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 in real time when responding to emergencies. Requirements for public-safety communications networks are changing with the adoption of new broadband-based multimedia applications, IP-based Land Mobile Radio/Private Mobile Radio (LMR/PMR) and Long Term Evolution (LTE). As a result, public safety agencies are replacing their dedicated TDM-based backhaul networks with converged WANs in preparation for such transitions.

The Alcatel-Lucent IP/MPLS-based solution for public safety communications networks offers strong resiliency and quality of service, network virtualization flexibility, fortified security and precise synchronization. Public safety agencies can migrate to converged networks that support both new IP-based applications and legacy TDM-based applications. 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 eventual LTE deployment.

TABLE OF CONTENTS

EVOLVING FROM TRADITIONAL PUBLIC SAFETY COMMUNICATIONS NETWORKS

The Detroit, United States police department first started to use Land Mobile Radio (LMR), also known as Private/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 applications such as a geographic information system (GIS) and sharing of tactical field information with dispatch or command center. 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 for backhaul. 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 critical applications 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 inter-agency 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, eds., *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 new IP-based multimedia applications, which are bursty, dynamic and bandwidth intensive.[2] 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.

LMR/PMR evolution

Many public safety network operators are upgrading their current LMR systems to support a new generation of LMR standards (P25 phase 2 and TETRA Plus, also known as TETRA Enhanced Data Service or simply TEDS) in order to take advantage of increased channel capacity and improved spectrum efficiency, as well as more efficient voice encoding. These IP-based system upgrades, together with new adoption of IP-based video surveillance, require packet-based backhaul networks to provide communication between radio sites and switching sites. The adoption of IP-based communications also makes establishing connectivity among agencies and jurisdictions easier, facilitating seamless collaborations. For example, ad hoc connectivity between a city's emergency center and a national disaster center can be established using inter-domain IP routing via a national IP backbone network. Furthermore, new IP-based peripherals such as scanners and video devices can now be used. New IP-based applications can also enable first responders to have quick access to critical information databases including video archives, a GIS and all-time protection under an automatic person location system (APLS).

Despite the LMR upgrade to packet, many legacy TDM-based systems (for example, order wire communications and mutual aid communications among agencies at radio sites) will remain in use in the foreseeable future. These established applications still require the use of TDM T1/E1 interfaces, as well as analog voice interfaces such as E&M and FSX/FSO. Therefore the new packet-based backhaul network needs to do the following:

- Support legacy interfaces
- Carry the packetized traffic with the same quality of service (QoS) as before
- Transport frequency synchronization end-to-end for legacy applications via line timing or other synchronization technologies such as IEEE 1588v2

2 A detailed survey of application bandwidth throughput can be found in Table 15 of U.S. National Public Safety Telecommunications Council's final report on public safety communications assessment. A detailed survey of application bandwidth throughput can be found in Table 15 of U.S. National Public Safety Telecommunications Council's final report on public safety communications assessment: **http://www.npstc.org/download.jsp?tableId = 37&column = 217&id = 2446&file = AFST_NPSTC_Report_06232012.pdf**

Adopting LTE for public safety mobile communications

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

- 2G, 3G and 4G LTE (abbreviated as LTE below) 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 LTE mobile services, the public has been enjoying enhanced multimedia capabilities and instant access to a plethora of information on the Internet, enabled by high–bandwidth LTE data services and innovative personal devices and applications that are not available to LMR/PMR users. Recognizing that the real-time sharing of multimedia information and instant access to databases can greatly enable public safety agencies to more quickly respond and provide critical help, major public safety associations have endorsed[3] or are looking to LTE as the successor technology of existing LMR/PMR systems. Consequently, many public safety organizations are now studying how to augment their existing system with LTE.

3GPP LTE standards and spectrum allocation for public safety

While LTE holds immense potential for public safety mobile broadband data communications, it will also have to fulfill requirements of some niche public safety applications, particularly critical voice communications,[4] before it can completely replace current LMR/PMR systems. Key features of critical voice communications include direct communications and group communications.[5]

The 3rd Generation Partnership Project (3GPP) telecommunications association, which has developed cellular radio network technology standards, including 3G and 4G LTE, has taken on the challenge. First, 3GPP Release 11 LTE[6] extends the Use Equipment (UE) power class to include class 1 to improve the uplink for extended coverage performance for the North and South American region (also known as region 2). Subsequently 3GPP Release 12 LTE[7] standardizes enhanced LTE to meet public safety application requirements; it includes the first step of 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. Further on, 3GPP Release 13 LTE will continue to enhance resiliency by allowing isolated operation of E-UTRAN by allowing a standalone evolved Node B (eNB) to operate, as well as further proximity services enhancements and mission-critical push-to-talk (MCPTT).[8]

In 2012, the United States passed federal legislation to allocate a portion of the 700 MHz spectrum, commonly known as LTE band 14, 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”.[9] Various local agencies, together with Alcatel-Lucent, have successfully conducted multiple trials, including a trial in Las Vegas, Nevada.[10]

3 Both the Association of Public-Safety Communications (APCO) and the TETRA and Critical Communications Association (TCCA) have endorsed LTE as standard for emergency communications broadband network **http://apcoalliance.org/4g.html**; **http://www.tetratoday.com/news/tcca-signs-lte-agreement**

4 For a more detailed discussion, please consult the NPSTC report: *Public Safety Communications Assessment 2012 – 2022* **http://www.npstc.org/download.jsp?tableId=37&column=217&id=2413&file=AFST_NPSTC_Report_08102012.pdf**

