Broadening public safety backhaul for smart cities

Harness your backhaul network to meet smart city goals

White paper

To accomplish their smart city goals, many local governments are upgrading their infrastructure and considering a private LTE network. A cost-effective solution is to leverage the existing public safety backhaul network as a multiservice network to carry smart city data. This paper explains how IP/MPLS can overcome the challenges involved while assuring the communications performance required for first responders.

Contents

Smart city communications infrastructure requirements	3
Challenges for smart city public safety backhaul	3
Assured delivery of LMR traffic	4
Cyber security	4
Interworking with the cloud	5
Readiness for 5G	6
How IP/MPLS can help overcome challenges	6
Deterministic QoS for assured LMR traffic delivery	6
IP/MPLS VPN with encryption for cyber security	7
Network-cloud interworking	8
Support for 5G transport	10
Conclusion	11
Abbreviations	11

Smart city communications infrastructure requirements

Smart cities offer the promise of safe, prosperous and sustainable living for all citizens. Today, local governments strive to deliver highly effective emergency services, provide citizens with better public services, and stimulate economic development. Consequently, many local governments are already upgrading their land mobile radio (LMR) system and harnessing broadband LTE services such as the US FirstNet for more coordinated emergency response. To accomplish their smart city goals, local governments are planning for other connected city infrastructure deployment that encompasses a wide range of systems such as CCTV, smart lighting and an intelligent transportation system.

Fundamental to a smart city infrastructure is a high-performance broadband connectivity platform connecting its associated assets. Because the infrastructure has a large footprint, to reach all assets economically, a private wireless network is the natural choice. Among the various wireless technologies, open standard-based LTE is the preferred radio technology because of its rich ecosystem, robust security and an evolutionary path to 5G.

In the past, a lack of spectrum has hampered local governments' efforts to deploy private LTE networks for smart city infrastructure. However, national radio authorities around the world have now started to make suitable spectrum available.

In the US, the FCC has opened up the 3.5 GHz band (also known as band 48 with 3GPP). In Europe, countries such as France have also made the 2.6 GHz band available for vertical industries. These spectrum initiatives have prompted many infrastructure operators, including local governments, to investigate or plan for a private LTE network.

An essential element of a private LTE network is the backhaul network connecting LTE base stations (eNBs) and the LTE core. However, deploying a backhaul network adds significant cost and effort, causing additional time for the project.

Fortunately, there is an alternate option. Many local governments already have backhaul networks dedicated to public safety communications. If they can use those backhaul networks as multiservice networks to transport the private LTE traffic, this will improve the project economics and expedite smart city application deployment.

However, when using a public safety backhaul network as a multiservice network, it is imperative that public safety application performance is never degraded and the communications are never compromised. The rest of this paper explores how IP/MPLS can broaden public safety backhaul networks to meet these important requirements.

Challenges for smart city public safety backhaul

To provide the required performance, a public safety backhaul network transporting smart city private LTE traffic must meet the following challenges:

- Assured delivery of LMR traffic
- Cyber security
- Interworking with the cloud
- Readiness for 5G

Assured delivery of LMR traffic

Radio communication is a lifeline for first responders. It needs to be up and running 24 x 7. It is also a real-time application that is sensitive to network delay. When the backhaul network expands to transport the smart city private LTE traffic, there is a diverse set of smart city applications cross the smart city infrastructure that run atop the network and compete for network bandwidth. Examples include intelligent traffic management system, smart lighting and CCTV

In addition, real-time, mission-critical LMR traffic requires strict delay with the highest possible reliability while smart-city 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 constantly communicate with their radios without disruptions.

