Mobile Campus Network Solution

Transform your business with a network infrastructure that supports digital technologies, seamless mobility and the Internet of Things

Alcatel·Lucent Enterprise

Table of Contents

Building a digital enterprise

Enterprises are seeking to gain a competitive advantage by adding digital technologies to their internal and external operations. They want to evolve and grow their businesses by using digitalization to take flexibility, collaboration, efficiency and reliability to new levels.

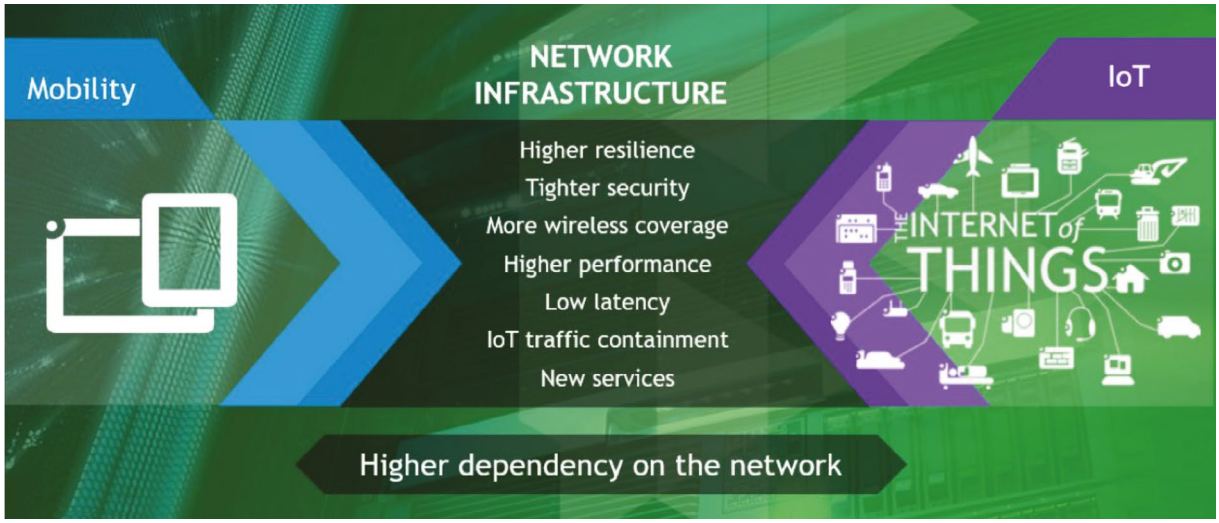
Four key technology trends are driving this quest for digital transformation: Demand for always-on mobility, the proliferation of connected things, the rise of data analytics and the shift to the cloud. These trends bring new pressure and complexity to your network. But they also present crucial opportunities to streamline your operations and stand out from the competition.

To seize these opportunities, you need a simpler network infrastructure that is easy to deploy, manage and takes advantage of digital technology. This infrastructure must allow your IT organization to:

- Automate provisioning and tuning processes to address the unpredictable bandwidth use and security risks that come with increased mobility
- Provide seamless connectivity and a high quality of experience (QoE) to everyone who uses your network
- Develop an effective strategy for containing and profiting from the Internet of Things (IoT)

The Alcatel-Lucent Enterprise (ALE) Mobile Campus Network solution provides a simplified, end. to-end infrastructure that lets you meet the demands of new applications, connected devices, virtualization and mobile workers. This architecture optimizes resource use, delivers a consistent QoE and simplifies overall management. With ALE's network technologies and software, you can deliver the bandwidth, wireless local area network (WLAN) capabilities and network performance you need to build a digital enterprise.

Figure 1. Mobility and the IoT are shaping tomorrow's digital business



ALE's Mobile Campus Network solution provides the tools you need to become a modern, digital enterprise. Built on ALE technology innovations, this solution provides a resilient architecture with intelligent controls that dynamically tune network performance to the needs of users, devices and applications. You can use these capabilities to streamline operations, reduce network complexity and enhance the user experience.

With the Mobile Campus Network, you get a comprehensive solution that combines advanced management software with state-of-the-art network equipment, starting from wireless access points (APs) and extending to edge, distribution and core switches, and wide area network (WAN) routers. The solution provides four key technologies – Unified Access, Intelligent Fabric (iFab), Smart Analytics and IoT Containment – that help you use mobile and IoT innovations to address the evolving needs of your business and users.

Unified Access: Provide a seamless experience on wired or wireless access

In today's competitive environment, your employees need the ability to connect and share knowledge with peers and customers anytime and anywhere.

