Prepare your transport network for modern public safety

Evolve your LMR/PMR transport network to support new IP/MPLS, broadband and IoT-based public safety services.

White paper

The public safety landscape is evolving. To continue attaining their safety goals, many governments are upgrading their public safety infrastructure to expand the use of data and to usher in Internet of things (IoT)-based services. The transport network (also called the backhaul network) is foundational to these initiatives. A traditional approach is to deploy a new multiservice network to support the various safety-critical applications in addition to the legacy one. This dual-network approach incurs a high cost of deployment and operations, with an inefficient use of space and power. This white paper explains how an all-packet IP/MPLS network can be the common transport network to meet all of your needs.

Contents

The evolving public safety communications infrastructure landscape

Today, governments strive to deliver highly effective emergency services and provide citizens with better public safety protection. Consequently, many are already harnessing broadband LTE services – for example, FirstNet in the United States – to support new data-intensive applications for better coordinated public protection and emergency response.

At the same time, they have continued upgrading their land mobile radio (LMR) system to allow public safety agencies' mission-critical voice services to meet their short- to medium-term needs. Lastly, to accomplish their security mission, local and regional governments are planning to accelerate the rollout of digital services based on connected safety sensors. These include CCTV, audio, gunshot and smoke sensors to detect events more quickly and monitor emergency situations.

Fundamental to such public safety infrastructure evolution is the adoption of a high-performance broadband communication platform connecting its associated assets everywhere. Because the infrastructure needs to be spread countrywide, a broadband wireless network is the natural choice to reach all assets economically. Open standard-based LTE is the preferred radio access technology because of its rich ecosystem, robust security and an evolutionary path to 5G.

How is the transport network affected by these evolutions?

These market trends have a direct impact on existing transport networks managed by governments for public safety communications. The scope of this transformation will vary, depending on specific situations and the model adopted to evolve their public safety communications infrastructure.

1. Evolution toward mobile broadband

Governments willing to deploy broadband wireless public safety services, have three primary options to consider:

a. A shared network model, where the government will mostly rely on existing commercial service provider (CSP) networks. In the case of a central government, they will want to keep control on the service and subscriber database by deploying a secure-mobile virtual network operator model (S-MVNO), where the government owns the core network and applications. This is the model adopted in the US and in the UK, for instance, and currently is under consideration by many European countries.

b. A dedicated network model, where the government will invest in a private wireless network mainly for its own private use. This is the model chosen by the Dubai, Qatar and South Korea governments, and some local governments for their police forces.

c. A hybrid model, where the government will use a shared network and will build its own dedicated network in critical or remote geographical areas to strengthen network mission-criticality.

What does each of these models mean for public safety transport network transformation?

a. Shared wireless broadband network

In this model it is the responsibility of the CSP to manage the transport network that interconnects the LTE base stations to the wireless core. Because commercial networks were not designed to provide mission-critical-grade communications, they generally will have to expand network coverage and strengthen resilience.

It is therefore essential that government authorities discuss the evolution of the CSP transport network as part of the broader evolution toward mobile broadband for public safety communications.

b. Dedicated network

In this model agencies use the new broadband network for public safety services, complementing or replacing the existing narrowband one. Local governments may use the private wireless network to execute on their broadband and digital agenda. In such cases they would use the broadband network for non-mission-critical applications, such as air quality monitoring in different parts of a city, autonomous shuttles or to help bridge the digital divide in remote areas.

To optimize the time and project economics required to deploy such new network, the public safety network operator will want to leverage its existing tower and transport network assets. This means upgrading these assets to support both the legacy LMR and new LTE/5G networks.

Operators will need to support this broader set of services, which have different levels of criticality, with very strong network service prioritization, traffic segregation and security mechanisms – including in the transport network. This will ensure critical communications are prioritized over less-critical traffic.

c. Hybrid model

In this scenario the transport network will combine both previously described models.

Whatever the model chosen for the broadband public safety terrestrial network, it will be complemented by deployable wireless systems to allow first-responders to operate where coverage is missing or is out of order. These deployable systems will include a wireless transport technology to connect them to a central command and control room.

All of these models require the use of scalable, all-packet, IP/MPLS transport networks to optimally carry the range of critical network data and services.

2. LMR/PMR network upgrade

Despite the evolution toward mobile broadband, many governments already managing a public safety network want to keep their LMR/PMR system to provide mission-critical voice services for their public safety agencies. As these legacy LMR systems become obsolete or reach their end-of-life, operators will need to upgrade them using latest version of narrowband digital LMR technology, such as Project 25 (P25) or Tetra standards. Given these technologies now have natively adopted IP protocol to connect base stations to the core network, such evolution will require governments to migrate the transport network from TDM to IP.

Obviously, the choice of the model to deploy mobile broadband for public safety will impact the scope of the transport network renovation.

Regardless of which model is adopted to deploy mission-critical broadband, when using a public safety transport network in a multiservice capacity, it is imperative that public safety application performance is never degraded, and that first responders communications are never compromised. The rest of this paper explores how embracing all-packet and IP/MPLS architectures can broaden public safety transport networks to meet these important requirements.