5 For a more detailed discussion, please consult the NPSTC report: Mission Critical Voice Communications Requirements for Public Safety **http://www.npstc.org/download.jsp?tableId=37&column=217&id=2413&file=AFST_NPSTC_Report_08102012.pdf**

6 3GPP Release 11 LTE. **http://www.3gpp.org/specifications/releases/69-release-11**

7 3GPP Release 12 LTE. **http://www.3gpp.org/specifications/releases/68-release-12**

8 3GPP Release 13 LTE. **http://www.3gpp.org/release-13**

9 National Telecommunications and Information Administration, FirstNet. **http://www.ntia.doc.gov/category/firstnet**

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

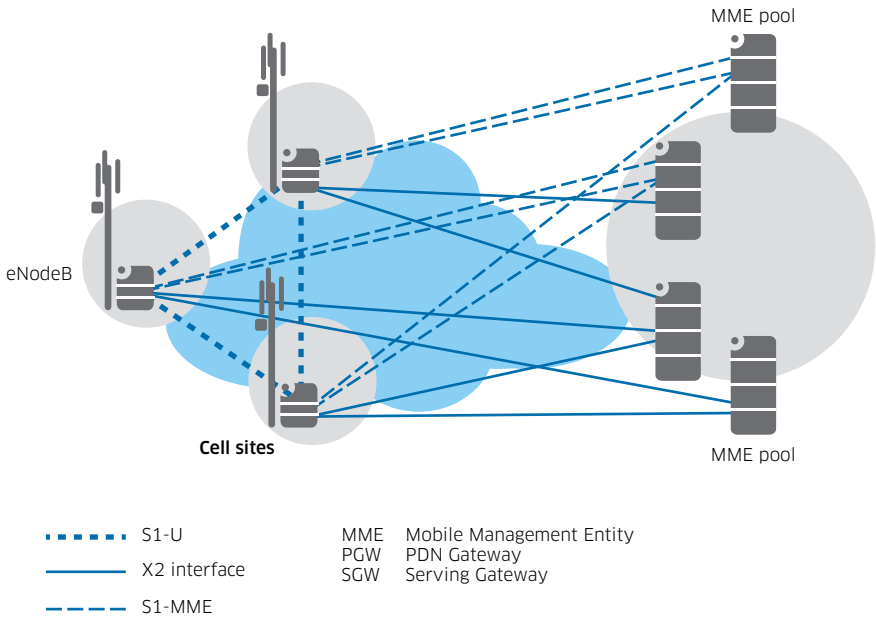
Today, allocation of dedicated spectrum for broadband public safety is being actively discussed in many regions. Some early adopters are either allocating or will allocate soon a portion of available spectrum for this application preparing for imminent deployment of LTE for public safety or other critical business applications. Allocated or targeted spectrum varies country by country but is usually less than 1 GHz.

4G LTE E-UTRAN architecture

LTE, with an evolved UMTS Terrestrial Radio Network (UTRAN), briefly known as E-UTRAN (see Figure 1), introduces new requirements for public safety backhaul networks. E-UTRAN comprises of a set of eNBs connecting among themselves via X2 interfaces, to a Serving Gateway (SGW) via S1-U interfaces, and to a Mobility Management Entity (MME) via S1-MME interfaces. It is a flat any-to-any, all-IP network as described in 3GPP standard TS 36.300,[11] instead of a hub-and-spoke network found in LMR or older 2G and 3G technology. The eNB communicates not just with the centralized SGW and MME, but also dynamically with neighboring eNBs as LTE user equipment roams. The direct inter-eNB communications enables more efficient handover during roaming and better subscriber load management. To support E-UTRAN load-balancing and high availability, LTE's S1-flex function allows for eNBs to connect with multiple SGWs and MMEs.

With the immense degree of connectivity among all E-UTRAN components, it is crucial to have a flexible backhaul network that is highly resilient and can enable operators to flexibly deploy MPLS-based and Carrier Ethernet-based any-to-any services with the precision of traffic engineering in a scalable manner. The use of the X2 interface, which requires minimum latency, calls for routing capability at the edge. Furthermore, with the future introduction of eMBMS-based mission-critical services, multicast capability and delivery of precise time and phase synchronization in the network are also pivotal.

Figure 1. LTE E-UTRAN Network



11 http://www.3gpp.org/DynaReport/36300.htm

Network infrastructure sharing

As governments aim to control budgets, it is imperative to maximize return on any infrastructure investment. Therefore, the proposition of network infrastructure sharing has become very attractive. While the degree and method of infrastructure sharing will vary in different countries depending on local regulatory frameworks, it is generally a paradigm that the backhaul network can also be used to serve other government departments, public communities and public utilities in order to generate revenue. This model can yield tremendous savings for all participating parties.

To support infrastructure sharing, the new public safety network must be a highly robust multiservice network with an architecture that is poised to grow and expand. It needs to be able to scale in size and grow in capacity, fully utilizing available network assets, including microwave spectrum and optical fiber. It also needs to support a flexible range of point-to-point and multipoint virtual private networks (VPNs) for TDM, Ethernet and IP services to meet the need for different organizations' applications. At the same time the network must maintain complete virtualization in the control plane and data plane among all the VPNs to ensure security, and service-aware traffic management to maintain agreed quality of service (QoS) for all organizations, since it is crucial that the quality level not be compromised at any time.

