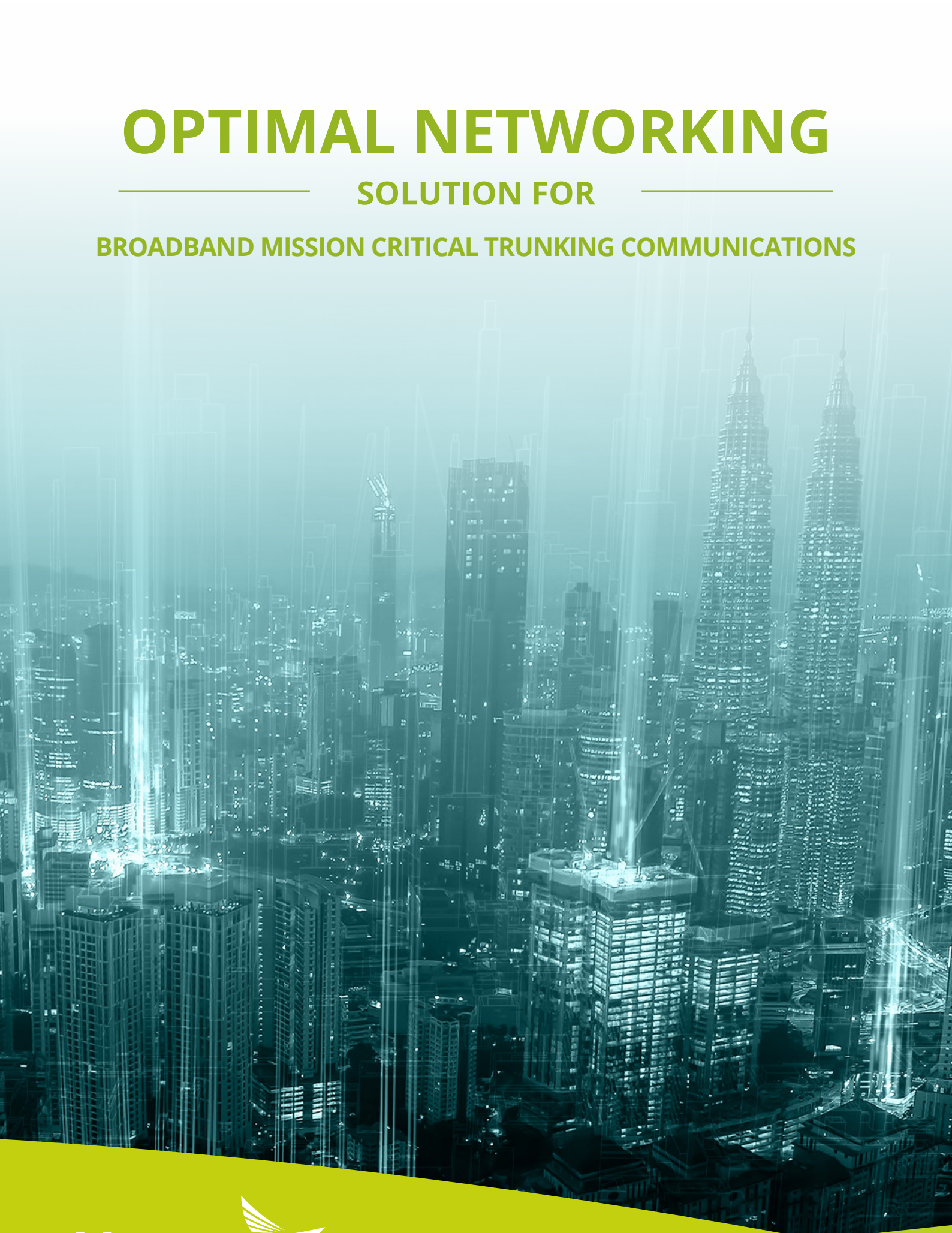
OPTIMAL NETWORKING

SOLUTION FOR

BROADBAND MISSION CRITICAL TRUNKING COMMUNICATIONS



Hytera

CONTENTS

INTRODUCTION

Mission-critical communications is widely used in public safety, utilities and many industries. It is an important means for users to command, dispatch and respond to emergencies.

Using the Push-to-talk (PTT) function in mission-critical communications, key message can be delivered to a large number of people at the same time through trunking system by easily pushing a button. Following the rapid development of industries like public safety, government affairs, public transportation and energy, the demand for broadband wireless data services, high-definition video surveillance, multimedia digital trunking command and dispatch has been increasing quickly upon the base of traditional voice transmission.

