# MISSION-CRITICAL COMMUNICATIONS NETWORKS FOR PUBLIC SAFETY

## PREPARING BACKHAUL NETWORKS FOR LTE AND BEYOND

TECHNOLOGY WHITE PAPER

Reliable communications are essential for public-safety first responders, who must keep connected with each other and the control center as well as acquire situational awareness when responding to emergencies. Requirements for public-safety communications networks are changing with the adoption of long term evolution (LTE) radio technology and new broadband-based multimedia applications. Public safety agencies are replacing their dedicated TDM-based backhaul networks with converged WANs designed for such mission-critical applications.

The Alcatel-Lucent IP/MPLS-based solution for public-safety communications networks offers strong resiliency and QoS, virtualization, synchronization and enhanced security. Public safety agencies can migrate to converged networks that support both new IP-based applications and TDM-based applications such as Land Mobile Radio (LMR) using P25 or TETRA technology. Integrated with packet microwave backhaul and optics with Coarse Wavelength Division Multiplexing (CWDM), converged IP/MPLS optimizes performance, reduces CAPEX/OPEX, and provides the foundation for LTE deployment.

Alcatel·Lucent

# TABLE OF CONTENTS

# EVOLVING FROM TRADITIONAL PUBLIC-SAFETY COMMUNICATIONS NETWORKS

The Detroit, United States police department started to use Land Mobile Radio (LMR), also known as Public/Professional Mobile Radio (PMR), in 1928[1]. Since then, secure and reliable communications networks for backhaul traffic have been critical for the operations of public safety agencies worldwide. Their responsiveness and effectiveness depend on the maintenance of emergency communications as well as access to and sharing of tactical information in the field. With continued security threats and demands for greater efficiency and cross-agency coordination, the modernization of public-safety communications networks has become a top government priority.

A traditional public-safety communications network uses Plesiochronous Digital Hierarchy (PDH) and/or SDH/SONET-based TDM technologies. As technologies evolve, IP-based voice, video and data systems are providing superior performance and richer information compared to traditional approaches for mission-critical applications. Many public-safety communications networks are evolving to IP/Multiprotocol Label Switching (MPLS) for the backhaul of first-responder LMR traffic from Project 25 (P25)-based and Terrestrial Trunked Radio (TETRA)-based systems, video surveillance, and eventually long term evolution (LTE).

The evolved networks enable improved interoperability and economies of scale as well as better integration with IT applications. Because many of these applications are computing-resource intensive and media-rich, they require substantially more bandwidth than current mission-critical voice and sensor traffic. Network operators can effectively address current and future requirements for public-safety IP communications and can control costs by deploying a converged IP/MPLS-based network.

## Alcatel-Lucent IP/MPLS-based backhaul solution

Alcatel-Lucent offers a state-of-the-art, highly reliable and secure IP/MPLS-based backhaul solution with integrated microwave and optical packet transport. The solution provides a flexible, resilient converged infrastructure for the backhaul of mission-critical TDM voice, packet voice and video, as well as surveillance data. This approach extends new mobile broadband capabilities to first responders while transforming traditional backhaul and site-to-site communications to a converged network that enables true interagency interoperability with enhanced safety and efficiency.

IP/MPLS improves the bandwidth efficiency of a public safety network, saves costs, and enables faster access to government databases. The network plays a key role in enhancing the safety of the general public and personnel who deliver these services. The Alcatel-Lucent management platform further improves efficiency by automating and simplifying commissioning and operations management for communication services, thereby reducing barriers to the introduction of IP/MPLS-based technologies and services.

[1] T.A. Peters & L. Bell, Ed., The Handheld Library: Mobile Technology and the Librarian (Santa Barbara: Libraries Unlimited, 2013) P. xi

# PUBLIC-SAFETY COMMUNICATIONS CHALLENGES

The primary purpose of a public safety network is to carry mission-critical field communications traffic. The communications network must provide reliable connectivity between first responders and the control center and among various agencies for seamless collaboration. The network must also be expandable into new areas and easily managed end-to-end. The emergence of innovative, media-rich applications such as live video feed and camera surveillance and the growing need for resiliency, interoperability and enhanced collaboration among agencies are important reasons for transformation.

In TDM-based networks, efficient bandwidth use is limited when handling IP-based multimedia applications, which are bursty and dynamic. Improved communications and interoperability are now possible with the introduction of IP-based communications. Driven by a range of technological trends, together with a growing need to increase network efficiency and bandwidth and centralize high-impact applications, many agencies are modernizing from TDM-based to IP/MPLS-based converged backhaul networks.

## Adopting LTE for public-safety mobile broadband

Today, there are two separate technology families for wireless communications:

- 2G, 3G and 4G LTE for commercial cellular networks that serve consumers and businesses
- Dedicated LMR, including P25 and TETRA, for public safety organizations

With the phenomenal market acceptance of next-generation 4G LTE mobile services, the public has been enjoying enhanced multimedia capabilities, enabled by innovative personal devices and applications that were not available in LMR systems. Recognizing that the timely and efficient sharing of multimedia information enables public safety agencies to more quickly respond and provide critical help, network operators are starting to embrace 4G LTE as the next step in the evolution from their current P25/TETRA-based LMR systems.

### 3GPP LTE standards and spectrum allocation

The 3rd Generation Partnership Project (3GPP™) telecommunications association has developed new cellular radio network technologies, including 3G and 4G LTE. 3GPP Release 12 LTE[2] standardizes enhanced LTE to meet public-safety application requirements, including proximity services that facilitate discovery and communications between nearby users over a radio connection and a group call system that enables one-to-many calling as well as dispatcher communications.

In 2012, the US passed federal legislation reserving the 700 MHz spectrum for public safety communications. The First Responder Network Authority (FirstNet™) was subsequently formed "to provide emergency responders with the first high-speed, nationwide network dedicated to public safety".[3] Various local agencies, together with Alcatel-Lucent, have successfully conducted multiple trials, including a trial in Las Vegas, Nevada.[4]

[2] 3GPP Release 12 LTE. http://www.3gpp.org/specifications/releases/68-release-1

[3] National Telecommunications and Information Administration, FirstNet. http://www.ntia.doc.gov/category/firstnet

