Magma
Fixed Wireless Access
Product Specifications

PUBLICATION DATE:
May 2020

Version 1.0

Fixed Wireless Access

powered by **Magma**

Magma
FWA Product Specifications

Table of Contents

Purpose and Scope

The purpose of this document is to provide a deeper understanding of the following aspects of Magma FWA solution.

- High Level Architecture
- Network Diagrams
- Key Components and Features
- Reference bill of materials
- KPIs and Configurations
- Supported procedures

Resources

- Introduction to Magma
- Sample BOM
- Magma Deployment and Installation Guide
- Magma Network Management System (NMS)
- Network Architecture 2020

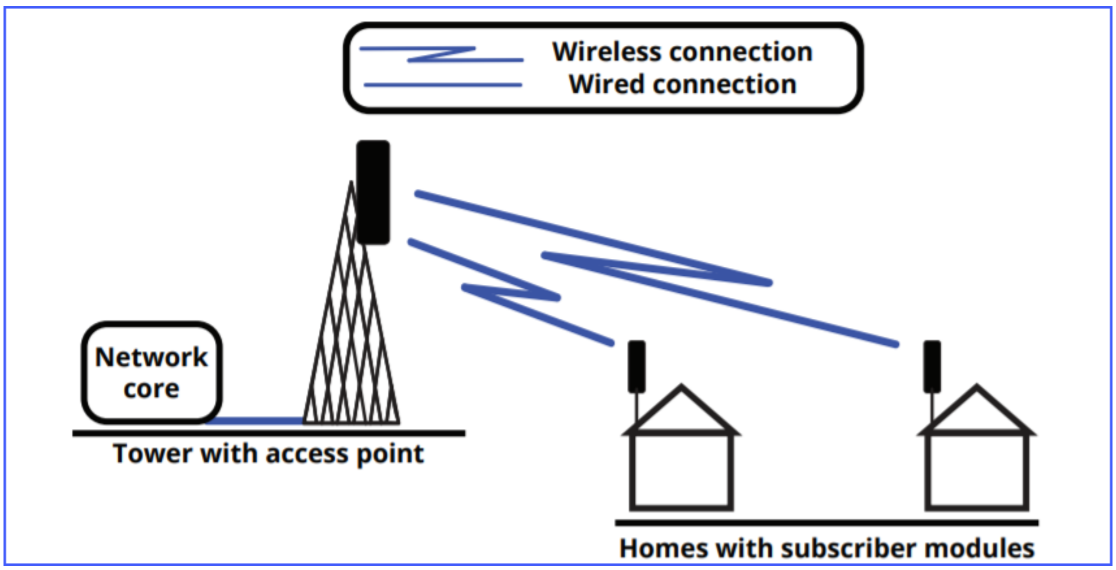
1. Introduction

What is Fixed Wireless Access (FWA)

FWA is a set of technologies designed to provide fixed outdoor wireless networking, to allow long-distance data connectivity between one or more network endpoints, without the need for physical cable across the entire distance between them. Unlike cellular technologies, which are designed to accommodate devices which are physically moving relative to the base station such as cellular phones, FWA technologies are designed to connect two or more network nodes with physically fixed positions.

Unlike Wi-Fi networks, which are predominantly designed for indoor operation, FWA is designed for outdoor operation at considerably longer ranges than indoor wireless networks. FWA connections spanning 5 to 10 km are common, with much longer distances frequently seen. Imagine a FWA network connection spanning 245 km, from the top of a mountain.

The diagram below shows a simplified example FWA deployment. A broad network topology typically conforms to a hub and spoke or Point to Multipoint (PMP) network, . .



Why use LTE Fixed Wireless Access

There are several features and factors on why we recommend Fixed Wireless Access to expand your network, here are a few prime reasons to use LTE FWA:

1) Non-Line-of-Sight (NLOS) Performance: This is the foundation of FWA, allowing to penetrate foliage and buildings so Customer Premise Equipment (CPE) can be indoor. This allows for point to multi point last mile access. Indoor CPEs provide theft proof which can be an issue in some regions.

2) Clean Spectrum Access: Noise and interference is not an issue due to FWA being a licensed spectrum. Particularly with 5GHz as more and more devices move to that band there is noise.