LTE (Long Term Evolution) is a long-range evolution of Universal Mobile Telecommunications System (UMTS) which is a technical standard defined by the 3rd Generation Partnership Project (3GPP). LTE has an array of outstanding features such as wide bandwidth, high speed and all-IP architecture, owning a lot of successful commercial case studies and a mature ecosystem comprised by device, infrastructure and network facilities. 3GPP has actively responded to the demand from users and finalized the MCS standards (including MCPTT, MCVideo and MCData) in versions starting from R13.

Generally speaking, public network has a lot of advantages in terms of network construction and technology development over private network. It is a feasible solution to build up a private LTE network for radio trunking communications with low cost, secure coverage, great reliability and guaranteed QoS by adopting the extensive coverage of public network and deploying private network base stations to provide mission critical communications and supplement the network coverage at the place where public network is insufficient.

“COMMUNICATION SYSTEMS IN MANY COUNTRIES LIKE THE UK, SOUTH KOREA AND THE US ARE BEING TRANSFORMED TO BROADBAND.”

HOW TO CHOOSE A NETWORKING SOLUTION

Following the ever-changing demand of users and continuous development of technology, mission-critical communications networks in a lot countries have been changing constantly in multiple ways:

1. ***ADDING NEW BASE STATIONS TO ENHANCE COVERAGE.***
2. ***BUILDING UP A NEW AND ADVANCED NATIONWIDE NETWORK.***
3. ***UPGRADING THE EXISTING NETWORK TO MEET THE INCREASING DEMAND FOR IMAGE, VIDEO AND DATA TRANSMISSION.***

How to choose the optimal networking solution for a mission critical communications network on its way of transformation to broadband? In general, users from public safety and utilities put their concern in the factors below:

1. ***NETWORK SAFETY & RELIABILITY***
2. ***CONSTRUCTION COST & LEAD-TIME***
3. ***MAINTENANCE COST***
4. ***FREQUENCY & SPECTRUM***

Let's look at some world-leading cutting-edge examples.

Emergency Services Network (ESN) in UK, ESN can be accessed through Mobile Network Operators (MNO). Public network and private network users share the operators' frequency resources. ESN owns its independent private core network to provide broadband trunking services for PMR users.

Korea Telecom (KT) & SK Telecom (SKT) in South Korea, KT and SKT have started to deploy a nationwide LTE network for mission critical communications adopting Band 28 as the frequency of the network.

First Responders Network (FirstNet) in US, United States plans to use Band14 (700 MHz) from MNO to provide national broadband trunking services.

TYPES OF NETWORKING

	New Network	MVNO*	MVNO + New Network	Overlap
Frequency & E-UTRAN	Dedicated	Sharing	Sharing + Dedicated	Sharing
Core Network	Dedicated	Dedicated	Dedicated	Sharing
Cost	High	Low	Medium	Very Low
Safety	Very High	High	High	Low
Delivery Lead-time	Long	Short	MVNO - Short New Network - Long	Very Short
Country of Networking Application	South Korea	UK	Australia New Zealand	N/A

*MVNO, Mobile Virtual Network Operator
MVNO does not own the network, instead it leases network from a network provider, and then sells services to consumers under its own band.

NETWORKING SOLUTIONS

1. New Network

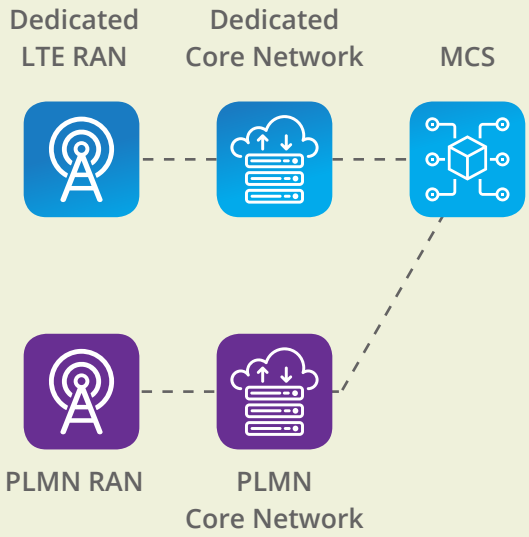
A newly built LTE network can work independently or connect to public network to extend coverage.