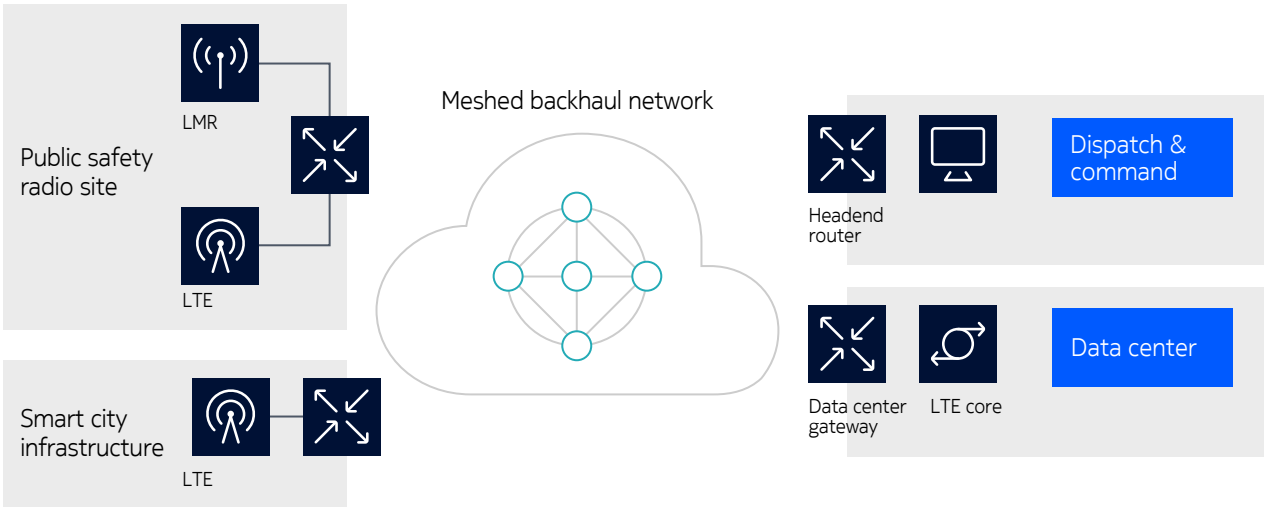
Table 1. Deployed applications have diverse QoS requirements

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

Cyber security

A backhaul network provides meshed connectivity so that any device can reach any other device attached to the network. With more application systems such as the LTE system, the attack surface increases. (see Figure 1).

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



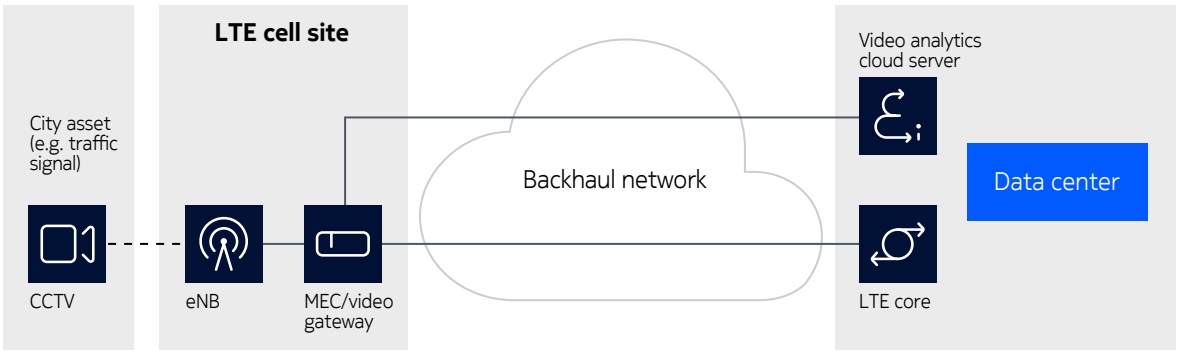
Furthermore, when the use of the backhaul network is further broadened to connect to city offices and public amenities, the attack surface expands further. And because these facilities are easily physically accessed, there is a concern that network vulnerabilities are increased significantly. When attached devices are compromised, attackers can use them as launching pads to move across the backhaul network and penetrate into the LMR and other critical systems to cause serious disruptions.

Interworking with the cloud

Smart city applications such as video analytics[1] are evolving to a distributed, cloud-based architecture so they can scale up to process a large number of high-definition video streams, improve anomaly detection time, and optimize backhaul bandwidth.

This architecture takes advantage of LTE local breakout capability and places the video analytics gateway function on a mobile edge computing (MEC) platform at the edge of the network. The MEC is even colocated with the eNB in some circumstances, with the general operations, administration and maintenance (OAM) functions of the video analytics system remaining in a video analytics 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 from one server to another and from one data center to another for server upgrade, optimization or maintenance.