Challenges for multiservice public safety transport networks

To provide the required performance, a multiservice public safety transport network must meet the following challenges:

- Network resilience
- Assured delivery of high-priority public safety LMR or LTE traffic
- Network security
- Interworking with the cloud to support other safe-critical digital services
- Readiness for 5G

Network resilience

Resilience of the transport network means utilizing path diversity to ensure critical communications are maintained when a link or node fails. This will be particularly important in sensitive, strategic geographic areas of the network. Typical ways to improve the resilience of transport networks are “ring configurations” and full hardware redundancy. Specific backup batteries to support a very long power supply outage will also be needed to keep the network running in critical situations.

Assured delivery of LMR or LTE traffic

Radio communication is a lifeline for first responders. It needs to be up and running 24 x 7. Many of the applications used have real-time requirements. Therefore, network delay is an important issue to address. With use cases expanding towards less-critical safety or smart city applications, there will be diverse applications that run atop the network and compete for bandwidth. Examples include CCTV, administrative tasks, intelligent traffic management systems and smart lighting for local governments.

As mentioned above, real-time mission-critical LMR public safety traffic requires the network to meet strict latency characteristics with the highest possible reliability, while other applications have less demanding requirements (see Table 1). It is crucial that the network is application-aware to classify traffic for different quality of service (QoS) so that it always reliably delivers critical LMR traffic – even when there is network congestion – so that first responders can communicate whenever needed with their radios without disruptions.

Table 1. Examples of applications with diverse QoS requirements

Application type	Latency	Bandwidth	Reliability	Criticality
LMR	Low	Medium	High	High
LTE GBR type (e.g. traffic signal control, streetlight)	Medium	Medium/Low	Medium	Medium
LTE non-GBR type (e.g. CCTV)	High	High	Medium	Medium
Public Wi-Fi	High	High	Low	Low

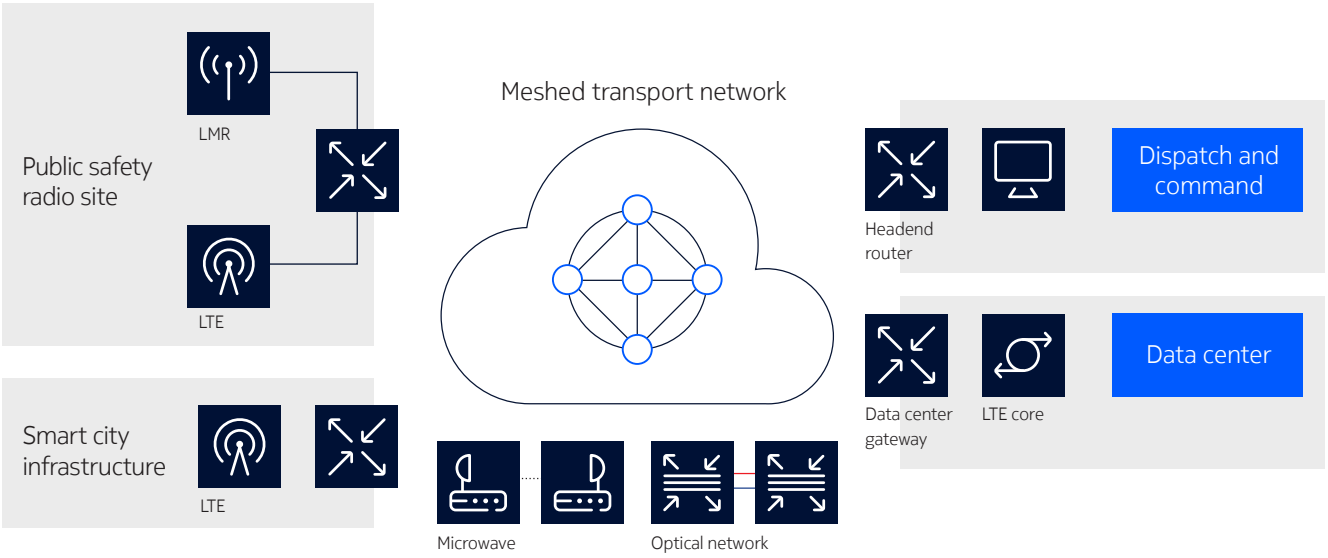
3GPP has standardized five QoS class identifiers (QCIs) specific for mission-critical networks:

QCI	Bearer type	Priority	Packet delay	Packet loss	Example
65	GBR	0.7	75 ms	10^{-2}	Mission-critical user plane PTT voice
66		2.0	100 ms	10^{-2}	Non-mission-critical user plane PTT voice
67		1.5	100 ms	10^{-3}	Mission-critical video user plane
69	Non-GBR	0.5	60 ms	10^{-6}	Mission-critical delay sensitive signaling
70		5.5	200 ms	10^{-6}	Mission-critical data

Network security

A typical public safety transport network architecture features meshed connectivity so that any device can reach any other device attached to the network. With more application systems, such as an LTE system, the attack surface increases (see Figure 1).

Figure 1. A transport network providing any-to-any connectivity for all connected devices



Additionally, when governments broaden the transport network to connect to city offices and public amenities, the attack surface expands further. Because these facilities are easily physically accessed, network vulnerabilities increase significantly. When attached devices are compromised, attackers can use them as launching pads to move across the transport network and penetrate into the LMR and other critical systems to cause serious disruptions.