3) Standards Based Solution (Interoperability): The LTE standard creates an exchange across multi-vendor, multi-carrier inter-connections and between LTE systems.

4) Scalability: LTE is designed for scalability. Although configuring an LTE network initially takes more effort, once correctly configured, adding additional CPEs etc. is easy.

5) Speed to Deploy: Whether installed for permanent or temporary use, the speed of deploying an FWA network for outdoor connectivity is considerably faster than a comparable deployment with wired technologies. The main differentiator is the time required to bury or lay physical cable to each network endpoint with wired technologies, which can increase exponentially when it comes to crossing road or other property not owned by the organization deploying the network.

Why Use Magma FWA ?

Magma is an open-source software platform that gives network operators an open, flexible and extendable mobile core network solution. Magma enables better connectivity by:

- Allows for a try Before you Buy: Distributed EPC architecture allows for site by site expansion capacity as the business grows. This, unlike with incumbent EPC based solutions results in very low upfront cap-ex.

- Solution focus: The Magma FWA solutions comes prebuilt with RAN management and CPE monitoring. Well defined cloud API hooks for monitoring and provisioning allows operators to easily implement their monitoring and business processes on Magma. for integrated eNodeB management, CPE monitoring, API hooks for business process integration, and more. There is automation, less downtime, better predictability, and more agility to add new services and applications.

- Local Breakout and of Signaling and User planes allows for supporting unreliable backhaul (unlicensed). The ability to terminate 3GPP interfaces at the edge location such that it is only IP traffic beyond the edge. Data and control can be independently broken out locally. Running backhaul over unlicensed spectrum is prone to jitter and can result in control plane disconnects thus disconnecting UEs.

- Cloud Hosted and Multi-Tenant: Allows System Integrators to offer cross ISP solutions managed through a single orchestration layer, called the Magma Orchestrator (Orc8r). Data collected by the Magma Orchestrator sends data via RESTful API's to the NMS, information captured includes:

    - Device Location Map
    - Network Status Metrics
    - Outage Alerts
    - Subscriber Management
    - Gateways Management
    - eNodeB Devices
    - Network Configuration

- Magma is Opensource, it's free to use, free to deploy and is flexible and configurable for effectively expanding mobile core networks. To extend the network, Magma adds AGWs as the size of deployments increase. Magma is built using a microservice plugin architecture for easy integration with external systems.

- Pre-integrated Solutions through distributor partnerships: Allowing for pre-integrated solutions to be shipped (similar to embedded EPCs).

Magma is Purpose Built for FWA. It's an operationally simple core supporting the essential Fixed Wireless Access feature set, including metering and bandwidth caps.

