STRATEGIC WHITE PAPER

Mission-critical Communications for Defense

Increasing flexibility, enabling agile mobility, improving command and control and protecting critical infrastructure with the Alcatel-Lucent Mission-critical WAN Infrastructure

Key issues for defense departments are the enabling of a highly mobile, situation-aware force; full C4I capabilities regardless of the network topology; flexibility to handle legacy and new packet-based applications over one geographically dispersed network in constant churn; critical-infrastructure protection; and leveraging of the fast-paced technological advances of commercial, off-the-shelf telecommunications products in military networks. The Alcatel-Lucent Mission-critical WAN Infrastructure helps defense departments address these challenges with a foundation that allows always-on communications to be securely shared among entities. It cost-effectively expands into new areas, scaling bandwidth to accommodate new applications that enhance mission effectiveness. Built-in application awareness, traffic optimization and end-to-end management boost overall mission effectiveness and flexibility by ensuring traffic gets from source to destination, cost-effectively, without degradation.

Table of contents

1. Introduction

The role of defense forces has evolved drastically over the past decade. In addition to their traditional combat function, twenty-first century defense operations often include:

- Humanitarian assistance and disaster relief
- Counter-insurgency and counter-terrorism response
- Stability operations and peace keeping

A higher tempo of operations, the requirement for increased agility and mobility of forces in the field, full command and control capabilities regardless of the network capability or force deployment, flexibility in the topology and traffic mix, critical infrastructure protection (CIP), and the ability to leverage the advances of commercial, off-the-shelf (COTS) technology in military networks are major challenges for today's defense departments. A robust, scalable, flexible and highly available network is essential to support all these mandates. Sensors, closed-circuit television (CCTV), applications, procedures, tactical networks, and other assets combine with the network to enable enhanced operational capabilities.

1.1 Mobility

In practical terms, mobility for defense departments is reflected in the level of their ability to easily relocate a task force to or around the operational area without compromising operational efficiency with degraded levels of communications or logistics support. A force with a higher level of mobility can move faster and establish full capabilities more quickly than forces with a lower level of mobility, creating a tactical advantage that can outlast the duration of deployment. Alternatively, reduced mobility can result in a degraded situation such as increased casualties; entrenched insurgency; or starvation, malnutrition and epidemics of cholera or dysentery among the survivors of natural or man-made disasters.

The increased emphasis on national security requires improved levels of agility and responsiveness. With the shift from sea to air transport, the time to move, position and sustain task forces and capabilities from one part of the world to another is now measured in hours instead of weeks. Task forces are often required to rapidly deploy to remote locations, often where existing telecommunications or infrastructure or services are non-existent or no longer functional. They must establish communications ahead of main force deployment and utilize whatever communications facilities they can quickly set up. These facilities integrate forces into the main defense network and may include fiber, satellite, Worldwide Interoperability for Microwave Access (WiMAX®), Long Term Evolution (LTE), IEEE 802.11, Terrestrial Trunked Radio (TETRA), Project 25 (P25) or other specialized tactical radio links, depending on the available infrastructure.

However, until recently communications capability in the field was limited to technology that was designed and manufactured for the military decades ago, and technology has advanced considerably since then. The IT capability of an advanced operations base has been far inferior to those of the main operations base. Basic priorities for warriors have traditionally been ammunition, water, food and medical supplies, and quantities are limited to what they can carry on their person or in patrol vehicles: anything that competes for weight or space must be minimized.

The design of advanced communications equipment must take the above conditions into account. Technical obstacles to mobility, such as the physical size and weight of portable telecommunications equipment, low battery life, heavy power consumption, limited bandwidth available for rich media applications, signal strength and quality, encryption, security and standards compliance have traditionally been limitations to providing advanced communications capabilities to field personnel.

In addition, while advanced technical expertise to install and maintain equipment is readily available back at the base, the mobile field force needs to minimize this labor overhead by using equipment requiring only basic technical expertise, ideally using self-configuration and setup at the push of a button. These issues have been overcome to a large extent and continue to be refined by leveraging the development and technical innovations in COTS products, most notably by mobile phone and personal mobile computing technology.

1.2 Effective command and control

While the scope of operations may have evolved, the need for a fully networked force is now greater than ever. Precise, current intelligence at headquarters is essential for effective command and control, and the need for enhanced situational awareness in the field is arguably even more critical in the stabilization operation of a failed state than it is in a traditional combat operation. Non-governmental organizations (NGOs) are often on the ground and operating independently of the military. Many in the civilian population are struggling to merely survive and are forced to take responsibility for their own personal security. It is often impossible to differentiate between innocent civilians and insurgents.

The networking of knowledgeable entities and sensors that are geographically or hierarchically dispersed is critical to enabling the gathering and sharing of current information, the development of shared situational awareness through collaboration, and the achievement of self-synchronization for personnel in the field. The end goal is increased mission effectiveness by achieving greater speed of command and increasing lethality, survivability and responsiveness.

The networking of CCTV, remote sensors, decision makers and weapon systems, as well as military, governmental and non-governmental agencies, creates a seamless, collaborative planning, assessment and execution environment. The following are examples:

- Networks of CCTV, remote sensors, virtual whiteboards, smart maps and collaborative-planning applications help decision makers and field personnel to enable shared battle-space awareness. The networking of CCTV and remote sensors provides estimates of position, velocity and friendly/hostile object identification.
- Field personnel are empowered to make decisions and act based on the content, quality and timeliness of information. The information advantage is translated to combat power by field personnel and decision makers.
- Decision makers have access to more information than ever. Data-mining and data-warehousing applications provide intelligence analysts with significantly improved access to large volumes of source data for analysis and integration. Field personnel can interact in new ways to enable new modes of operation. A key example is the ability to get status information on demand (self-synchronization).
- Combat service support (CSS), otherwise known as logistics support, is an integral component of all military operations. Effective logistics support maximizes capabilities by being responsive to commanders' needs for agility, deployability, lethality, versatility, survivability and sustainability. A reliable, ubiquitous and far-reaching network enables effective logistics support.
- The network enables military assets and functions to be relocated or reallocated across the military force as required.
- Deployed forces have access to distance learning and enjoy an improved quality of life, with increased frequency and timeliness of communications with families using e-mail, telephone or virtual teleconferencing.

1.3 Flexibility

To be useful in this environment, the network must provide for the timely exchange of secure information. The communications network enabling this capability must be ubiquitous, interoperable and robust, supporting the timely collection, fusion, analysis and sharing of information. It requires a mission-critical network infrastructure, which is generally accepted to mean:

- An IP/Multi-Protocol Label Switching (MPLS) network with or without a SONET/SDH/wavelength division multiplexing (WDM) foundation
- End-to-end encryption with denial of service (DoS) protection
- High availability
- Scalability, connectivity and accessibility
- Multiple-application capability
- Quality of service (QoS) sensitive to transaction type, with deterministic delay

In the current environment, several types of independent voice, video and data networks — for example, the United Kingdom Defense Information Infrastructure (DII) and the United States Tactical Digital Information Links (TADILs) — operate as independent networks for multiple reasons. One of the primary drivers for separate networks was the need for deterministic delay. Tactical data links, such as Link 16 and Cooperative Engagement Capability (CEC), operated with protocols separate and distinct from the protocols employed with Transmission Control Protocol (TCP)/IP-based networks, such as the Secret Internet Protocol Router Network (SIPRNET). Another primary driver for separate networks is that until recently, IP-networking technology could not enable QoS to be linked to transaction type.

In other cases, security requirements, combined with technology limitations, conspired to dictate separate networks. For example, the Non-classified Internet Protocol Router Network (NIPRNET) and the SIPRNET were carried over separate networks because secure virtual private networks (VPNs) such as virtual private LAN service (VPLS) did not exist. A key challenge was to eliminate communication silos as a step toward a collaborative environment and greater mission effectiveness.

The network requires multimode data-transport capabilities — including military and commercial satellite communications, fiber and microwave data links, and tactical radios — as well as connections using commercial information services. These various data-transport capabilities provide users with access to appropriate elements of a distributed computing environment as well as the interconnecting fabric for a wide range of computational and storage capabilities.