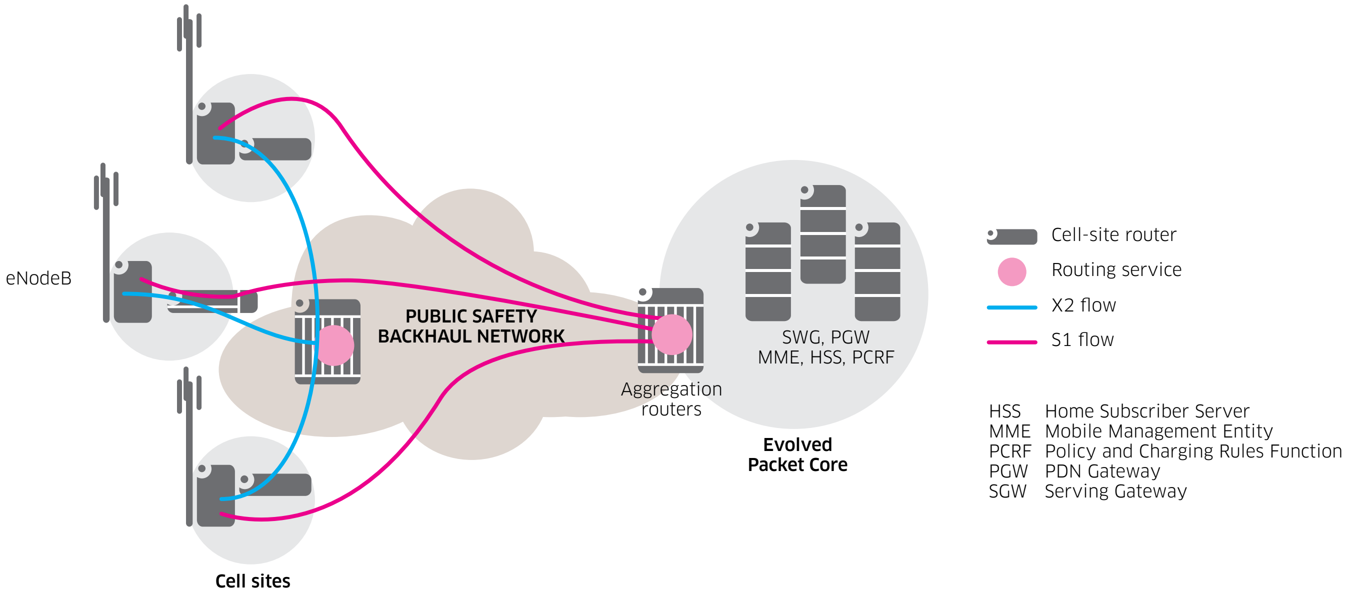
[4] Alcatel-Lucent, Alcatel-Lucent and first responders conduct trial of 4G LTE public safety broadband mobile network. November 25, 2013. http://www.alcatel-lucent.com/press/2013/002955

In 2012, the TETRA and Critical Communications Association (TCCA) and the National Public Safety Telecommunications Council (NPSTC) announced that they had signed a memorandum of agreement “to underscore their joint commitment of the need to develop mission-critical public-safety communications standards for Long Term Evolution (LTE)-based technology”.[5] Today, governments worldwide are in different stages of defining their spectrum allocation strategies.

### 4G LTE network architecture

LTE introduces new challenges for backhaul networks. LTE radio brings spectral efficiency improvements that support higher traffic volumes and compel evolution to an all-IP network. The Evolved Node B (eNode B) X2 interface enables direct connectivity among neighboring eNodeBs with improved latency and handoff performance. To capitalize on the X2 interface, a network needs corresponding multipoint IP connectivity, enabled strategically at the edge. In addition to the typical base station-to-controller traffic (S1 flow), the X2 flow represents a new element in network design and dimensioning. Figure 1 shows the high-level 4G LTE network architecture with S1 and X2 flows.

**Figure 1. LTE network architecture with S1 and X2 flows**



## LMR evolution

Some LMR systems have already evolved to an IP-based solution because of its many benefits. For example, IP-based LMR voice messages can be sent in compressed and encrypted IP packets end-to-end, providing a high level of security while maintaining voice quality. IP-based communications also enable easier connectivity among agencies and jurisdictions. For example, ad hoc connectivity between a city’s emergency center and a national disaster center can be established using interdomain IP routing.

[5] TETRA Today, *TCCA signs LTE agreement.* June 19, 2012. http://www.tetratoday.com/news/tcca-signs-lte-agreement

Additional benefits include integration of the network with commercial IP data applications and interconnection of peripherals, such as scanners and video devices. First responders therefore have faster access to many critical information databases, such as video archives, building plans and GPS coordinates.

However, many legacy LMR systems remain in use, requiring communication between the controller and base stations using a TDM interface such as T1 or E1. Therefore, transport of TDM traffic is still necessary for a few more years, and it is essential to maintain T1/E1 transport services in the new communications network.

### IP video surveillance

Video surveillance is integral to public safety agencies' security measures and is deployed in extended areas wherever possible. A large agency that uses extensive video surveillance may have many video sources that require video traffic to be sent to multiple viewing sites and archives. Because traditional TDM-based networks lack multicast capabilities, they are not well equipped to efficiently support such applications. Successful implementation of an IP-based solution requires a highly reliable mission-critical WAN that can support a broad range of new applications, from broadband data and video to voice without compromising delivery.

The Alcatel-Lucent IP/MPLS network can address requirements for the guaranteed delivery of mission-critical video surveillance traffic and the concurrent support of other critical data and voice traffic in a single converged network. The network can handle current video traffic levels and future growth, including significant bandwidth increases.

## PREPARING BACKHAUL NETWORKS FOR LTE

To prepare for the evolution to LTE, public safety agencies need a backhaul network architecture that is designed with:

- Scalable network size and capacity
- Versatile transmission media and topologies
- Multiservice backhaul for infrastructure sharing
- Advanced traffic management and Quality of Service (QoS)
- Strong network resiliency
- Fortified security protection
- Precise synchronization distribution
- Efficient end-to-end network management and LTE synergy

### Scalable network size and capacity

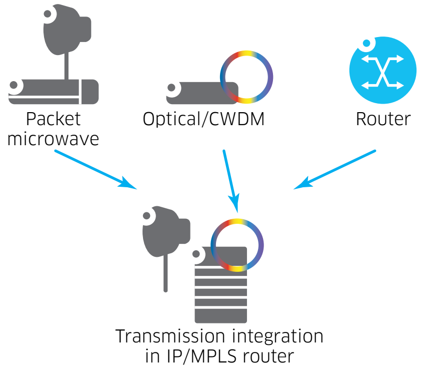
To meet public safety agencies' growing requirements for service coverage, more cell sites are being commissioned. The network must be able to scale to hundreds or even thousands of nodes for all sites. Sites may have different capacity requirements depending on their locations in the network, including in an outdoor environment. The network must therefore be built with nodes of the appropriate capacity and dimensions, including weather-hardened chassis with suitable network interfaces for outdoor deployment. In addition, to reduce OPEX and training requirements, all nodes should be based on the same operating system and managed by a unified network manager and command line interface.

## Versatile transmission media and topologies

Because network coverage may span dense urban areas to remote terrain, operators must be resourceful in using the means of transmission, such as fiber, microwave, copper and even third-party leased lines if necessary. An IP/MPLS router platform must therefore support transmission integration. Integration can consolidate different underlying transmission layers, simplify network design and operations, and ensure consistent commissioning and operations procedures for all network sites regardless of the medium.