PREPARING BACKHAUL NETWORKS FOR LTE AND BEYOND

To tackle the trends and associated requirements discussed above, public safety agencies need a backhaul network architecture with the following attributes:

- Readiness to scale and expand
- Versatile and efficient use of transmission media and topologies
- Advanced traffic management and QoS
- Strong network resiliency and rapid recovery
- Graceful legacy TDM migration
- Multiservice backhaul for infrastructure sharing
- Fortified security protection
- Precise synchronization distribution
- Efficient end-to-end network management and LTE synergy

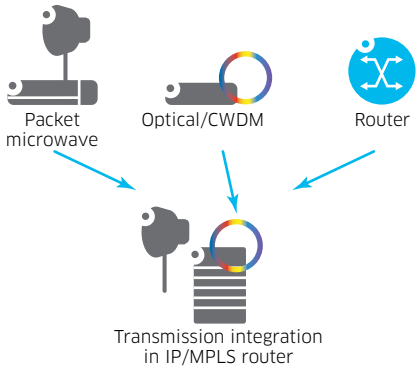
Scalable network size and capacity

The backhaul network must scale seamlessly to support increasing numbers of locations at higher capacities. The network platform needs to accommodate different interface speed and capacity requirements depending on their locations in the network. It should also render installation versatility for small enclosures and full outdoor environments if required. In addition, to reduce OPEX and training requirements, all nodes should be based on the same operating system and be managed by a unified network manager and command line interface.

Versatile and efficient use of transmission media and topologies

Because backhaul network coverage spans dense urban areas to remote terrain, operators must be resourceful in using the means of transmission, such as microwave, fiber, copper and even third-party leased lines if necessary. The backhaul equipment must therefore support transmission layer integration (see Figure 2) to consolidate and simplify network design and operations, and ensure consistent commissioning and operations procedures for all network sites, regardless of the medium.

Figure 2. Transmission Integration in an IP/MPLS router



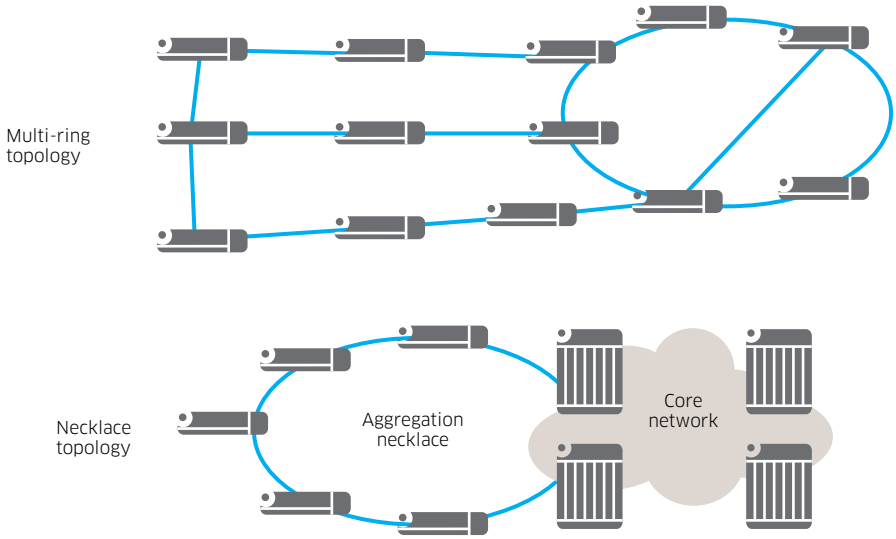
The most common transmission media are packet microwave complemented by optical fiber when available. For microwave, depending on geographic practice and site setting, either outdoor or indoor microwave radios can be deployed. To maximize the bandwidth throughput of available microwave spectrum, the following advanced microwave capabilities are essential:

- **Service-driven adaptive modulation:** This feature optimizes overall microwave channel throughput, even in adverse weather conditions. High-priority traffic is always given bandwidth using advanced QoS prioritization and scheduling techniques if modulation levels need to drop to deliver capacity under adverse weather conditions.
- **Cross-polar interference cancelation (XPIC):** This capability doubles the capacity of a single frequency by using both horizontal and vertical electromagnetic polarizations. This increases capacity while also saving spectrum and antenna costs.
- **Higher order quadrature amplitude modulation (H-QAM):** Higher QAM levels increase the number of transported symbols per hertz to help squeeze more bandwidth out of scarce microwave spectrum.
- **Multi-channel link scaling:** When a high-capacity link is required, multiple radio channels need to bond together into a bigger link, particularly between large aggregation sites.
- **MPLS-aware packet throughput booster:** Uses advanced packet compression to reduce Ethernet and IPv4/IPv6 protocol header, increasing radio link throughput over the air interface by as much as 300 percent. With the associated MPLS label awareness, the compression is the perfect companion to the MPLS network.

When fiber is available, the operators should be able to utilize it fully by using wavelength division multiplexing (WDM) technology. Coarse WDM (CWDM), with its compelling economics, can allow up to eight 1 Gb/s and/or 10 Gb/s wavelengths to be carried in the same strand of fiber.

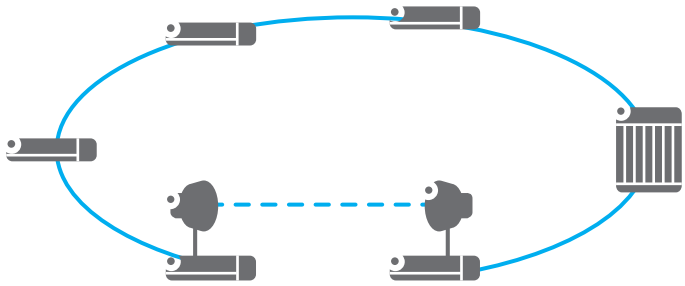
The network should also support advanced resilient topologies — such as multi-ring (also known as ladder), necklace and hybrid — to improve network robustness (see Figure 3 and Figure 4). Particularly, the multi-ring's rich path diversity, when fully capitalized by dynamic IP/MPLS, can provide the utmost redundancy protection even in multi-fault scenarios during a disaster.