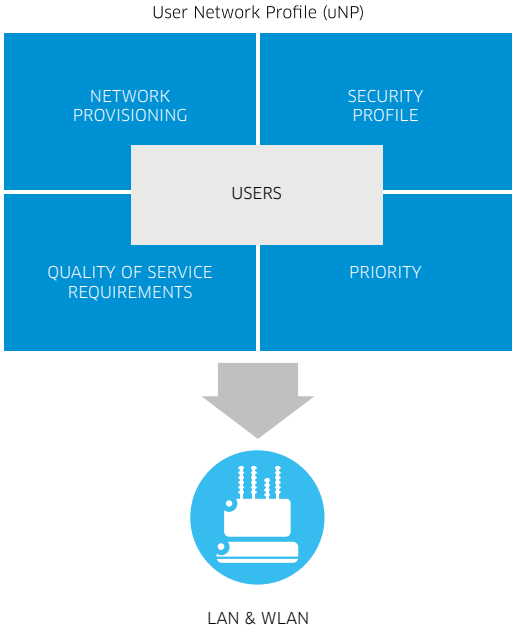
ALE's Unified Access approach ensures that employees get the same high-quality application delivery, policies and network services on wired and wireless connections. Built with the latest IEEE 802.11ac technology, ALE's APs make wireless network performance comparable to that of wired networks and enable the speeds, quality of service (QoS) and reliability required for real-time applications.

Unified Access also streamlines your IT operations. For example, it allows you to offer common policies on both wired and wireless access with the same level of security. A single management infrastructure gives you end-to-end network visibility and better troubleshooting tools.

User Network Profile

ALE's access layer switches and APs let you use the Alcatel-Lucent Enterprise User Network Profile (uNP) to manage conversations contextually. The uNP can be configured once and applied to both wired and wireless users. Figure 2 shows the uNP, which surrounds users with the information required to support them. This unique feature is available only in Alcatel-Lucent Enterprise solutions.

Figure 2. User Network Profile parameters



The uNP enables the network to follow users by automatically adjusting the network configuration based on where they are connected. This approach differs from traditional static configurations based on switch ports, APs or service set identifiers (SSIDs). With the uNP, you can:

- Minimize IT effort by eliminating the need to manually adjust the network
- Improve mobile application delivery performance and offer the same experience everywhere by dynamically fine-tuning the network wherever users are connected
- Provide consistent security throughout the network

High quality multimedia delivery

ALE offers a unique multimedia fluency technology that can help you support the increasing use of multimedia applications. This technology allows the Unified Access layer to:

- Detect any application session running on the network (more than 2000 signatures)
- Assign a specific QoS to the session depending on the application, user, device, time of the day, location and any other rules set by the administrator
- Monitor the actual QoS received
- Equip IT administrators with a dashboard that provides visibility into session quality within the network

For example, multimedia fluency allows you to provide specific users with a higher QoS for voice and video sessions and a lower QoS for other applications. You can also address users' specific needs by providing them with a different QoS for individual voice and video sessions.

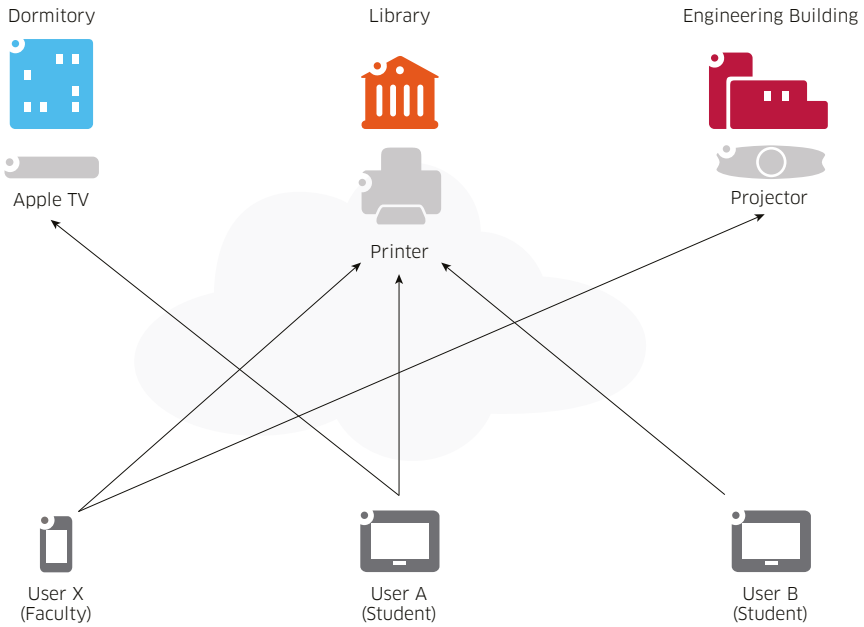
Consumer device support

Consumer devices – such as Apple TV® and Digital Living Network Alliance (DLNA)-compatible TVs, projectors and printers – use special protocols that make them easy to discover on a network. However, protocols such as Apple® Bonjour® and Universal Plug-and-Play (UPnP) are designed to work on residential networks that have a single virtual local area network (VLAN). These protocols don't work in corporate networks.