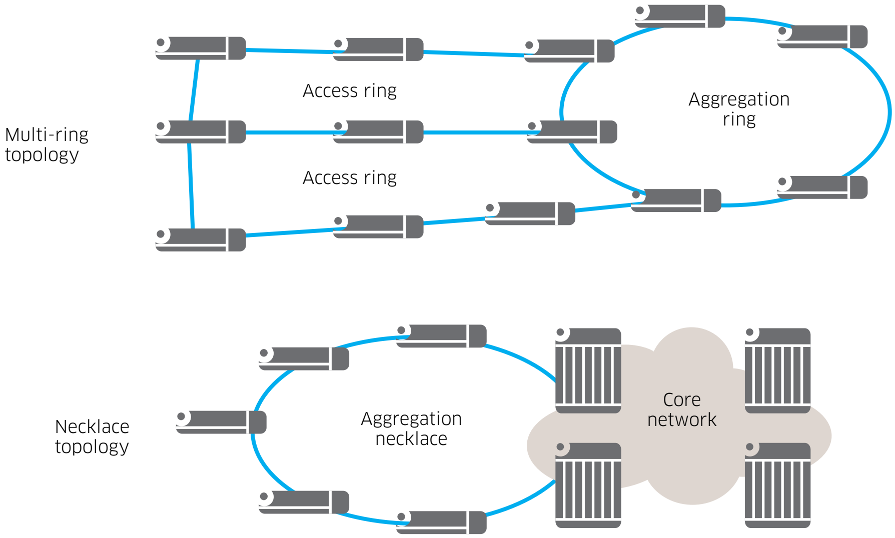
The most common transmission media are packet microwave and optical with Coarse Wavelength Division Multiplexing (CWDM) (see Figure 2). Microwave media, with less bandwidth than fiber, is also widely deployed, particularly outside urban areas. Microwave radio that can perform MPLS-aware header compression can further improve bandwidth utilization efficiency.

Figure 2. Transmission integration in an IP/MPLS router



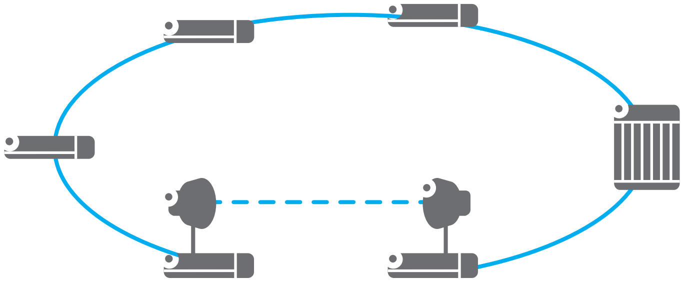
The network should also support advanced topologies — such as multi-ring (also known as ladder), necklace and hybrid — to improve network robustness (see Figure 3 and Figure 4).

Figure 3. Networks with multi-ring and necklace topologies



Operators should also be able to mix and match transmission media when building a network. For example, in Figure 4, a microwave link is deployed to complete a fiber ring for enhanced network resiliency.

**Figure 4. Hybrid ring topology**



## Multiservice backhaul for infrastructure sharing

Support of infrastructure sharing is a fundamental requirement for new public-safety networks. To maximize efficiency, the infrastructure can be used to serve local governments and utilities, including power, water, oil and gas. These public-private partnerships can yield tremendous savings for all parties.

For infrastructure sharing, the backhaul network must support new IP/Ethernet-based applications with a flexible range of point-to-point and multipoint Layer 2/Layer 3 virtual private network (VPN) services and TDM-based applications. All services converge at the network access, where the required packet handling, such as encapsulation, QoS treatment and data-plane forwarding decisions, is performed. Applications from different agencies are simultaneously transported through dedicated VPNs over the common network tunnels without service degradation.

## Traffic management and QoS

The network ingress node must incorporate extensive traffic management tools, with advanced rate scheduling and prioritization mechanisms to enable service bandwidth segregation and hierarchies. While optimizing uplink utilization, these hierarchies provide maximum isolation and fairness across applications traffic in order of priority. With multiple levels and instances of hardware-based shaping, queuing and priority scheduling, the network can manage traffic flows to ensure that application performance parameters, such as bandwidth, delay and jitter, are met.

To virtualize the infrastructure without compromising users, a strong QoS mechanism with advanced traffic management capabilities is essential. For LTE traffic backhaul, a QoS Class Identifier (QCI) is associated with each bearer (IP flow) between the user's mobile device and the Evolved Packet Core (EPC). The QCI information is mapped to the packets sent from the eNodeB to the EPC. The required resources for the defined service-class characteristics can then be made available in the Radio Access Network (RAN). The RAN must classify traffic based on a rich set of attributes from Layer 1 to Layer 4 and ensure the transmission of higher-priority traffic.

## Strong network resiliency

Strong resiliency is essential for a public-safety communications network, which carries mission-critical voice, video and data information. The network should have high reliability levels for uninterrupted operations. MPLS Fast Reroute (FRR) enables the network to consistently reroute connections around a failure at SDH/SONET speeds, regardless of the underlying network topology and size.[6] Because the network is service aware, FRR can distinguish and prioritize traffic redirection depending on the MPLS tunnel. To protect the network against node or interconnection failures, end-to-end standby MPLS paths can also be provisioned.

The network should also have the high availability features of Non-Stop Routing (NSR) and Non-Stop Services (NSS). The benefits of NSR and NSS are unparalleled availability and reliability, which are essential for aggregation sites. NSR ensures that a control card failure has no service impact. MPLS signaling adjacencies and sessions, as well as the Label Information Base, remain intact if there is a switchover. NSR also ensures that VPN services are not affected in a control-fabric module switchover.

Other resiliency features, such as pseudowire redundancy,[7] multichassis Link Aggregation Group (LAG), multichassis automatic protection switching (APS), and synchronization redundancy can also be deployed to further enhance network resiliency.

A key element for rapid restoration is the router's early detection of a link failure, particularly for a microwave link. However, a router with integrated microwave radio can effectively detect such failures at SDH/SONET speeds.

## Fortified security protection

Cybersecurity is paramount for public safety agencies to safeguard their critical infrastructures. The network should have extensive integrated security features to defend against cybersecurity threats, ensure communications and data privacy, and help deliver uninterrupted services. Strong mechanisms should protect the management, control and data planes against security threats from outside or inside the agency.

For external threats, Access Control Lists (ACLs), traffic rate control and queuing can be used for all three planes to stop illegitimate senders and denial of service (DoS) attacks. Comprehensive user Authentication, Authorization and Accounting (AAA), strong password security provided by Simple Network Management Protocol version 3 (SNMPv3) confidentiality, integrity features, Secure Shell (SSH) encryption, and exponential backoff are used to stop illicit logins and dictionary attacks. Hash-Based Message Authentication Code - Message Digest 5 (HMAC-MD5) is used to authenticate control plane packets.

IEEE 802.1X-2010[8] can help to prevent unauthorized device connections to ports on network nodes. Network Address Translation (NAT) is used to protect and hide private addressing spaces from external entities, and encryption is used for data confidentiality and authentication. Inherent to IP/MPLS, Label Switched Paths (LSPs) behave as Virtual Leased Lines (VLLs), effectively stopping remote attackers from injecting traffic in the middle of a tunnel.

In some cases, a threat can originate from a disgruntled internal employee. Detailed event logging and features such as user profiles that limit employees' scope of network access mitigate such risks.

