Network Strategy and Vision for the Enterprise – Where Everything Connects

Laying the network foundation for digital transformation

Strategic White Paper
Network Strategy and Vision for the Enterprise – Where Everything Connects
December 2019

Alcatel·Lucent Enterprise

Contents

Introduction: New technologies are driving the network evolution

Companies and institutions need to integrate the latest digital innovations in mobility, data analytics, cloud computing and IoT to their existing business and computing systems if they are to gain business advantages. This process, known as digital transformation, delivers many benefits, enabling businesses and organizations to create more efficient processes, differentiate products and services, better satisfy customers and employees, increase revenues and reduce costs.

As companies and institutions embark on digital transformation, they learn that their underlying network infrastructure is the fundamental enabler of digital transformation. Yesterday's network architectures aren't equipped to support today's user needs—or the new technologies that enterprises must implement to keep ahead of the competition and support digital transformation.

Evolutions in mobility, the Internet of Things (IoT) and data analytics are directly impacting network infrastructures, driving enterprises to reconsider their network technology choices. Legacy infrastructures are often unable to support the new use cases and business scenarios that integrate these new technologies, and are unable to ensure they can operate securely and efficiently. These aging infrastructures may not support the new wave of multimedia applications because they were never designed to provide the capacity needed to meet the instant-on, multi-device load generated by today's business. In this landscape of transformation, companies and institutions must rethink the very foundation of the network to reduce costs, improve performance and security, and support new devices, technologies and business use cases.

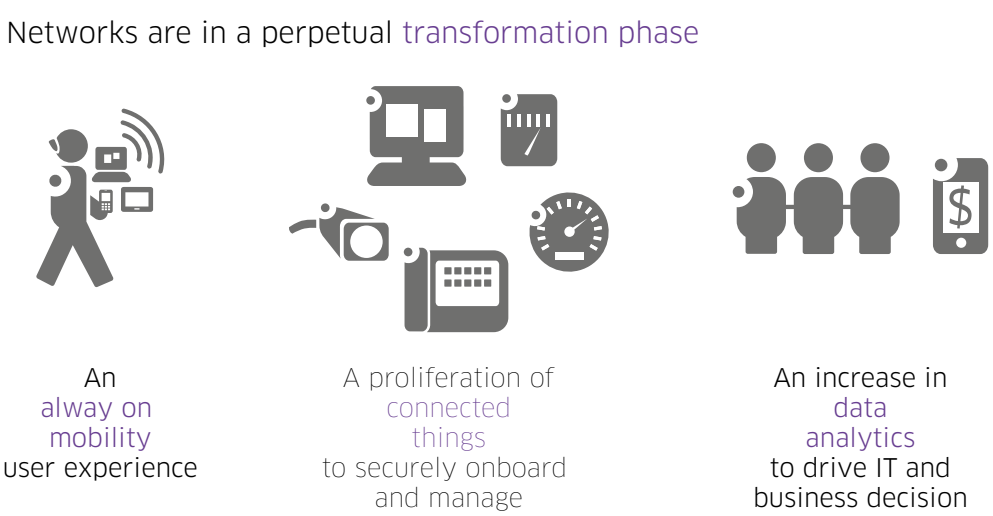
Drivers for network transformation

A set of key trends is driving the need for transformation of enterprise networks and the evolution of network infrastructure in key vertical markets.

Mobility. The proliferation of mobile devices connecting to the corporate network is the single most important factor driving the need for evolving the network. Wireless connectivity has become the lifeblood of the enterprise, as users now expect an always-on mobility experience, with mobile-first networking models becoming the norm, requiring pervasive wireless connectivity. Wi-Fi is the dominant wireless networking standard, as it allows users to be located virtually anywhere and to use almost any device. However, as use of mobile devices increases, existing networks can easily be overwhelmed with increasing bandwidth demands.

New mobile-ready networks will need to ensure that all devices coming into the enterprise environment get their fair share of network resources with connectivity everywhere and the same quality of experience (QoE) and quality of service (QoS) over wired or wireless networks.

Figure 1. Mobility, IoT, and data analytics are key drivers of network transformation



A subset of the larger mobility trend is the Bring Your Own Device (BYOD) movement: Employees bring their own private devices to work and connect them to the corporate network. This can be a cost-saving benefit to the organization and a convenience to employees, but implementing BYOD securely and effectively presents a lot of challenges to IT staff. Many vertical IT networks weren't designed to easily onboard and support a diversity of devices and protocols, and the underlying infrastructure must be sound enough to support multiple disparate devices and networks while guaranteeing interoperability and security.

IoT. The Internet of Things' automated data flows, derived from mass networks of connected devices and sensors has the potential to transform business in significant ways. Organizations that deploy IoT networks can successfully analyze real-time data to better understand customer needs, proactively monitor critical infrastructure and create more efficient processes. With potential benefits like these, it's no wonder IoT networks are increasingly popular: According to analyst firm Gartner, 20.4 billion IoT devices will be deployed globally by 2020.[1]

However, IoT networks generate unprecedented volumes of data, opening challenges for network management and security. Even small IoT systems can put a tremendous amount of pressure on an organization's underlying network infrastructure, as each IoT sensor and device represents an entry point for potential security threats. To gain the benefits of IoT, organizations will require a cost-effective network infrastructure that simplifies IoT device on-boarding, ensures system security and is easy to manage and operate.