1) Pure Private Network

The network adopts proprietary spectrum resources to deploy LTE base stations, core networks and MCS services.

- Safe and highly stable.
- High cost and long delivery lead-time.

FIGURE 1. TOPOLOGY OF PURE PRIVATE NETWORK



2) Combination of Public and Private Network

In the places where are critical or having insufficient coverage, private network base stations can be deployed for trunking services and extended coverage. PLMN* is a network established and operated by the government or its authorized operators for the purpose of providing land mobile communications services to the public.

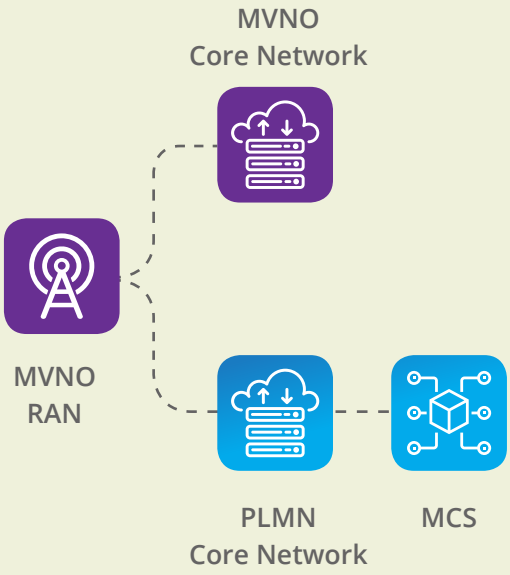
- Highly safe. However, there will be less stability in the area having public network coverage than those having private network coverage.
- Project delivery lead-time and investment will depend on the quantity of new base station.

FIGURE 2. TOPOLOGY OF PUBLIC AND PRIVATE NETWORK COMBINATION.

*PLMN (Public Land Mobile Network)

2. MVNO

MVNO has two ways of implementation, RAN Sharing and Network Element Sharing.



1) RAN Sharing

The LTE network is completely independent. Base stations and spectrum resources are being shared between operators to reduce the cost of network construction.

The dedicated core network needs to be connected with all base stations of MVNO.

Every time MVNO builds a new base station or upgrades its base stations, reconfiguration will be needed, which increases the maintenance cost.

FIGURE 3. TOPOLOGY OF RAN SHARING

2) Network Element Sharing

MME and SGW are being shared between MVNOs, while HSS, PGW, PCRF and MCS servers are newly built and dedicated. Once MVNO's RAN gets updated, MCS services will be enabled:

eMBMS (enhanced Multimedia Broadcasting Multicast Services) greatly enhances the spectrum utilization.

IOPS (Isolated e-utran Operation for Public Safety) improves the reliability of the system.

QoS guarantees the highest priority, low latency and data rate of mission-critical services.

Every time MVNO builds a new base station or upgrades its base stations, reconfiguration will be needed, which increases the maintenance cost.