2. Magma FWA Architecture

2.1 Based LTE Network Architecture

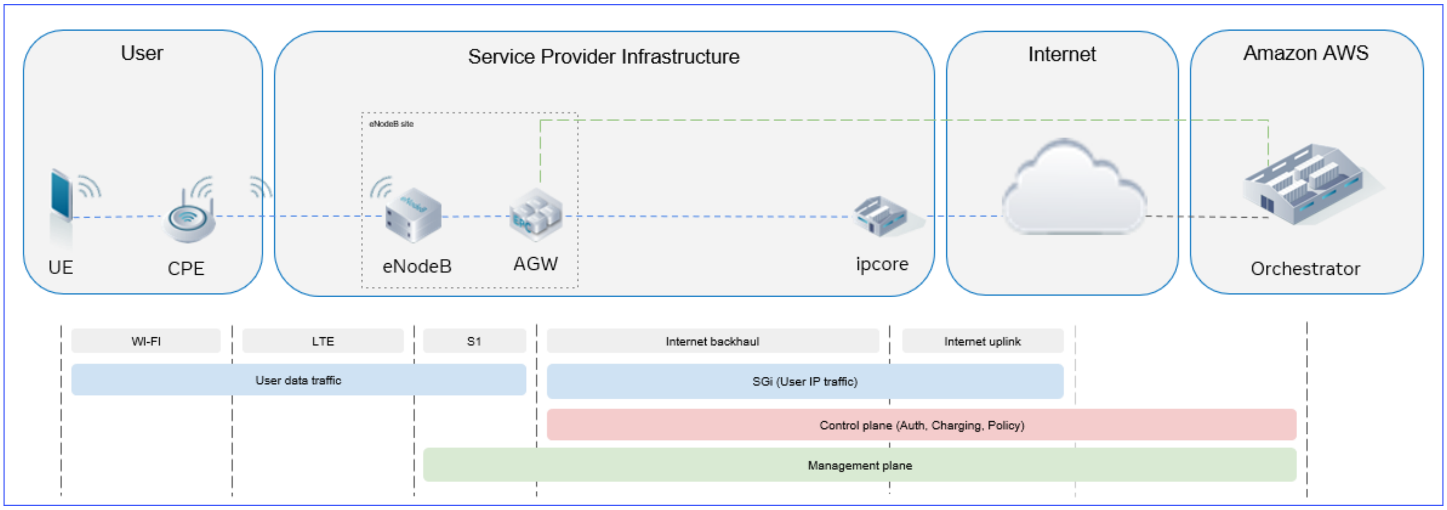


Figure 2.1

2.2 Fixed Wireless Architecture

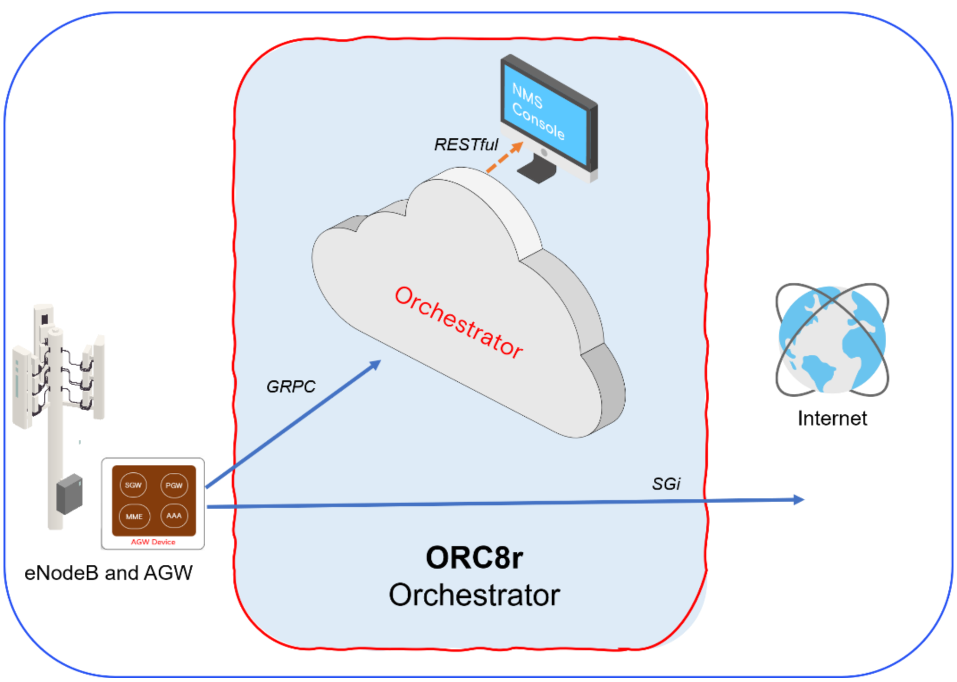


Figure 2.2

2.3 Magma System Architecture

Magma FWA consists of following 2 key components as shown in the below diagram:

Access Gateway (AGW) - 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. The recommended deployment is a single AGW per site. Each access gateway can support up to 12 eNBs

Orchestrator (ORC8r) - 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.