Data analytics. Organizations increasingly rely on big data analytics to drive IT and business decisions. All of an organization's internal data flows through the enterprise network, which must be resilient, high performing and scalable to handle ever increasing volumes of traffic. These network data flows now also produce their own performance and inspection data, enabling new IT services and providing insights into network operational efficiency and agility. These network services create a kind of self-monitoring network consciousness and intelligence that enables automation of certain IT functions, increasing network security, resiliency and management simplicity.

Increased security. With the growth of mobility and IoT also comes an explosion of cyber security threats, as proliferation of sensors and mobile and connected devices greatly expand the network attack surface. Cyber-attacks are increasing in volume, in complexity and in recovery cost, and the expense isn't limited to direct financial loss or remediation (the global average cost of a data breach is US$3.62 million, or an average cost of US$141 for each lost or stolen record[2]). Cyber attacks and security breaches also result in high cost or damage toa company's brand and reputation.

Cyber attacks can take on many forms, and some of the most dramatic involve vulnerabilities in mobile and IoT networks. The distributed denial-of-service attack on Dyn in October 2016 that brought down much of the Internet was perpetrated through hacked networked devices such as security cameras and digital video recorders.[3] Hackers attacked the network of San Francisco public transit system Muni in November 2016, rendering ticket machines and other computing infrastructure inoperable as part of a ransomware scheme.[4]

The electronic key system at Austria's Romantik Seehotel Jaegerwirt was hacked in January 2017, leaving guests locked out of their rooms and the hotel locked out of its own computer system, until the hotel paid the ransom.[5]

More flexible investment models. The need for increased bandwidth, security and manageability aren't the only trends that impact modern networks. New investment models that better align with today's business environment and the requirements of specific vertical industries are also necessary. In addition to traditional CAPEX investment, the network infrastructure market also demands cloud services and pay-as-you-go, network-on-demand models that reflect how modern businesses operate.

1 Gartner Says 8.4 Billion Connected «Things» Will Be in Use in 2017, Up 31 Percent From 2016
2 2017 Ponemon Cost of Data Breach Study
3 Hacked Cameras Were Behind Friday's Massive Web Outage
4 Metro transport systems eyed after hack attack in San Francisco
5 Hackers Use New Tactic at Austrian Hotel: Locking the Doors

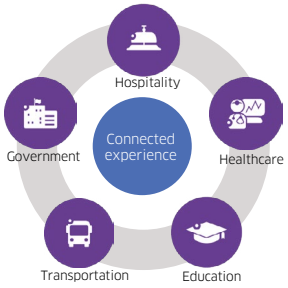
A strategic approach to a more connected enterprise

An organization's network infrastructure has a critical role to play in mitigating these risks while allowing businesses to take full advantage of increased mobility and connected devices.

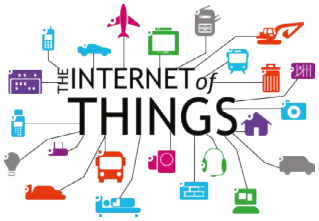
ALE has a strategy to address these challenges and opportunities. Our strategy is supported by three pillars:

- **Deliver secure mobile and IoT networks** by properly onboarding, managing and securing all elements of the network. ALE is a technology leader in secure mobile and IoT-enabled networks, backed up with sophisticated analytics and management systems.
- **Deliver network business services** that align with our customer's business objectives and their investment strategies. ALE offers flexible business models for providing network services, including CAPEX, OPEX and cloud-managed hybrid infrastructures.
- **Deliver a verticalized connected experience** for our customers by providing value-added solutions and dedicated integration and capabilities designed for specific industry ecosystems in healthcare, education, transportation, government and hospitality.

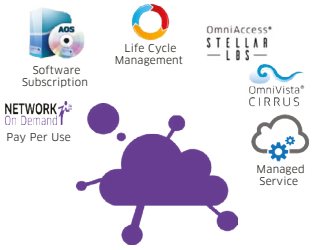
Figure 2. Three pillars of the ALE strategy for Networks



Verticals' connected experience



Secured networks for mobility and IoT



Network business services

ALE provides high performance networks for mobility and IoT

ALE provides high performing products and services across the entire network infrastructure, with high-bandwidth capability at all levels. ALE switches, access points and controllers support the latest generation of high bandwidth, low latency capabilities and can manage large numbers of devices in high density environments.