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



Traffic management and QoS

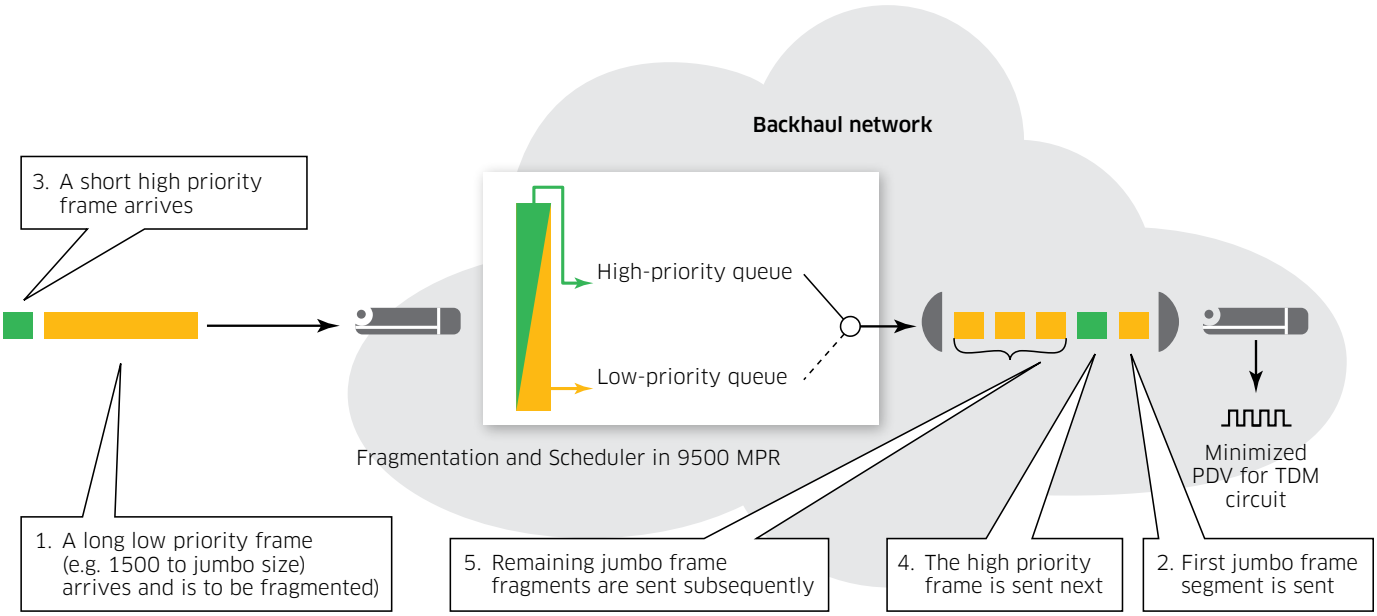
To virtualize the infrastructure without compromising users, a strong QoS mechanism with advanced traffic management capabilities is essential. The backhaul network must incorporate extensive traffic management tools such as advanced hierarchical rate scheduling and prioritization mechanisms on a per-access interface basis to ensure equitable network bandwidth aggregation. These techniques optimize uplink utilization while maintaining maximum isolation and fairness among different application traffic flows 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 critical application performance parameters, such as bandwidth, delay and jitter, are always met in a properly designed network.

Even with advanced traffic scheduling, it is sometimes unavoidable for a high-priority packet to wait for its turn when a jumbo best-effort packet has started transmission. This phenomenon is commonly known as head-of-line blocking, which causes high jitter. While its impact on jitter is negligible on optical Ethernet as the transmission bit rate is in the order of 1 Gb/s or higher, it becomes significant for lower speed links like microwave whose bandwidth is in the order of hundreds of bits per second or lower. Packet fragmentation and interleave, a technique that fragments all packets before queuing and scheduling, can bring down the time high-priority packets have to wait to the value of one segment of transmission, thus minimizing jitter, which is key to the high quality of real-time applications and packet synchronization technology such as IEEE 1588v2.

The essence of the technique is described below (see Figure 5):

1. As long, low-priority frames arrive, they are fragmented into multiple shorter fragments, and subsequently placed in the appropriate lower priority queue.
2. If there are no higher priority frames, the first low-priority fragment starts the transmission process.
3. If a subsequent high-priority frame arrives, it is placed in a high-priority queue to wait for transmission. If the frame length is shorter than that of a fragment, no fragmentation is required for these higher priority frames.
4. When the transmission of the first low-priority fragment has finished, the transmitter serves the high-priority frames, interleaving with the previously sent low-priority fragments.
5. After the high-priority frames are served, the transmitter switches back to service the low-priority frame fragments.

Figure 5. Fragmentation and interleave techniques



Strong network resiliency and rapid recovery

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. Platform protection is a key step in achieving that. Deploying a fully redundant platform that supports hitless control/fabric protection is a significant improvement from adopting a two-node architecture, which effectively doubles the size of the network. Complementary to platform redundancy are 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.