1.4 Critical infrastructure protection

CIP relates to preparedness and response to serious incidents involving municipal, regional or national infrastructure that is so critical to its normal functioning that damage or destruction would interrupt normal commerce, create serious hardship for its citizens or cause loss of life. Transportation corridors, rail lines, water reservoirs and power-generation stations are some examples of critical infrastructure. We normally view CIP with respect to protection against terrorist activity. However, naturally occurring incidents, such as the eruption of the Eyjafjallajökull volcano in Iceland, and man-made accidents, such as the explosion on the offshore oil-drilling platform and the resulting oil spill in the Gulf of Mexico, are also to be considered. Legislation regulating CIP has been passed in regions around the globe.

The US legislation was originally passed under Presidential Decision Directive 63 (PDD 63) in May 1998.[1] This was updated in 2003 in Homeland Security Presidential Directive 7 (HSPD 7), *Critical Infrastructure Identification, Prioritization, and Protection*. The directive broadened the definition of infrastructure as "so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being."[2]

In the European Economic Union, the equivalent is the European Programme for Critical Infrastructure Protection (EPCIP). The program is the outcome of European Commission directive COM(2006) 786,[3] which defines critical infrastructure in Europe as follows: "European Critical Infrastructures constitute those designated critical infrastructures which are of the highest importance for the Community and which if disrupted or destroyed would affect two or more MS, or a single Member State if the critical infrastructure is located in another Member State." The areas covered include energy, nuclear-industry, information, communication, technologies, water, food, health, financial, transport, chemical-industry, space and research facilities.

While the defense department is also a key agency in civilian CIP, CIP in the context of defense — sometimes referred to as defense critical infrastructure (DCI) — refers to both defense department and non-defense department networked assets that are essential to support and sustain military forces and operations. Activity on or around patrol routes, power stations, water reservoirs or railway lines; the positive identification of approaching VIP convoys; the swarming of insurgents a few blocks away; or the existence of a makeshift checkpoint around the corner are all examples of time-critical information to the soldier on the ground and back at the command and control center. Information sources may be permanent cameras mounted on buildings, unmanned aerial vehicles, aerostats, mast-based surveillance systems, reconnaissance vehicles, satellites, proximity detectors, audio sensors, intrusion alarm systems or human intelligence.

The ability to gather, process and share intelligence from any source or sensor is crucial for the protection of critical infrastructure. Other less-obvious but equally important requirements for CIP are:

- The implementation of emergency communications networks for critical users in the event of crisis, on a separate private-network overlay or by enabling priority communications on existing public networks. In some cases — for example, in commercial wireless networks — the latter is not always practical.
- Improvement in the security and availability of Internet, telephone and wireless networks to make them less vulnerable to DoS, cyber and physical attacks
- Video- and data-analysis applications to facilitate the screening and detection of undesirables as well as the detection of hostile reconnaissance
- Communications and collaboration capabilities to facilitate the exchange and dissemination of information, experience and best practices among the departments, organizations and agencies responsible for the protection of critical infrastructure

1.5 COTS communications equipment

Today's defense business model must keep pace with the changing nature of war-fighting challenges. Healthcare, social programs and government bailouts are competing with defense for public funds, resulting in increased financial accountability. Funds to develop or sponsor the development of specialized military-communications equipment are becoming harder to justify.

[1] PDD 63: *Protecting America's Critical Infrastructures*, May 1998.

[2] HSPD 7: *Critical Infrastructure Identification, Prioritization, and Protection*, December 2003.

[3] COM(2006) 786: *Communication From the Commission on a European Programme for Critical Infrastructure Protection*, December 2006.

The demand for consumer broadband in all areas from smartphones to IP video, along with commercial trends for network transformation, is driving the demand for more powerful, packet-based network elements (NEs). Telecommunications vendors are competing intensely, adding new features and functionality at a staggering pace to differentiate their products and improve market share. The demand for faster, smaller and more energy-efficient components is so intense that, even during periods of decreased economic growth, major telecommunications vendors are facing component shortages. This demand, combined with the high-tech downturn a decade ago, has fueled innovation among semiconductor vendors, accelerating processing capability, decreasing component sizes and reducing power consumption.

The market for fully ruggedized and militarized telecommunications equipment is considerably smaller than that of high-availability COTS products. Considerable levels of engineering resources and investment are associated with being fully compliant with most military specifications. Many vendors, especially those with aggressive development programs, cannot make a successful business case to develop products to military specifications without significantly inflating their prices. As a result, while military-grade equipment excels in ruggedness, it often lags in features and functionality or is far more expensive compared with the equivalent COTS products.

Fortunately for the defense market, the commercial market is insisting on higher levels of reliability and availability than ever before. NEs, such as routers and Ethernet switches, used to carry only best-effort traffic and now carry mission-critical voice, data and video traffic from the energy, public safety and transportation sectors. High-availability and service-aware routers and switches are a relatively recent development, developed for carriers as they underwent network transformations and found themselves carrying increasing mission-critical packet traffic. While some telephone company equipment is located in environment-controlled rooms, these companies are also insisting on high levels of availability as they deploy COTS telecommunications equipment in outside cabinets from the Arctic to the tropics.

In some situations, such as in mobile tactical units, more ruggedized NEs are required. The key to leveraging the advances and cost-effectiveness of COTS, without sacrificing reliability, is to use standards-based equipment that is rugged enough for the environment in which it will be used. For example, COTS equipment housed in controlled environments back at headquarters can seamlessly interwork with COTS equipment in outside enclosures at an advanced operations base as well as the ruggedized, media-rich tactical equipment in forward-operations bases or mobile-reconnaissance units.

For mission-critical defense environments, Alcatel-Lucent leverages its feature-rich COTS products and technologies, originally designed for high-availability carrier networks, in combination with ruggedized products ideal for tactical environments.

1.6 Defense department WAN transformation

Transformation of today's defense department WAN is a typical first step in addressing the numerous challenges and realizing the benefits of new applications. The transformation includes expanded bandwidth and network reach along with new capabilities to cost-effectively address the growing IP-based applications traffic.

The Alcatel-Lucent Mission-critical WAN Infrastructure provides a converged backbone that enables always-on communications to securely interconnect all entities. The flexibility of the infrastructure enables the connection of sensors, video surveillance sources, tactical networks, military bases, forward joint air operating centers, forward-operations bases, hospitals and national defense headquarters while cost-effectively enabling the inclusion of new sites and bandwidth scaling to accommodate new applications that boost mission effectiveness. Built-in application awareness, traffic optimization and end-to-end management enhance effectiveness and flexibility.

The IP/MPLS-based network enables multiple standalone networks to be integrated into an adaptive and reconfigurable “network-of-networks.” This operational flexibility enables commanders to plug and play sensors, shooters, command and control, and support capabilities into task-organized combat packages, including the appropriate collections of sensors and weapons.

Carrier Ethernet is a fundamental technology in the multiservice Alcatel-Lucent Mission-critical WAN Infrastructure. The benefits of Ethernet are combined with the reliability, protection and operations, administration and maintenance (OA&M) provided by technologies such as SONET/SDH, WDM and MPLS. Within the Alcatel-Lucent Mission-critical WAN Infrastructure, Carrier Ethernet consists of Carrier Ethernet transport and IP/MPLS.

Growing packet traffic, with applications such as video surveillance and graphic-rich web site content, is triggering changes to facilitate efficient WAN transport. This shift often begins with an evolution to hybrid packet and circuit transport, with increased capacity, and then full packet convergence as packet traffic begins to dominate. MPLS Transport Profile (MPLS-TP) is the evolution of SONET/SDH to better accommodate native packet applications while retaining Carrier Ethernet transport performance. New Packet Optical Transport Systems, microwave packet radios and Zero Touch Photonics offer the resiliency, increased bandwidth capacity, effectiveness and flexibility to enable true, smooth network convergence.

