept
	Attach Complete
	Attach Reject
PDN Connectivity with Attach	PDN Connectivity Request
	Activate default EPS bearer context request
	Activate default EPS bearer context accept
	PDN Connectivity Reject
	Activate default EPS bearer context reject
Authentication	Authentication Request
	Authentication Response
	Authentication Failure
	Authentication Reject
Security Mode Command	Security Mode Command
	Security Mode Complete
	Security Mode Reject

NAS Procedures	Message Names
	Authentication failure
Tracking Area Update	Tracking Area Update Accept
Service Request	Service Request
	Service Reject
Extended Service Request	Extended Service Request
EMM Information	
Identity	Identity request
	Identity response
CS Service notification	CS Service notification
DL CS-SMS	Downlink NAS transport
UL CS-SMS	Uplink NAS transport
Detach	Detach Request
	Detach Accept
Activate dedicated EPS bearer	Activate dedicated EPS bearer context request
	Activate dedicated EPS bearer context accept
	Activate dedicated EPS bearer context reject
De-activate dedicated EPS bearer	Deactivate EPS bearer context request
	Deactivate EPS bearer context accept
Stand alone PDN Connection	PDN Connectivity Request
	Activate default EPS bearer context request
	Activate default EPS bearer context accept
	PDN Connectivity Reject
Disconnect Stand alone PDN Connection	PDN disconnect request
	PDN disconnect reject
ESM Information	ESM information request
	ESM information response

3.3.4 GRPC Interface with a Federated Gateway

The federated gateway provides remote procedure calls (GRPC) based interfaces to standard 3GPP components, such as HSS (S6a, SWx), OCS (Gy), and PCRF (Gx). The exposed RPC provides versioning & backward compatibility, security (HTTP2 & TLS) as well as support for multiple programming languages. The Remote Procedures below provide simple, extensible, multi-language interfaces based on GRPC which allow developers to avoid dealing with the complexities of 3GPP protocols. Please see the ***Magma Developers Guide*** (*coming soon*) for detailed information.

- S6a Proxy - The S6a Proxy creates and processes the following subscriber authentication information:
 - Subscriber Location Information
 - Access Point Configuration
 - Reset Requests
- Session Proxy - The Session Proxy controls the session of each subscriber with the following interfaces:
 - Notifies the OCS/PCRF of a new session and returns rules associated with subscriber along with credits for each rule
 - Updates the OCS/PCRF with each used credit and terminations from the gateway
 - Terminates the session in OCS/PCRF for a subscriber
 - Updates a monitor given its usage and session information
 - Processes QoS information
 - Creates a Session Request
 - Updates rules for each session

For a more detailed description of the function call interfaces, go to:

<https://github.com/facebookincubator/magma>

3.4 Subcomponents

MME (S1AP, MME APP and NAS)

In the above diagram MME includes S1AP, NAS and MME_APP subcomponents. MME functions include:

1. S1AP external Interface with eNB
 1. S1AP ASN.1 encode/decode
 2. S1AP Procedures

2. NAS external Interface with UE
 - a. NAS message encode/decode
 - b. NAS Procedures
 - c. NAS state-machine for NAS EMM and NAS ESM protocols
3. S11 like Interface with unified S-GW & P-GW
 - a. Create and delete PDN Sessions
 - b. Create/modify/delete default and dedicated bearers
4. GRPC based S6a like interface towards FeGW
 - a. To get authentication vector and subscriber profile to authenticate and authorize the subscriber
 - b. To register the serving MME-id with HSS
 - c. To receive the HSS initiated subscriber de-registration request
 - d. To send purge request to HSS during UE de-registration
 - e. To receive HSS reset indication
5. GRPC based SGs like interface towards FeGW
 1. To support NON-EPS services for the subscriber (CS voice and CS-SMS)
6. Update serving GW-id for the subscriber to the FeGW
7. Statistics to track the number of eNodeBs connected, number of registered UEs, number of connected UEs and number of idle UEs.
8. MME APP maintains UE state machine and routes the message to appropriate modules based on UE state, context and received message.

S-PGW Control Plane

S-PGW Control Plane functions include:

1. S11 like interface Interface with MME
 - a. Create and delete PDN Sessions
 - b. Create/modify/delete default and dedicate bearers
2. Interface with MobilityD to allocate and release IP address for the subscriber during PDN connection establishment and release, respectively
3. Interface with Sessiond/PCEF to trigger Gx and Gy session establishment for the subscriber during PDN connection establishment
4. Establish and release GTP tunnel during bearer setup and release

Mobilityd

Mobilityd functions include:

Interface with orchestrator to receive IP address block during system bring-up.
Allocate and release IP address for the subscriber on the request from S-PGW Control Plane.

Sessiond/PCEF

Sessiond implements the control plane for the PCEF functionality in Magma. Sessiond is responsible for the lifecycle management of the session state (credit and rules) associated with a user. It interacts with the PCEF datapath through pipelined for L2-L4 and DPId for L4-L7 policies.

Pipelined

Pipelined is the control application that programs the OVS openflow rules. In implementation pipelined is a set of services that are chained together. These services can be chained and enabled/disabled through the REST API. The [README](#) describes the contract in greater detail.

PolicyDB

PolicyDB is the service that supports static PCRF rules. This service runs in both the AGW and the orchestrator. Rules managed through the rest API are streamed to the policydb instances on the AGW. Sessiond ensures these policies are implemented as specified.

Ssubscriberdb

Subscriberdb is Magma's local version of HSS. Magma uses Subscriberdb to enable LTE data services through one network node like AGW for LTE subscribers. It is deactivated for the deployments that make use of the MNO's HSS. It supports the following two S6a procedures:

1. S6a: Authentication Information Request and Answer (AIR/AIA)
2. S6a: Update Location Request and Answer (ULR/ULA)

Suscriberdb functions include:

1. Interface with Orchestrator to receive subscriber information such as IMSI, secret key (K) , OP, user-profile during system bring-up.
2. Generate Authentication vectors using Milenage Algorithm and share these with MME.
3. Share user profile with MME.

OVS - Data path

OVS (<http://www.openvswitch.org/>) is used to implement basic PCEF functionality for user plane traffic. The control plane applications interacting with OVS are implemented in pipelined.