Fast switching is one key pillar of rapid recovery. 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.[12] FRR can distinguish and provide protection to applications depending on the MPLS tunnel priority. To protect the network against node or interconnection failures, end-to-end standby MPLS paths can also be provisioned. When Ethernet ring is deployed, the Ethernet Ring Protection (ERP) G.8032 technique is also an available option.

The other key pillar of rapid recovery is fast fault detection. In a common scenario of deploying microwave between backhaul equipment, the microwave link degradation condition (for example, high bit error rate condition or loss of signal) cannot be communicated quickly to backhaul equipment. The use of fault propagation mechanism backhaul equipment and the integrated microwave radio system for fast fault detection can reduce fault detection time from hundreds of milliseconds to very low tens of milliseconds. These two pillars are pivotal to enable network recovery with minimum application performance impact.

Other resiliency features, such as pseudowire redundancy for geodiversity protection,[13] Multi-chassis Link Aggregation Group (MC-LAG) and automatic protection switching (APS) for core equipment nodal protection can also be deployed individually or together to further enhance end-to-end network resiliency.

For microwave links, 1 + 1 protection with hitless radio protection switching, space diversity and N + 0 radio LAG are techniques that can render different levels of protection.

Graceful legacy TDM migration

As legacy and TDM-based migration will still be in use in the foreseeable future, the performance of the new backhaul network needs to resemble a TDM-based network in resiliency and performance to preserve the same service quality and reliability. They have been explained in the discussion above. However, a wide portfolio of legacy interfaces (E&M, FSX/FSO, V.24/V.35/X.21 serial) and T1/E1 TDM interface are commonly deployed. To gracefully migrate such applications, the support of such interfaces is required.

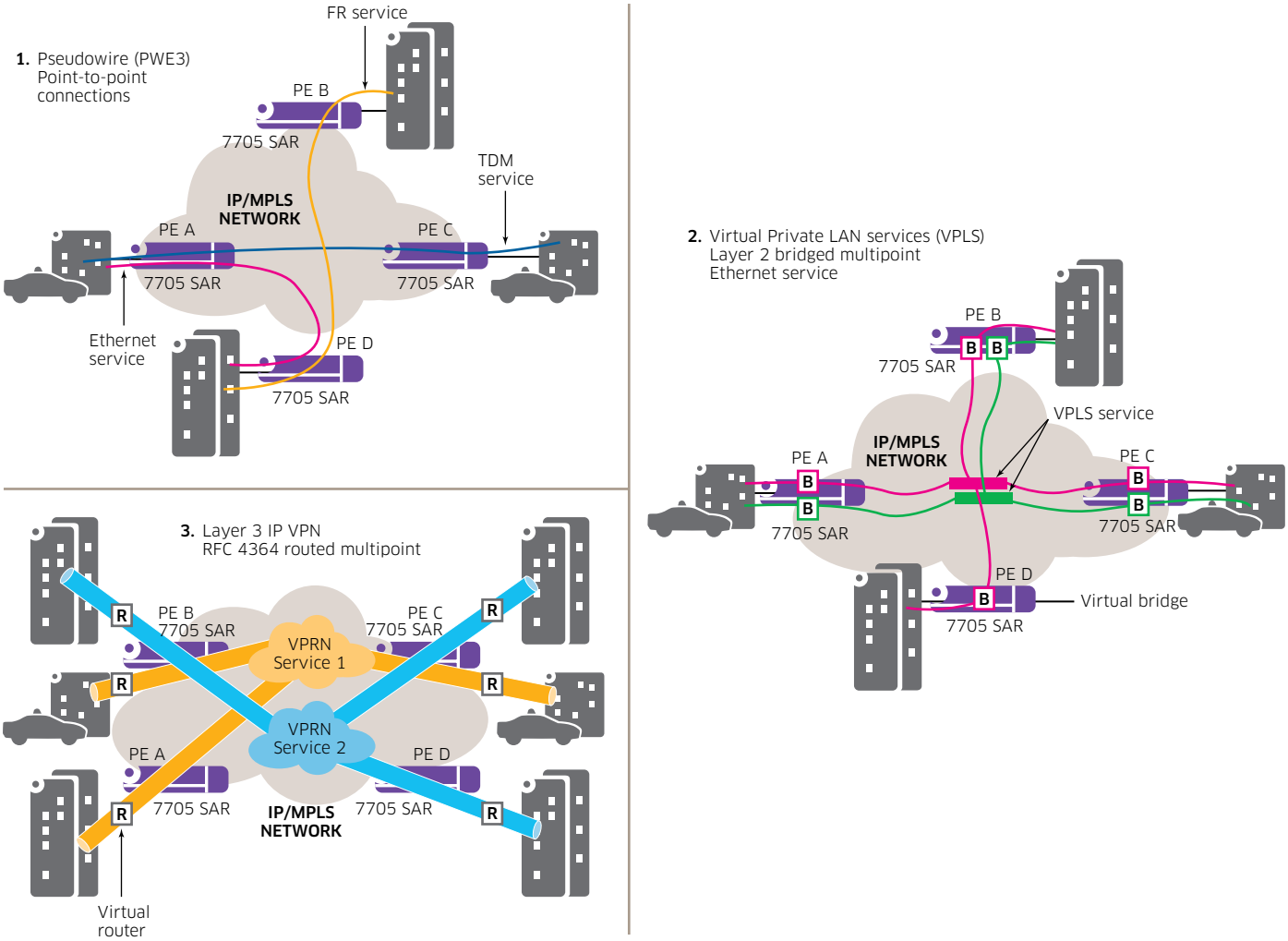
12 International Engineering Task Force, RFC 4090: Fast Reroute Extensions to RSVP-TE for LSP Tunnels. May 2005. http://www.ietf.org/rfc/rfc4090.txt

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

Multiservice backhaul for infrastructure sharing

The IP/MPLS-based network is ideal for multiservice backhaul. Its full range of MPLS-based VPN services has been deployed in many mission-critical networks and commercial carriers have used the technology with the most demanding applications under the most trying environments with no compromise (see Figure 6). Multiservice backhaul can be deployed for all kinds of topology and connectivity required by the applications.