To capitalize on the wide range of new time-critical applications that increase efficiency, IP/MPLS capabilities are being added in the WAN core. IP/MPLS provides the efficient foundation for the growing IP-based applications traffic as well as multiservice flexibility to deliver mission-critical and legacy traffic in an operationally consistent manner. In a greenfield application or when packet traffic is the dominant traffic type, an end-to-end IP/MPLS WAN can be an appropriate architecture. The IP/MPLS-based core and access enable the reliable support of all types of traffic in a single network, with Carrier Ethernet to simplify and lower operating costs.

IP/MPLS with Carrier Ethernet transport supports the full range of new IP-based applications — applications that current networks do not have the bandwidth and flexibility to handle efficiently. IP/MPLS with Carrier Ethernet transport also provides the required foundation for broadband streaming video, imaging and video surveillance capabilities for enhanced mission effectiveness.

Driving defense departments’ need to enhance the WAN is not that today’s WANs are inadequate for the purposes they have traditionally served, but that they are now required to perform new tasks with new purposes that are beyond their current capabilities. Transformed communications are needed as a foundation for a more collaborative, rapid multi-department effort. However, the WAN must continue to provide carrier-grade reliability and manageability for the mission-critical traffic that is essential to flawless, effective mission execution.

2. Taking control

In the Cold War era, defense was a prime concern for most nations and many allocated significant portions of their budgets to defense. With the lessening of global tensions, increased focus on homeland security, support for natural disasters, and the lingering effects of the latest economic depression, defense departments are now facing increasing competition with other government agencies for public funds. They are caught in the struggle to balance between the growing complexity of their environment and the need for rapid deployment.

Improving communications among decision makers, information infrastructures and field personnel is essential. These communication enhancements may include new traffic types such as packet voice, streaming video, sensor data or digital imaging. Lowest total cost of ownership (TCO) is a key concern when increasing network flexibility and capabilities.

Supporting a growing set of advanced communications capabilities and applications is the Alcatel-Lucent Mission-critical WAN Infrastructure. This flexible infrastructure enables full collaborative services and therefore dramatically enhances day-to-day and operational activities. Some of these capabilities include:

- Streaming video (for example, lightweight tactical camera)
- Broadcast audio or video sent simultaneously to multiple handsets
- Digital imaging
- Computer-aided tasking
- E-mail, text messaging and Web access
- Mapping/geographic information system (GIS)
- Remote database access
- Telemetry/remote equipment diagnostics
- Voice over IP (VoIP) and Push-to-Talk (PTT) radio, including interoperability with legacy and new Land Mobile Radio (LMR) infrastructure using gateways
- Remote access to databases to streamline routine tasks and decrease paperwork
- Mission-critical information exchanged in near-real time — anytime, anywhere — including operational topology, operations plans, dossiers, incident stills, surveillance feeds and tactical video
- Simplified, secure sharing of voice, video and multimedia data among field personnel, command posts and/or command centers
- The Alcatel-Lucent 9907 Rapidly Deployable Network (RDN) can provide ruggedized, highly mobile and quickly deployable (less than ten minutes) wireless voice and data operational and tactical networks for forward-operations bases. The Alcatel-Lucent 9907 RDN can dynamically expand and contract as required to extend command, control, communications, computers, and (military) intelligence (C4I) to any point on the globe.

Over the past decade, communications networks have evolved from more-or-less passive systems of information transfer to active tools with strategic value. The networks have become key components in the delivery of rich-media situation reports and intelligence. New applications with direct impact on defense department operations — voice collaboration, digital imaging and streaming video — expand the capability to rapidly coordinate and equip field personnel with critical information from specialists and new sources. However, for these advantages to be realized, the WAN must change to deliver the required bandwidth and efficiently support the applications' IP-based traffic while maintaining the ability to support legacy applications and traffic.

Today, defense departments typically maintain a segregated communications network for each application. A single network is dedicated to tactical voice communications, another to voice communications among the department's fixed sites, another to secure communications, another to unclassified data, and so on. This inefficiency is caused partly by fit-for-purpose responses to changing communication needs. Although network-asset life is measured in decades, maintaining the status quo has become increasingly high-risk as field personnel serve in an ever more complex environment.

By enhancing microwave and optical transport technology and adopting IP/MPLS technology, defense departments have the opportunity to converge their WANs and enjoy a whole range of benefits, including greater flexibility, lower costs and improved security.

WHAT IS IP/MPLS?

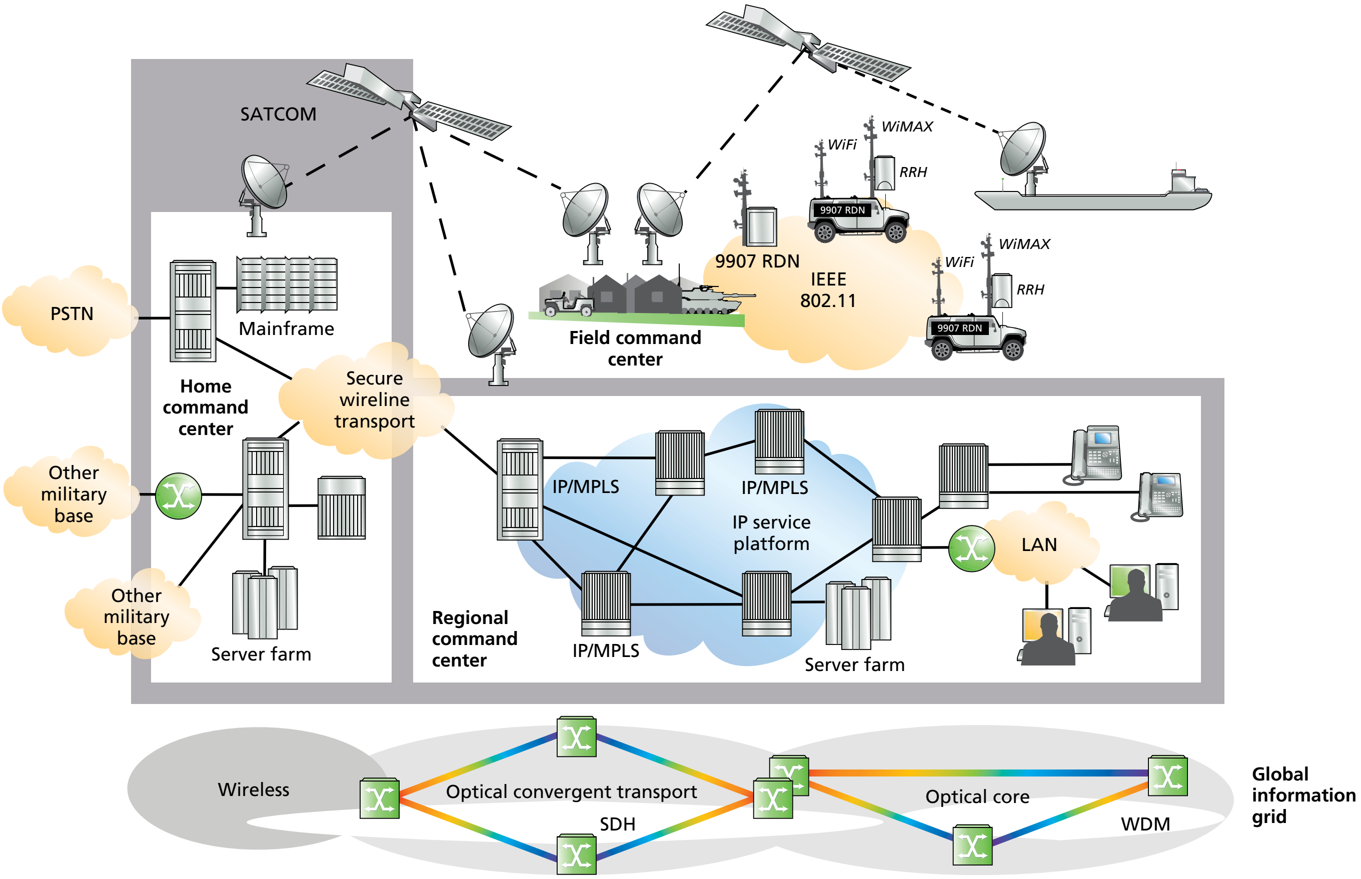
IP/MPLS uses Multi-Protocol Label Switching to deliver IP-based applications traffic and services. MPLS is designed to achieve high reliability in converged WANs and has the ability to assign and guarantee QoS for specific traffic. IP/MPLS is particularly valuable for its openness and interoperability, bandwidth efficiency and flexibility for supporting mission-critical operations and IT voice/data applications.