Magma Main Components Network Diagram

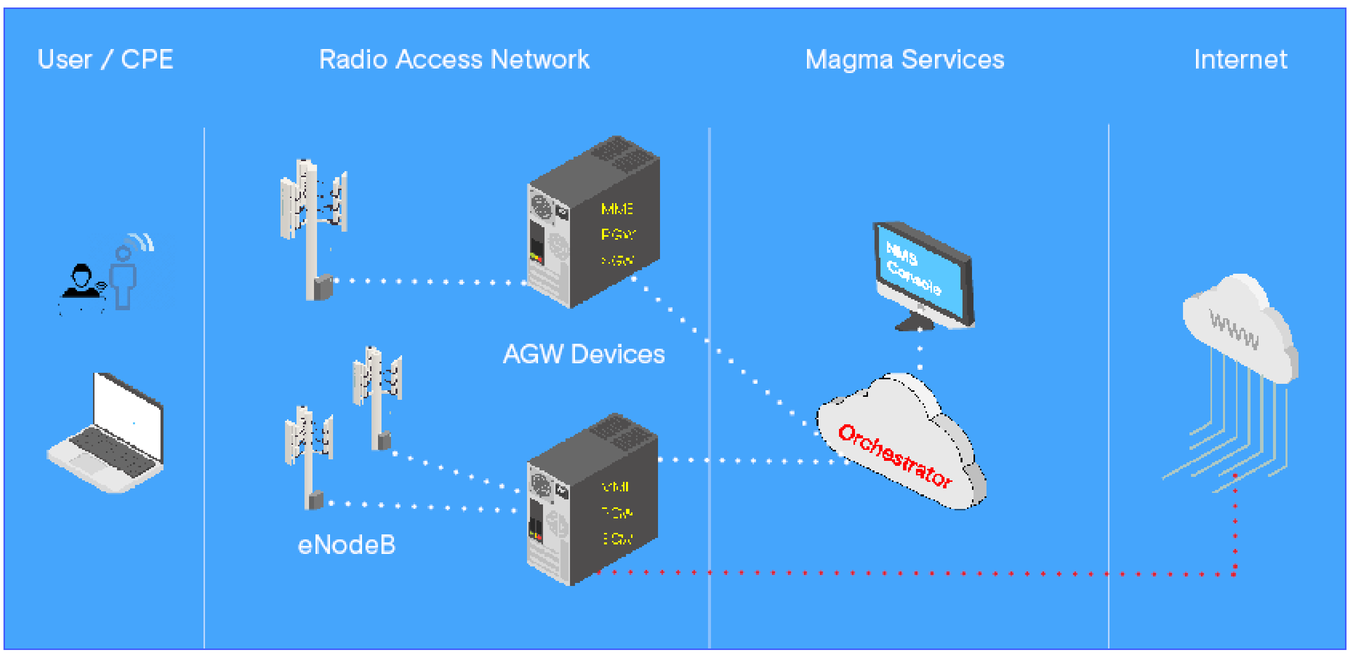


Figure 2.3

2.4 System Level Features

Magma FWA provides the following system level features

- Network Management Software (NMS)
  - Configuration (includes eNodeB configuration)
  - Key Performance Indicators (KPI) data metrics
  - User-Interface to manage the network

- Charging Policy and QoS Policy Enforcement (PCRF)
  - Installation and activation of static policies managed through the orchestrator

- Subscriber Data Base (SubDB)
  - HSS like functionality to manage subscribers built into the orchestrator