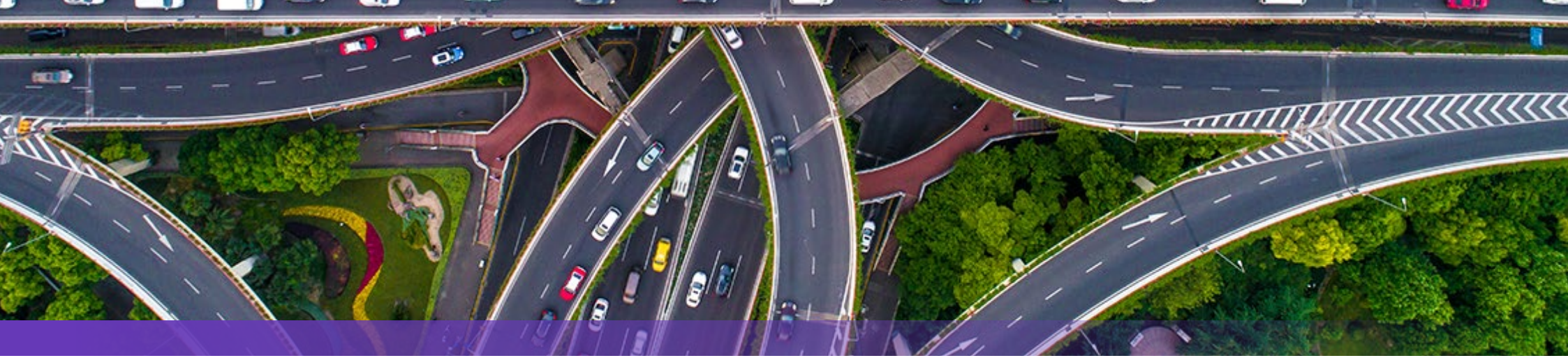
In addition, ALE networking products and solutions can address the networking needs for organizations of all sizes.

ALE also provides a single, integrated operating system that enables its customers to address the complexities of managing campus and data center networks with a truly unified approach.

Key elements of ALE network infrastructure are:

- Network core products, which include high-performance wire-rate and data center switches that provide high port density and switching capacity from 10G to 100G.
- WLAN infrastructure with innovative distributed intelligence control to deliver high speed wireless services to small, medium and large networks, built on the latest 802.11ac protocol for high density deployments.
- The ALE Unified Access framework, which allows wired and wireless technologies to work together as a single, robust network. Users experience the same high-quality performance using Wi-Fi or connections via an Ethernet cable.
- Unified policy management, which provides a common set of network services, a policy framework, a common authentication scheme and a single authentication database, is applied to all users accessing the network with either wired or wireless devices.
- A truly unified management solution, which provides a single-pane-of-glass view to manage and filter the complexity of the networking infrastructure, providing in one single place all the tools needed to provision, monitor, analyze and troubleshoot the network.
- WAN access routers and switches to ensure high-speed, secure access to internal resources from anywhere within the network.
- ALE network technologies enable full network virtualization, with high performance and end- to-end redundancy through a secure and isolated virtual container provisioned automatically from the access network to the core and WAN. Virtualization of the network layer is a key differentiator of ALE's solution, enabling IT managers to automate the deployment of new IT services while reducing the cost and complexity of operations.

Figure 3. ALE Network portfolio



High performance, secured networks by design

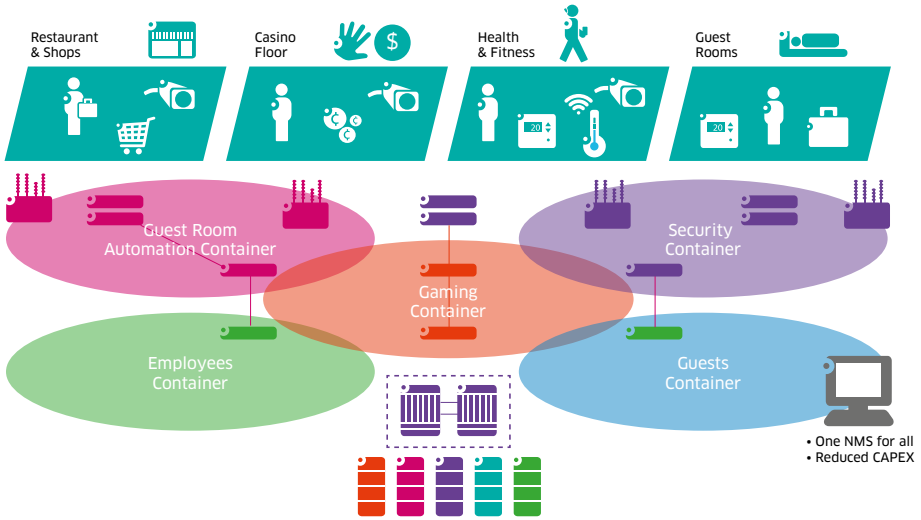
ALE recommends an optimized high performance network design based on a single network infrastructure with a secure, automated, efficient, virtual private network (VPN) for every department. ALE leverages the latest wire-speed (LAN) and Wave 2 (Wi-Fi) technologies to provide the highest level of network performance possible.

From a security standpoint, ALE provides a multi-layered approach to securing the network from the edge, to the core, using a variety of techniques, including user and device profiles, applications and analytics, operating system hardening and IoT containment. ALE uses the award-winning iFab technology to automate the deployment, configuration and management of the network including future moves, adds, and changes. ALE also recommends Shortest Path Bridging (SPB) to optimize network performance and minimize network downtime when adding, removing, or replacing network devices -- no matter the underlying physical architectural design, whether it is a virtual chassis, a pod, a mesh or a spine and leaf configuration.

To ensure that every department's network is separated from each other, we recommend using VPN with IoT containment, so just like physical network separation, IoT containment secures the VPN from access breaches should they occur in other parts of the network. Now, with one physical network infrastructure, you only need one network management system. OmniVista 2500 (server or cloud-based) has the capability to not only configure, manage and control your network, but it can also predict future usage via proactive network statistics, to ensure the network remains capable and scales to support your applications and IoT devices. When combined with Smart Analytics, you know which applications are running in your network and you can optimize and secure your network, users and devices, at the application level. And to ensure the network remains up to date with the latest security enhancements, software and services, Proactive Lifecycle Management (PALM) automates the maintenance of your network on an ongoing basis.