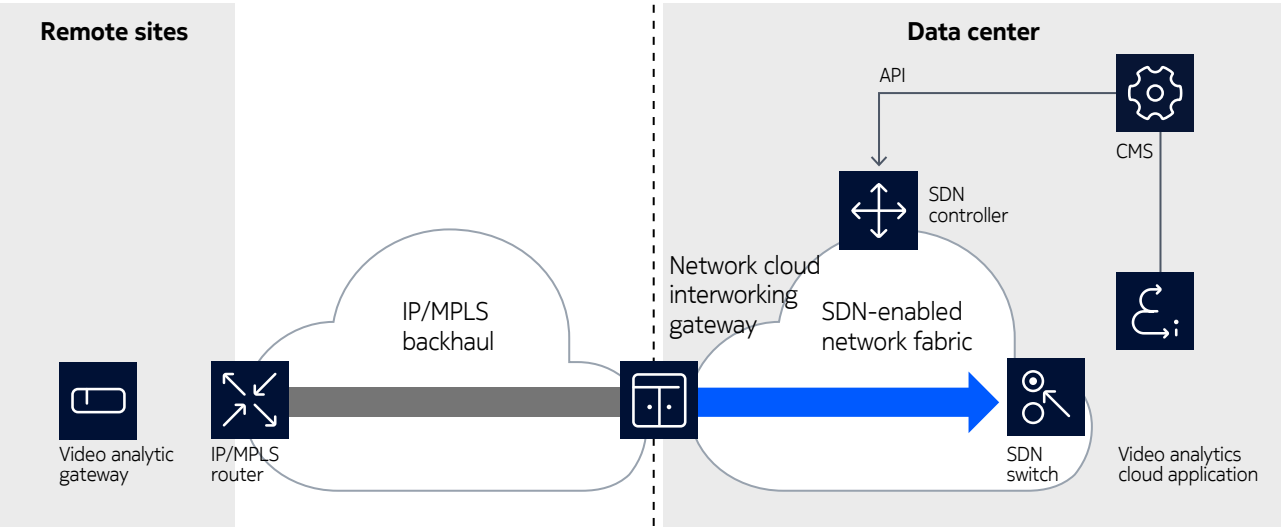
When this happens, the traditional data center network fabric connecting all servers does not learn about these events in an automated way, and the connectivity to the applications is disrupted. Consequently, many data centers have transformed their network fabric with software-defined networking (SDN) so that the network fabric can adapt its connectivity to compute resource events in an automated way.

This automation brings two challenges to the communications between the video gateway in the field and the cloud server application:

- Interworking between the backhaul network and the cloud (referred as network-cloud interworking hereafter): A new network function called a network-cloud interworking gateway is required to seamlessly extend connection from the backhaul network domain across the data center SDN fabric domain to reach the application (see Figure 3).
- Determining how to make the cross-domain connection adaptive when the application migrates to another data center.

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).

Figure 3. Network-cloud interworking



Readiness for 5G

Because LTE is a 3GPP technology, local 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 backhaul network is also ready to provide backhaul for the 5G network.

How IP/MPLS can help overcome challenges

IP/MPLS brings the following capabilities to a public safety backhaul network to help overcome the challenges described:

- Deterministic QoS for assured LMR traffic delivery
- IP/MPLS VPN with encryption for cyber security
- Network-cloud interworking
- Support for 5G transport