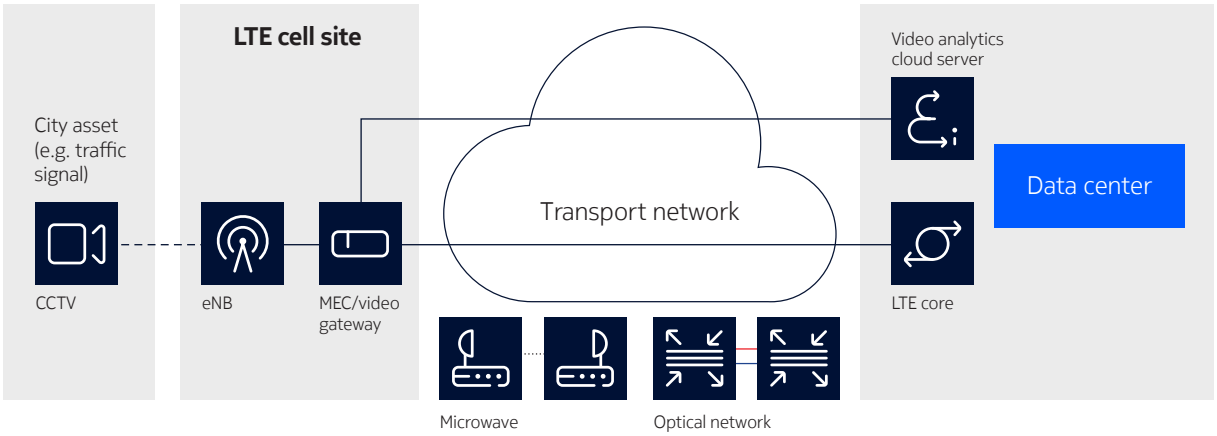
Interworking with the cloud for enhanced video services

New applications such as video analytics[1] are evolving to a distributed, cloud-based architecture. This allows them to scale up to process a large number of high-definition video streams close to the cameras, shorten anomaly detection time and optimize transport bandwidth.

1 Harnessing machine learning and computer vision, video analytics applications enable automated real-time ingestion and analysis of multitudes of video streams, detecting anomalous events that include people flow reversal, forbidden zone intrusion, and even gunshot detection via sound-enabled cameras.

This architecture takes advantage of LTE local breakout capability and places the video analytics gateway function on a multi-access edge computing (MEC) platform at the edge of the network. The MEC is even co-located with the base station in some circumstances, with the general operations, administration and maintenance (OAM) functions of the video analytics system remaining in a cloud server application in the data center (see Figure 2).

Figure 2. A distributed, cloud-based video analytics architecture



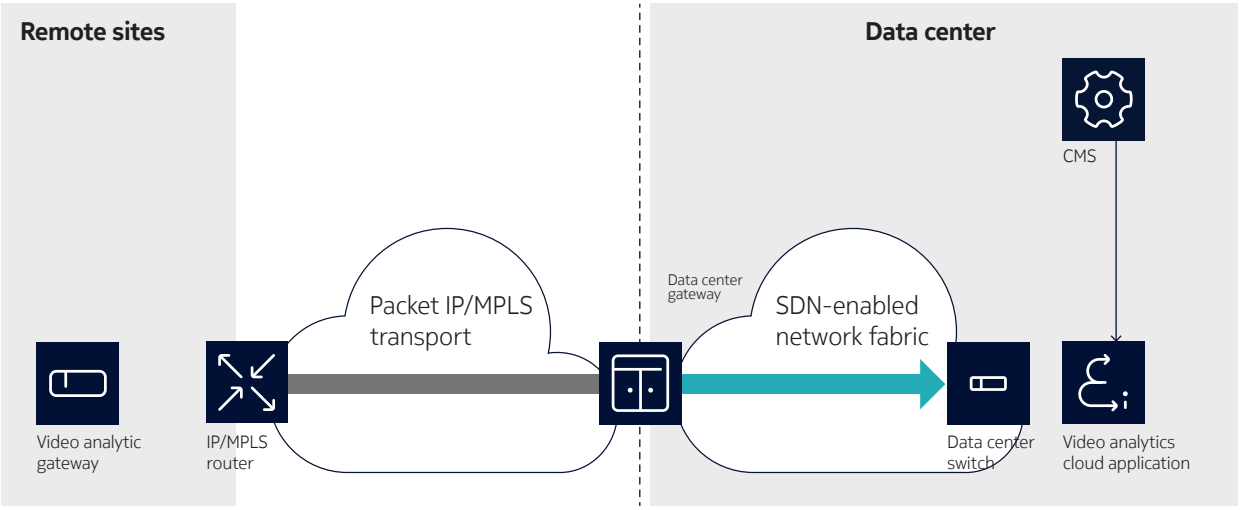
With data centers embracing cloud technology, the compute resource hosting the video analytics cloud server application becomes dynamic and mobile. The cloud management system (CMS) can create, delete and migrate compute resources and applications (or workloads in IT jargon) from one server to another server in another rack or pod, and from one data center to another, for server upgrade, resource optimization or maintenance.