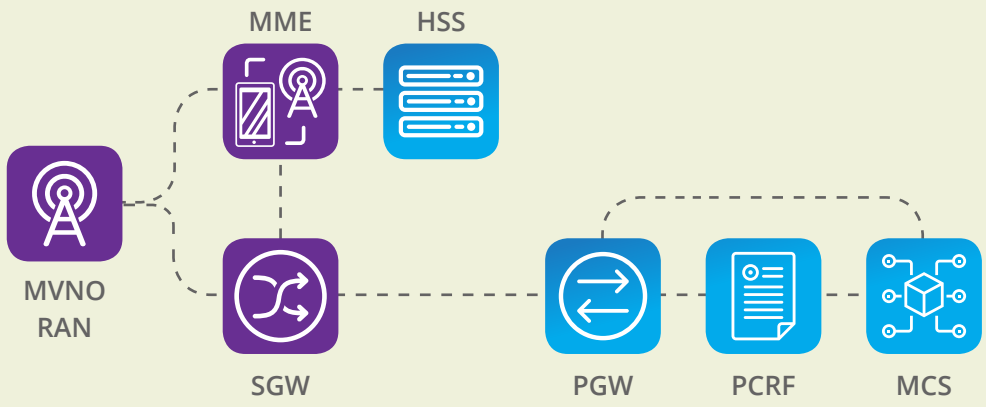


FIGURE 4. TOPOLOGY OF NETWORK ELEMENT SHARING

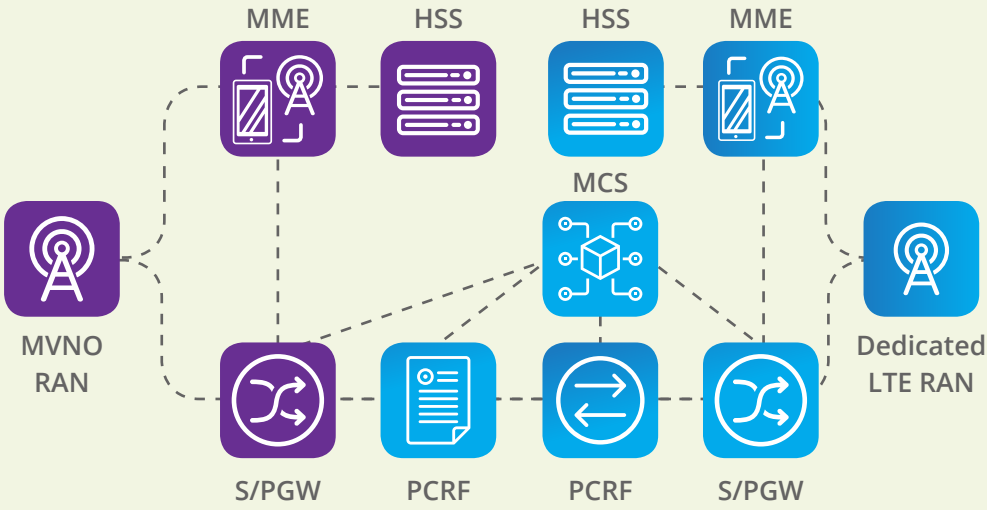


FIGURE 5. TOPOLOGY OF MVNO + NEW NETWORK

3. MVNO + New Network

Network deployment conforms to 3GPP protocols.

LTE network is completely independent, which guarantees the reliability and safety of the network.

Within coverage of LTE private network, private EPC provides access for terminals. Trunking services are provided by adopting 2/3/4G of public network to extend LTE network's coverage.

Only Rx connection is required for the network deployment, which is extraordinarily suitable for those scenarios of connecting multiple public network operators and makes future operation and maintenance more easier.

4. Overlap

This solution completely relies on the existence of public network and has low reliability and stability, which is not an optimal option for users of mission-critical communications

FIGURE 6. TOPOLOGY OF OVERLAP

Summary

The adoption of combination of Public and Private LTE Network can build up a private LTE network for radio trunking communications with lower cost, wider coverage and shorter lead-time.