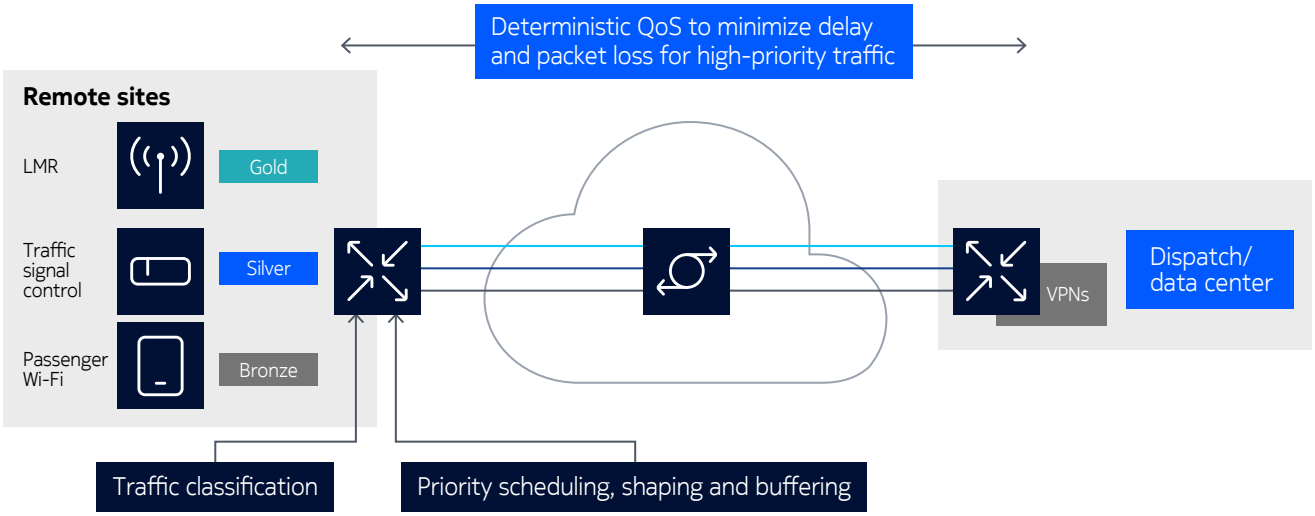
Deterministic QoS for assured LMR traffic delivery

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 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 and flexible QoS capabilities to deliver critical LMR traffic with assurance[2]. A wide range of applications send intensive data with a diverse range of QoS requirements based on a customized QoS policy for each service created for each individual application. IP/MPLS backhaul routers can intelligently classify, buffer, schedule and shape traffic to constantly satisfy the requirements of LMR traffic and of various other applications. This capability of constantly meeting the service requirement is called deterministic QoS (see Figure 4).

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

Figure 4. IP/MPLS backhaul network delivering QoS assurance



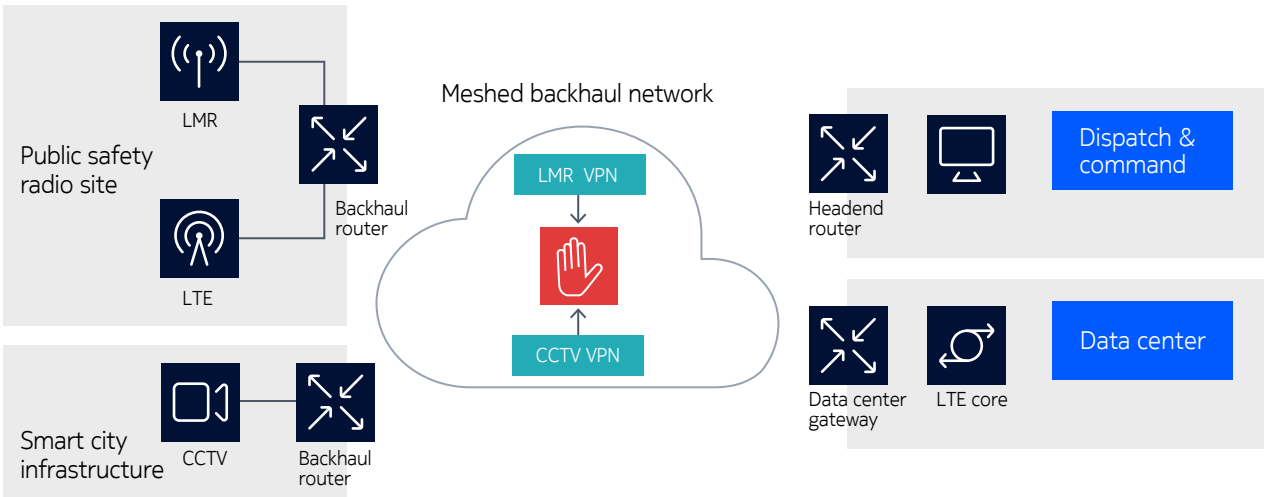
As an example, when the IP/MPLS router is receiving a lot of public Wi-Fi data sent by citizens, as soon as the LMR radio sends critical voice or data traffic, the router recognizes the LMR traffic and strictly prioritizes it over other data traffic, minimizing delay and jitter and avoiding packet discard when link congestion occurs. This is essential to ensure high LMR communications performance.