Figure 6. Multiservice backhaul



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[14] 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.

Microwave link, by its very nature, is inherently secure. The radio equipment at each end of a microwave link has no provision for transmitting to or receiving from a device other than the far-end radio. Because they communicate only to the far-end antenna, the antennas are also narrow-beam and highly directional. Therefore, an attacker would encounter significant challenges to actually detect and receive the microwave signals. First, the attacker needs to know the radio modem profile to receive the signals properly. Even if an attacker were able to do that, they would still need to locate the right radio frequency variant of radio to demodulate the signal with the modem profile in use. Furthermore, the use of link identifiers at both ends of the radio path can prevent a rogue radio from impersonating a legitimate radio and receiving valuable network information. For ultimate protection in mission-critical networks, a FIP-197-compliant encryption scheme such as Advanced Encryption Standard (AES) 256 scheme can be used to ensure confidentiality. This can be enabled in locations vulnerable to eavesdropping only.

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) in a central location. To deliver TDM services over the new backhaul network, similar 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 (from SDH/SONET, T1/E1)
- Adaptive clock recovery and differential clock recovery timing
- Synchronous Ethernet
- IEEE 1588v2-2008[15] (also known as IEEE 1588v2) Precision Timing Protocol (PTP) (master, boundary clock, transparent clock and slave)
- Integrated GPS receiver

14 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**

15 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**

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.

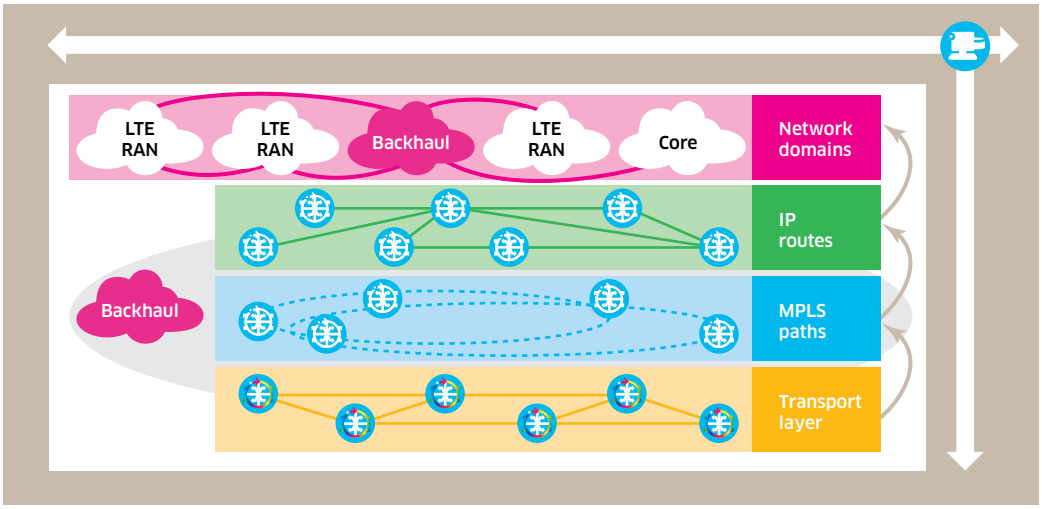
End-to-end network management and LTE synergy

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.

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 7.

Figure 7. Multi-domain service-aware manager for end-to-end public-safety LTE networks



ALCATEL-LUCENT PUBLIC SAFETY IP/MPLS NETWORK SOLUTION

With the Alcatel-Lucent public safety IP/MPLS network solution, public safety agencies gain an IP/MPLS network that has all the architecture attributes described above. Solution highlights are:

- Scalable and flexible VPN services for TDM, Ethernet and IP
- Installation flexibility, which includes DIN mounting in small enclosures and outdoor mounting on a wall, pole or stand without cabinet
- Integration with versatile packet microwave
- Built-in CWDM networking
- Graceful transmission medium migration from microwave and optics
- Synchronization based on Bell Labs technology
- End-to-end multi-domain IP management, including MPLS, microwave, optics and LTE

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)[16]
- Alcatel-Lucent 7705 Service Aggregation Router (SAR)[17]
- Alcatel-Lucent 7450 Ethernet Service Switch (ESS)[18]
- Alcatel-Lucent 7210 Service Access Switch (SAS)[19]
- Alcatel-Lucent 9500 Microwave Packet Radio (MPR), providing a packet microwave link to connect MPLS nodes[20]
- Alcatel-Lucent 1830 Photonic Service Switch (PSS), the optical layer underlying the IP/MPLS network[21]
- Alcatel-Lucent 5620 Service Aware Manager (SAM) for service and network management[22]