OPTIMAL NETWORKING FOR BROADBAND MISSION-CRITICAL TRUNKING

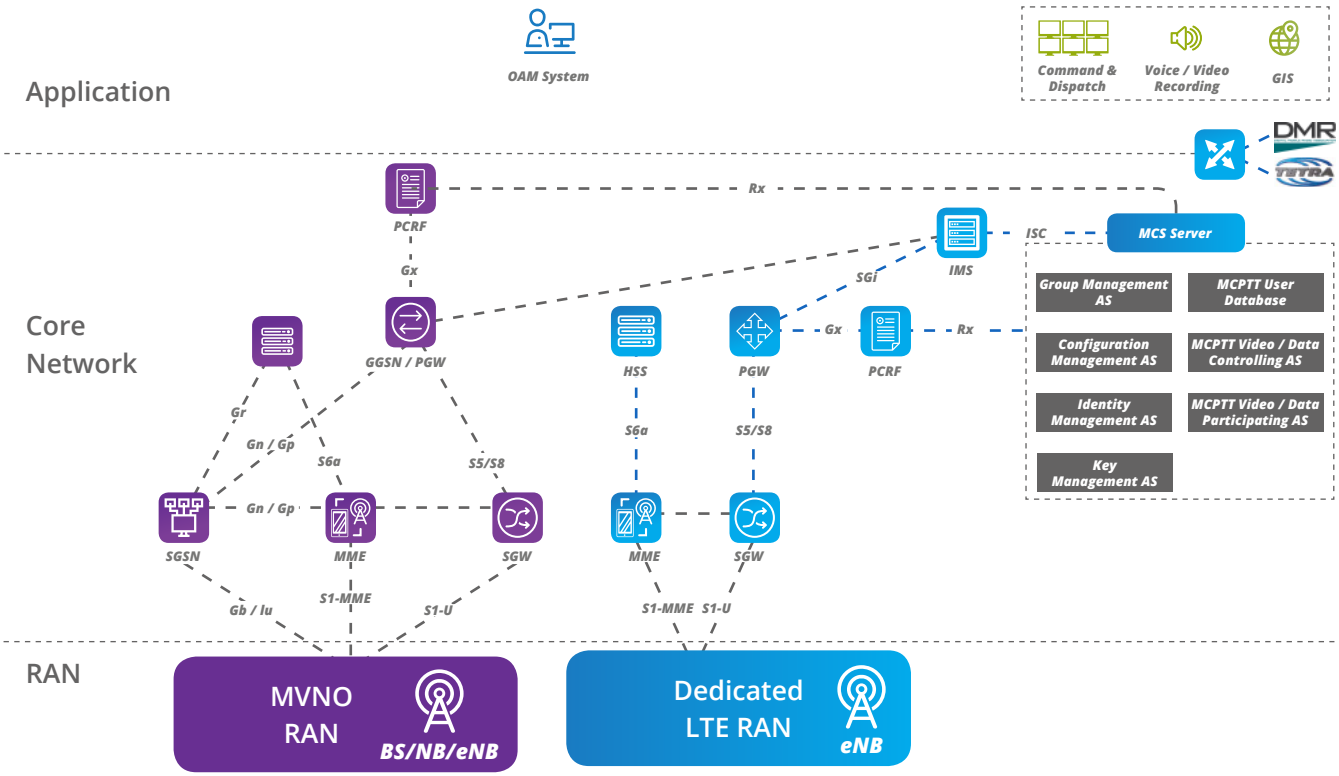


FIGURE 7. TOPOLOGY OF MVNO + PRIVATE LTE NETWORK

- MVNO provides wide coverage, efficiently utilizes existing network resources to save the cost of network construction and accelerate the deployment of private network system.
- Private network needs to be deployed in key areas or areas with poor MVNO coverage.
- The independent broadband trunking core network is invisible to MVNO. Two core networks are being operated and maintained separately.
- The IDs and data of private network users are stored in the private network system to ensure data safety.
- Broadband trunking system can provide QoS to ensure reliability.

APPENDIX

	Entry	Function
MVNO	MME (Mobility Management Entity)	• NAS signaling and security • Tracking Area list management • PDN GW and Serving GW selection • MME selection for handovers with MME change • Roaming (S6a towards home HSS) • Authentication • Bearer management functions including dedicated bearer establishment and eMBMS bearer establishment
	HSS/HLR (Home Subscriber Server) / (Home Location Register)	HSS: • subscription data management • Location Management • Authentication • Fault Recovery HLR: • Home Location Register is a database responsible for the management of mobile users. It permanently stores and records the subscription data of users in the area under its jurisdiction, and dynamically updates the location information of users in order to provide the network routing of the called users in the call service.
	SGW (Serving GateWay)	• The local Mobility Anchor point for inter-eNodeB handover • ECM-IDLE mode downlink packet buffering and initiation of network triggered service request procedure and optionally Paging Policy Differentiation • Packet routing and forwarding • Transport level packet marking in the uplink and the downlink, e.g. setting the DiffServ Code Point based on the QCI and optionally the ARP priority level of the associated EPS bearer.
	PGW (PDN GateWay)	• UE IP address allocation • Transport level packet marking in the uplink and downlink, e.g. setting the DiffServ Code Point based on the QCI and optionally the ARP priority level of the associated EPS bearer • UL and DL service level gating control as defined in TS 23.203 • UL and DL service level rate enforcement as defined in TS 23.203 (e.g. by rate policing/shaping per SDF) • UL and DL rate enforcement based on APN-AMBR (e.g. by rate policing/ shaping per aggregate of traffic of all SDFs of the same APN that are associated with Non-GBR QCIs) • DL rate enforcement based on the accumulated MBRs of the aggregate of SDFs with the same GBR QCI (e.g. by rate policing/shaping)