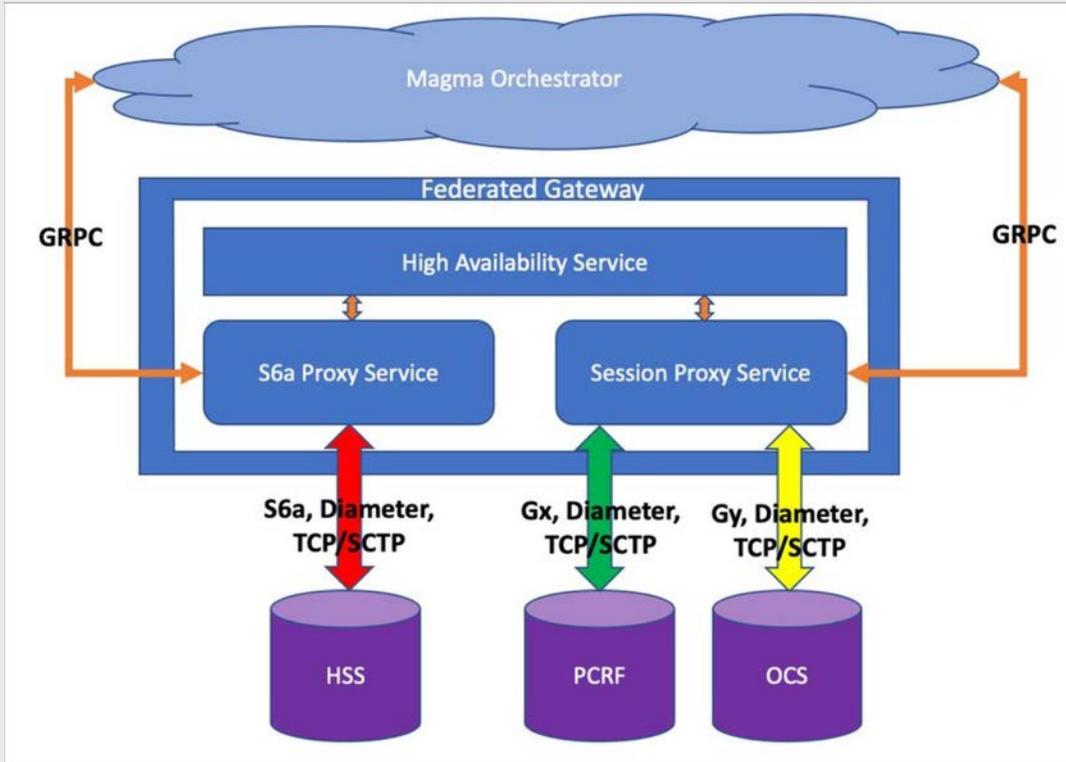
Control proxy:

Control proxy manages the network transport between the gateways and the controller.

1. Control proxy abstract the service addressability, by providing a service registry which maps a user addressable name to its remote IP and port.
2. All traffic over HTTP/2, and are encrypted using TLS. The traffic is routed to individual services by encoding the service name in the HTTP/2 :authority: header.
3. Individual GRPC calls between a gateway and the controller are multiplexed over the same HTTP/2 connection, and this helps to avoid the connection setup time per RPC call.

4. Federation Gateway

4.1 Block Diagram



4.2 Features

Federation Gateway supports following features and functionalities:

1. Federation Gateway hosts centralized control plane interface towards HSS, PCRF , OCS and MSC/VLR on behalf of distributed AGW/EPCs.
2. Establish diameter connection with HSS, PCRF and OCS directly as 1:1 or via DRA.
3. Establish SCTP/IP connection with MSC/VLR.
4. It interfaces with AGW over GPRC interface by responding to remote calls from EPC (MME and Sessiond/PCEF) components and converts these to 3GPP compliant messages and send these messages to the appropriate core network components such as HSS, PCRF, OCS and MSC. Similarly it receives 3GPP compliant messages from HSS, PCRF, OCS and MSC and converts theses to appropriate GPRC calls to AGW. For a list of 3GPP interfaces and messages supported by Federation gateway refer section “Interfaces and Messages” below.

4.3 Interfaces and Messages

4.3.1 S6a

The following S6a Procedures are currently supported:

S6a Procedure	Command Names
Authentication	AIR
	AIA
Location Management	ULR
	ULA
Cancel Location (Subscription Withdrawal)	CLR
	CLA
Purge	PUR
	PUA
Reset	RSR
	RSA

4.3.2 Gx Interface

The following Gx Procedures are currently supported:

Gx Procedure	Command Names
IP CAN Gx Session Establishment and installation of PCC rules (Pull method)	Credit Control Request- Initial (CCR-I)
	Credit Control Answer - Initial (CCA-I)
Usage Monitoring Updates/ Revalidation Timeout event	Credit Control Request- Update (CCR-U)
	Credit Control Answer - Update (CCA-U)
IP CAN Gx Session Termination	Credit Control Request- Terminate (CCR-T)
	Credit Control Answer- Terminate (CCA-T)
PCRF initiated Rule addition/modification/Deletion (Push Method)	Reauth Request (RAR)
	Reauth Answer (RAA)

4.3.3 Gy Interface

The following Gy Procedures are currently supported:

Gy Procedure	Command Names
IP CAN Gy Session Establishment and request for grant for data flows with same and/or different RGs	Credit Control Request- Initial (CCR-I)
	Credit Control Answer - Initial (CCA-I)
Actual used units updates and request for more grants	Credit Control Request- Update (CCR-U)
	Credit Control Answer - Update (CCA-U)
IP CAN Gy Session Termination	Credit Control Request- Terminate (CCR-T)
	Credit Control Answer- Terminate (CCA-T)

4.3.4 SGs Interface

The following SGs Procedures (to support CS-voice and CS-SMS services) are currently supported:

SGs Procedures	Message Names to add TODO
Location update for non-EPS services procedure	SGsAP-LOCATION-UPDATE-REQUEST SGsAP-LOCATION-UPDATE-ACCEPT SGsAP-LOCATION-UPDATE-REJECT
Paging for non-EPS services procedure	SGsAP-PAGING-REQUEST SGsAP-PAGING-REJECT
Service request procedure	SGsAP-SERVICE-REQUEST SGsAP-SERVICE-ABORT-REQUEST
SMS message(tunnelling of NAS messages)	SGsAP-DOWNLINK-UNITDATA SGsAP-UPLINK-UNITDATA
Alert/Activity Ind	SGsAP-ALERT-REQUEST SGsAP-ALERT-ACK SGsAP-ALERT-REJECT SGsAP-UE-ACTIVITY-INDICATION