IP/MPLS VPN with encryption for cyber security

An IP/MPLS backhaul network supports a service-centric paradigm. For different applications, IP/MPLS segments the network into many different, totally segregated virtual domains called virtual private networks (VPNs). With this paradigm, the backhaul network is a multiservice network, with each service supporting one application.

For example, an LMR VPN provides a VPN service to connect all LMR base station, the LMR core and the dispatch center. Because a VPN is a segregated domain, non-LMR subsystems are not able to communicate with any LMR subsystems. Even when an attacker can successfully compromise a device outside the LMR VPN, the efforts to communicate with the LMR subsystems will be stopped (see Figure 5).

Figure 5. Network segmentation with VPN stopping unauthorized traffic



Furthermore, 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 flows with a specified range of port numbers, protecting vulnerable open ports in attached devices. This security capability is commonly known as microsegmentation.

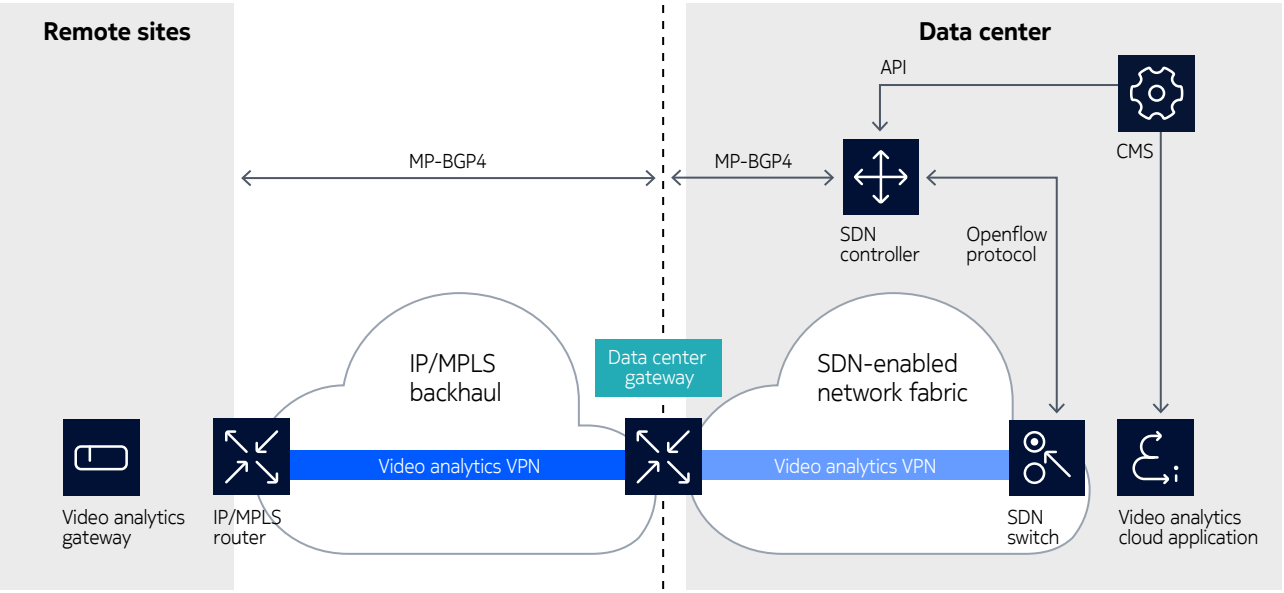
In addition, an IP/MPLS VPN can harness the MPLS-based encryption capability offered by Network Group Encryption (NGE), which natively encrypts MPLS traffic based on VPN-specific security policies. For example, the LMR VPN can have a policy with more frequent re-keying to attain a higher level of security.