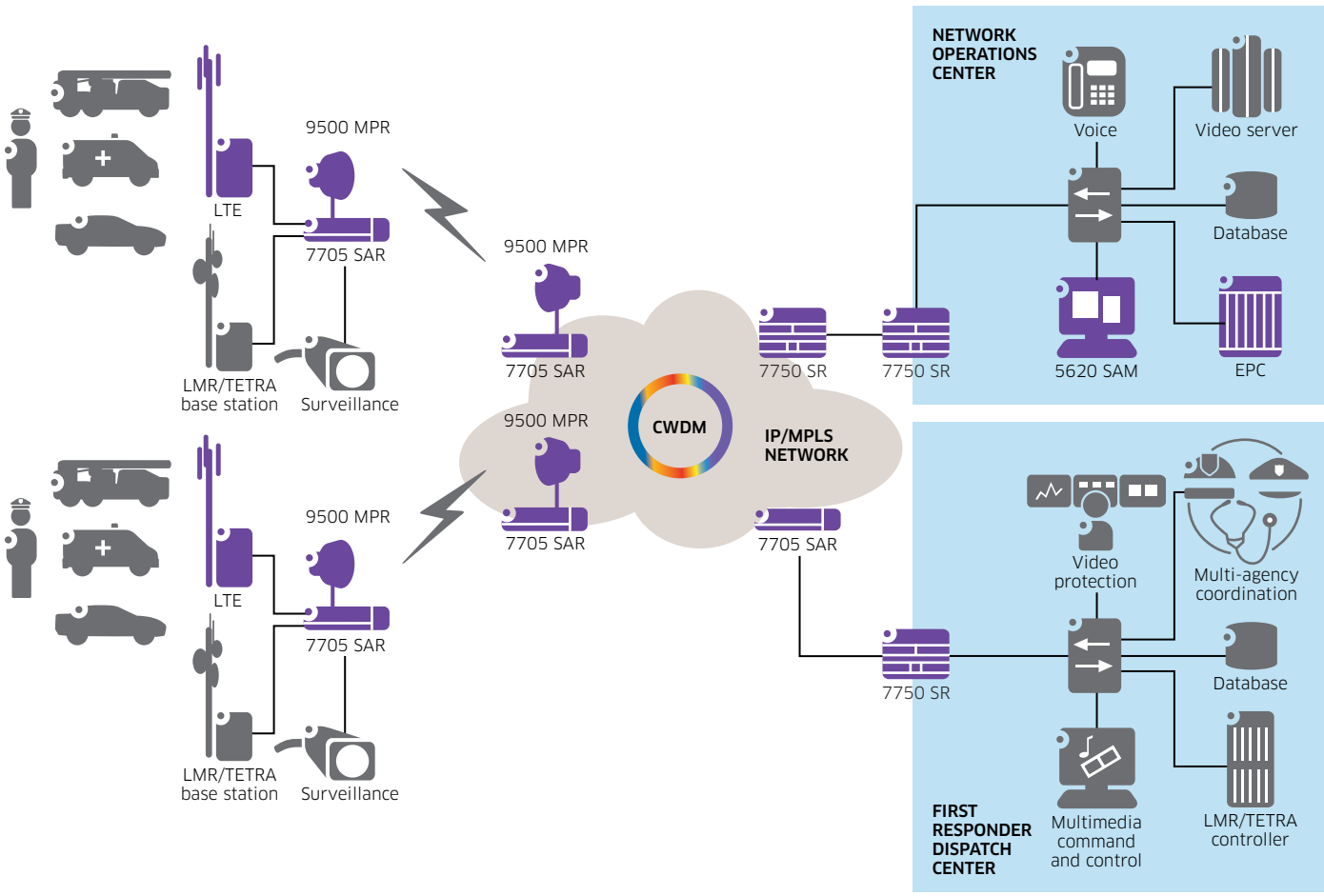
Blueprint backhaul network architecture

The Alcatel-Lucent IP/MPLS network solution helps public safety agencies to deploy converged networks for all applications while preserving QoS and reliability. This mission-critical design is ideal for public safety because it is capable of coping with LMR traffic now and scaling up for LTE traffic in the future. With strong solution components, network operators can design a network with a flexible architecture according to their unique set of requirements.

Figure 8 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.

16 Alcatel-Lucent 7750 Service Router. **http://www.alcatel-lucent.com/products/7750-service-router**
17 Alcatel-Lucent 7705 Service Aggregation Router. **http://www.alcatel-lucent.com/products/7705-service-aggregation-router**
18 Alcatel-Lucent 7450 Ethernet Service Switch. **http://www.alcatel-lucent.com/products/7450-ethernet-service-switch**
19 Alcatel-Lucent 7210 Service Access Switch. **http://www.alcatel-lucent.com/products/7210-service-access-switch**
20 Alcatel-Lucent 9500 Microwave Packet Radio. **http://www.alcatel-lucent.com/products/9500-microwave-packet-radio**
21 Alcatel-Lucent 1830 Photonic Service Switch. **http://www.alcatel-lucent.com/products/1830-photonic-service-switch**
22 Alcatel-Lucent 5620 Service Aware Manager. **http://www.alcatel-lucent.com/products/5620-service-aware-manager**

Figure 8. Alcatel-Lucent IP/MPLS blueprint network architecture for public safety