SGs Procedures	Message Names to add TODO
Reset	SGsAP-RESET-INDICATION SGsAP-RESET-ACK
TMSI reallocation	SGsAP-TMSI-REALLOCATION-COMPLETE
EPS detach indication	SGsAP-EPS-DETACH-INDICATION SGsAP-EPS-DETACH-ACK
IMSI detach from EPS services	SGsAP-IMSI-DETACH-INDICATION SGsAP-IMSI-DETACH-ACK
HSS Failure	SGsAP-RESET-INDICATION SGsAP-RESET-ACK
MM information	SGsAP-MM-INFORMATION-REQUEST
STATUS/Error Indication	SGsAP-STATUS
Release Request/Rsp	SGsAP-RELEASE-REQUEST

Subcomponents

Federation Gateway includes the following core services:

- S6a Proxy - provides GRPC based interface to HSS S6a
- SWx Proxy - provides GRPC based interface to HSS SWx
- Session Proxy - controls the session of each subscriber and provides functionality scoped GRPC interfaces to PCRF & OCS (Gx, Gy)
- CSFB - Supports NAS, S1AP, and SGs procedures to support CSFB for incoming and outgoing CS call and CS-SMS

5. Orchestrator

5.1 Functionalities and features

Orchestrator provides the capabilities for configuration and monitoring of the network and the gateways.

5.2 Configuration:

- Provides a network centric view of the system. The network as a whole can be configured through a single API call (eg. changing the mnc/mcc), or individual access gateways can be managed by it (eg. disable a single enodeb)
- Provides a REST interface for APIs, which can be used for building UI or scripts for tooling. Swagger is used as the API language, and leverages tools for autogenerating code from the API specification.
- The north bound configs are applied to the gateways consistently. The gateways periodically poll the controller for their configs.

5.3 Monitoring:

- **Current Network State:** Each gateway does a checkin every minute with its current state (number of UEs, GPS location, CPU, memory, etc.), which are exposed through a REST API.
- **Time-series Metrics:** Supports Prometheus as the backend for aggregating time-series metrics for monitoring and alerting. Different exporters can be added as well if needed.
- **Structured Logging:** Supports logging of structured JSON data. For instance, individual gateway checkin data are logged, and data from the HTTP/2 proxy about the RPC type, response code and latency are logged.

5.4 Deployment:

- Orchestrator is built using a microservices framework where individual services can be developed and deployed independently and are loosely coupled.
- The controller is multi-tenant, supports multiple networks in a single deployment, and provides access control for the APIs for each network.
- The Orchestrator can be deployed in a public cloud or private cloud. Tooling has been provided for using CodeDeploy.
- Docker support for development and deployment is currently in the works.

5.4 Subcomponents

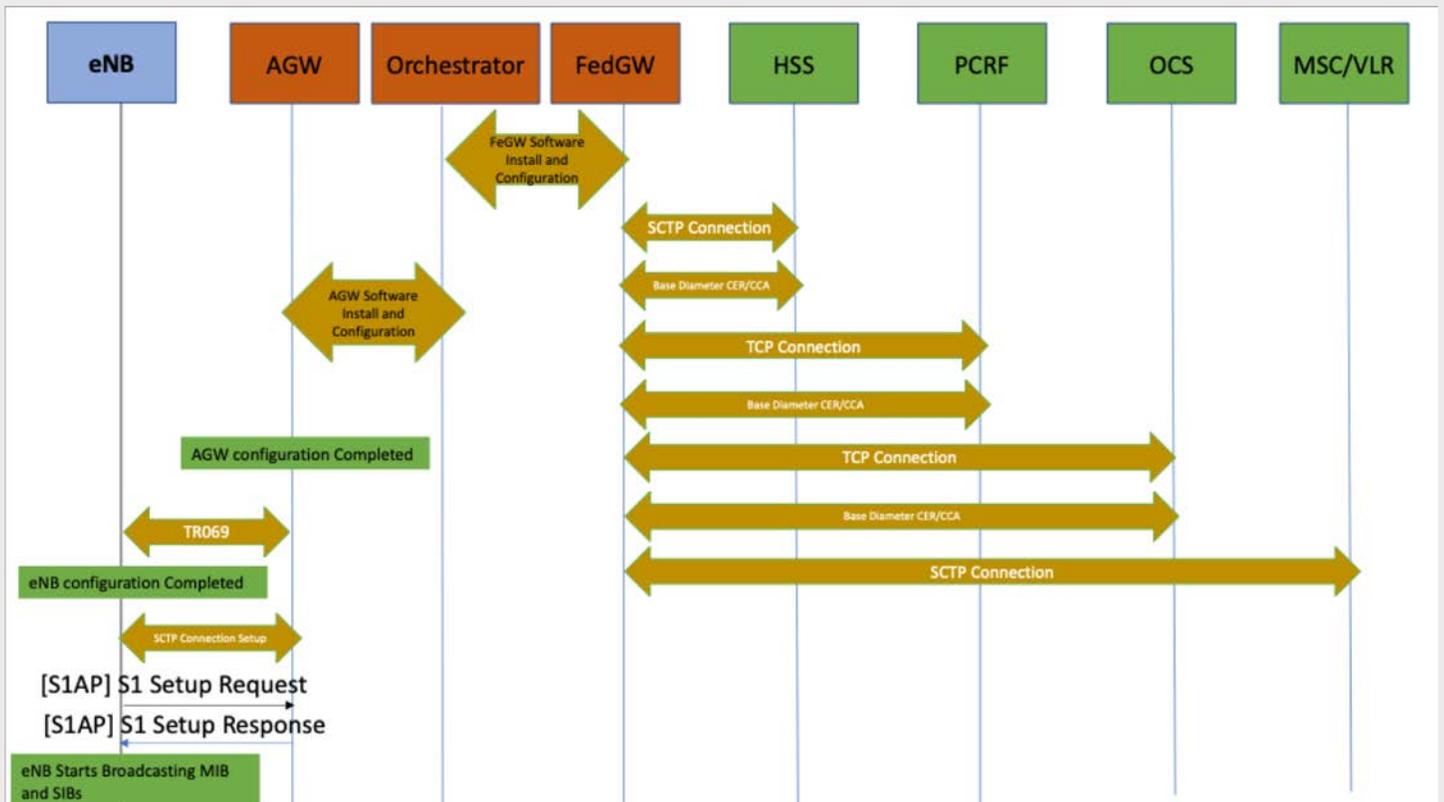
Orchestrator consists of the following microservices:

- **nghttpx**: HTTP/2 proxy which terminates TLS, and used client certs for authentication of devices and REST clients.
- **obsidian**: REST services which provides access control functionalities
- **certifier**: certificate authority to create short lived certs for session
- **bootstrapper**: authenticates gateways and allows access for gateways to every other service
- **config**: provides a CRUD interface for building config entities as REST resources
- **streamer**: provides a framework for converting the north bound APIs from the users, into south bound APIs per gateway.
- **metricsd**: Periodically fetches the time series data from the gateways
- **datastore**: provides a key-value interface for the services.