Network-cloud interworking

As explained earlier, as data centers embrace cloud technology, applications (called workloads in cloud terminology) can migrate from one compute resource to another compute resource orchestrated by the CMS. Consequently, SDN has been introduced to transform the data center network fabric to adapt to compute resource migration, creation and deletion. With SDN, the network fabric can learn from the CMS about any compute resource events and adapt the connectivity accordingly in an automated way.

A data center gateway that straddles the backhaul network domain and the SDN domain is key to attain network-cloud interworking. The gateway is an IP/MPLS router with SDN interworking functionality. The gateway seamlessly stitches together the video analytics VPN in the backhaul domain and the corresponding VPN in the SDN domain to link the video analytics gateway to the cloud server application. In addition, when the SDN learns about compute resource-related events (migration, creation or deletion) for the cloud server application, SDN can update the backhaul network immediately using the MP-BGP4 routing protocol (see Figure 6).

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

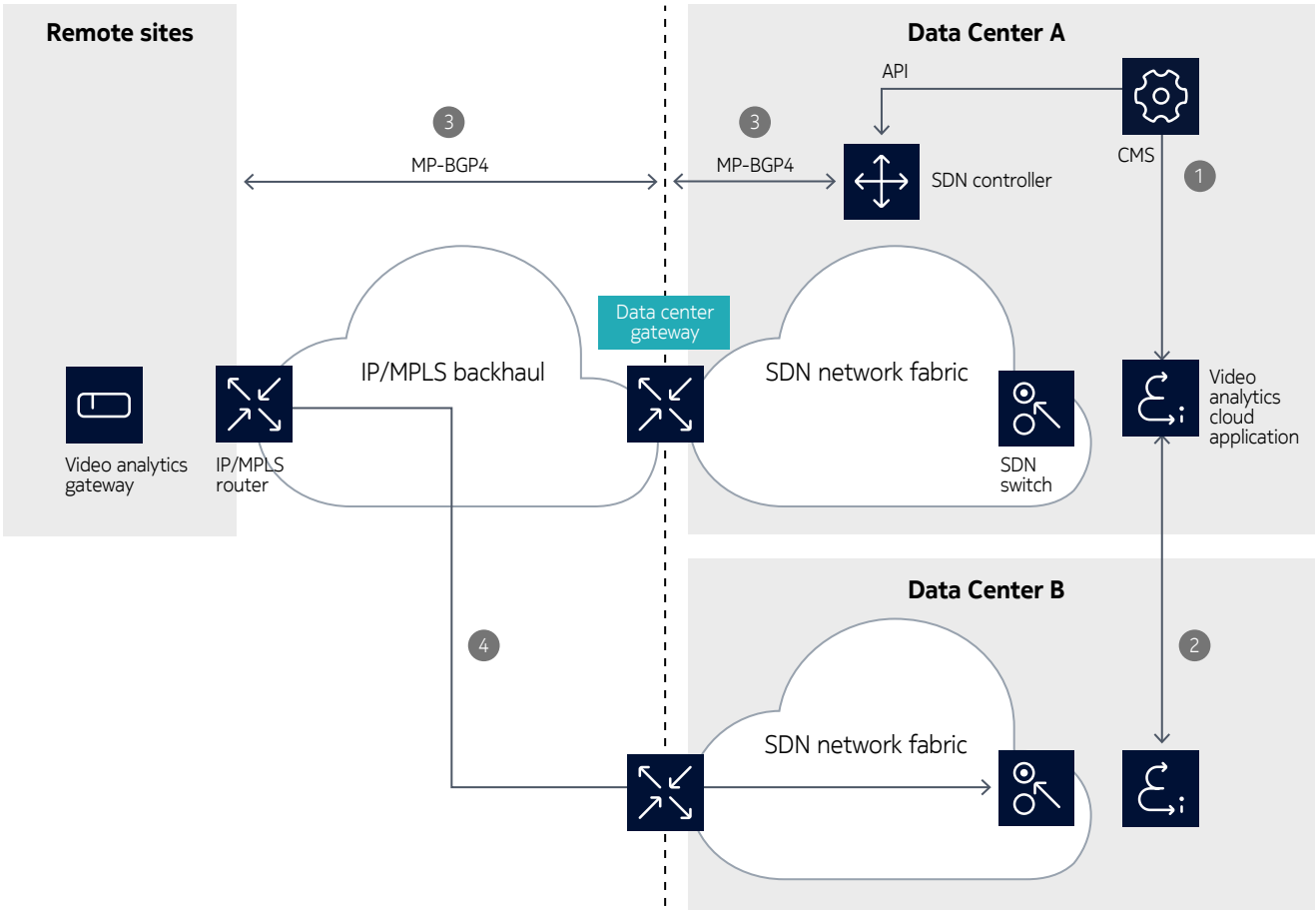


When a compute resource migrates (for example, Figure 7 shows a compute resource hosting a video analytics cloud application migrating from Data Center A to Data Center B), it is crucial that the backhaul network can learn about the migration in an automated way and be able to adapt to the changes so that the traffic from the video in Figure 7 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. SDN learns about the event and notifies the backhaul network using MP-BGP4.