Mission-critical information can be rapidly communicated with extremely high reliability in such a converged environment. The physical connectivity of a department's fixed sites with a common WAN for all types of communication — voice, data, video, and so on — provides a key communications foundation for better intra-/inter-department communication. At the same time, IP traffic associated with digital LMR/Professional Mobile Radio (PMR), voice, data and other new applications — including voice collaboration and streaming video to improve productivity and security — is also supported. One network can host the full suite of applications traffic required by the defense department while protecting critical traffic to ensure that it always receives priority treatment. In addition, centralization allows greater information sharing and compilation.

2.1 How the converged network looks

The Alcatel-Lucent Mission-critical WAN Infrastructure, shown in Figure 1, utilizes a combination of IP/MPLS, SONET/SDH, Ethernet and MPLS-TP capabilities to support the convergence of legacy and growing IP traffic reliably, flexibly and cost-effectively in a broad range of applications. Microwave transport is deployed where fiber connectivity between sites is not available, and WDM is used to scale fiber capacity.

Figure 1. Defense department WAN-communications transformation with the Alcatel-Lucent Mission-critical WAN Infrastructure



2.2 Role of Carrier Ethernet with Carrier Ethernet transport and IP/MPLS

The Alcatel-Lucent Mission-critical WAN Infrastructure delivers multiservice support, allowing the convergence of all traffic in a single reliable, secure and scalable Carrier Ethernet-based network. Ethernet, as a packet-based data-communications technology, has had appeal for WAN applications for several years because of the desire to build infrastructure based on Ethernet's attractive economics (high performance/price ratio and low cost per transported bit). Combined with Ethernet's ease of use, familiarity and virtual ubiquity in LANs, it is easy to see why organizations have attempted to capitalize on what was once a "best-effort," only-in-the-LAN technology.

The term "Carrier Ethernet" was defined and promoted by the MEF (formerly Metro Ethernet Forum) to differentiate from traditional LAN-based Ethernet. This has helped take Ethernet outside the LAN to become more of a WAN technology. The benefits of Ethernet are combined with the reliability, protection and OA&M provided by technologies such as SONET/SDH, WDM and MPLS.

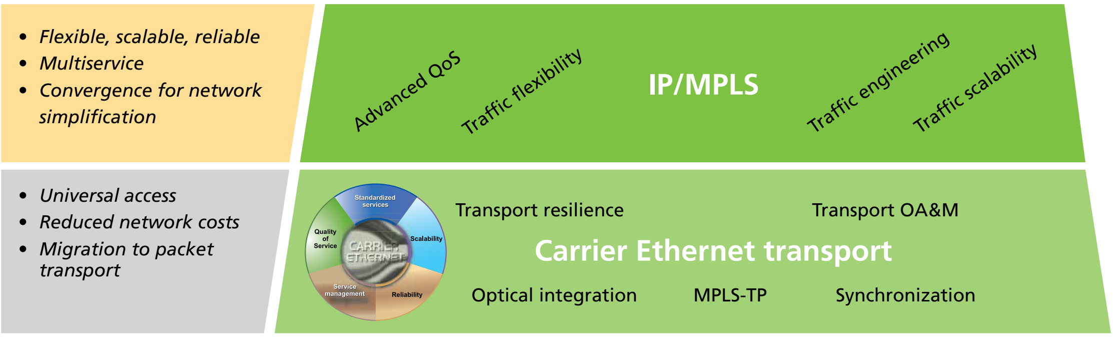
WHAT IS CARRIER ETHERNET TRANSPORT?

Carrier Ethernet transport combines the traditional efficiencies of Ethernet with the carrier-class transport capabilities of OA&M, manageability and protection. With low-cost Ethernet interfaces, EoS efficiently delivers Carrier Ethernet transport for the increasing packet traffic while the majority of traffic is TDM. As packet traffic begins to dominate, MPLS-TP becomes the choice for Carrier Ethernet transport. This connection-oriented packet-transport technology, based on MPLS frame formats, provides resiliency and OA&M capabilities similar to SONET/SDH while maintaining the benefits associated with packet-based networking. MPLS-TP evolves to enable operational convergence with IP/MPLS domains.

Carrier Ethernet is a fundamental technology throughout the Alcatel-Lucent Mission-critical WAN Infrastructure. Carrier Ethernet consists of the following, as shown in Figure 2:

- *Carrier Ethernet transport* — Provides cost-efficient, resilient, bulk transport, with:
  - ¬ Flexibility to create, route and monitor capacity where and when it is required
  - ¬ Operational efficiency
- *IP/MPLS* — Allows abstraction of the service layer from the transport layer, with ubiquitous, scalable, far-reaching and operationally consistent means of delivering mission-critical, legacy and new broadband-multimedia packet-applications traffic and the associated attributes (for example, high availability, QoS, traffic engineering, ease of provisioning and flexibility)

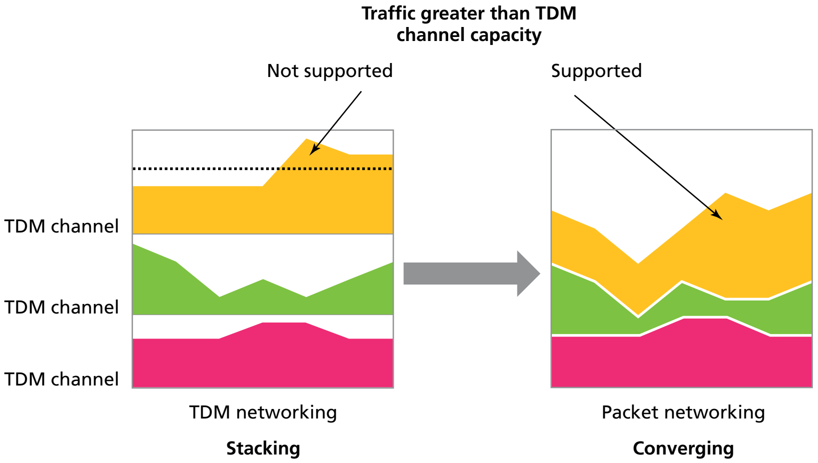
Figure 2. Alcatel-Lucent Carrier Ethernet



Microwave and optical SONET/SDH transport evolve with the addition of Ethernet capabilities to provide Carrier Ethernet transport. This evolution is essential as IP traffic increasingly dominates the network with new applications for bandwidth efficiency and seamless traffic migration.

Rather than stacking individual time division multiplexing (TDM) channels to increase bandwidth to support increasing applications traffic, TDM, IP and ATM are converged and packetized for more efficient support while providing priority to mission-critical traffic. (See Figure 3.) This is particularly important for the cost-effective support of new bandwidth-intensive IP applications that include streaming video and digital imaging. With constrained funding, current investments must cost-effectively scale to address many years of new applications-traffic growth.