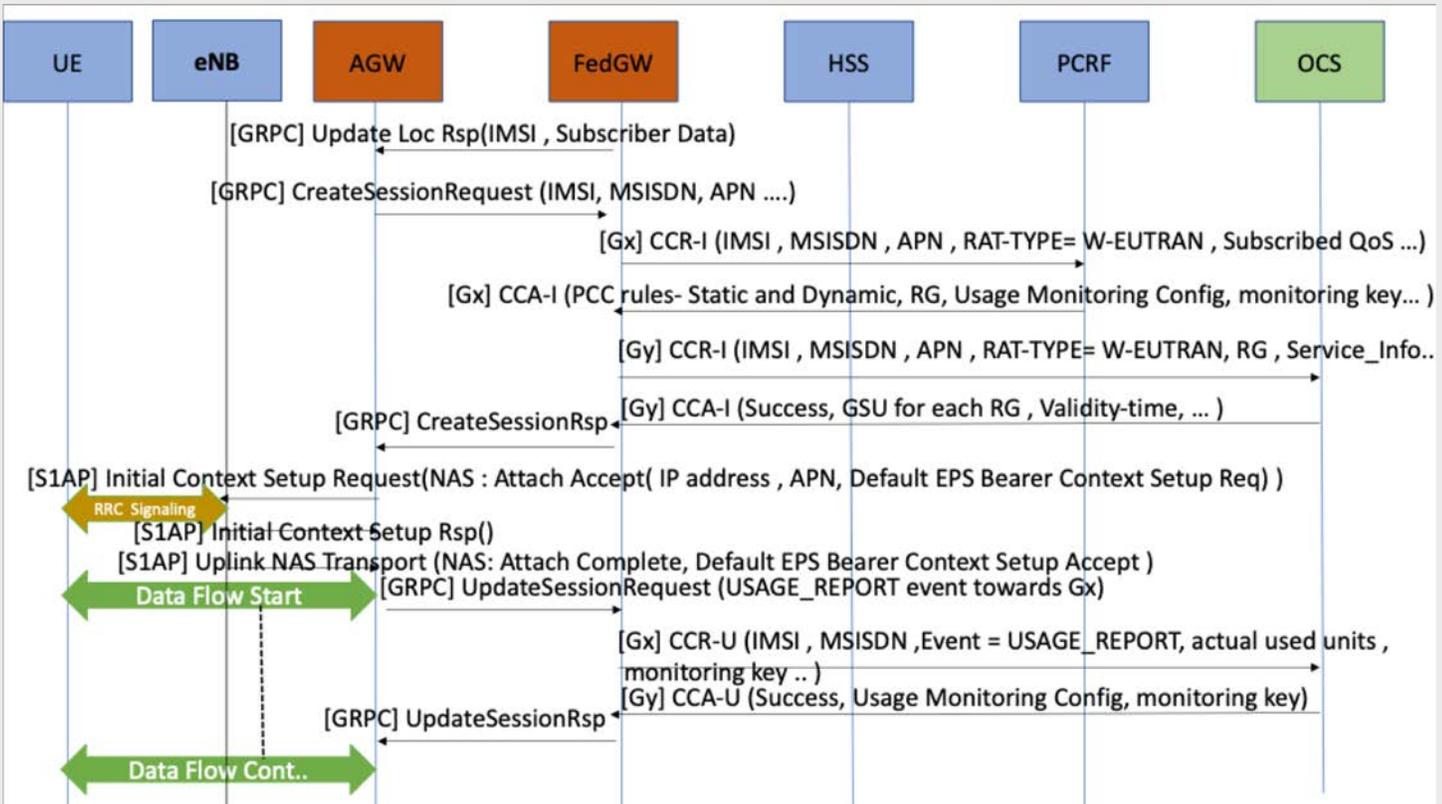
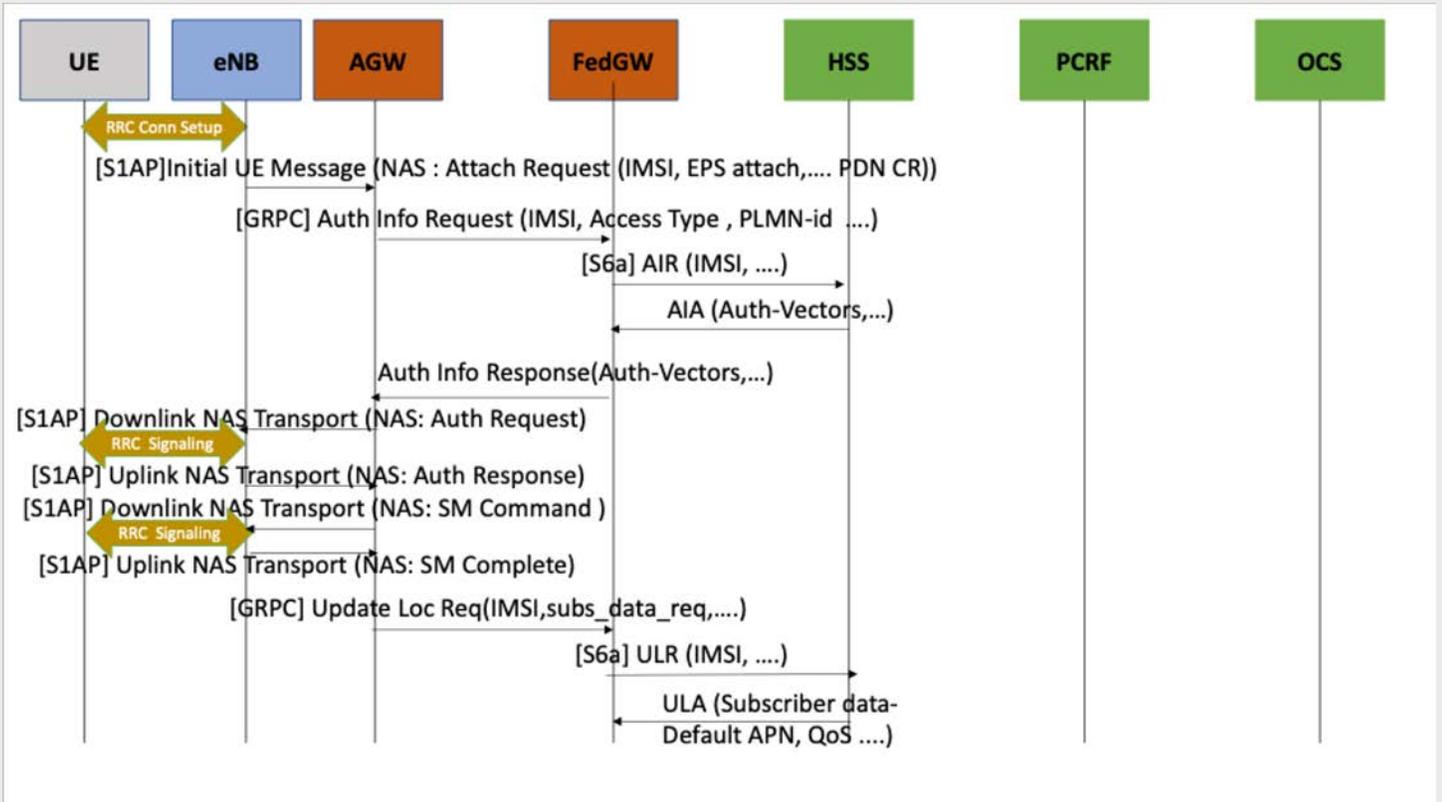
6. End-to-End Call Flow