[6] International Engineering Task Force, RFC 4090: *Fast Reroute Extensions to RSVP-TE for LSP Tunnels.* May 2005. **http://www.ietf.org/rfc/rfc4090.txt**

[7] International Engineering Task Force, RFC 6718: *Pseudowire Redundancy.* August 2012. **http://tools.ietf.org/html/rfc6718**

[8] Institute of Electrical and Electronics Engineers, IEEE 802.X-2010: *IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control.* **http://standards.ieee.org/findstds/standard/802.1X-2010.html**

## Precise synchronization distribution

Precise frequency and time-of-day/phase synchronization is critical for maintaining operations and applications integrity in communications networks. In most TDM networks, synchronization is distributed within the network using SDH/SONET mechanisms built into the physical layer to distribute a reference clock, such as one obtained from a global positioning system (GPS). To deliver TDM services over the new network, the same or better synchronization accuracy must be achieved.

To enable rapid and smooth migration as well as future LTE deployment, public-safety communications networks must support a wide range of synchronization technology options, including:

- External reference timing
- Line timing
- Adaptive clock recovery and differential clock recovery timing
- Synchronous Ethernet
- IEEE 1588v2-2008[9] (also known as IEEE 1588v2) Precision Timing Protocol (PTP) (master, boundary clock, transparent clock and slave)
- Integrated GPS receiver

Synchronization requirements can sometimes be met by installing a local GPS — with an external receiver or an integrated receiver in the network node — at each site. However, because of growing concerns about the vulnerability of GPS to accidental or intentional interference, network-wide time-of-day synchronization distribution with IEEE 1588v2 as a backup source is becoming crucial.

The high-performance Alcatel-Lucent IP/MPLS-based backhaul solution capitalizes on a combination of built-in architectural features, including port-based timestamping of IEEE 1588v2 packets, efficiently tuned Alcatel-Lucent Bell Labs-based algorithms, advanced QoS mechanisms, and a powerful synchronization manager. With proper network engineering, the Alcatel-Lucent IEEE 1588v2 solution enables network operators to provide synchronization with the required accuracy and protection.

## End-to-end network management and LTE synergy

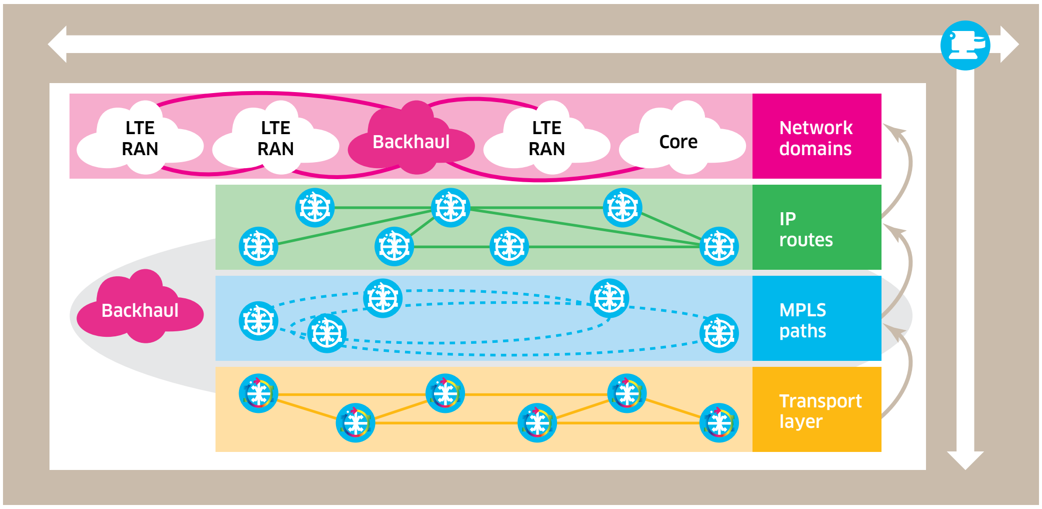
Unified end-to-end management by a network manager and a command-line interface (CLI) across all platforms can minimize operations complexity and staff technical training. A consistent platform architecture base and capabilities can optimize network design and performance.

Simplified management tools can provide easy network configuration and control, effective problem isolation and resolution, and support for new management applications. Operations, administration and maintenance (OAM) tools simplify the deployment and day-to-day operations of a public-safety communications network. For example, service, interface and tunnel tests enable rapid troubleshooting and proactive awareness of the state of traffic flows to help minimize service down time. Periodic OAM tests enable the continuous monitoring of network delay and jitter conditions to facilitate preventive maintenance.

[9] Institute of Electrical and Electronics Engineers, IEEE 1588-2008: IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. http://standards.ieee.org/findstds/standard/1588-2008.html

A service-aware network manager can maximize management synergy by extending coverage to the microwave and optical transport domains and the LTE network domains, as shown in Figure 5.

**Figure 5. Multidomain service aware manager for end-to-end public-safety LTE networks**



## ALCATEL-LUCENT IP/MPLS NETWORK SOLUTION

Many public safety agencies have deployed or are deploying IP-based core networks to support all their backhaul and WAN communications needs. However, not all IP-based solutions are suitable for public safety. An IP/MPLS-based communications network is the only viable option to simultaneously support all levels of mission-critical and non-mission-critical traffic for agencies that share the same network infrastructure. Non-MPLS-based IP networks have been recently deployed, but they often lack the necessary service capabilities to support traffic that requires QoS levels for mission-critical operations or the VPN functionality to flexibly partition network resources. Instead of using an end-to-end service-aware network manager for reduced training costs and OPEX, non-MPLS-based IP networks are often managed by CLI and element management systems.

With the Alcatel-Lucent IP/MPLS network solution, public safety agencies gain an IP network that has the robustness and predictability of a circuit-based network along with high capacity and support for future applications. The Alcatel-Lucent IP/MPLS network solution enables the deployment of new IP/Ethernet applications as well as support for TDM-based applications so that the agency can improve services for its users. The secure backhaul network offers a range of features:

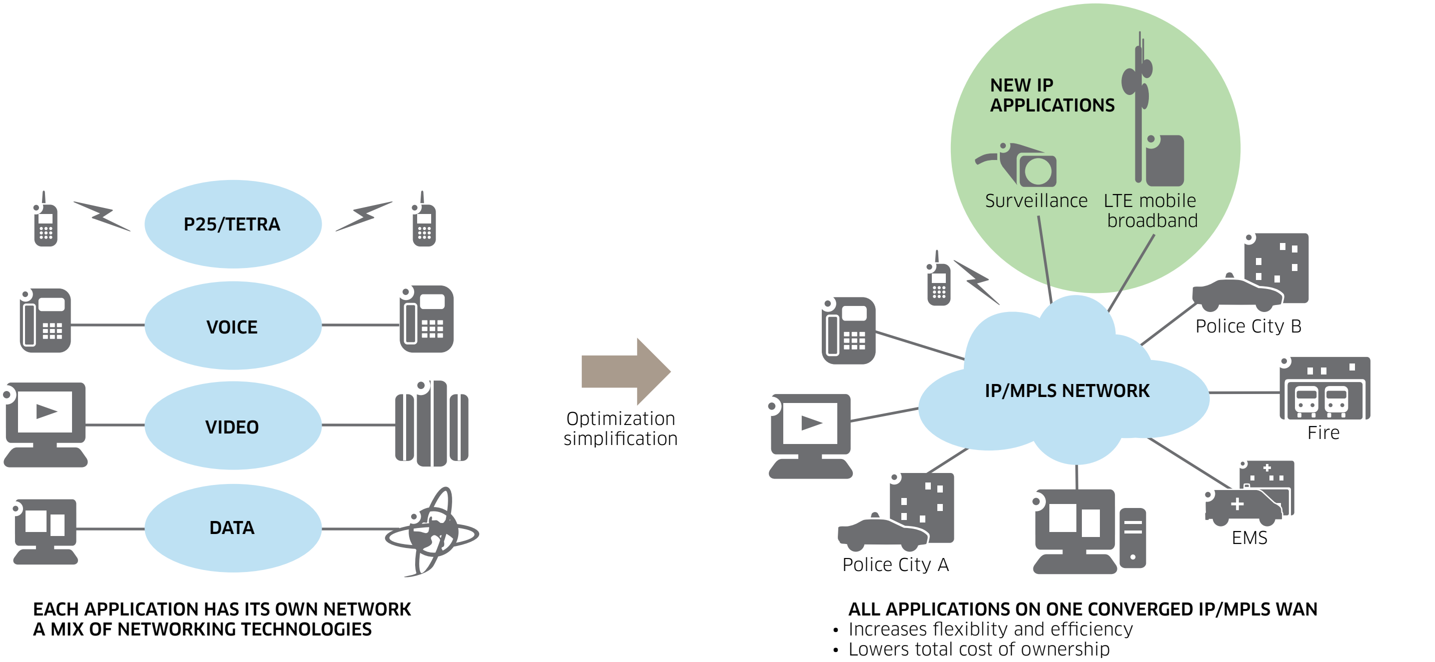
- Scalable MPLS-based VPN services that enable infrastructure sharing
- Flexible network topology options, including multi-ring, necklace and hybrid
- Highly predictable and reliable SDH/SONET-speed recovery with pseudowire redundancy, multichassis LAG and FRR capabilities
- Configurable and flexible hierarchical QoS options for stringent real-time to best-effort requirements
- Optimization of bandwidth usage with MPLS-aware microwave compression
- Advanced traffic engineering for flexible traffic load sharing
- Bell Labs-based IEEE 1588v2 synchronization

- Advanced network and service management to simplify operations, troubleshooting and maintenance
- Readiness for immediate or future LTE deployments

Each network application has unique requirements for bandwidth, QoS and availability. The Alcatel-Lucent IP/MPLS network solution enables public safety agencies to set service parameters for each service and traffic type — for example, multiple types of voice, video and data traffic — according to operations requirements. The network is also capable of supporting low jitter and delay to handle all traffic types effectively and reliably in real time. The Alcatel-Lucent IP/MPLS network solution includes advanced capabilities such as FRR, NSR and NSR to maintain high network resiliency.

Figure 6 shows a converged IP/MPLS network. Using this model, a public safety agency no longer needs to deploy separate dedicated networks for individual applications. Instead, the agency can cost-effectively support all applications on a single physical infrastructure with network virtualization, resulting in greater overall network capacity, efficiency, performance and availability.

**Figure 6. Converged IP/MPLS network model**



P25/TETRA
VOICE
VIDEO
DATA
EACH APPLICATION HAS ITS OWN NETWORK
A MIX OF NETWORKING TECHNOLOGIES
Optimization simplification
NEW IP APPLICATIONS
Surveillance
LTE mobile broadband
IP/MPLS NETWORK
Police City B
Fire
EMS
Police City A
ALL APPLICATIONS ON ONE CONVERGED IP/MPLS WAN
• Increases flexiblity and efficiency
• Lowers total cost of ownership

## Infrastructure sharing with VPNs

Using VPNs, the Alcatel-Lucent IP/MPLS network solution enables virtual control-plane isolation and data-plane hardware-based traffic queuing of various applications on a single infrastructure. The VPNs enable the separation of traffic from different applications or agencies that share the network, offering a secure environment and effective bandwidth allocation. Advanced IP/MPLS VPNs — for example, Circuit Emulation Service (CES), Virtual Private LAN Service (VPLS) and IP VPN — are supported to provide applications in an environment that is private and unaffected by other traffic.

## CES

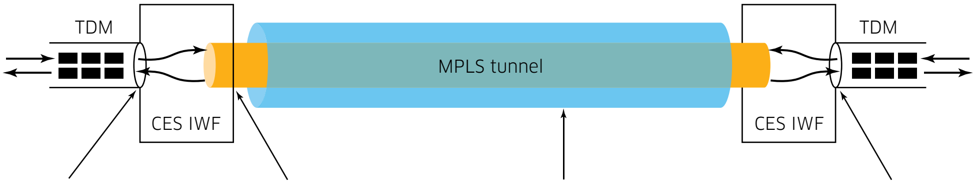
Agencies can use IP/MPLS CES for the gradual migration of legacy TDM applications, preserving the same service quality and predictability as in the TDM network infrastructure.

The Alcatel-Lucent IP/MPLS network solution uses standards-based TDM pseudowires and incorporates the CES InterWorking Function (IWF). The CES IWF ensures the maintenance of all information required by a TDM circuit across the packet network and is transparent to end devices. This approach provides a full transition to a packet network while providing TDM service continuity.

Two main types of circuit emulation can be used: CES over Packet Switched Network (CESoPSN)[10] and Structure-Agnostic TDM over Packet (SAToP).[11] CESoPSN enables NxDS0 service, including full T1/E1 capability. SAToP provides the capability to carry unstructured T1/E1 circuits across the IP/MPLS network.

In an IP/MPLS network, the MPLS tunnel (LSP) is used as the transport layer. A pseudowire is created to identify the specific TDM circuit within the MPLS tunnel (see Figure 7).

**Figure 7. CES functionality**



The CES interworking function (IWF) applies to the proper encapsulation to teh NxDS0 or T1/E1 traffic.

Pseudowires identify the specific CES connection.

MPLS tunnels transport traffic from Point A to Point B.

Flexible configuration to buffers within the CES IWF allows control of packetization, latency and jitter (to meet the requirements for TDM services).