Figure 3. Transforming to packet networking to optimize overall bandwidth

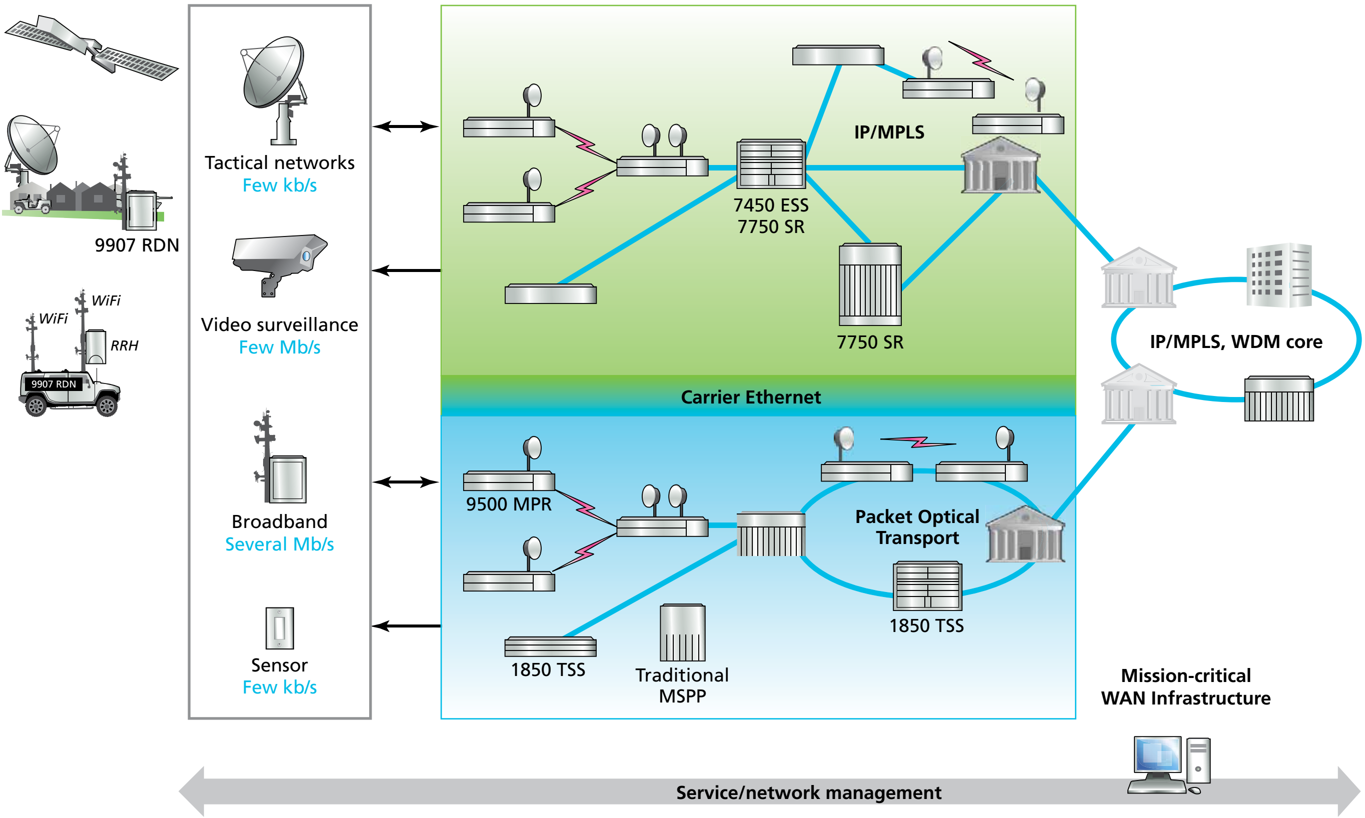


Efficient Carrier Ethernet transport can be realized with the SONET/SDH network support of increasing packet traffic using Ethernet over SONET/SDH (EoS) while the majority of traffic is TDM. The increasing packet traffic is supported using low-cost Ethernet interfaces while offering carrier-class capabilities for OA&M, manageability and protection. Because TDM traffic is still the majority of traffic on most defense department WANs, multiservice provisioning platforms (MSPPs) are well suited to provide Carrier Ethernet transport by adapting a circuit-switched technology, SONET/SDH, to transparently carry IP/Ethernet traffic.

A new category of transport devices, Packet Optical Transport Systems, allows defense departments to leverage their existing SONET/SDH networks while concurrently deploying and migrating to robust packet transport with feature-rich Ethernet — all using the same Packet Optical Transport platform. These platforms effectively support both TDM and packet traffic in any ratio, SONET/SDH and Ethernet, and the emerging MPLSTP. Seamless TDM-to-packet migration can be achieved with Packet Optical Transport while realizing the benefits of Carrier Ethernet transport.

The expansion of a WAN to bring together new packet-applications traffic and communications for a growing number of defense departments often compels the addition of an IP/MPLS core to a Carrier Ethernet transport solution, as shown in Figure 4. IP/MPLS flexibly delivers the required performance for new packet- and legacy-applications traffic in a converged network, in an operationally consistent manner. Alcatel-Lucent carrier-grade “always-on” Carrier Ethernet solutions over IP/MPLS are engineered for high reliability, and convergence across the core IP and optical layers enables continuously scalable and dynamic bandwidth. Integrating the optical and IP domains using cross-layer automation greatly improves operational efficiencies while reducing costs and carbon footprint.

Figure 4. Alcatel-Lucent Mission-critical WAN Infrastructure enables cost-effective, reliable IP transformation for a range of topologies



In a greenfield application or when the majority of traffic is packet-based, a fully converged, IP/MPLS-based Alcatel-Lucent Mission-critical WAN Infrastructure can be the optimal path. From a network-architecture perspective, this consists of a converged IP/MPLS-based core complemented by a converged, IP/MPLS-based access. Transformation to an all-IP/MPLS WAN provides the required scalability, reliability and QoS while dramatically simplifying the network and lowering operating expenditures (OPEX). This single converged, multiservice network, which leverages the power and commonality of Ethernet and IP and is application aware, can cost-effectively enable the creation and delivery of more dynamic, flexible applications traffic to boost mission effectiveness.

The converged Alcatel-Lucent Mission-critical WAN Infrastructure simplifies and reduces OPEX with end-to-end service and network management that includes integrated MPLS/microwave management and optical/microwave transport management. Evolution to a converged network is essential for improving management efficiencies and reduces training requirements for technical staff. In addition, a converged network provides industry-standard interfaces for operations support system (OSS) integration.

This infrastructure builds on key elements of the Alcatel-Lucent High Leverage Network™ (HLN) architecture for carriers. High availability, scalability and application awareness ensure the delivery of all essential information, when and where it is needed, for a coordinated multi-department response. Real-time, mission-critical operations information and routine voice and data information are reliably communicated in this converged environment, between decision makers and warriors and/or securely between deployed forces in the battle space.

WHAT IS THE ALCATEL-LUCENT HIGH LEVERAGE NETWORK?

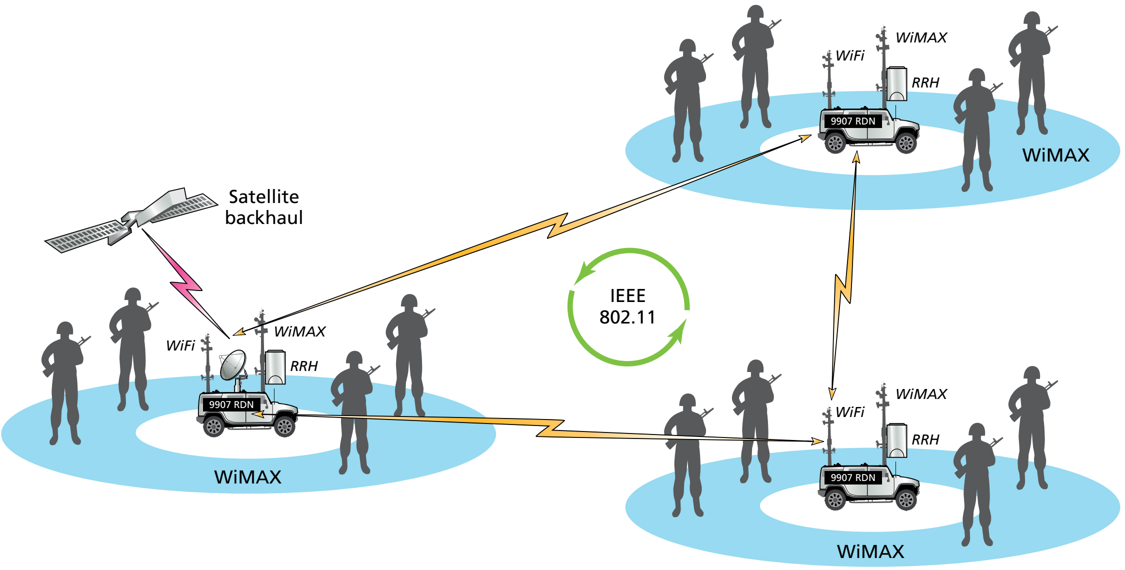
The Alcatel-Lucent HLN is a fully converged network that provides continuous scaling of bandwidth across multiple dimensions, from access to transport, at the lowest TCO. At the same time, the network is equipped with built-in application awareness, QoS and traffic optimization to provide the appropriate levels of network intelligence at the optimum cost. In addition, the Alcatel-Lucent HLN offers high reliability and availability, improved security, application assurance and enhanced policy management.