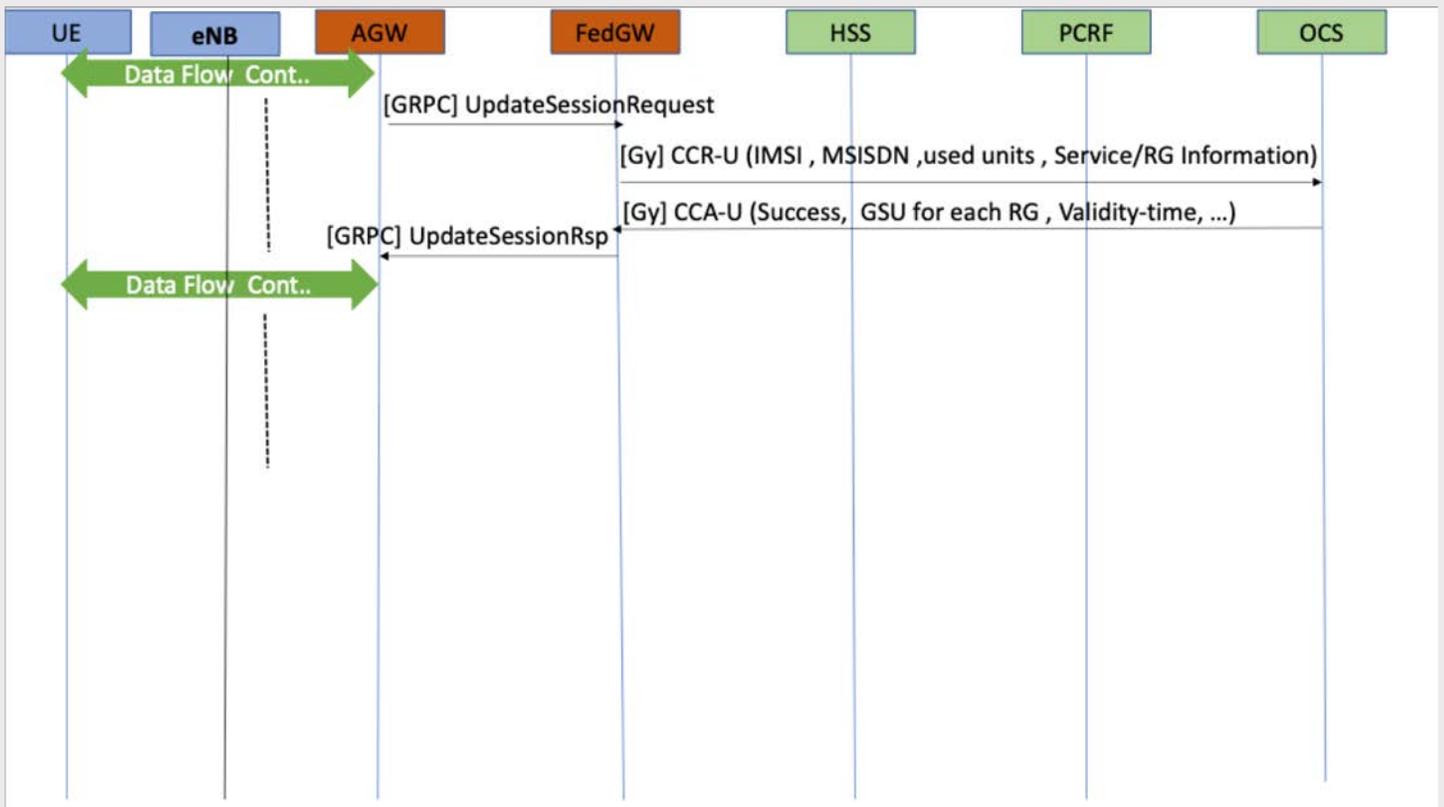
Below are the end-to-end call flows from the eNodeB to the MNO.