	Entry	Function
MVNO	SGSN (Serving GPRS Support Node)	SGSN, as an important component of packet domain equipment in GPRS/WCDMA (TD-SCDMA) core network of mobile communication network, has the following functions: packet routing, mobility management, session management, logical link management, authentication and encryption, bill generation and output.
	GGSN (Gateway GPRS Support Node)	Gateway GSN (Gateway GSN) is mainly used as a gateway. It can connect with many different data networks, such as ISDN, PSPDN and LAN.
	PCRF (Policy and Charging Rules Function)	PCRF is the policy and charging control element. PCRF functions are described in more detail in TS 23.203. In non-roaming scenario, there is only a single PCRF in the HPLMN associated with one UE's IP-CAN session. The PCRF terminates the Rx interface and the Gx interface.
Private LTE Network	MME (Mobility Management Entity)	Same as the MME above
	HSS (Home Subscriber Server)	Same as the HSS above
	SGW (Serving GateWay)	Same as the SGW above
	PGW (PDN GateWay)	Same as the PGW above
	PCRF (Policy and Charging Rules Function)	Same as the PCRF above
MCS Server	GMS (Group Man-agement Server)	The group management server functional entity provides management of groups supported within the MCS service provider. The group management server functional entity is supported by the SIP AS and HTTP server functional entities of the signaling control plane.
	CMS (Configuration Management Server)	The configuration management server is a functional entity used to configure the MCS application with non-group management MCS service related information and configure data on the configuration management client. The configuration management server manages MCS service configuration supported within the MCS service provider. The configuration management server functional entity is supported by the SIP AS and HTTP server functional entities of the signaling control plane.

	Entry	Function
MCS Server	IDMS (Identity Management Server)	The identity management server is a functional entity that is capable of authenticating the MC ID. It contains the knowledge and means to do authentication by verifying the credentials supplied by the user.
	KMS (Key management AS)	Manage and storage the encryption key information.
	MCPTT User Database	Manage the register information of user.
	Controlling AS	• Call control (e.g. policy enforcement for participation in the MCPTT group calls) towards all the MCPTT users of the group call and private call. • Interfacing with the group management server for group policy and a翻 liation status information of this MCPTT server' s served a翻 liated users. • Managing floor control entity in a group call and private call. • Managing media handling entity in call i.e. conferencing, transcoding.
	Participating AS	• Call control (e.g. authorization for participation in the MCPTT group calls) to its MCPTT users for group call and private call; • Group a翻 liation support for MCPTT user, including enforcement of maximum N2 number of simultaneous group a翻 liations by a user; • Relaying the call control and floor control messages between the MCPTT client and the MCPTT server performing the controlling role; and • Media handling in call for its MCPTT users, i.e. transcoding, recording, lawful interception for both unicast and multicast media.

The network interface reference points involved in the figure are as follows:

S1-MME: Control plane protocol reference point between E-UTRAN and MME.

S1-U: User plane tunnel reference point for each bearer between E-UTRAN and S-GW.

S6a: For the authentication and confirmation of the user access enhancement system, the acknowledgment data is transmitted between the MME and the HSS.

S5/S8: An interface between the S-GW and the P-GW in the network. The interface should provide the S-GW relocation function during the user mobility in the case of the S-GW and the P-GW.
S11: Reference point between the MME and the S-GW.

SGi: A reference point between the P-GW and the packet data network. The packet data network may be an external public or private data network, or an internal packet data network, for example, serving IMS. This reference node is similar to the Gi node of the 3GPP access network.

SGs: SGs is the interface between MME and MSC/VLR. It is used for Mobility management (MM) and paging procedures between the EPS (Evolved Packet Services) and CS (Circuit Switched) domain.

Gb/lu: The Gb interface in GSM connects the BSS and the SGSN. It shows that the network supports GPRS 2.5G.

Gn/Gp: Gn is the interface between the GGSN and the SGSN. The interface protocol supports mobility management (MM) and the transmission of user data and signaling. Gn interface uses TCP/IP protocol.

Gs: SGSN coordinates with MSC through the Gs interface to support the mobility management of MS, which includes combined attach/detach and combined RA/LA update.

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. These rules contain charging related information as well as Quality of Service (QoS) parameters that will be used in the bearer establishment. Diameter protocol is used in the Gx interface.

ISC: IP multimedia Service Control interface enables the complete separation between user plane and control plane.

Rx: The Rx node is located between AF and PCRF.

Hytera

Keep up to date with Hytera on social media.

Hytera Communications (Australia) Pty Ltd
53 Brandl St, Eight Mile Plains QLD 4113 Australia
Telephone: 1300 498 372
Email: sales_aus@hytera.com