2.3 Alcatel-Lucent 9907 Rapidly Deployable Network (RDN)

The Alcatel-Lucent 9907 Rapidly Deployable Network (RDN) allows a highly mobile force — for example, an advance party or patrol — to quickly establish secure tactical or operational voice, data, video and sensor communications, extending C4I into areas where communications do not exist or are unsuitable for military use. The Alcatel-Lucent 9907 RDN can be up and running in less than ten minutes, set up by personnel using only basic technical skills. When the power, WAN and antenna connections have been made, the unit self-configures with the push of a button and continually self-optimizes.

At only 10 kg (22 lb) and the size of a shoebox, the Alcatel-Lucent 9907 RDN is incredibly compact and mobile while maintaining a standards-based approach. The unit connects to the Alcatel-Lucent Mission-critical WAN Infrastructure using satellite, wireless, microwave or terrestrial facilities through its IP/Ethernet or WiMAX WAN connections. Multiple Alcatel-Lucent 9907 RDNs within range of each other can mesh together using IEEE 802.11, creating an ad hoc network as shown in Figure 5. User connections are Ethernet — Category 5 cabling (CAT5e)/Gigabit Ethernet (GigE) — or WiMAX, allowing for incredible application and user-terminal flexibility.

Figure 5. Mobile ad hoc Alcatel-Lucent 9907 RDNs



In addition to its ruggedized construction (temperature, shock and vibration), Alcatel-Lucent 9907 RDN support for the following makes it ideal for tactical military communications:

- Advanced Encryption Standard 128 (AES-128) and AES256 encryption
- Certification to Federal Information Processing Standard (FIPS) 140-2 Level 2
- Common Criteria for Information Technology Security Evaluation (CC) Evaluation Assurance Level (EAL) 3+ compliant security

With power options of +12 V DC, +24 V DC and -48 V DC and power consumption of less than 90 W — 200 W with recommended radio frequency (RF) equipment — the Alcatel-Lucent 9907 RDN is well suited for both semi-permanent and highly mobile environments that have solar backup.

WHAT IS THE ALCATEL-LUCENT 9907 RAPIDLY DEPLOYABLE NETWORK?

The Alcatel-Lucent 9907 RDN is a compact, self-contained Fourth Generation (4G) network-in-a-box that enables highly mobile units to quickly establish a trusted network for secure, real-time mission-critical voice, video, data and sensor communications. With auto-configuration and dynamic, real-time optimization features, the Alcatel-Lucent 9907 RDN can be fully operational in ten minutes or less and operates with minimal user intervention. The Alcatel-Lucent 9907 RDN can be deployed as a single-cell solution for local communications, or optionally as an ad hoc network with multiple nodes. The fully rugged system is approximately the size of a shoebox and weighs about 10 kg (22 lb). The system utilizes standards-based interfaces such as Ethernet or WiMAX (IEEE 802.16e-2005), with a software upgrade path to LTE.

3. New applications, new capabilities

The majority of today's defense department communications networks are not equipped to support dynamic communications and real-time monitoring. Key capabilities that are driving changes in the department WANs include enhancing intra-/inter-department communications, LMR/PMR digital upgrades, remote monitoring, and rapid access of field personnel to new broadband applications that include new sources of streaming video and digital images.

3.1 Convergence and physical connectivity: the foundation for effective communications

The environment in which personnel operate continues to grow in complexity as new technologies are integrated into our everyday life and into terrorist threats. The involvement of specialists and experts in a coordinated joint task-force operation is often critical for delivering the appropriate response and ensuring rapid recovery. Defense departments are first converging their existing traffic as well as new IP-based applications traffic onto a common WAN backbone to reduce complexity and lower OPEX. At the same time, they are dynamically extending their WAN footprint to include forward-operations areas in a single converged network.

Within this common WAN, a VPN can be created to securely transport the department's traffic among its sites along with gaining flexibility for the sharing of specific information at designated times within alliance forces. This new connectivity may also enable improvements in reliability, including new redundant physical paths and backup centers — for example, when communications back to a command post are interrupted, calls may be automatically rerouted to an alternate location that is also connected to the WAN, creating redundancy that may not have previously been feasible.

Managing the whole is simpler and less expensive than managing current application-specific networks because of the addition of end-to-end IP/MPLS/Ethernet service management and common optical and microwave transport management. Management centers can be safely located in secure territory, reducing the load on field personnel and facilitating access to civilian-vendor support. Advantages are amplified because there is a single network to manage instead of multiple, application-specific networks, each of which could require separate management. Security policies can be centralized, ensuring their application and improving their enforceability. IP-address management is also centralized, along with distributed protection, for a truly secure, scalable solution.

3.2 Microwave packet radio

Microwave packet radio, which is capable of natively handling multiple packet types, introduces a new concept in backhaul applications: the ability to transport multimedia traffic efficiently and still support legacy TDM traffic. Microwave packet radio aggregates packet and legacy TDM traffic, increases bandwidth utilization and optimizes Ethernet connectivity, enabling the non-linear cost-capacity model required to support broadband traffic. Microwave packet radio technology is a long-term enabler for defense departments to smoothly transition their backhaul networks from TDM to IP and include broadband wireless, for dramatic reductions in OPEX — for example, up to 40 percent TCO reduction with the Alcatel-Lucent 9500 Microwave Packet Radio (MPR) compared with a TDM current mode of operation.

WHAT IS MICROWAVE PACKET RADIO TECHNOLOGY?

The Alcatel-Lucent 9500 Microwave Packet Radio uses a multiservice aggregation layer to provide the capacity to use Ethernet as a common transmission layer to transport any kind of traffic. All traffic is converged over a single packet-transport layer using industry-standard pseudowire and circuit-emulation technologies. Service awareness supports different traffic types with different requirements and priorities, optimizing bandwidth with the option of overbooking radio capacity for non-real-time traffic and variable bit-rate traffic.

3.3 Broadband applications in the field

Access to high-speed data and multimedia allows personnel to have a virtual “desktop in the field” and enhances communications among warriors and decision makers. Arming personnel with advanced multimedia capabilities allows instant access to mission-critical data, giving them the ability to exchange information such as surveillance and tactical video, digital imaging, 3-D mapping/GIS and remote database access across multinational or elemental boundaries. This accurate, up-to-date information can help save lives and minimize additional risks by achieving greater speed of command while increasing lethality, survivability and responsiveness.

Capacity is just one element to consider in planning for the addition of broadband capabilities for mobile personnel. When broadband is added to existing voice, multiple traffic types are simultaneously introduced, with different requirements in terms of capacity, availability, quality and use of available resources. With the Alcatel-Lucent 9907 RDN and the service-aware Alcatel-Lucent Mission-critical WAN Infrastructure, Alcatel-Lucent has the unique ability to provide highly mobile broadband tactical networks, with service-aware QoS mechanisms to ensure the integrity of all traffic types over a single network, from source to destination.