System bring up and S1 Connection Setup

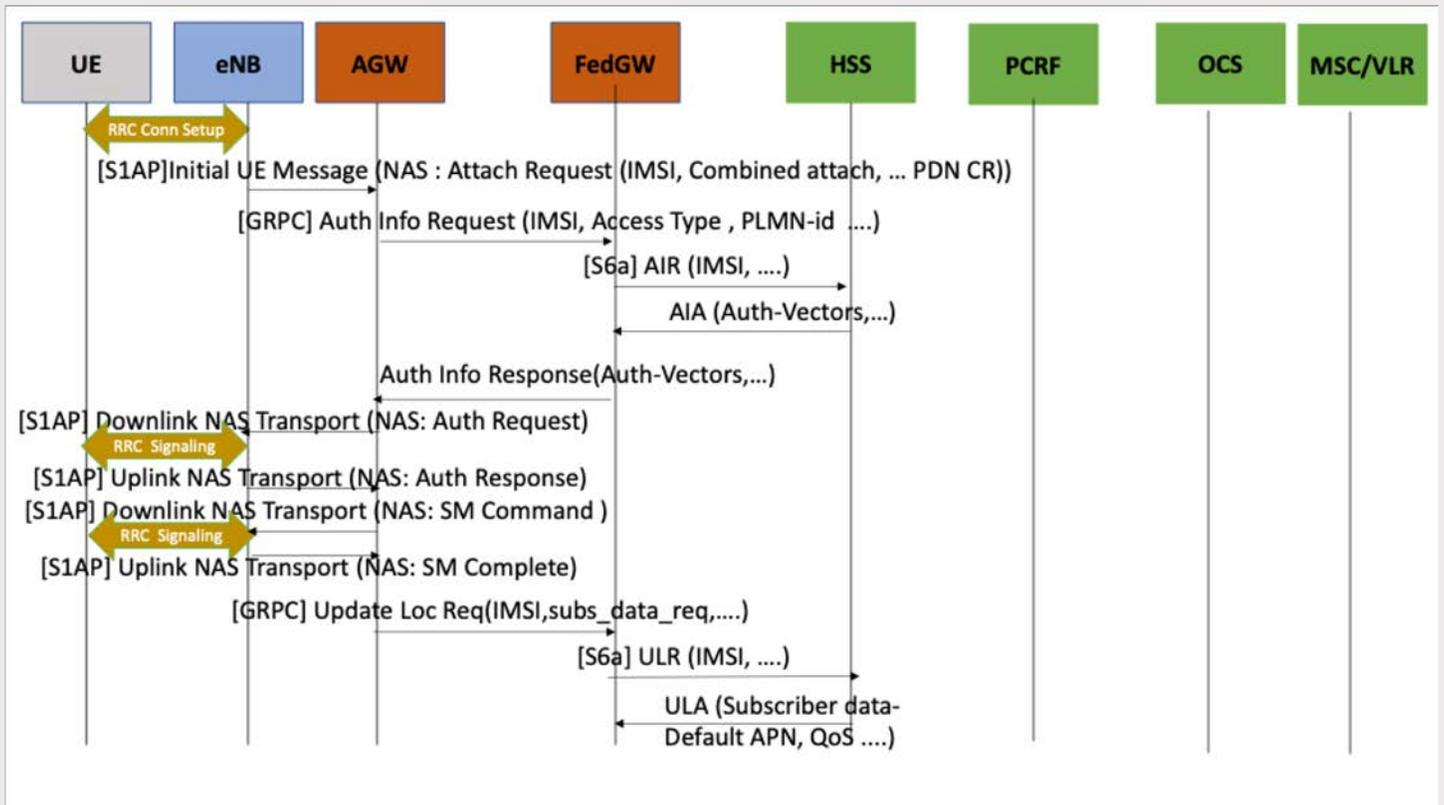


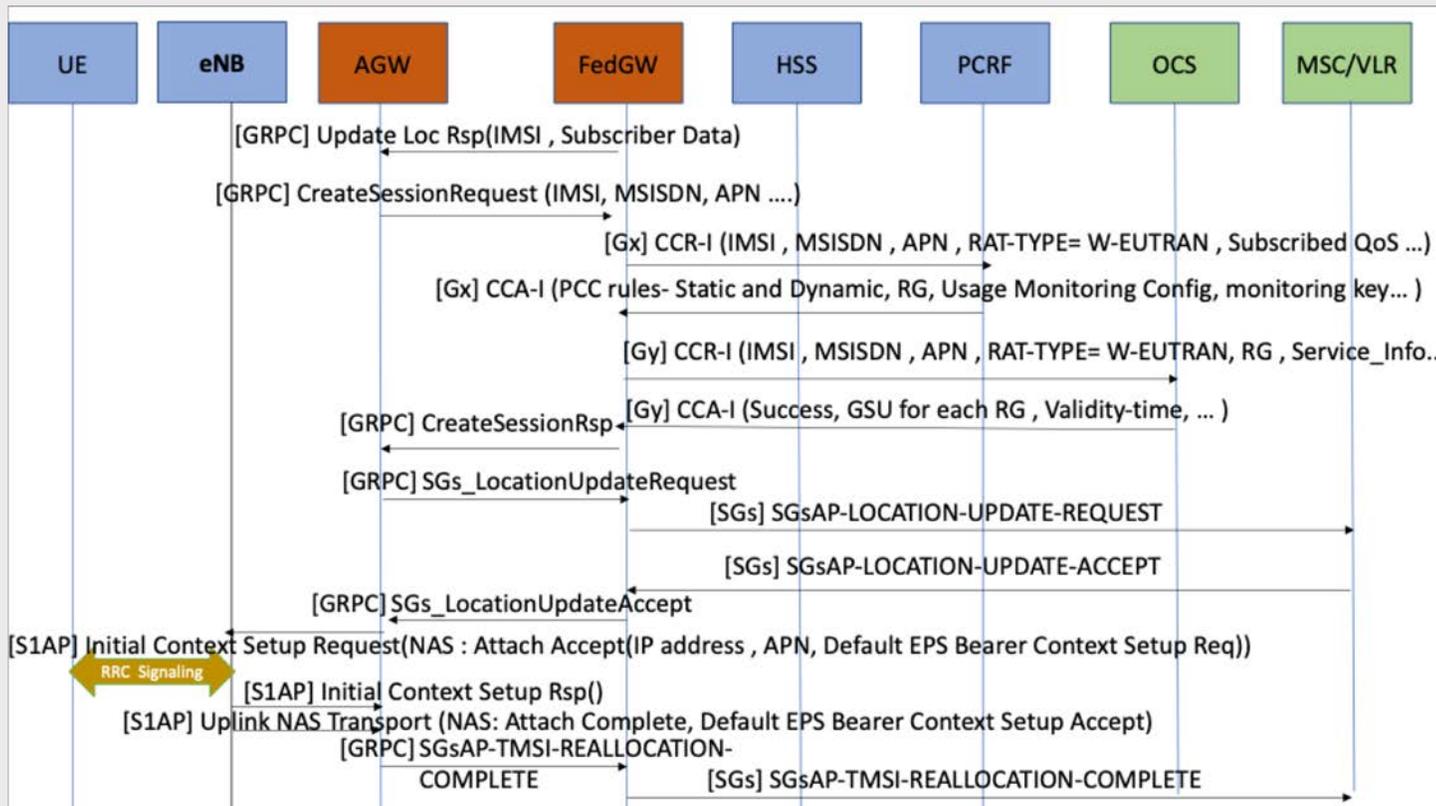
Attach (EPS attach) and Data Flow





Attach (Combined attach - EPS and IMSI)





7. Configuration and KPIs

7.1 eNB specific Configuration

Magma currently allows configuration of the following settings:

- Physical Cell Identity (PCI) of eNB
- RF - Transmit frequency, TDD/FDD, band, bandwidth, subframe settings
- MME connection settings
- Performance management settings
- RAN (cell reserved, cell barred)
- CSFB - Target RAT 2G:ARFCN