A simple networking approach to solving a multitude of networking challenges, for today and tomorrow.

Figure 4. Multiple virtual private networks over one physical IoT network



Distributed intelligence control. Thanks to the ALE distributed intelligence control technology in WLAN access points architecture, ALE's solution also removes a single point of failure from the network, whether it's a physical or virtual controller. When a central controller is employed, all network traffic must flow through it increasing the latency and the length of the route that the packet must travel to get to its destination.

Due to the speed and capacity of the processors embedded in the access points, the distributed intelligence control technology enables access points to distribute controller features among all the access points in the cluster, as in a blockchain model approach, instead of centralizing controls in a single physical or virtual location. With built-in distributed intelligence, the packet route is always the shortest possible, and thus the latency is the lowest, ensuring that the flow of traffic is always able to properly support the needs of individual users and applications. This helps guarantee that real-time applications, such as voice and video, won't have hiccups, resulting in superior user experience.

With a full set of controller features implemented and running on the distributed intelligence control technology, the system can exceed typical physical and virtual controller performance, enabling such options as:

- Automatic, smart radio optimization
- Coordination among neighboring applications
- Band steering
- Smart load balancing
- Airtime fairness

These options do not rely on a central physical or virtual controller, as they are distributed among all the access points. One of the biggest advantages of this technology is that the network is empowered to self-heal. If one access point goes down, the remaining will increase power to counteract the lost capacity of the failing access point within the network.

A distributed intelligence network also allows easy scalability. A network administrator can simply add an additional access point into the cluster, and the distributed intelligence will take care of the configuration. It also ensures high availability in the WLAN network infrastructure. There is no single point of failure in the architecture, and even in the case of an access point failure, the system counteracts it intelligently bypassing the inactive access point, allowing the infrastructure to self-heal and continue to deliver network services.

Distributed intelligence control architecture also allows QoS, security, application and firewalling rules to be immediately enforced at the edge (the access points) of the network. This is important because these tools allow network administrators to ensure that the network is not wasting bandwidth and the maximum level of security is enforced, starting from the access layer of the network. Finally, distributed intelligence control lowers TCO as there is no need to buy, deploy, power up, manage and maintain a physical controller.

Unified Access framework for policy integration and consistent user experiences

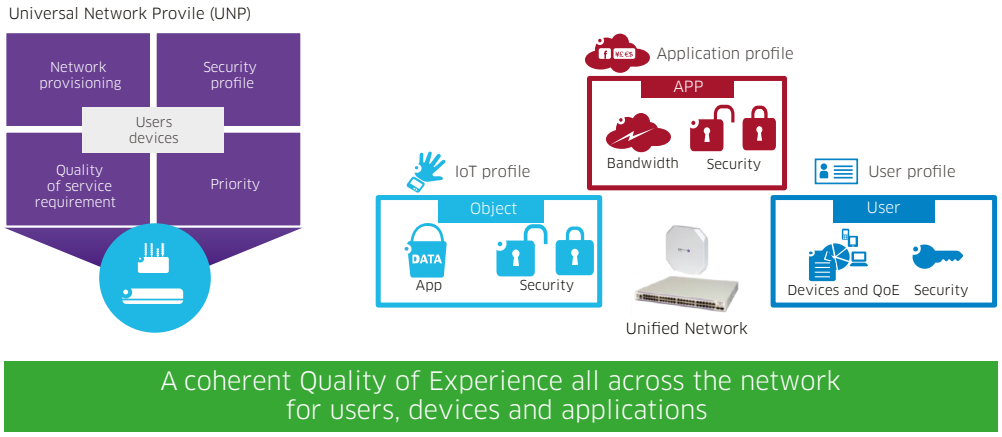
The increasing use of mobility and IoT in the enterprise brings unprecedented challenges to IT departments. IT teams are asked to support more devices with a variety of operating systems, investigate unauthorized applications, support BYOD scenarios, power-up instant-on multimedia devices, and maintain a high-quality user experience—all while IT budgets remain flat or shrink. Given these challenges, a key component needed to achieve these objectives is a comprehensive and unified network policy implementation system.

The Unified Access framework from ALE provides users with a single set of credentials that grants them access to wireless or wired services with maximum security, regardless of the device they use to log in.

The solution provides a common set of network services, policy rules, a single authentication scheme, and a database that is applied to all users, integrated with the corporate user directory. Each user, device and application is assigned a specific profile which includes QoS, priority, security and permissions. It applies no matter whether the connection is wired or wireless.

Unified Access enforces a coherent quality of experience across the network for users, devices and applications; as users move around the organization, they will be treated consistently by the network. It also maintains a consistent level of security throughout the network, and supports always-on, high-density mobile scenarios and pervasive IoT systems. Because both wired and wireless networks are operated by one integrated network with consistent policies, the solution also reduces IT effort.

Figure 5. Mobility and IoT
Unified Access: authentication, authorization, classification



Support for BYOD and IoT. Today's employees expect to be able to connect their own devices to the network, especially those that use smartphones and tablets for both personal and work use. However, the unregulated use of these devices creates unpredictable bandwidth use and increases security risks. To address the complexities of BYOD, ALE provides policy enforcement mechanisms which rely on a management platform that addresses the nuances and capabilities of different devices and operating systems, while guaranteeing a consistent quality of service and security.