When this happens, the traditional data center network fabric connecting all servers does not learn about these events in an automated way, and the connectivity to the applications is disrupted. Essentially, the workload and network layers are not in synchronization. Consequently, many data centers have transformed their network fabric to introduce fabric automation with tight integration with the CMS to adapt. The network fabric is now in lockstep with workloads.

This new workload architecture brings two challenges to the communications between the video gateway in the field and the cloud server application in the data center:

- Interworking between the transport network and the cloud (referred to as data center gateway hereafter): This requires a new network function called a network-cloud interworking gateway to seamlessly extend connection from the transport network domain across the data center fabric domain to reach the application (see Figure 3).
- Making the cross-domain connection adaptive when the application migrates to another data center.

Figure 3. Network-cloud interworking



Readiness for 5G

Because LTE is a 3GPP technology, governments will benefit from a smooth evolution to 5G when and where needed for more bandwidth-intensive and time-sensitive applications while they continue to use the LTE coverage. Therefore, it is essential that the existing transport network is also ready to provide transport for the 5G network.

How packet transport and IP/MPLS can help overcome challenges

An all-packet transport network with IP/MPLS brings the following capabilities to a public safety transport network to help overcome the challenges described:

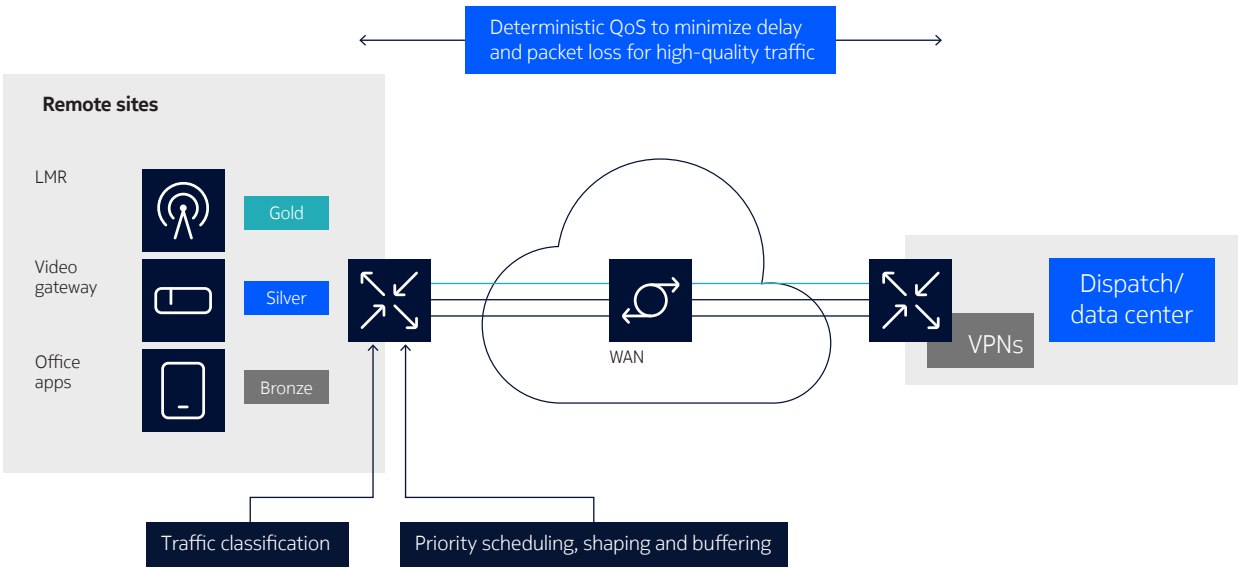
- Deterministic QoS for assured LMR traffic delivery
- Enhanced network resilience
- Zero-trust network security with segmentation and encryption
- Network-cloud interworking
- Support for 5G transport

Deterministic QoS for assured LMR traffic delivery

QoS is a set of network capabilities to control delay, jitter and packet loss for data traffic flowing through the network. This is done by controlling and managing bandwidth and packet scheduling resources in network equipment.

Although IP and Ethernet platforms do offer QoS, next-generation IP/MPLS routers, with their extensive packet classification, queuing and scheduling capabilities, have advanced flexible QoS capabilities to deliver critical LMR/public safety LTE traffic with assurance[2]- and with full application awareness. Consequently, with a wide range of applications sending data with a diverse range of QoS requirements based on a customized policy, IP/MPLS transport routers can intelligently classify, buffer, schedule and shape traffic to constantly satisfy the requirements of LMR/public safety LTE traffic and various other applications. This capability of constantly meeting the service requirement is called deterministic QoS (see Figure 4).

Figure 4. IP/MPLS transport network delivering QoS assurance



2 For a detailed discussion of traffic management, read the Nokia application note “Better backhaul.”

As an example, when the IP/MPLS router is receiving a high volume of videos data sent by CCTV, as soon as the LMR radio sends critical voice or data traffic the router is aware of its LMR origin. It strictly prioritizes it over other video traffic, minimizing delay and jitter while avoiding packet discard when link congestion occurs. This is essential to ensure constantly high mission-critical communications performance.