The list below displays the TR196 data model parameters that an eNodeB reads from local database and compares. For a detailed list of parameters that each eNodeB supports, refer to the Magma Github at:

- <https://github.com/facebookincubator/magma/blob/master/lte/gateway/python/magma/enodebd/devices/baicells.py>
- https://github.com/facebookincubator/magma/blob/master/lte/gateway/python/magma/enodebd/devices/baicells_old.py
- https://github.com/facebookincubator/magma/blob/master/lte/gateway/python/magma/enodebd/devices/baicells_qafb.py
- <https://github.com/facebookincubator/magma/blob/master/lte/gateway/python/magma/enodebd/devices/cavium.py>

TR-181 Parameters	Data Model Specification
Device.DeviceInfo.X_BAICELLS_COM_GPS_Status	TR-181
Device.DeviceInfo.X_BAICELLS_COM_1588_Status	TR-181
Device.DeviceInfo.X_BAICELLS_COM_MME_Status	TR-181
Device.Services.FAPService.1.REM.X_BAICELLS_COM_REM_Status	TR-181
Device.DeviceInfo.X_BAICELLS_COM_LTE_LGW_Switch	TR-181
Device.FAP.GPS.LockedLatitude	TR-181
Device.FAP.GPS.LockedLongitude	TR-181
Device.DeviceInfo.SoftwareVersion	TR-181
Device.Services.FAPService.1.Capabilities.LTE.DuplexMode	TR-181
Device.Services.FAPService.1.Capabilities.LTE.BandsSupported	TR-181
Device.Services.FAPService.1.X_BAICELLS_COM_LTE.EARFCNDLInUse	TR-181
Device.Services.FAPService.1.X_BAICELLS_COM_LTE.EARFCNULInUse	TR-181
Device.Services.FAPService.1.CellConfig.LTE.RAN.RF.FreqBandIndicator	TR-181
Device.Services.FAPService.1.CellConfig.LTE.RAN.RF.PhyCellID	TR-181
Device.Services.FAPService.1.CellConfig.LTE.RAN.RF.DLBandwidth	TR-181
Device.Services.FAPService.1.CellConfig.LTE.RAN.RF.ULBandwidth	TR-181
Device.Services.FAPService.1.CellConfig.LTE.RAN.PHY.TDDFrame.SubFrameAssignment	TR-181
Device.Services.FAPService.1.CellConfig.LTE.RAN.PHY.TDDFrame.SpecialSubframePatterns	TR-181
Device.Services.FAPService.1.FAPControl.LTE.AdminState	TR-181
Device.Services.FAPService.1.FAPControl.LTE.OpState	TR-181
Device.Services.FAPService.1.FAPControl.LTE.RFTxStatus	TR-181
Device.Services.FAPService.1.CellConfig.LTE.RAN.CellRestriction.CellReservedForOperatorUse	TR-181
Device.Services.FAPService.1.CellConfig.LTE.RAN.CellRestriction.CellBarred	TR-181
Device.Services.FAPService.1.FAPControl.LTE.Gateway.S1SigLinkServerList	TR-181
Device.Services.FAPService.1.FAPControl.LTE.Gateway.S1SigLinkPort	TR-181
Device.Services.FAPService.1.CellConfig.LTE.EPC.PLMNListNumberOfEntries	TR-181
Device.Services.FAPService.1.CellConfig.LTE.EPC.PLMNList.	TR-181
Device.Services.FAPService.1.CellConfig.LTE.EPC.TAC	TR-181
Device.Services.FAPService.Ipsec.IPSEC_ENABLE	TR-181
Device.Services.FAPService.1.FAPControl.LTE.Gateway.X_BAICELLS_COM_MmePool.Enable	TR-181
Device.ManagementServer.PeriodicInformEnable	TR-181
Device.ManagementServer.PeriodicInformInterval	TR-181
Device.FAP.PerfMgmt.Config.1.Enable	TR-181
Device.FAP.PerfMgmt.Config.1.PeriodicUploadInterval	TR-181
Device.FAP.PerfMgmt.Config.1.URL	TR-181
Device.Services.FAPService.1.CellConfig.LTE.EPC.PLMNList.%d.	TR-181
Device.Services.FAPService.1.CellConfig.LTE.EPC.PLMNList.%d.CellReservedForOperatorUse	TR-181
Device.Services.FAPService.1.CellConfig.LTE.EPC.PLMNList.%d.Enable	TR-181
Device.Services.FAPService.1.CellConfig.LTE.EPC.PLMNList.%d.IsPrimary	TR-181
Device.Services.FAPService.1.CellConfig.LTE.EPC.PLMNList.%d.PLMNID	TR-181

TR-098 Parameters	Data Model Specifications
InternetGatewayDevice.	TR-098
InternetGatewayDevice.Services.FAPService.1.	TR-098
InternetGatewayDevice.Services.FAPService.1.CellConfig.1.LTE.X_QUALCOMM_FAPControl.OpState	TR-098
InternetGatewayDevice.FAP.GPS.latitude	TR-098
InternetGatewayDevice.FAP.GPS.longitude	TR-098
InternetGatewayDevice.DeviceInfo.SoftwareVersion	TR-098
boardconf.status.eepromInfo.div_multiple	TR-098
boardconf.status.eepromInfo.work_mode	TR-098
InternetGatewayDevice.Services.FAPService.1.CellConfig.1.LTE.RAN.RF.EARFCNDL	TR-098
InternetGatewayDevice.Services.FAPService.1.CellConfig.1.LTE.RAN.RF.PhyCellID	TR-098
InternetGatewayDevice.Services.RfConfig.1.RfCarrierCommon.carrierBwMhz	TR-098
InternetGatewayDevice.Services.FAPService.1.CellConfig.1.LTE.RAN.PHY.TDDFrame.SubFrameAssignmentpool	TR-098
InternetGatewayDevice.Services.FAPService.1.CellConfig.1.LTE.RAN.PHY.TDDFrame.SpecialSubframePatterns	TR-098
InternetGatewayDevice.Services.FAPService.1.CellConfig.1.LTE.X_QUALCOMM_FAPControl.AdminState	TR-098
InternetGatewayDevice.Services.FAPService.1.CellConfig.1.LTE.X_QUALCOMM_FAPControl.OpState	TR-098
InternetGatewayDevice.Services.FAPService.1.CellConfig.1.LTE.X_QUALCOMM_FAPControl.OpState	TR-098
InternetGatewayDevice.Services.FAPService.1.FAPControl.LTE.Gateway.S1SigLinkServerList	TR-098
InternetGatewayDevice.Services.FAPService.1.FAPControl.LTE.Gateway.S1SigLinkPort	TR-098
InternetGatewayDevice.Services.FAPService.1.CellConfig.1.LTE.EPC.TAC	TR-098
boardconf.ipsec.ipsecConfig.onBoot	TR-098
InternetGatewayDevice.ManagementServer.PeriodicInformEnable	TR-098
InternetGatewayDevice.ManagementServer.PeriodicInformInterval	TR-098
InternetGatewayDevice.Services.FAPService.1.CellConfig.1.X_QUALCOMM_PerfMgmt.Config.Enable	TR-098
InternetGatewayDevice.FAP.PerfMgmt.Config.PeriodicUploadInterval	TR-098
InternetGatewayDevice.FAP.PerfMgmt.Config.URL	TR-098
InternetGatewayDevice.Services.FAPService.1.CellConfig.1.LTE.EPC.PLMNList.%d.	TR-098
InternetGatewayDevice.Services.FAPService.1.CellConfig.1.LTE.EPC.PLMNList.%d.CellReservedForOperatorUse	TR-098
InternetGatewayDevice.Services.FAPService.1.CellConfig.1.LTE.EPC.PLMNList.%d.Enable	TR-098
InternetGatewayDevice.Services.FAPService.1.CellConfig.1.LTE.EPC.PLMNList.%d.IsPrimary	TR-098
InternetGatewayDevice.Services.FAPService.1.CellConfig.1.LTE.EPC.PLMNList.%d.PLMNID	TR-098