ALE network solutions also offer the ability for enterprise visitors, hotel guests, hospital patients and visitors, university students or public transit passengers to easily and securely connect to the internet, leveraging a dedicated and controlled portion of the network.

This comprehensive guest management solution includes:

- Embedded captive portals with different connectivity options offering pre-created credentials, social media login, or live credential validation.
- Integration with external captive portals.
- Automated Virtual LAN (VLAN) logical separation to ensure segregation between guest traffic and employee traffic.

ALE networks also enable IoT devices to easily and securely connect to the network, either wired or wirelessly. ALE provides all the technologies to offer IoT containment, which simplifies the onboarding and management of IoT devices while keeping the network secure.

- When a new device is connected, the network will automatically recognize its profile and place the device in a virtual private network (VPN), ensuring that the device can only access the application platform that it is authorized to connect to.
- In virtual containers, quality of service and security rules are applied to ensure that the IoT system has the necessary resources to run efficiently and securely.
- Multiple virtual containers can be created, deployed, and operated on the same physical infrastructure, creating a virtual segmentation of the physical network.
- By segmenting the network into different virtual containers, if a breach occurs in one, it does not affect the others.

Simplified network operations for greater IT efficiency

In 2015, ALE introduced an award-wining technology called Intelligent Fabric (iFab) to help improve IT efficiency. iFab simplifies design, deployment and operation of the network by automating many tasks that are traditionally performed manually, such as link aggregation creation and Shortest Path Bridging (SPB) neighbor adjacency definition, eliminating human error during configuration. It leverages standards-based protocols for complete interoperability with third-party components and legacy infrastructure. iFab is also applicable in a campus LAN environment to help reduce administrative overhead.

Networks based on iFab offer:

- **Self-configuration.** Administrators define the rules for network management, push them to the core of the network, and the core will automatically configure the rest of the network settings to align with the defined network consciousness.
- **Self-attachment.** Connect access switches and servers to the core network and iFab automatically takes care of the configuration.
- **Automated moves, adds and changes.** iFab dynamically follows users, devices and applications to automatically adapt the right profile for classification, security, bandwidth and priority. Moves and changes are easy: when VMs move, the network dynamically detects and adjusts.
- **Self-healing capabilities** to minimize or eliminate downtime. iFab is resilient and provides redundancy to keep the network running without any impact to the applications. The fabric maximizes the use of all links to provide the best possible network performance.

Smart network management

ALE also offers a unified management solution, the Alcatel-Lucent OmniVista® 2500 Network Management System (OV2500). It provides simple and effective management for both wired LAN and wireless WLAN networks, including OmniAccess® Stellar WLAN, with smart analytics to support more strategic decisions by delivering monitoring and control for users, devices and applications. The OmniVista 2500 avoids duplication of tasks, keeps policies consistent on the entire network infrastructure and simplifies IT operations.

OmniVista 2500 provides a single dashboard to manage the entire network, including:

- Unified policy and topology controls
- Wired and wireless configuration and management
- Unified applications visibility
- Unified alarms and notifications
- Full reporting capabilities
- Full visibility into users, devices and applications, with the ability to control or blacklist applications, or realign network routing based on profiles and policies

Visibility, monitoring and reporting are the key ingredients for company infrastructure management. Every click on a connected device generates data that helps drive management decisions. The way that users work with applications, the patterns of traffic across a network, the peaks and troughs of demand—all these and many more factors contribute to a virtual picture of daily operations, and an indication of opportunities and challenges ahead.

OmniVista 2500 provides application analytics dashboards that show all relevant information regarding network use, ensuring the alignment of investments with business strategy. These reports empower IT to prioritize business-critical applications, stop non-compliant applications, and manage the coexistence of business and personal applications. It enables an open environment where employees can explore new applications, and IT can secure and optimize the delivery of key applications to employees and customers.

Smart analytics. Smart analytics allows for improved business decisions and network planning by providing visibility and detailed information about the network, users, devices and applications being used on the network. It also provides predictive analysis reports that gives visibility into potential future bottlenecks, enabling proactive planning of network capacity and expansion.

ALE smart analytics also provide deep inspection capabilities with details about which applications are being used most often. This data can then be aggregated, presented, and acted upon. For example, certain apps can be restricted and bandwidth can be reserved or limited.

Network administrators can gain insight on which tools are most frequently used and which users are consuming the most bandwidth.

An artificial intelligence (AI) algorithm built into the analytics tool creates a baseline of "normal" network traffic behavior, which is then used to predict what will happen in the future. For example, smart analytics regarding network use could predict future bandwidth consumption, or provide a warning when it's time to upgrade a switch that is about to run out of available bandwidth.

Analytics can also be used to improve security. Based on the same established baselines, the AI algorithm sends notifications when unusual network traffic patterns are detected.

Figure 6. OmniVista 2500 Network Management System – Analytics dashboards

A layered approach to network security

A high quality user experience can only be assured if the network is always running and the information is protected. Security is a fundamental component in the corporate network architecture, especially now that companies are embracing BYOD, IoT and exploring new applications from the cloud. More than ever before, security needs to be built in from the ground up and applied universally across all methods of access for the network, wired or wireless.