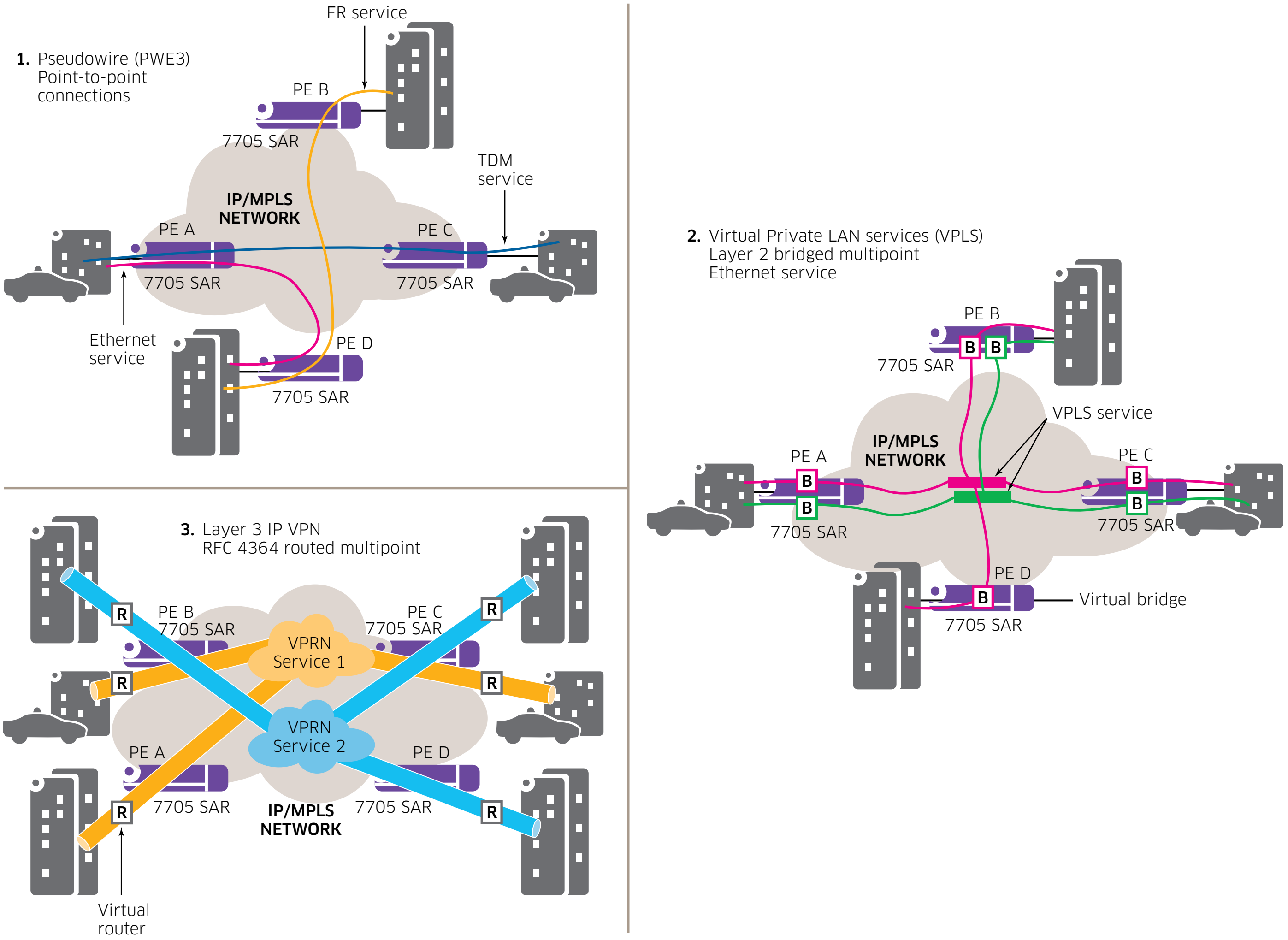
## Pseudowires

A pseudowire, also known as a VLL, encapsulates traffic over LSPs to create a point-to-point connection between two end devices. An MPLS pseudowire is analogous to a private line within the IP/MPLS network. Figure 8-1 shows three types of pseudowires used in IP/MPLS-based VPN services: TDM, Frame Relay and Ethernet. The pseudowire can be used for applications that require dedicated point-to-point connectivity. For example, pseudowires support the transport of legacy voice, data and alarm applications as well as LMR/TETRA traffic backhaul using T1/E1, serial and E&M interfaces. This support enables the migration of SDH/SONET networks to IP without impacting the long life cycle of traditional applications.

[10] International Engineering Task Force, RFC 5086: *Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)*. December 2007. **http://www.ietf.org/rfc/rfc5086.txt**

[11] International Engineering Task Force, RFC 4553: *Structure-Agnostic TDM over Packet (SAToP)*. June 2006. **http://tools.ietf.org/html/rfc4553**

**Figure 8. IP/MPLS-based VPN services**



## VPLS

VPLS is a bridged multipoint service that forwards traffic based on the Media Access Control (MAC) address. A VPLS is protocol-independent and enables multipoint connectivity at Layer 2 within the IP/MPLS network. Figure 8-2 shows two VPLS instances in a network.

VPLS comprises virtual bridges at each node. Each virtual bridge performs MAC learning and constructs a table that maps MAC addresses and corresponding MPLS paths. VPLS is similar to a logical LAN connection: all end devices connected to the VPLS appear as if they are within the same LAN segment.

## IP VPN

An IP VPN is implemented only for IP traffic and is a Layer 3 routed service that forwards traffic based on the IP address.[12] As shown in Figure 8-3, An IP VPN enables multipoint connectivity within the IP/MPLS infrastructure, with each IP/MPLS node supporting Virtual Routing and Forwarding instances.

[12] International Engineering Task Force, RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs). February 2006. http://tools.ietf.org/search/rfc4364

## Service-aware infrastructure

The Alcatel-Lucent IP/MPLS network solution provides a service-oriented approach that focuses on scalability and quality as well as per-service OAM. With a service-aware infrastructure, public safety agencies can tailor services and mission-critical applications with guaranteed bandwidth to meet peak requirements. The Alcatel-Lucent Service Routers provide IP routing and switching so that public safety agencies can support real-time Layer 1, 2 and 3 applications.

## Solution components

The Alcatel-Lucent converged IP/MPLS network leverages multiple state-of-the-art technologies. The network extends IP/MPLS capabilities from the core to access and can include the following main components:

- Alcatel-Lucent 7750 Service Router (SR)[13]
- Alcatel-Lucent 7705 Service Aggregation Router (SAR)[14]
- Alcatel-Lucent 7450 Ethernet Services Switch (ESS)[15]
- Alcatel-Lucent 7210 Service Access Switch (SAS)[16]
- Alcatel-Lucent 9500 Microwave Packet Radio (MPR), providing a packet microwave link to connect MPLS nodes[17]
- Alcatel-Lucent 1830 Photonic Service Switch (PSS), the optical layer underlying the IP/MPLS network[18]
- Alcatel-Lucent 5620 Service Aware Manager (SAM) for service and network management[19]

## Blueprint backhaul network architecture

The Alcatel-Lucent IP/MPLS network solution helps public safety agencies to deploy converged networks for all applications while maintaining QoS. This mission-critical design is ideal for public safety because it is capable of coping with LMR/TETRA voice traffic as well as thousands of other media and data applications.

Figure 9 shows a blueprint of an Alcatel-Lucent converged IP/MPLS communications network with microwave and optical integration for public safety. Packet microwave and optical assets are deployed to optimize connectivity and bandwidth. Pseudowires, VPLS and IP VPNs provide network virtualization for different applications.