7.2 eNB specific KPIs

Following eNB specific KPIs are pulled from eNB and sent to orchestrator for display.

1. Connected UEs
2. GPS
3. MME, PTP, GPS Connection Uptime
4. Whether the device is transmitting
5. DL/UL Throughput

In general following statistics are pulled from the eNodeB.

Metric
Connected UEs
GPS
MME, PTP, GPS Connection Uptime
DL/UL Throughput
RRC establishment attempts
RRC establishment successes
RRC re-establishment attempts
RRC re-establishment attempts due to reconfiguration failure
RRC re-establishment attempts due to handover failure
RRC re-establishment attempts due to other cause
RRC re-establishment successes
ERAB establishment attempts
ERAB establishment successes
ERAB establishment failures
ERAB release requests
ERAB release requests due to user inactivity
ERAB release requests due to normal cause
ERAB release requests due to radio resources not available
ERAB release requests due to reducing load in serving cell
ERAB release requests due to failure in the radio interface procedure
ERAB release requests due to EUTRAN generated reasons
ERAB release requests due to radio connection with UE lost
ERAB release requests due to OAM intervention
User plane uplink bytes at PDCP
User plane downlink bytes at PDCP

7.3 EPC Specific configuration

The following list are EPC configuration options that are supported for Magma.

- Service control
 - EPS service only
 - EPS and NON EPS (SMS only)
 - EPS and NON EPS (CS Voice + SMS)
- List of IP address for users
- Feature control
 - Use of 3rd party HSS or Local HSS/SUSBCRIBERDB
 - Policy and Credit Management (Gx/Gy interface)
- Static Policies /PCC Rules
- MME IP address
- NAS timer durations
- Supported algorithms for encryption and integrity protection
- SGS timer durations
- SGW IP address

7.4 EPC Specific KPIs

The following list are EPC KPI metrics that can be used to provide metric data for Magma.

- Number of connected eNBs
- Number of Registered (UE)s
- Number of Connected UEs
- Number of Idle UEs
- OAI EPC - Metrics on failure scenarios, and alerts (time outs, failures in OAI EPC)
 - MME restarted
 - S1 Setup Failure
 - SCTP Reset
 - SCTP Shutdown
 - S1 Reset from eNB
 - SCTP HeartBeat Timer Expired
 - S6a Connection with Subscriberdb Failure
 - Attach Accept timer Expired
 - Authentication Request timer expired
 - Security mode command timer expired
 - Tracking area update Accept timer expired
 - Initial Context Setup Request timer expired
 - UE Context Release Command timer expired
 - Initial Context Setup Failure Received
 - Attach Abort
 - Service Reject Sent
 - Tracking area update reject Sent
 - UE Context Release Request due to RLF
 - Duplicate Attach Request received
 - Authentication Failure with cause MAC Failure

- Authentication Failure with cause Resync
- Authentication Reject Sent
- Security mode command Reject received
- S6a Auth Info Reject from HSS
- S6a Auth Info Response timer expired (no or delayed response from subscriberdb)
- S1AP Error Indication received
- GTP-U Error Indication received
- nas-non-delivery indication received
- EMM status received
- IP address allocation failure
- IP address already allocated
- IPv4v6 PDN type Requested
- Stand alone PDN connectivity Request with Default APN
- Stand alone PDN connectivity Request with non-sefault APN
- Implicit Detach Timer expired
- Network Initiated Detach
- OAI EPC - Procedure level metrics
 - S1 Setup
 - Attempts
 - Success
 - Failure
 - Attach/Registration
 - Attempts
 - Success
 - Failure
 - Service Request (idle to connected mode Transition)
 - Attempts
 - Success
 - Failure
 - Detach/De-registration
 - Attempts
 - Success
 - Failure

7.5 HSS/SUSBCRIBERDB Specific configuration

Below are configuration options for HSS and Subscriberdb.

- List of subscribers
 - IMSI
 - Subscription state
 - Auth algorithm
 - K secret key
 - OP
- OP
- Data Plans
 - Data plan names
 - Download speed
 - Upload speed
 - Subscriber count

7.6 Internal Stats and Alarms to track system performance and health

In addition to the KPIs from eNodeB and EPC, the individual gateways provide the following system level metrics for monitoring their health:

- CPU utilization
- Disk utilization
- Memory utilization
- Temperature
- Virtual memory
- Backhaul latency
- Controller connectivity status

8. Hardware Recommendations for Magma

Below are the recommendations for hardware configurations to run each part of Magma software.

- Orchestrator
 - Hardware Recommendation:
 - 2 vCPU
 - 8GB ram
 - Debian or Ubuntu Linux recommended
 - The hardware requirements will scale depending on the number of subscribers
- Access Gateway
 - 2GB+ RAM
 - 2x 1.9GHz CPU or better (E3845 or equivalent)
 - Linux w/ kernel 4.9.6+
 - 16GB disk
- Federation Gateway
 - 2 vCPU
 - 8GB RAM for each VM required
 - 16GB Disk
 - Debian or Ubuntu Linux recommended



facebook
connectivity