Microwave transport must be able to leverage traffic classification and prioritization (QoS) and adaptive modulation. The adaptive modulation works so that the transmission bandwidth is dynamically adapted according to the changing propagation conditions. Thanks to the QoS, the committed capacity (high priority) is carried errorless according to the KPIs defined during the microwave network design phase.

Enhanced network resilience

Mission-critical applications need to rely on resilient networks. Microwave can typically be the fiber backup, but sometimes even can be the sole solution to provide connectivity wherever the topography does not allow laying fiber.

In addition to constant monitoring by the network management system, a suite of analytics can leverage predictive analysis and automatic workflows to achieve the most value from the microwave network's behavior; i.e., preventing congestion/underutilization, while optimizing power consumption and resource use.

Weather conditions can affect microwave propagation. High-frequency bands are impacted mainly by precipitation, while low-frequency bands are subject to multipath fading. Additionally, the stations to be connected require line-of-sight (LOS) configuration. Nevertheless, proper design of the microwave solution, i.e., selection of the suitable configuration and proper microwave link design, can ensure that the network meets even the most stringent requirements in terms of throughput, availability, latency and protection.

Nokia Wavence microwave radios can be interconnected directly to Nokia AirScale base stations – a simplified microwave radio (SMR) solution – or directly with the Nokia 7250/7705 (service aggregation router (SAR), exploiting the zero indoor footprint and optimizing energy consumption and total cost of ownership (TCO), while also improving the mean time between failures (MTBF).

On the IP/MPLS side, high-availability features must be implemented to ensure no service impact, even during control card switchover. Rapid recovery mechanisms with fast re-route and fault detection features must be supported to provide highest network and applications availability.

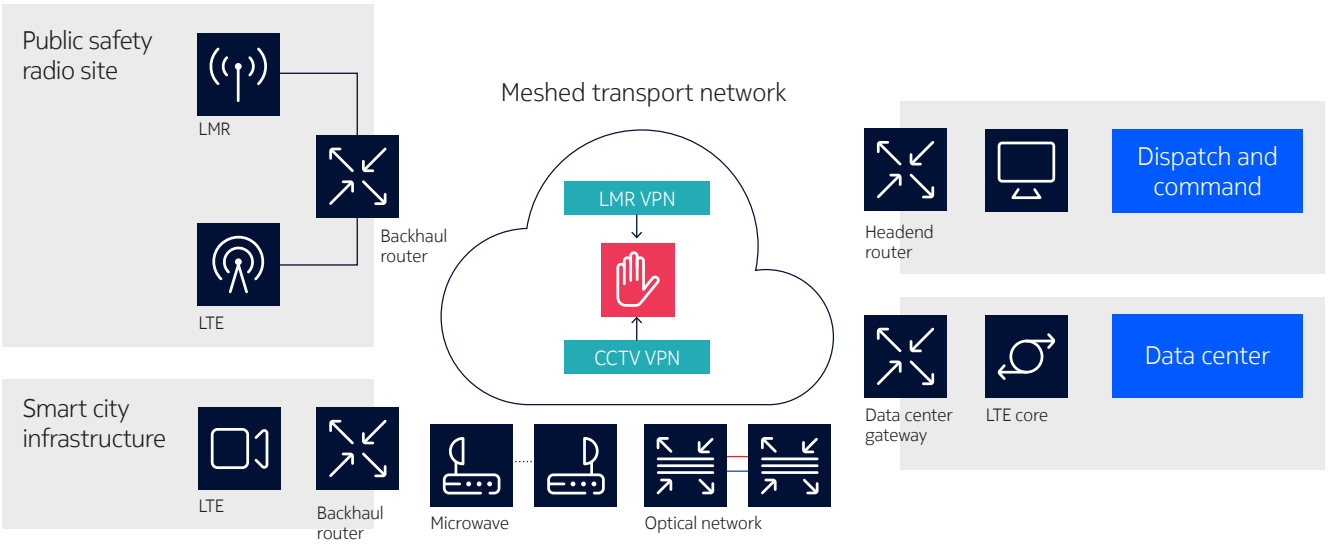
As previously noted, using deployable systems is a way to enhance public safety network resilience. Typically, to establish the transport link, the cell-on-wheels, which hosts the small-cell for coverage and the edge cloud, can also host a compact microwave radio, such as the ultra-small form factor E-Band radio in the Nokia Wavence microwave portfolio: the UBT-mU (ultra broadband transceiver - millimeter wave urban), which is designed for the urban environment. It is the most compact and light E-Band radio in the market, and also embeds a 38 dBi Class 3 antenna.

Zero-trust network security with segmentation and encryption

An IP/MPLS transport network offers a service-centric paradigm using IP/MPLS virtual private networks (VPNs), where multiple applications are segmented into many different, totally segregated virtual domains. With this paradigm, the transport network is a multiservice network, with each service dedicated to one application.

For example, an LMR VPN provides service to connect all LMR base stations, the LMR core and the dispatch center. Because a VPN is a segregated in a virtual network segment, subsystems in other VPN services are not able to communicate with the LMR system. Even when an attacker can successfully compromise a device outside the LMR VPN, communications with the LMR systems will be blocked (see Figure 5).