3. Magma Access Gateway (AGW)

3.1 AGW Architecture

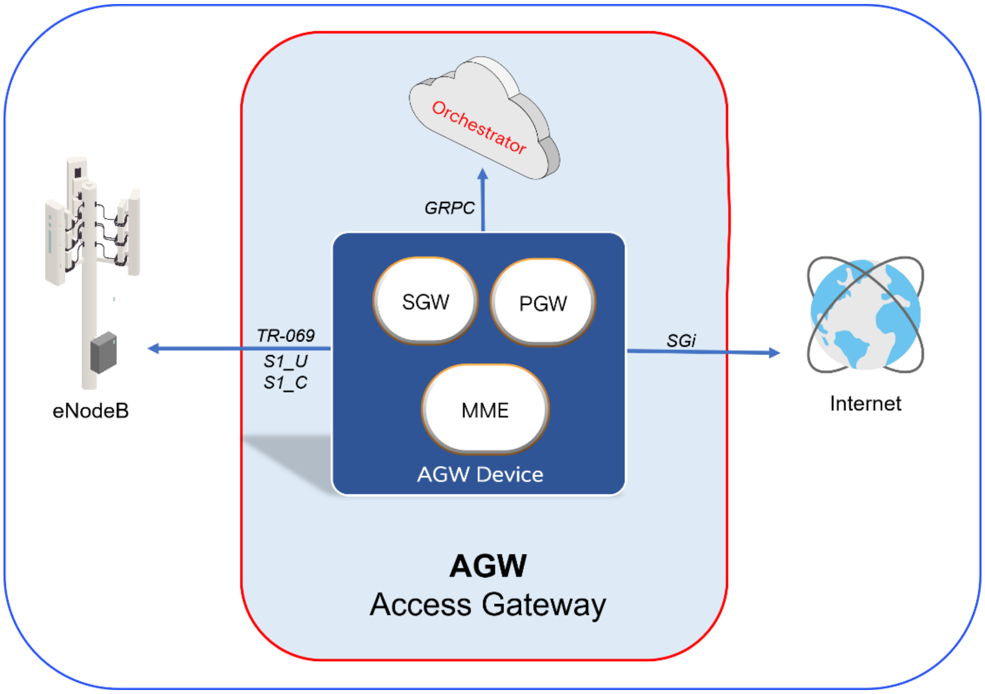


Figure 3.1

3.2 Features and Functionalities

The 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
- eNodeB 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-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 signal
- 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

Supports QCI to DSCP mapping for GBR bearers (QC1 bearer for VoLTE)

Circuit Switched FallBack (CSFB) Supports NAS, S1AP, and SGs procedures to support CSFB for incoming and outgoing CS call and CS-SMS

3.3 Subcomponents

MME
The Mobile Management Entity functions include S1AP, NAS and MME_APP subcomponents. The MME is the key control node for the LTE access-network. It is responsible for idle mode UE (User Equipment) paging and tagging procedure including retransmissions.

1. S1AP external Interface with eNodeB
   a. S1AP ASN.1 encode/decode
   b. 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. Statistics to track the number of eNodeBs connected, number of registered UEs, number of connected UEs and number of idle UEs.

5. 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 (Packet Data Network Gateway)
The PGW acts as the interface between the LTE network and other packet data networks, such as the Internet or SIP-based IMS networks.

S-PGW Control Plane functions include:

1. S11 like 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

- Gx: this interface is used by the P-GW to communicate with the Policy and Charging Rules Function (PCRF) in order to handle Policy and Charging Rules (PCC) rules.

- Gy: this interface is used by the P-GW to communicate with the Online Charging System (OCS). The P-GW informs the charging system about pre-paid users payload in real time

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 data path through pipelined for L2-L4 and DPId for L4-L7 policies.

Pipelined
Pipelined is the control application that programs the OVS (Open vSwitch) 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.

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.

Susbcriberdb
Subscriberdb is Magma's local version of HSS. Magma uses Susbcriberdb 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)

Susbcriberdb 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 - Open vSwitch 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:
The Control Proxy manages the network transport between the gateways and the controller.

1. Control proxy abstracts 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.

3.4 Data Plane Functionality

Data Path

OVS (http://www.openvswitch.org/) is used to implement the policy and charging enforcement function (PCEF), QoS, application-based policy enforcement, and the collection of statistics for user plane traffic. The control plane applications interacting with OVS are implemented in pipelined. The README in pipelined describes OVS programming in greater detail.

QoS

Magma supports flow-based traffic shaping and uses Linux classful qdiscs to provide this functionality. OVS marks packets that match a flow with QoS requirements, with a QoS ID. Tc filters are used to steer those packets to different traffic classes based on the QoS configuration. Packets that match flows with no QoS configuration are sent to the default traffic class.

3.5 Resiliency, Redundancy and Backup Functionality

High availability, resiliency and backup features for each Magma component include:

Access Gateway

- *Resiliency*
  All Magma services on gateway continue restarting on failure. Any config changes can be enforced through a service restart. The EPC implements retransmission of Authentication Request and Security Mode Command on timer expiry.

- *Redundancy*
  In future, we plan to have a standby instance of MME for every active MME. When the main MME process goes down, the standby instance can take over using the persistent state.

- Backup
  In future, a stateless MME can ensure that EPC state is made persistent on the disk and periodically backed up in the cloud. This state would include information of the eNodeB's that are connected to the AGW.

Orchestrator

- *Resiliency*
  The Orchestrator microservices are stateless. Any service crash would result in the service auto restart, and the service would resume operation. Health checks are performed to ensure the liveliness of the services. Software upgrades are pushed by bringing up the new service instance, and the old service instance is terminated only after the new service is healthy.