[13] Alcatel-Lucent 7705 Service Router. http://www.alcatel-lucent.com/products/7750-service-router

[14] Alcatel-Lucent 7705 Service Aggregation Router. http://www.alcatel-lucent.com/products/7705-service-aggregation-router

[15] Alcatel-Lucent 7450 Ethernet Service Switch. http://www.alcatel-lucent.com/products/7450-ethernet-service-switch

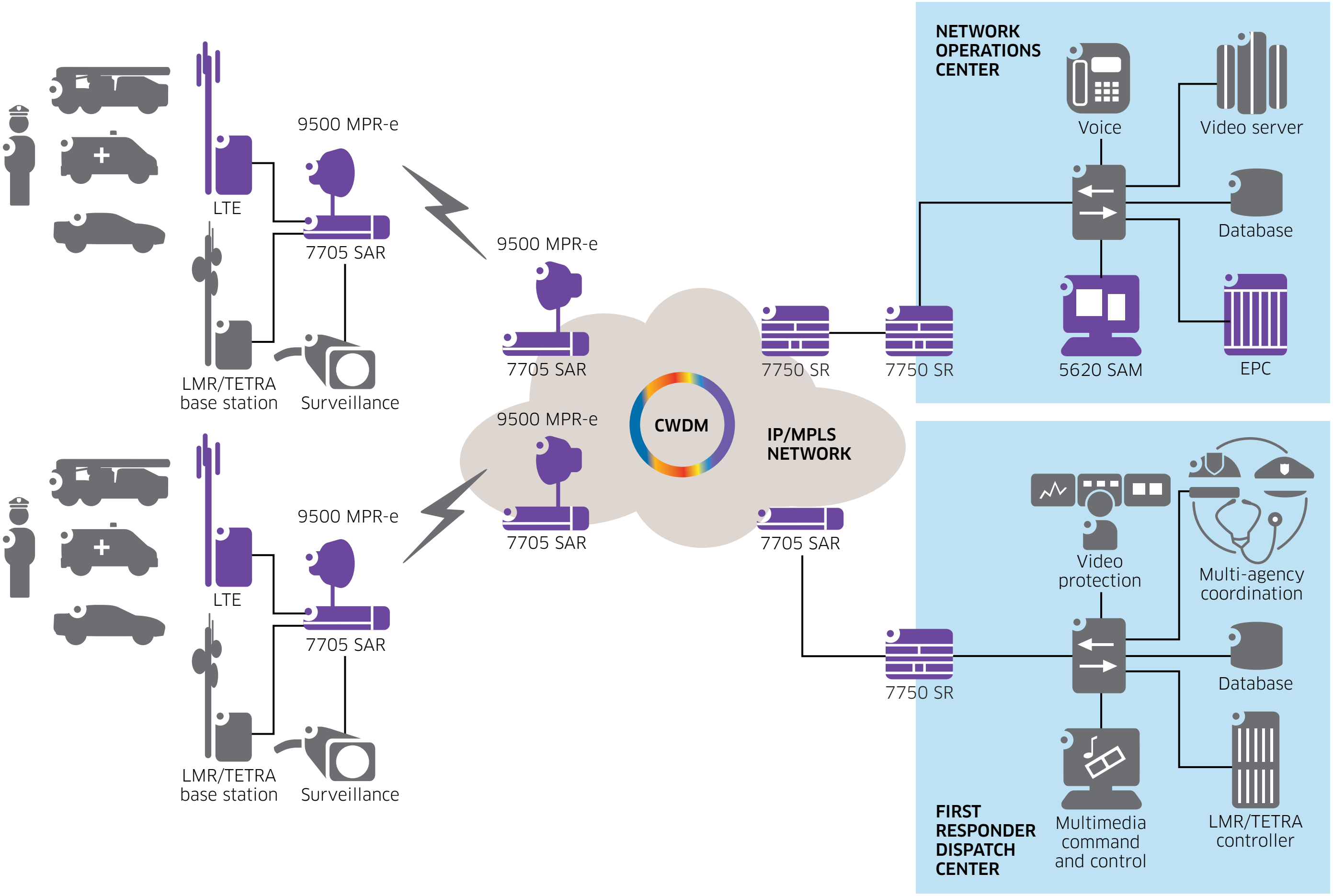
[16] Alcatel-Lucent 7210 Service Access Switch. http://www.alcatel-lucent.com/products/7210-service-access-switch

[17] Alcatel-Lucent 9500 Microwave Packet Radio. http://www.alcatel-lucent.com/products/9500-microwave-packet-radio

[18] Alcatel-Lucent 1830 Photonic Service Switch. http://www.alcatel-lucent.com/products/1830-photonic-service-switch

[19] Alcatel-Lucent 5620 Service Aware Manager.
http://www.alcatel-lucent.com/products/5620-service-aware-manager

Figure 9. Alcatel-Lucent IP/MPLS blueprint network architecture for public safety



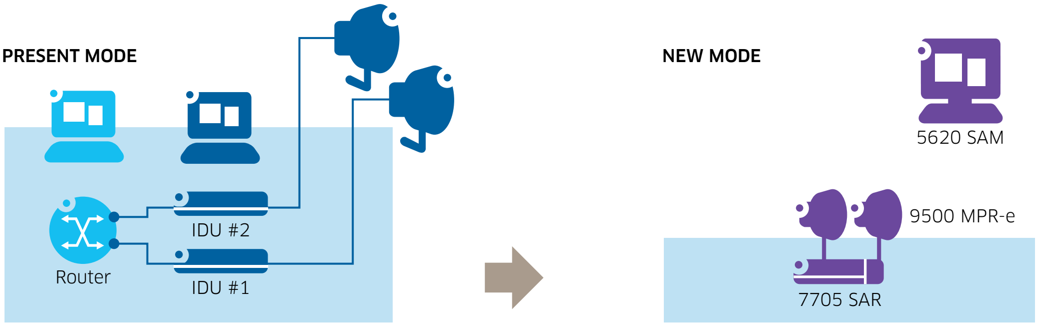
## Integrated IP and microwave domains

In a traditional architecture, IP/MPLS is overlaid over microwave transmission between two platforms. In the Alcatel-Lucent IP/MPLS network solution, the 9500 MPR-e is fully integrated with the 7705 SAR for a single seamless platform that converges the IP and microwave domains. Integration provides many benefits when microwave media are widely deployed:

- Elimination of multiple network managers
- Convergence of multiple indoor units (IDUs) and IP/MPLS router into one platform
- Rapid detection of microwave link degradation, including high bit error rates
- Reduced equipment space, sparing requirements, power consumption and cooling needs
- Streamlined installation and operations management

Figure 10 shows the integrated 7705 SAR and 9500 MPR-e configuration.

**Figure 10. Integrated IP/MPLS and packet microwave transport**



- Two platforms (for IP and microwave domains)
- Two network managers
- Multi-chasses
  - One IDU or each MW direction typically

A daunting task for deployment and operation

Integrating microwave into 7705 SAR makes life easy

- One platform replaces all chassis
- One network manager for both domains

# CONCLUSION

Public safety agencies are migrating their backhaul networks from TDM to IP for the efficient support of mission-critical LMR/TETRA voice and video surveillance and the eventual adoption of LTE mobile broadband. Agencies should ensure that their transformation to converged communications includes an IP/MPLS network because only IP/MPLS can provide the capability and reliability that is mandated by mission-critical services.