Figure 5. Network segmentation with VPN stopping unauthorized traffic



Each VPN can have its own security policy to further limit communications to necessary flows. For example, a security policy can restrict user datagram protocol (UDP) flows down to a specified range of port numbers, protecting vulnerable open ports in attached devices and permitting only legitimate traffic. This fine-grained security capability is commonly known as micro-segmentation and is a foundation for a zero-trust network architecture.

In addition, an IP/MPLS VPN can harness the MPLS-based encryption capability offered by network group encryption (NGE) to secure data traffic. NGE natively encrypts MPLS traffic with AES-256 based on VPN-specific security policies. For example, the LMR VPN can have a policy with more frequent re-keying to attain a higher level of security.

Finally, at the foundation of the entire transport network is layer 1 transport, constructed with optical and microwave equipment to provide connectivity among routers through either optical fiber or free space. These links should be encrypted to further safeguard against theft or intrusion of sensitive data. Strong ciphers such as AES-256 and a robust, high-quality key generation and distribution architecture can ensure additional safety against sophisticated quantum computer attacks.

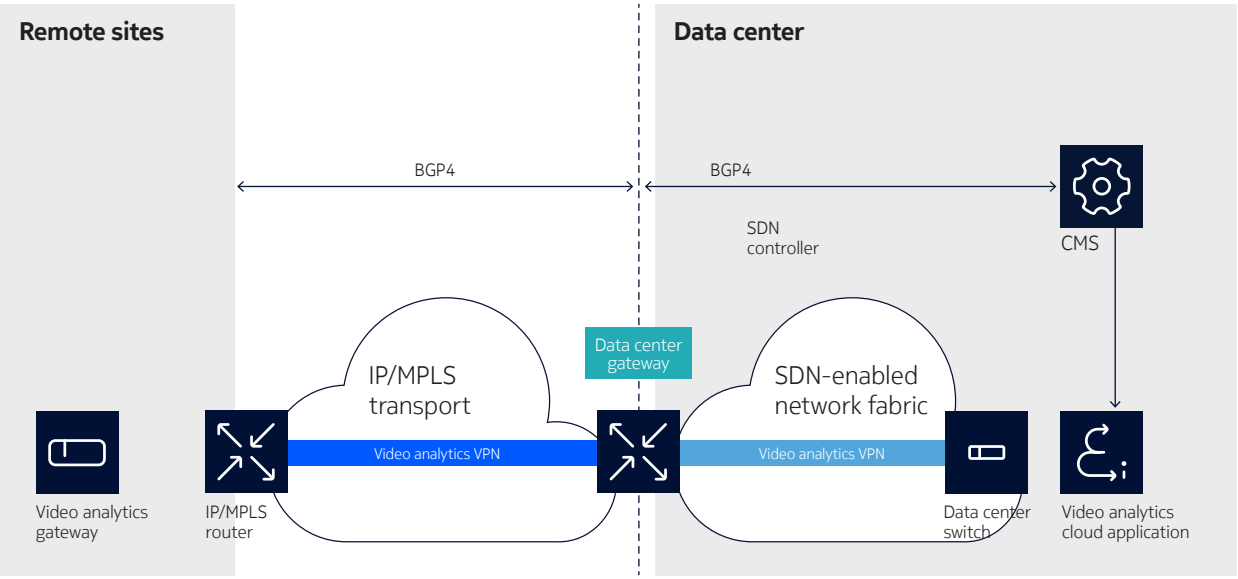
Network-cloud internetworking

As applications adopt the cloud computing-paradigm and become cloud-native, they can migrate from one compute resource to another across multiple data centers orchestrated by the cloud management system (CMS). Consequently, the data center network fabric needs fabric automation and cloud integration to adapt to compute resource migration, creation and deletion. This ensures that fabric service configurations are synchronized with the applications.

Additionally, applications also connect to field devices that collect and pre-process data. Therefore, it is also important to connect workloads and field devices through the two network domains: the transport network and the data center fabric for network-cloud internetworking.

A data center gateway that straddles the transport network and the fabric is key to attain network-cloud interworking. The gateway is an IP/MPLS router with fabric internetworking functionality. For example, the gateway seamlessly stitches together the video analytics VPN in the backhaul domain with the corresponding VPN in the fabric in order to link the video analytics gateway to the video cloud server application. In addition, when the cloud server application moves, the gateway can update the backhaul network immediately using the BGP4 routing protocol (see Figure 6).