4. The backhaul network updates the VPN forwarding table; video gateway traffic is now sent to Data Center B.

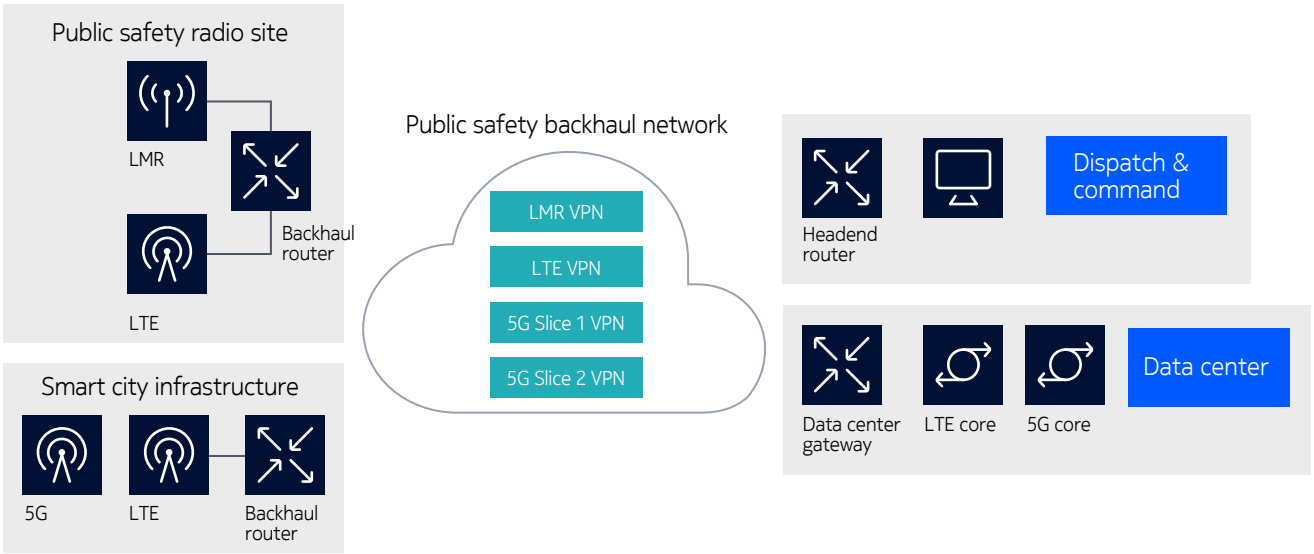
Figure 7. Data center gateway enables adaptive, end-to-end connections across two domains



Support for 5G transport

As a multiservice network, the public safety backhaul network can readily support 5G transport when 5G is introduced by provisioning additional VPN services (see Figure 8).

Figure 8. Support for 5G transport



Conclusion

As more cities are considering a private LTE network as a foundation for their smart city project, those that have already deployed an IP/MPLS backhaul network for their public safety communication infrastructure can leverage this important network asset to simplify and accelerate the deployment of a private wireless network. IP/MPLS is the technology already chosen by most mobile service providers around the world to backhaul their LTE networks. Due to its deterministic QoS capability, ability to support network segmentation with secure IP/MPLS VPNs, and network-cloud interworking as well as its 5G readiness, an IP/MPLS backhaul network delivers the performance and economics needed to support both public safety communications and the future connected smart city services reliably.

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
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: CID207399 (February)