ALE networks provide layered security starting with network integrity, device security, user profiles, application analytics and then moving to the levels of IoT containment, the operating system and code validation.

ALE layered security includes:

- At the user level, verifying that users are always authenticated and authorized with the correct access rights (using policies and profiles).
- At the device level, checking that devices are authenticated and compliant with IT-established security rules. This can be achieved with agents installed on devices that perform a quick security scan before devices connect to the network. For instance, the scan can ensure that the devices joining the network have up-to-date anti-virus software, and the latest version of their operating system.
- At the application level, setting rules associated with specific applications (including blocking, limiting bandwidth or identifying who can use them).
- At the network level, ALE switches and access points offer smart analytic capabilities that provide visibility and detailed information about the network, users, devices and applications being used on the network.
- ALE's smart analytics also provides deep packet inspection capabilities, which detect the type of data and applications moving through the network, making it possible to identify unusual network traffic patterns and unauthorized activity and network intrusion.
- At the IoT level, devices are placed in virtual containers using network virtualization techniques that allow multiple devices and networks to use the same physical infrastructure, while remaining isolated from the rest of the network. By segregating the network with virtual containers, if a breach does occur in one part of the virtual network, it does not affect other applications.

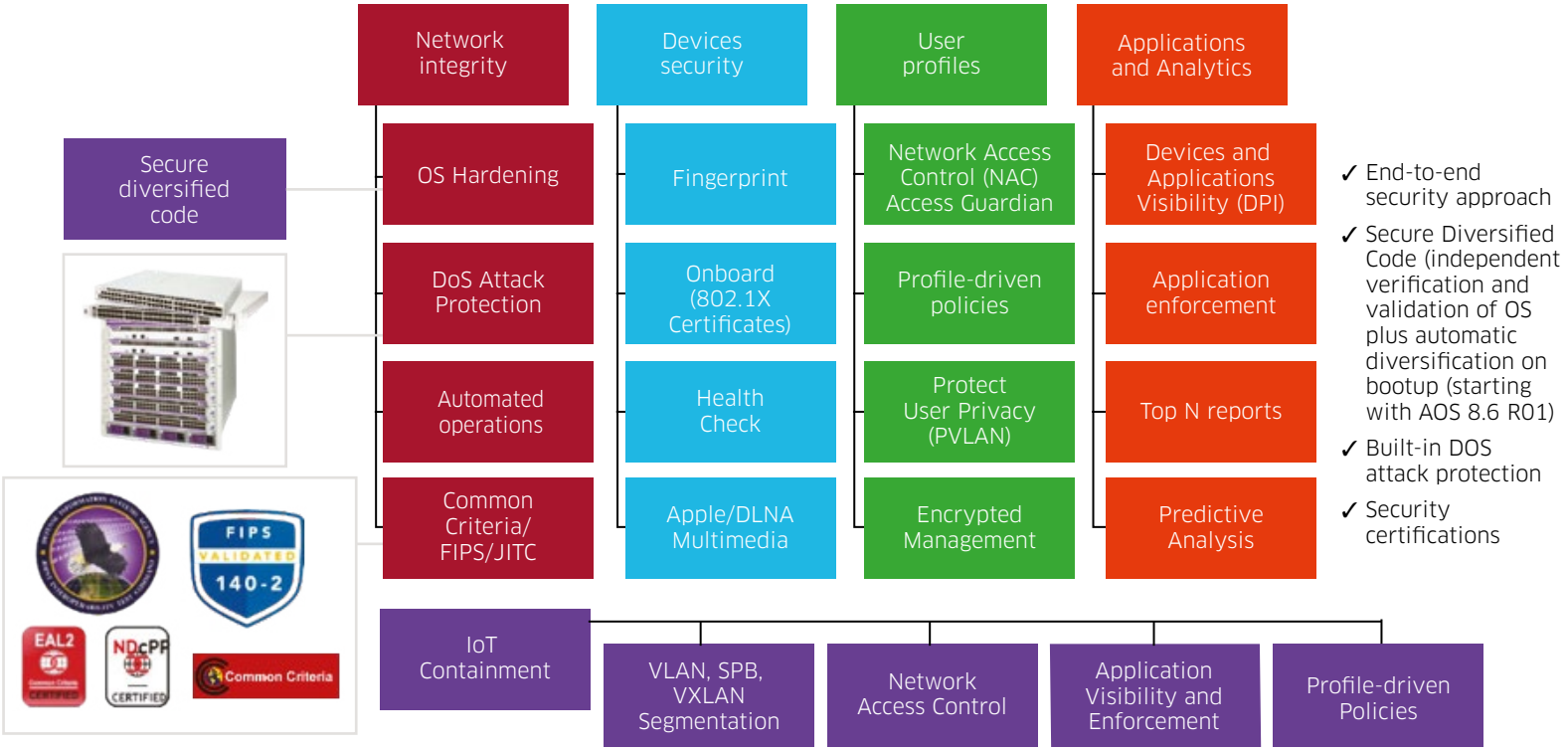
To further advance ALE's network integrity strategy, ALE has developed the OmniSwitch AOS secure diversified code to another layer of security against network cyber-security attacks.