- *Redundancy*
  Orchestrator maintains a global view of all Gateway health, and is responsible for setting which gateway is active and for routing traffic to that gateway.

  The Orchestrator can be scaled horizontally, and the containers are behind a load balancer which uses DNS to distribute the requests in a round robin fashion.

- *Backup*
  The state for the Orchestrator is in the SQL database. The database should be configured for periodic snapshots. Backup should be done for the Orchestrator configs and secrets like certs.

4. Orchestrator

4.1 Functionalities and Features

The Orchestrator provides a network centric view of the system. It also has capabilities for configuring and monitoring of the network and gateways.

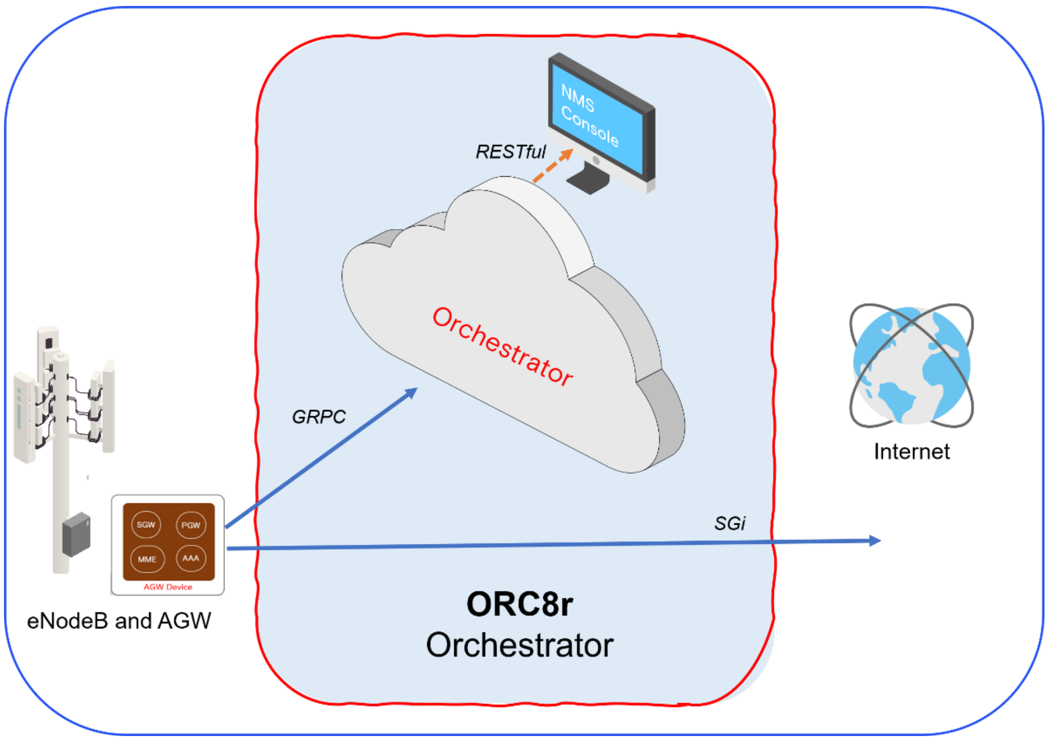


Figure 4.1

- The network as a whole can be configured through a single API call (e.g. changing the mnc/mcc), or individual access gateways can be managed the Orchestrator (e.g. 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 auto-generating code from the API specification.
- The north bound configs are applied to the gateways consistently. The gateways periodically poll the controller for their configs.

4.2 Monitoring:

- *Current Network State*
  Each gateway does a check-in 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 check-in data are logged, and data from the HTTP/2 proxy about the RPC type, response code and latency are logged.

4.3 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.

4.4 Subcomponent Microservices

Orchestrator consists of the following microservices:

MicroService	Description
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 sound bound APIs per gateway.
metricsd	Periodically fetches the time series data from the gateways
datastore	provides a key-value interface for the services

Table 4.4

Appendix A – Supported Procedures, Configurations & KPI's

A1. eNodeB 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 following tables display the TR-181 & TR-098 data model parameters that an eNodeB reads from the local database and compares. For a detailed list of parameters that each eNodeB supports, refer to the Magma GitHub at:

- Baicells Devices

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

Table TR181

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.SubFrameAssignmentbool	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

Table TR098

eNodeB Specific KPIs

The following eNodeB specific KPIs are pulled from the eNodeB and sent to the Orchestrator for display.