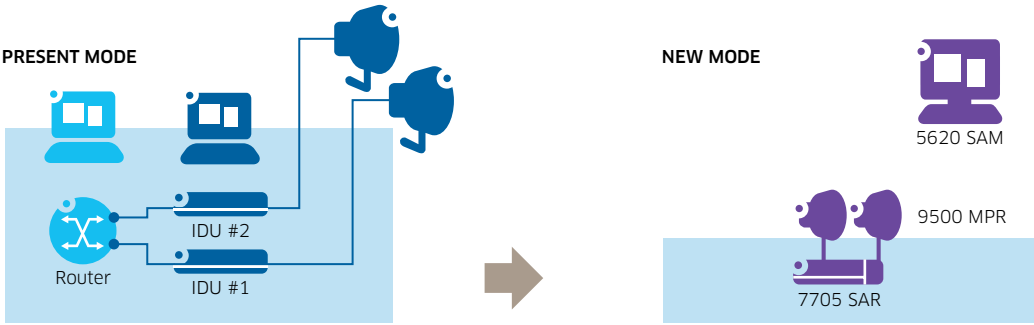
Integrated IP/MPLS and microwave domains

In a traditional architecture, IP/MPLS is overlaid over microwave transmission across two platforms. In the Alcatel-Lucent IP/MPLS network solution, the 9500 MPR is fully integrated with the 7705 SAR as a single, seamless, managed platform that converges the IP and microwave domains (see Figure 9).

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 rate condition
- Reduced equipment space, sparing requirements, power consumption and cooling needs
- Streamlined installation and operations management

Figure 9. Integrated 7705 SAR and 9500 MPR configuration



- 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 packet for the efficient support of mission-critical LMR/TETRA applications 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 breadth and depth in IP/MPLS, microwave, optics, LTE and network management, Alcatel-Lucent offers an unparalleled end-to-end managed backhaul solution, which has been deployed in many mission-critical networks and commercial cellular networks globally. With its vast network design and deployment experience, Alcatel-Lucent is the ideal partner for public safety agencies looking to transform their backhaul network in preparation for the future.

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
AES	Advanced Encryption Standard
APCO	Association of Public-Safety Communications
APLS	automatic person location system
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
eNB	Evolved Node B
e-UTRAN	Evolved UMTS Terrestrial Radio Access Network
EPC	Evolved Packet Core
FirstNet™	First Responder Network Authority
FR	Frame Relay
FRR	Fast Reroute
GIS	Geographic Information System
GPS	Global Positioning System
H-QAM	Higher order quadrature amplitude modulation
HMAC-MD5	Hash-Based Message Authentication Code - Message Digest 5
HSS	Home Subscriber Server
IDU	indoor unit
IP VPN	IP virtual private network
IT	information technology
IWF	InterWorking Function
LAG	Link Aggregation Group
LMR	Land Mobile Radio
LSP	Label Switched Path
LTE	Long Term Evolution
MAC	Media Access Control
MC-LAG	Multi-chassis Link Aggregation Group
MCPTT	Mission Critical Push-to-talk
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	Private/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
TEDS	TETRA Enhanced Data Services
TETRA	Terrestrial Trunked Radio
UTRAN	UMTS Terrestrial Radio Network
VLL	Virtual Leased Line
VPLS	Virtual Private LAN Service
VPN	virtual private network
VPRN	Virtual Private Routed Network
XPIC	Cross-polar interference cancellation

REFERENCES

1. 3GPP Release 11 LTE. **http://www.3gpp.org/specifications/releases/69-release-11**
2. 3GPP Release 12 LTE. **http://www.3gpp.org/specifications/releases/68-release-12**
3. 3GPP Release 13 LTE. **http://www.3gpp.org/release-13**
4. Alcatel-Lucent 1830 Photonic Service Switch. **http://www.alcatel-lucent.com/products/1830-photonic-service-switch**
5. Alcatel-Lucent 5620 Service Aware Manager. **http://www.alcatel-lucent.com/products/5620-service-aware-manager**
6. Alcatel-Lucent 7210 Service Access Switch. **http://www.alcatel-lucent.com/products/7210-service-access-switch**
7. Alcatel-Lucent 7450 Ethernet Service Switch. **http://www.alcatel-lucent.com/products/7450-ethernet-service-switch**
8. Alcatel-Lucent 7705 Service Aggregation Router. **http://www.alcatel-lucent.com/products/7705-service-aggregation-router**
9. Alcatel-Lucent 7750 Service Router. **http://www.alcatel-lucent.com/products/7750-service-router**
10. Alcatel-Lucent 9500 Microwave Packet Radio. **http://www.alcatel-lucent.com/products/9500-microwave-packet-radio**
11. Alcatel-Lucent. Press release: Alcatel-Lucent and Las Vegas first responders conduct trial of 4G LTE public safety broadband mobile network. November 25, 2013. **http://www.alcatel-lucent.com/press/2013/002955**
12. 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**
13. 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**
14. International Engineering Task Force. RFC 4090: *Fast Reroute Extensions to RSVP-TE for LSP Tunnels.* May 2005. **http://www.ietf.org/rfc/rfc4090.txt**
15. International Engineering Task Force. RFC 4364: *BGP/MPLS IP Virtual Private Networks (VPNs)*. February 2006. **http://tools.ietf.org/search/rfc4364**
16. International Engineering Task Force. RFC 4553: *Structure-Agnostic TDM over Packet (SAToP)*. June 2006. **http://tools.ietf.org/html/rfc4553**
17. 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**
18. International Engineering Task Force. RFC 6718: *Pseudowire Redundancy*. August 2012 **http://tools.ietf.org/html/rfc6718**
19. National Telecommunications and Information Administration. FirstNet. **http://www.ntia.doc.gov/category/firstnet**
20. TETRA Today. TCCA signs LTE agreement. June 19, 2012. **http://www.tetratoday.com/news/tcca-signs-lte-agreement**

www.alcatel-lucent.com Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.
Copyright © 2014 Alcatel-Lucent. All rights reserved. MKT2014055902EN (June)

Alcatel·Lucent