Secure diversified code is designed to protect networks from intrinsic vulnerabilities, code exploits, malware and potential back doors that could compromise mission-critical operations. The technology is designed to mitigate larger enterprise security risks at the source, enabling an enhanced security profile through:

- Independent verification and validation of Alcatel-Lucent OmniSwitch® source code
- Addressing space randomization to protect the OmniSwitch operating system without changing functionality
- Secure delivery of OmniSwitch software by ALE to help prevent tampering

ALE's in-depth security strategy has received the highest levels of certification from major governmental agencies, including Common Criteria (EAL2 and NDcPP), JITC, FIPS 140-2 and NIST.

Figure 7. ALE Network in-depth security layered approach



ALE offers flexible network business services

While ALE's technologies are always evolving to meet the networking needs of tomorrow, the company is also adapting its business services to meet the changing requirements of new and disruptive business models.

ALE offers multiple, flexible investment options, providing choices for how customers acquire the same proven ALE solutions and technologies but with payment strategies that align with individual business needs.

ALE offers the following investment models:

- Traditional CAPEX, where customers buy and manage their own equipment
- OmniVista Cirrus, a hybrid CAPEX-OPEX model in which the customer owns the physical infrastructure and outsources the network management services from the cloud

Figure 8. ALE Network flexible investment models

	Traditional	OmniVista Cirrus	Universal NoD NoD	Flexible NoD
Expenditure	CAPEX	Hybrid	OPEX	OPEX
Payment base	Equipment	Equipment	Daily connections	Equipment
Payments	Cash on delivery	Upfront	Monthly post-paid	Monthly pre-paid
Duration	Lifetime	1Y/3Y/5Y	24-72 months	24-72 months
Elasticity	Up	Up and down	Up and down	Up and down
Service and support	Sold separately	Included	Included	Included
Network management	Sold separately	Included SaaS	Included, mandatory	Included, optional

OmniVista Cirrus also offers a cloud-based SaaS model for unified network management to simplify administration of the network. This model:

- Eases complexity of establishing guest access or BYOD permissions.
- Enables on-demand monitoring and control with network dashboards and smart analytics.
- Supports business continuity with cloud data protection strategies.

- Universal Network on Demand (NoD), an OPEX model that offers consumption-based operational expenditure as an IaaS managed service, offered through ALE authorized resellers. This investment model matches monthly expenditures with actual use of the network infrastructure.

- Flexible Network on Demand, an OPEX model that offers equipment-based operational expenditure as an IaaS managed service. This investment model matches monthly expenditures with the actual size of the network infrastructure.

In addition, cloud-based ProActive Lifecycle Management (PALM) services provide a real-time view of the network by:

- Automatic tracking of physical equipment inventory, software licenses and warranty information
- Reducing risk by ensuring that networks are up-to-date and operating within best practices
- Leveraging artificial intelligence and machine learning algorithms to enable proactive planning and set budget expenditures for future network infrastructure changes, such as upgrades, improvements and renewals

Figure 9. ALE ProActive Lifecycle Management displays essential lifecycle information for Alcatel-Lucent Enterprise Wi-Fi and LAN switching products

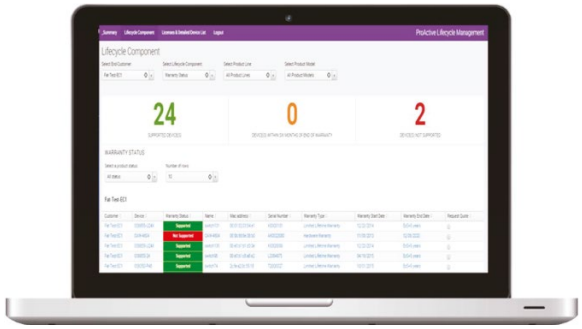


Figure 10. ALE Location based services – Wayfinding

New network offerings from ALE include location-based services that enable enterprises to leverage their network infrastructure to create new revenue streams and provide innovative ways to engage with their employees and customers.

These new network services include:

- Wayfinding, with interactive maps that provide users with directions inside buildings
- Geo-fencing, for contextual notifications, alerts and push communications. In a hotel setting, geo-fencing is used to offer targeted guest services with location-based messages.
- Asset tracking, for improved operational efficiency and cost savings. In hospitals, asset tracking improves staff efficiency by making it easier and faster to locate medical personnel and equipment.
- Location analytics, to better understand human traffic flows, use of areas, customer behaviors, etc. For instance, in an airport or a train station, location-based services are used to optimize passenger-flow patterns and capacity to improve the traveler experience.

ALE offers connected experiences for vertical industries

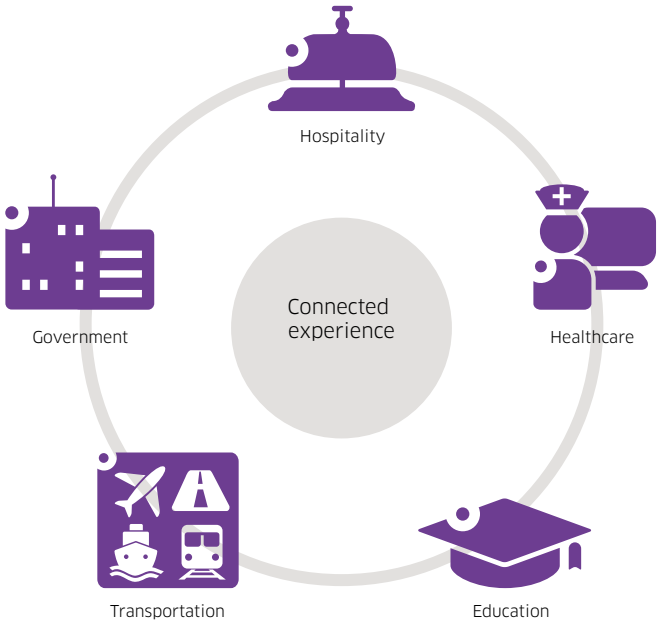
ALE delivers tailored network solutions that can be integrated with industry-specific business processes in five leading verticals. Our network infrastructures deliver seamless, end-to-end connected experiences for users in the healthcare, education, transportation, government and hospitality industries.