4. Enabling operational optimization

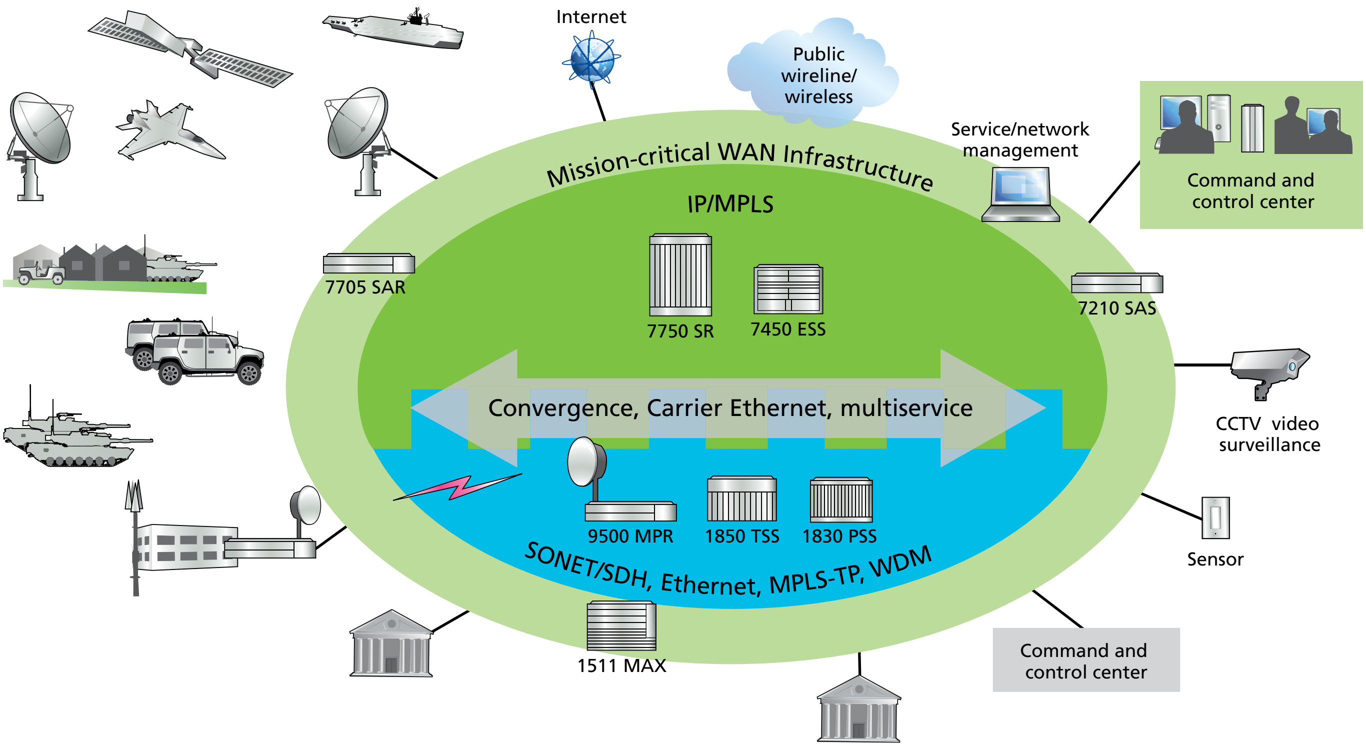
Service-oriented IP/MPLS and Carrier Ethernet transport networks have the inherent capability to support new applications, providing new ways for personnel to work efficiently, share information and interact responsively. New information systems provide the ideal opportunity for personnel to acquire knowledge, centralize it and make it accessible to the whole organization. The appropriate WAN gives the appropriate staff seamless, secure access to centralized information no matter where they are, thereby boosting productivity.

It is ironic that, when all is calm, communications traffic is at a minimum and the network is nearly idle aside from internal administrative and operational applications. For example, packet-based video surveillance systems update video frames only when there is a change in the video picture, and packet voice communication rarely transmits silence. Both these techniques save considerable amounts of bandwidth when used correctly. However, as soon as peace is shattered by fast-moving vehicles, massing crowds, riots or other threats, data throughput increases instantaneously.

CCTV video traffic increases, security-force voice traffic increases, and collaboration tools such as database queries and document transfers increase substantially as status is acquired. The network, which is instantaneously flooded with traffic from all sources, must know which data streams contain delay- and jitter-sensitive applications traffic and which can tolerate delay and or jitter without negatively impacting user experience or application integrity so that it can deal with each appropriately.

The nodes in the Alcatel-Lucent Mission-critical WAN Infrastructure, shown in Figure 6, have been designed from the ground up for high availability, using advanced hierarchical QoS (H-QoS) technology that guarantees on-time delivery of the most critical and time-sensitive communications. Alcatel-Lucent Carrier Ethernet allows specific applications traffic to be optimized using service-adapter modules, within Ethernet service switches and service routers that are designed to enhance specific application flows.

Figure 6. Alcatel-Lucent Mission-critical WAN Infrastructure for reliable communications, select applications-traffic optimization and reduced OPEX


Internet
Public wireline/ wireless
Service/network management
Command and control center
Mission-critical WAN Infrastructure
IP/MPLS
7705 SAR
7750 SR
7450 ESS
7210 SAS
Convergence, Carrier Ethernet, multiservice
9500 MPR
1850 TSS
1830 PSS
SONET/SDH, Ethernet, MPLS-TP, WDM
1511 MAX
CCTV video surveillance
Sensor
Command and control center

The evolution of a defense department's WAN by adding IP/MPLS or a new microwave link often allows the department to cost-effectively introduce a higher level of redundancy to parts of its network where SONET/SDH is not present, making extensive use of Ethernet interfaces to reduce costs. The continuing evolution of current optics and microwave technology with Carrier Ethernet transport allows the reliable, scaled aggregation and transport of any traffic type, at the lowest cost per bit.

The widespread value that next-generation SONET/SDH and WDM are bringing to support TDM has emerged during the lengthy TDM evolution. The addition of MPLS-TP extends this value as packet traffic dominates and provides further evolution toward operations consistency across transport and IP/MPLS domains, simplifying operations and reducing costs. These technologies can simultaneously handle TDM and IP, reducing investment risk and allowing seamless switching between the two depending on the traffic mix.

Advanced service and network management systems allow for centralized network management and advanced diagnostic capabilities, minimizing TCO and reducing down time. A Forrester® Research, Inc. study identified a 75 percent increase in provisioning productivity and 25 percent fewer dispatches with Alcatel-Lucent 5620 Service Aware Manager (SAM) management of four carrier networks that have infrastructure similar to that of a large, multiple defense department WAN.

5. Ensuring security

Defense departments rely heavily on increased connectivity among sensors, command nodes and weapons. Network security is a high priority: securing critical infrastructure from physical and electronic threats is of paramount importance to defense departments worldwide. Optical and microwave SONET/SDH networks are, by definition, carrier-grade, implementing security at the physical layer.

Using MPLS, which is also carrier-grade, network virtualization is possible, with separate virtual networks for different voice, video and data applications such as VoIP, video surveillance and LMR/PMR traffic backhaul. These virtual networks are securely separated as if they were individual networks. Using MPLS VPN technologies, it is possible to provision virtual networks with controlled levels of security and QoS for different applications or defense organizations. For example, a VoIP application can be provisioned with reserved bandwidth to ensure the quality of the conversation even during peak usage. Within the Alcatel-Lucent Mission-critical WAN Infrastructure, a VPN can be created with MPLS for secure inter-department sharing of specific information at designated times.

Evolving from many application-specific networks to a service-oriented IP/MPLS network allows for centralized security-policy enforcement and the implementation of sophisticated electronic security measures that protect communications from being compromised.