- Connected UEs
- GPS
- MME, PTP, GPS Connection Uptime
- Whether the device is transmitting
- DL/UL Throughput

The 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

eNodeB Metrics Table

A2. 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 (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

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-default 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

A3. HSS/SubscriberDB 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

A4. Internal Stats and Alarms

In addition to the KPIs from eNodeB and EPC, the individual gateways provide the following system level metrics to monitor and track system performance and health:

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

Appendix B - Interfaces

TR-069

TR-069 is a technical specification that defines an application layer protocol for remote management of customer-premises equipment (CPE) connected to an Internet Protocol (IP) network. 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. (ACS - Auto Configuration Server)

B1.1 Device Data model : TR-181 and TR-098
B1.2 Information Data model : TR-196

The following RPC methods are supported and used by the AGW.

RPC Methods Supported by ACS	CPE's RPC Methods used by ACS
Inform	GetParametersValues
GetROCMethods	SetParametersValue
TransferComplete	Add Object (part of objects)
	Delete Object (part of objects)
	Reboot
	Download

Table TR69

S1 Interface

The S1 interface is the interface between the LTE RAN and evolved packet core. Magma supports 3GPP compliant S1AP over SCTP and GTP over UDP protocols to support c-plane and u-plane interfaces, respectively with eNodeBs.

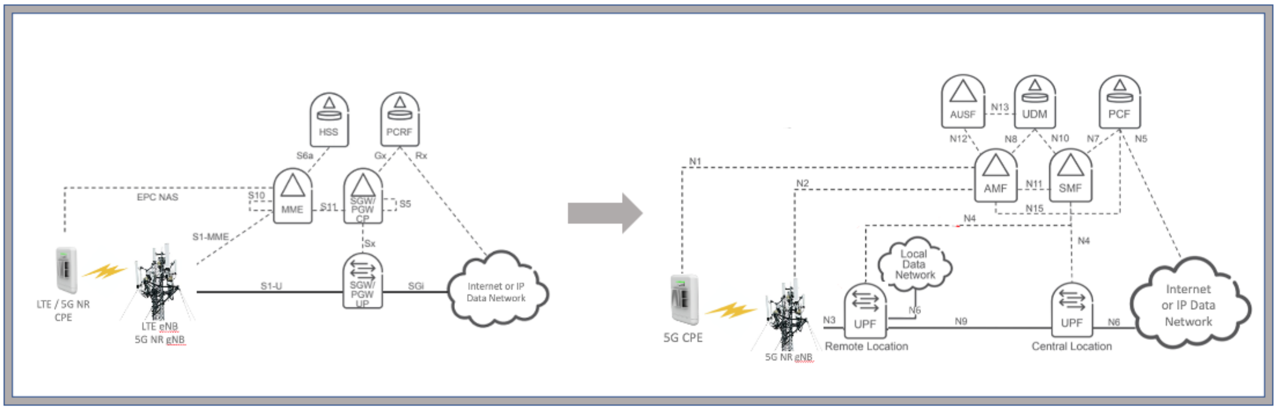
The following S1AP Procedures are currently supported:

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
Reset eNodeB Initiated	Reset Request Reset Ack
Paging	Paging for DS 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
S1AP Table	

NAS (Non Access Stratum)

The Non-Access Stratum is a set of protocols in the Evolved Packet System. The NAS is used to convey non-radio signaling between the User Equipment (UE) and the Mobility Management Entity (MME) for an LTE/E-UTRAN access

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 with Attach 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
Tracking Area Update	Tracking Area Update Accept
Service Request	Service Reject

Extended Service Request	Extended Service Request
EMM Information	EMM Information Request EMM Information Response
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

Appendix C - Hardware Recommendations for Magma FWA

Prerequisites

The prerequisites for preparing to deploy a private LTE FWA Magma network are listed below. It is preferred to use a MAC Laptop or PC. Prepare or install the following hardware and software before you begin. A wired internet connection is recommended, do NOT to use a VPN during installation as it may affect connectivity between VM's.