Figure 6. Data center gateway providing dynamic, seamless, end-to-end connection

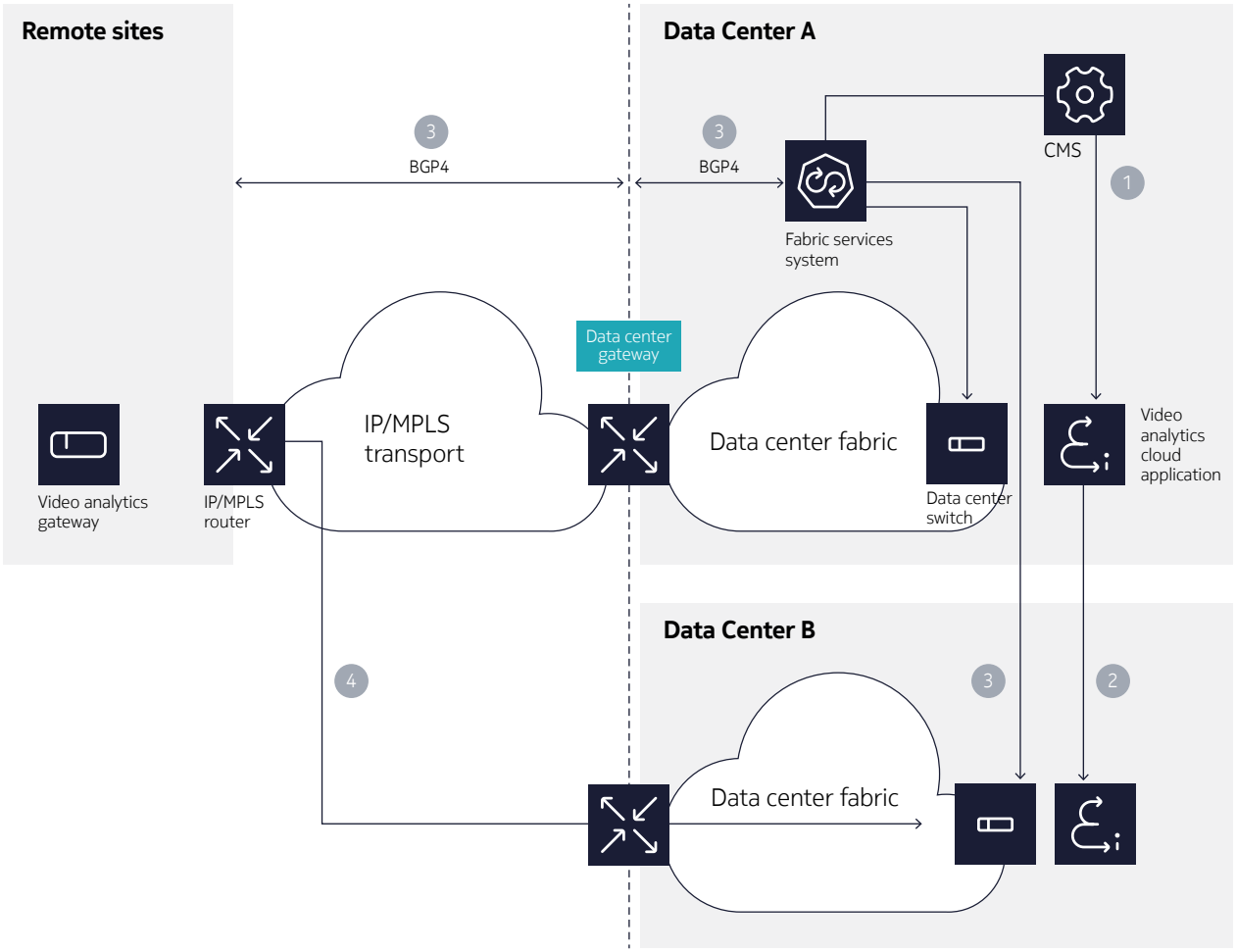


When a compute resource migrates (for example, Figure 7 shows a compute resource hosting a video analytics cloud application migrating from Data Center A to Data Center B), it is crucial that the backhaul network can learn about the migration in an automated way and be able to adapt to the changes so that the traffic is transmitted to Data Center B.

In this example:

1. The CMS orchestrates the migration of the compute resource hosting the server application from Data Center A to Data Center B.
2. The compute resource migrates.
3. Fabric learns about the event, auto-adapts to the change and notifies the backhaul network using BGP-4.
4. The backhaul network updates the VPN forwarding table. The video gateway traffic is now sent to Data Center B.

Figure 7. Data center gateway enabling adaptive, end-to-end connections across two domains



Connectivity between data centers is usually founded on dedicated layer 1 optical transport, commonly called data center interconnect (DCI). This typically uses a dedicated wavelength on a fiber pair as part of the overall transport solution. Specific DCI capacity, protection topology and transmission protocols depend on local requirements, embedded equipment and economic factors.

Support for 5G transport

As a multiservice network, the public safety transport network will readily support 5G transport by provisioning additional VPN services (see Figure 8) – similar to VPNs configured for the LMR services. In addition, the network management platform will allow network automation across the microwave, optical and IP/MPLS segments to support 5G network slicing for the transport network.