6. The Alcatel-Lucent offering

As a proven telecommunications partner, Alcatel-Lucent understands defense department-specific communications requirements. Our market-leading communications portfolio delivers solutions for mission-critical communications in complex environments. With the Alcatel-Lucent Mission-critical WAN Infrastructure, defense departments gain the benefits of:

- **Mobility**
  Innovative products such as the Alcatel-Lucent 9907 RDN, advanced network and service management, and our broad family of standards-based products enable highly mobile operations while providing the full voice, data, video and sensor capabilities necessary to improve situational awareness and increase mission effectiveness.
- **Critical-infrastructure protection**
  CCTV or video surveillance and remote sensors help facilitate early detection and improve situational awareness. Physical assets can also be protected and centrally monitored by extending WAN communications to these sites. Video surveillance can help protect critical infrastructure in high-risk or politically unstable areas. The Alcatel-Lucent converged WAN can cost-effectively scale to deliver several megabits of bandwidth per site: a typical requirement for solutions with enhanced capabilities such as high resolution and remote operation. Using a combination of an IP multicast protocol and MPLS-based VPLS, video surveillance and sensor traffic can be distributed to primary and secondary remote monitoring centers with guaranteed QoS for increased reliability and flexibility.
- **Flexible, scalable convergence of growing packet (digital LMR/PMR, video surveillance, broadband applications) and legacy traffic**
  Alcatel-Lucent solutions deliver a flexible, scalable WAN with carrier-grade IP/MPLS and Ethernet capabilities, leveraging our broad, industry-leading access, IP, optical and microwave portfolio for cost-effective support of a range of applications.
- **Reliable C4I with an end-to-end, carrier-grade infrastructure**
  Alcatel-Lucent provides a rugged, reliable, scalable and secure WAN built on innovative, high-reliability products and backed by our expertise in delivering complex, mission-critical networking to meet defense department requirements. Alcatel-Lucent solutions incorporate non-stop routing, redundancy, MPLS task rerouting in IP/MPLS parts of the network, and ring protection for optical and microwave packet networks.
- **Simplified mission-critical WAN transformation and reduced OPEX**
  The Alcatel-Lucent MPLS/Ethernet solution provides end-to-end IP/MPLS and Ethernet service management as well as integrated optical/microwave transport management, cost-effectively addressing a range of applications with common management to simplify the network and reduce costs. Centralized security-policy administration and distributed protection simplify, scale and enhance security.
- **Packet evolution of transport networks**
  The longstanding leadership of Alcatel-Lucent in optical SONET/SDH and WDM technologies enables the optimal solutions to evolve and transform current optical and microwave networks, supporting increasing packet-based traffic with Carrier Ethernet transport.
- **Reduced risk and WAN-transformation costs**
  The Alcatel-Lucent Worldwide Services team provides end-to-end solution support and end-to-end management with multivendor capabilities, resulting in lowest TCO.

The Alcatel-Lucent Mission-critical WAN Infrastructure is a key component of the Alcatel-Lucent Dynamic Communication Solutions for Defense.

6.1 Innovations in eco-sustainability

Innovations in eco-sustainable networks and applications can help defense departments reduce costs while dramatically reducing their environmental footprint. Key focus areas for Alcatel-Lucent are energy efficiency, a reduced carbon footprint and environmental sustainability. Alcatel-Lucent helps defense departments realize benefits by reducing TCO and CO_2 emissions with a holistic approach across each network layer. Some proof points include:

- Packet microwave and optical transport platforms that use 62 percent to 65 percent less power per transported bit than traditional platforms by forwarding traffic to the most efficient and economic layer — packet, circuit or optics/wavelength
- IP/MPLS platforms that leverage intelligent, dynamic powering methods and operate at voltages and frequencies that are no higher than necessary to achieve the desired functionality and performance

7. Conclusion

Today's modern network is a key component in increasing mission effectiveness by providing shared battle space awareness: enhanced situational awareness in the field and precise, current intelligence at headquarters that is necessary for effective C4I. A robust, scalable, flexible and highly available network that enables a highly mobile force is essential. Sensors, CCTV, applications, procedures and other assets combine with the network to protect critical infrastructure and enable operational capabilities.

A transformation of the defense department WAN is a typical first step in addressing these challenges and realizing the benefits of new applications. The transformation includes expanded bandwidth, flexibility and network reach along with new capabilities to cost-effectively combine legacy traffic with the growing IP-based applications traffic. The transformed WAN provides the required foundation for sensors, broadband streaming video, imaging and video surveillance capabilities. The capital investment is significant, and the solution needs to be flexible, proven and reliable. A carrier-grade, mission-critical infrastructure is the only acceptable level of quality for military applications.

Alcatel-Lucent is driving the evolution and convergence of today's WANs with new IP/MPLS and packet transport standards. The Alcatel-Lucent Mission-critical WAN Infrastructure has been deployed by more than a dozen public-safety agencies and defense departments worldwide. The company is an expert multivendor integrator in mission-critical communications projects. With our broad microwave, IP/MPLS and optical portfolio, end-to-end management, defense industry experience and the Alcatel-Lucent Mission-critical WAN Infrastructure offering, Alcatel-Lucent has all the elements to simplify and reduce WAN-transformation risks.

8. Abbreviations

4G	Fourth Generation
1511 MAX	Alcatel-Lucent 1511 Media Access Cross-Connect
1830 PSS	Alcatel-Lucent 1830 Photonic Service Switch
1850 TSS	Alcatel-Lucent 1850 Transport 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
9907 RDN	Alcatel-Lucent 9907 Rapidly Deployable Network
AES	Advanced Encryption Standard
ATM	Asynchronous Transfer Mode
C4I	command, control, communications, computers, and intelligence
CAT5	Category 5 cabling
CCTV	closed-circuit television
CEC	Cooperative Engagement Capability
CIP	critical-infrastructure protection
COTS	commercial, off-the-shelf
CSS	combat service support
DCI	defense critical infrastructure
DII	Defense Information Infrastructure
DoS	denial of service
EoS	Ethernet over SONET/SDH
FIPS	Federal Information Processing Standard
GigE	Gigabit Ethernet
GIS	geographic information system
H-QoS	hierarchical QoS
HLN	High Leverage Network
IP	Internet Protocol
IT	information technology
LMR	Land Mobile Radio
LTE	Long Term Evolution
MEF	(former) Metro Ethernet Forum
MPLS	Multi-Protocol Label Switching
MPLS-TP	MPLS Transport Profile
MSPP	multi-service provisioning platform
NE	network element
NGO	non-governmental organization
NIPRNET	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
OA&M	operations, administration and maintenance
OPEX	operating expenditures
OSS	operations support system
P25	Project 25
PMR	Professional Mobile Radio
PSTN	Public Switched Telephone Network
PTT	Push-to-Talk
QoS	quality of service
RF	radio frequency
RRH	remote radar head
SATCOM	satellite communications
SDH	Synchronous Digital Hierarchy
SIPRNET	Secret Internet Protocol Router Network
SONET	Synchronous Optical Network
TADIL	Tactical Digital Information Link
TCO	total cost of ownership
TCP	Transmission Control Protocol
TDM	time division multiplexing
TETRA	Terrestrial Trunked Radio
VIP	very important person
VoIP	Voice over IP
VPLS	virtual private LAN service
VPN	virtual private network
WDM	wavelength division multiplexing
WiMAX	Worldwide Interoperability for Microwave Access

9. Further information

For more information about the Alcatel-Lucent Mission-critical WAN Infrastructure and the Alcatel-Lucent 9907 RDN, please visit www.alcatel-lucent.com or contact your Customer Team representative.

10. References

1. COM(2006) 786: *Communication From the Commission on a European Programme for Critical Infrastructure Protection*. December 12, 2006.
   http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf
2. Common Criteria for Information Technology Security Evaluation (CC).
   http://www.commoncriteriaportal.org/thecc.html
3. FIPS 140-2: *Security Requirements for Cryptographic Modules*. NIST, May 25, 2001.
   http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
4. FIPS 197: *Advanced Encryption Standard (AES)*. NIST, November 26, 2001.
   http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
5. HSPD 7: *Critical Infrastructure Identification, Prioritization, and Protection*. December 17, 2003.
   http://www.fas.org/irp/offdocs/nspd/hspd-7.html
6. IEEE 802.11: *LAN/MAN Wireless LANs*.
   http://standards.ieee.org/getieee802/802.11.html
7. IEEE 802.16e-2005: *Amendment to IEEE Standard for Local and Metropolitan Area Networks – Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands*. February 28, 2006.
   http://www.ieee802.org/16/pubs/80216e.html
8. PDD 63: *Protecting America's Critical Infrastructures*. May 22, 1998.
   http://www.fas.org/irp/offdocs/pdd-63.htm

Alcatel·Lucent