Currently, the Orchestrator deployment is supported for AWS only. The Access Gateway (AGW) installations are supported on bare metal Debian Linux computers.

Install the following onto the PC/Laptop that will be deploying the Magma Dev Package:

Development Tools

Install the following developer tools:

1. Docker Image Depository to deploy Magma containers
2. Homebrew *only* for MacOS users, see the pyenv installation instructions
3. VirtualBox Oracle Virtual Box, version 5.2 or higher
4. Kubectl kubernetes CLI tool allows you to run commands against Kubernetes clusters
5. Helm 2.0 manages Kubernetes applications; define, install, and upgrade
6. Python 3.5 Python for the Access Gateway Installation
7. Terraform manages the Orchestrator cloud deployment

Prepare the following hardware & software:

8. An eNodeB - the recommended and tested models are:

    - BaiCells Nova 233 TDD
    - BaiCells Nova 243 TDD Outdoor
    - Assorted Baicells indoor units for lab deployments
    - An Antenna connector for the eNodeB

    Support for other RAN hardware can be implemented inside the enodebd service on the AGW, it is recommended to start with one of the above eNodeB's.

9. An Access Gateway (AGW) - the recommended requirements are: Any 64bit-X86 machine, Dual-CPU, 2GHz clock speed or faster, 2GB RAM, 128GB-256GB SSD storage which can support a Debian Linux installation. With a minimum of 2+ physical ethernet interfaces (enp1s0=SGi and enp2s0= S1),

    - A USB stick with 2GB+ capacity to load a Debian Stretch ISO Used to build the AGW

    To add the Magma Access Gateway (AGW) to the new network, use the Magma Network Management System (NMS).

10. An AWS Account - with the permissions to create multiple Amazon EC2 virtual servers for the Magma Orchestrator, Network Management System (NMS) and Access Gateways if they are

deployed in the cloud. When using access and secret keys for an administrator account *do not use* the root account.

- Create Root account
- Create an Admin User account
- Obtain an <access key ID> for an administrator account
  Obtain a <secret key> for an administrator account

11. Magma Dev Package – clone from the Facebook Github repository

- Setup a GitHub Account
- Install Git to use command line

12. A Registered Domain/URL for Orchestrator endpoints

13. CPE such as smartphone or tablet SIM card with known key values for testing.

Example Bill of Materials (BOM)

Pure Play FWA Trial - BoM

Hardware per eNodeB site	Orchestrator in AWS	Dimensioning
Access Gateway - 1 unit per eNodeB site	**Orchestrator - 1 AWS setup (up to 50 AGWs)**	
• ITX4105G motherboard • Intel® Celeron® J4105 Processor (4 cores - 2.5GHz) • 4 GB DDR4 RAM Memory (expandable to 32 GB) • 1x SSD 2.5" 120 GB (supports up to 4x 2.5" SATA disks) • 2x 1Gbps NICs • Single Power Supply	• 1 x EKS cluster • 2 x t3.large EC2 workers • 4 x ELB • 2 x RDS instances • EFS access	**Access Gateway** up to 12 eNodeBs per site / 10k users **Orchestrator** up to 50 AWGs
Rack - 1 unit per eNodeB site	**Site Switch - 1 unit per eNodeB site**	

Rack: Huawei APM30H
 	
• Standard 1U module for 19 inch racks
 	
• Power Supply (standard)
  ◦ Input: 100-240 VAC, 50/60 Hz
  ◦ Max power consumption: 150 W
 	
• Redundant Power Supply (optional)
  ◦ Input: 100-240 VAC, 50/60 Hz
  ◦ Max power consumption: 120 W
 	
• Dimensions (W x H x L): 443.4mm x 44.45mm x 395mm
 	
Operating Environment
• Temperature: 0 - 50 C
• Humidity: 10-90 % non-condensing
 	
Storage
• Temperature: 0 - 50 C
• Humidity: 10-90 % non-condensing
	• Mikrotik 3 x RJ45 Gigabit Ethernet 10/100/1000 Mbps	

FACEBOOK
CONNECTIVITY