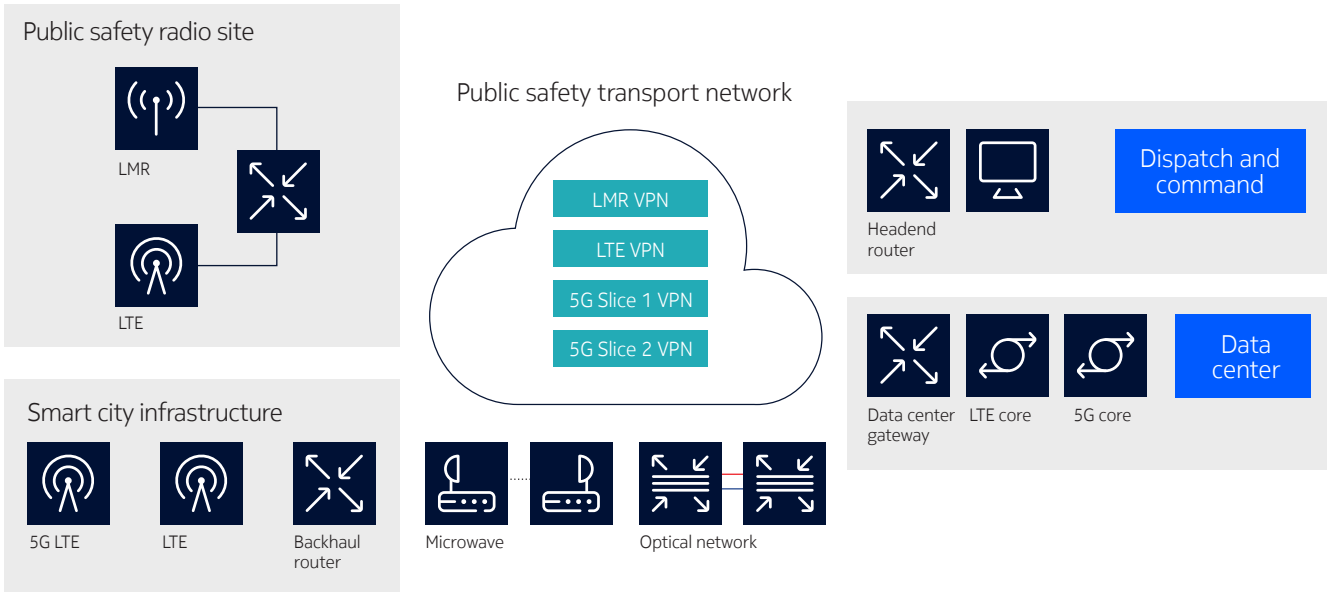
In many countries worldwide the light licensing regime and the relatively small fees of the E-Band spectrum (80 GHz), along with the availability of large channel bandwidth, are such that E-Band is the elected choice for 5G wireless backhaul, providing high throughput up 20 Gbps and latency down to 10 µsec (Wavence portfolio). High-system gain radios allow for stretching the microwave link length. And even in adverse weather conditions (heavy rain), where the sole E-Band might not be enough to grant the SLA compliancy, the carrier aggregation (CA) between E-Band and a lower microwave frequency band still allows carrying

the committed throughput over stretched distance, leveraging the higher robustness of low-frequency bands against the rain effect.

Note that the Wavence portfolio provides 100 percent efficiency in carrier aggregation. Only Wavence can ensure the actual sum of the aggregated traffic pipes without traffic loss.

Extremely high output power equipment is recommended for long distances. The Nokia dual-band radio UBT-T XP (Twin eXtended Power) is the market leader in long-haul full-outdoor transceivers, thanks to its output power of +37 dBm. UBT-T XP allows operators to keep the antenna sizes at a minimum and, in some cases, can even allow for avoiding space diversity, thus reducing TCO and load onto the infrastructure.

Figure 8. Support for 5G transport



Conclusion

Governments of all sizes are looking to modernize their public safety infrastructures by digitizing first responder communications and other public services, thereby driving the operational excellence of their teams. The transport network has a key role to play in such a transformation. This means governments must select the right technologies to ready it for the next decade, which is often the minimal life duration of such systems. An all-packet IP/MPLS optical/microwave transport network is certainly the optimal solution to continue carrying LMR voice traffic while supporting the new data-based services. With this technology government and public safety authorities can leverage their existing assets while modernizing their networks, simplifying their deployment of upgraded LMR, private wireless and IoT based services.

Due to its deterministic QoS capability, the ability to support network segmentation with secure IP/MPLS VPNs, network-cloud interworking and 5G readiness, an all-packet transport network delivers the performance and economics needed to support both public safety communications and future safe and connected city services reliably.

We at Nokia have extensive experience in designing and building such networks, with more than 130 mission-critical transport networks delivered to public safety customers across the world. Only we can provide end-to-end, optimized, mission-critical transport networks, thanks to our market-leading portfolio in microwave, IP/MPLS and optical networking technologies:

- We have delivered more than 750,000 microwave transceivers to more than 700 customers/partners worldwide.
- We are #1 worldwide in IP/MPLS edge routing and are trusted by more than 1,000 critical infrastructure operators.
- In optical networking, we have shipped more than 500,000 100G-equivalent coherent ports to more than 1,000 customers across the globe, including for some of the most critical networks.

For more information on Nokia solutions for public safety, visit our public safety web page.

Abbreviations

3GPP	3rd Generation Partnership Project
5G	fifth generation
API	application programming interface
CCTV	closed circuit television
CMS	cloud management system
eNB	enhanced Node B
FCC	Federal Communications Commission
FirstNet	First Responder Network Authority
GBR	guaranteed bit rate
IP	internet protocol
LMR	land mobile radio
LTE	long-term evolution
MEC	mobile edge computing
MP-BGP4	Multi-protocol Border Gateway Protocol Version 4
MPLS	multiprotocol label switching
PMR	professional mobile radio
QoS	quality of service
SDN	software-defined network
VPN	virtual private network

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: CID212895 (February)