The Alcatel-Lucent IP/MPLS network solution can help public safety agencies to extend and enhance their networks to support new IP-based applications while continuing to support TDM. These new technologies enable agencies to optimize their network flexibility and management and reduce CAPEX/OPEX without compromising safety, security or reliability. A service-aware IP/MPLS network enables the support of converged voice, data and video applications that can be managed using configurable QoS levels.

The Alcatel-Lucent IP/MPLS network provides public safety agencies with:

- Reliable mission-critical services with high network availability
- Infrastructure sharing with VPNs
- Deterministic QoS for high-priority real-time applications
- Support for current and future mission-critical services
- Flexible time and frequency synchronization options
- Opportunities for reduced OPEX and CAPEX
- Preparation for eventual LTE adoption
- Strong security protection

Leveraging its unique IP/MPLS and LTE product portfolios, Alcatel-Lucent can partner with public safety agencies worldwide to transform end-to-end mission-critical networks.

# ACRONYMS

| | |
|---|---|
| 1830 PSS | Alcatel-Lucent 1830 Photonic Service Switch |
| 5620 SAM | Alcatel-Lucent 5620 Service Aware Manager |
| 7210 SAS | Alcatel-Lucent 7210 Service Access Switch |
| 7450 ESS | Alcatel-Lucent 7450 Ethernet Service Switch |
| 7705 SAR | Alcatel-Lucent 7705 Service Aggregation Router |
| 7750 SR | Alcatel-Lucent 7750 Service Router |
| 9500 MPR | Alcatel-Lucent 9500 Microwave Packet Radio |
| 3GPP™ | 3rd Generation Partnership Project |
| 2G, 3G, 4G | Second Generation, Third Generation, Fourth Generation |
| AAA | Authentication, Authorization and Accounting |
| ACL | Access Control List |
| APS | automatic protection switching |
| CAPEX | capital expenditures |
| CES | Circuit Emulation Service |
| CESoPSN | Circuit Emulation Service over Packet Switched Network |
| CLI | command-line interface |
| CWDM | Coarse Wavelength Division Multiplexing |
| DoS | denial of service |
| EMS | emergency medical services |
| eNodeB | Evolved Node B |
| EPC | Evolved Packet Core |
| FirstNet™ | First Responder Network Authority |
| FR | Frame Relay |
| FRR | Fast Reroute |
| GPS | Global Positioning System |
| HMAC-MD5 | Hash-Based Message Authentication Code - Message Digest 5 |
| HSS | Home Subscriber Server |
| IDU | indoor unit |
| IP | Internet Protocol |
| IP VPN | IP virtual private network |
| IT | information technology |
| IWF | InterWorking Function |
| LAG | Link Aggregation Group |
| LAN | local area network |
| LMR | Land Mobile Radio |
| LSP | Label Switched Path |
| LTE | long term evolution |

| | |
|---|---|
| MAC | Media Access Control |
| MME | Mobile Management Entity |
| MPLS | Multiprotocol Label Switching |
| NAT | Network Address Translation |
| NPSTC | National Public Safety Telecommunications Council |
| NSR | Non-Stop Routing |
| NSS | Non-Stop Services |
| OAM | operations, administration and maintenance |
| OPEX | operating expenditures |
| P25 | Project 25 |
| PCRF | Policy and Charging Rules Function |
| PDH | Plesiochronous Digital Hierarchy |
| PDN | packet data network |
| PE | provider edge |
| PGW | PDN Gateway |
| PMR | Professional Mobile Radio |
| PTP | Precision Timing Protocol |
| PWE3 | Pseudowire Emulation Edge-to-Edge |
| QoS | Quality of Service |
| RAN | Radio Access Network |
| SAToP | Structure-Agnostic TDM over Packet |
| SDH | Synchronous Digital Hierarchy |
| SGW | Serving Gateway |
| SNMPv3 | Simple Network Management Protocol version 3 |
| SONET | Synchronous Optical Network |
| SSH | Secure Shell |
| TCCA | TETRA and Critical Communications Association |
| TDM | Time Division Multiplexing |
| TETRA | Terrestrial Trunked Radio |
| VLL | Virtual Leased Line |
| VPLS | Virtual Private LAN Service |
| VPN | virtual private network |
| VPRN | Virtual Private Routed Network |
| WAN | wide area network |
| Wi-Fi® | Wireless Fidelity |

# REFERENCES

1. 3GPP Release 12 LTE. **http://www.3gpp.org/specifications/releases/68-release-12**
2. Alcatel-Lucent 1830 Photonic Service Switch. **http://www.alcatel-lucent.com/products/1830-photonic-service-switch**
3. Alcatel-Lucent 5620 Service Aware Manager. **http://www.alcatel-lucent.com/products/5620-service-aware-manager**
4. Alcatel-Lucent 7210 Service Access Switch. **http://www.alcatel-lucent.com/products/7210-service-access-switch**
5. Alcatel-Lucent 7450 Ethernet Service Switch. **http://www.alcatel-lucent.com/products/7450-ethernet-service-switch**
6. Alcatel-Lucent 7705 Service Aggregation Router. **http://www.alcatel-lucent.com/products/7705-service-aggregation-router**
7. Alcatel-Lucent 7750 Service Router. **http://www.alcatel-lucent.com/products/7750-service-router**
8. Alcatel-Lucent 9500 Microwave Packet Radio. **http://www.alcatel-lucent.com/products/9500-microwave-packet-radio**
9. Alcatel-Lucent. Press release: *Alcatel-Lucent and first responders conduct trial of 4G LTE public safety broadband mobile network*. November 25, 2013. **http://www.alcatel-lucent.com/press/2013/002955**
10. Institute of Electrical and Electronics Engineers. IEEE 802.X-2010: *IEEE Standard for Local and metropolitan area networks* - Port-Based Network Access Control. **http://standards.ieee.org/findstds/standard/802.1X-2010.html**
11. Institute of Electrical and Electronics Engineers. IEEE 1588-2008: *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*. **http://standards.ieee.org/findstds/standard/1588-2008.html**
12. International Engineering Task Force. RFC 4090: *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*. May 2005. **http://www.ietf.org/rfc/rfc4090.txt**
13. International Engineering Task Force. RFC 4364: *BGP/MPLS IP Virtual Private Networks (VPNs)*. February 2006. **http://tools.ietf.org/search/rfc4364**
14. International Engineering Task Force. RFC 4553: *Structure-Agnostic TDM over Packet (SAToP)*. June 2006. **http://tools.ietf.org/html/rfc4553**
15. International Engineering Task Force. RFC 5086: *Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)*. December 2007. **http://www.ietf.org/rfc/rfc5086.txt**
16. International Engineering Task Force. RFC 6718: *Pseudowire Redundancy*. August 2012. **http://tools.ietf.org/html/rfc6718**
17. National Telecommunications and Information Administration. FirstNet. **http://www.ntia.doc.gov/category/firstnet**
18. TETRA Today. *TCCA signs LTE agreement*. June 19, 2012. **http://www.tetratoday.com/news/tcca-signs-lte-agreement**

Alcatel·Lucent