ALE's network technologies provide secure, high-performance infrastructures to optimize care and services, and ensure high availability for mission-critical operations and enhanced staff productivity. ALE delivers a robust, future-proof, easy-to-operate network infrastructure that optimizes network capacity while minimizing total cost of operations (TCO).

ALE works with key providers in each vertical to ensure that its industry-specific solutions natively provide the consciousness of the network by building in capabilities to recognize vertically-focused equipment, algorithms, security and protocols. Most IoT devices are pre- authorized so they are easily and automatically connected into the network.

ALE's management and analytics solutions provide customers insight into connections among users, devices and applications to increase the intelligence of the network and optimize configurations to drive business results.

Figure 11. ALE – A strong focus on vertical industries



Vertical industry strategies from ALE

ALE provides a complete portfolio of solutions and services for five key industry verticals.

Hospitality: ALE provides a network foundation to enable memorable guest experiences with comprehensive mobility and the latest in-room-automation services. ALE hospitality solutions also optimize staff efficiency, simplify IT operations and help management achieve maximum occupancy, increase revenue, and support competitive differentiation while maintaining a low TCO.

Education: ALE provides a state-of-the-art infrastructure that enables digital transformation in education. It empowers educators with next-generation digital learning tools and helps increase student success and retention. ALE network solutions help improve campus operations for staff, and contributes to achieving excellence in education while reducing the overall cost per student. It also helps to improve school and campus security through automated and secure management of CCTV and other surveillance systems.

Healthcare: ALE helps hospitals and clinics to connect patients, staff and the healthcare ecosystem by delivering network technologies that work across and beyond facilities. It optimizes the patient care pathway and improves staff efficiency through innovative network services like wayfinding and medical assets tracking, which run on top of reliable, secure and high-performance Wi-Fi connectivity. ALE technologies also ensure secure setup, onboarding and high QoS for medical IoT devices.

Transportation: ALE provides efficient, proven, end-to-end solutions for transportation businesses and organizations that fit in airports, rail stations, intelligent roads , tunnels, ports and logistics.. ALE technologies for the transportation industry include advanced rugged switches to address the need for resilient network capabilities to securely onboard and manage IoT devices in harsh environments. The portfolio also includes an advanced WLAN solution so that travelers can easily connect wherever they are and get access to innovative services.

Government: ALE networks are fully security certified, enabling government organizations, from the defense sector to local government units, to deploy secure and resilient data networks. ALE's advanced multi-layer network security core provides comprehensive BYOD and IoT services and protects highly available real-time communications systems for confidentiality, event awareness, notifications and response coordination. ALE networks also improve IT team efficiency through network automation that reduces the risk of human configuration errors ALE has also helped numerous customers contribute to smart cities initiatives.

ALE provides a network foundation for digital transformation

To maintain leadership in their industries, companies and institutions must undergo a digital transformation; a process that integrates technological advances such as mobility, data analytics, cloud computing and IoT into existing business and computing systems. While taking advantage of new technological advances provides many benefits, the process often presents enterprises with operational and security challenges.

The network infrastructure of a business or organization is the foundation for digital transformation, and ALE offers state-of-the-art network solutions at the access, core and data center layers to support and facilitate digital transformation. With unified wired and wireless networks that provide high performance and multiple layers of security, enterprises are empowered to offer user mobility, embrace IoT and explore the unlimited insights provided by analytics and AI. IT operations are simplified via automation and virtualization. Innovative services can be offered, including BYOD and location-based services. Additionally, ALE network solutions ensure that connectivity is provided to users everywhere, whether in offices, on the industrial floor, in harsh environments or outdoors.

To fulfill the diverse needs of customers, ALE provides a variety of deployment and investment models. ALE network solutions can be deployed on premises, in the cloud or as a hybrid cloud model; investment options range from CAPEX to OPEX or a mix of both.

The advanced features of these network products and solutions must be adapted and customized to maximize the benefits for each industry sector. ALE tailors its network products and technologies into vertical solutions for healthcare, education, transportation, hospitality and government to help organizations transform their technology investments into clear business benefits. These include better services to end customers–whether they are patients, students, passengers, guests or citizens–while boosting employee motivation and satisfaction, reducing costs and improving profitability.

ALE makes everything connect by delivering networking technology designed to work for your organization.

White Paper
Network Strategy and Vision for the Enterprise – Where Everything Connects
December 2019

We are ALE.

We make everything connect by delivering technology that works, for you.

With our global reach, and local focus, we deliver networking and communications.

On Premises. Hybrid. Cloud.

Alcatel·Lucent
Enterprise