ALE's solution addresses this challenge by making these wired or wireless consumer devices accessible in corporate environments. This service allows users to restrict access to their devices and self-register these devices without IT input. It also eliminates the need for your IT department to create special network configurations (such as VLANs or SSIDs) for consumer devices.

Figure 3. Application visibility starting from the Wi-Fi radio

Figure 4. Network services for Apple and DLNA-compatible devices



BYOD and guest services

ALE's BYOD services module simplifies device onboarding with automated device configuration. It ensures secure access to the network without IT intervention.

ALE's guest services module eases guest management by supporting sponsored and self-registration. It also supports advertising capabilities.

These modules also make it possible to define sophisticated policies based on a combination of the user's identity, device and other conditions, such as location and time of day.

End-to-end security

Security is a fundamental component of your corporate network architecture, especially if you are embracing BYOD and exploring new cloud applications. To provide a high-quality user experience, you need an always-on network that protects critical information. This means building security solutions from the ground up and applying them across all wired and wireless network access methods.

ALE's solution lets you apply network edge security services to users, devices and applications. These services use role-based profiles to authenticate users and assign user profiles that specify all network security behavior, including access control lists (ACLs) and firewall rules. Wherever users go, their unique security rules will follow.

By supporting the IEEE 802.1X clients and certificates, ALE's solution ensures that clients with the right to access the network can connect easily, with maximum security. It can also quarantine unauthorized devices and users in a dedicated VLAN. This approach includes:

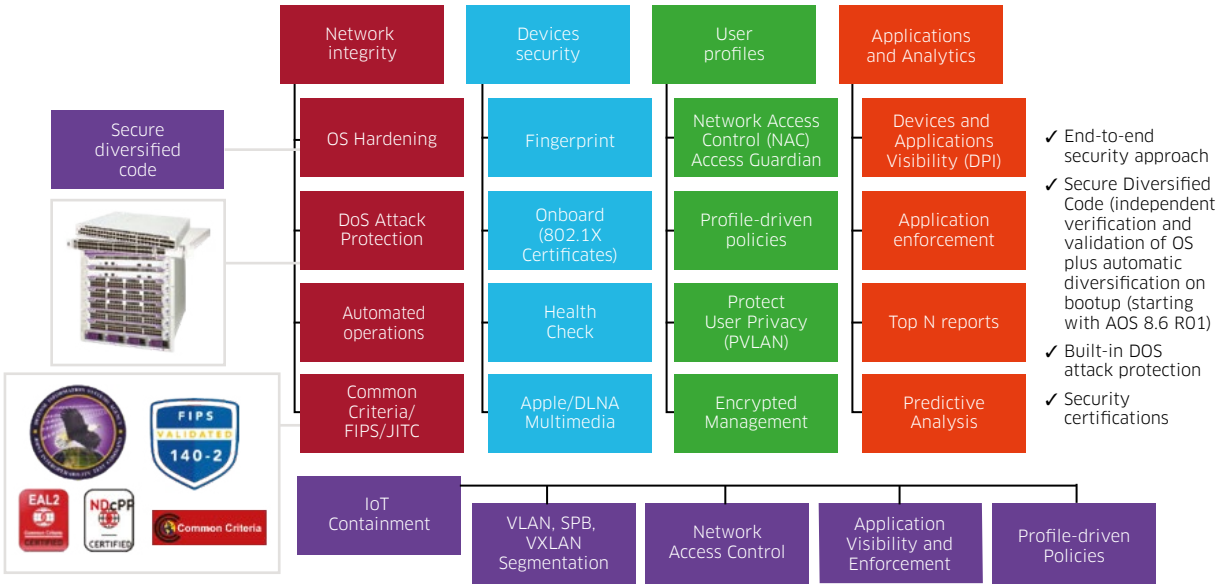
- Secure firmware built into network switches
- Embedded protection against denial-of-service attacks
- A secured network from edge to core
- Secured network service for IoT

The Alcatel-Lucent Enterprise solution uses secure diversified code to improve network integrity and provide added security against network cyber-attacks. Secure diversified code protects networks from intrinsic vulnerabilities, code exploits, malware and potential back doors that could compromise mission-critical operations. It mitigates larger security risks at the source and enables an enhanced security profile through:

- Independent verification and validation of Alcatel-Lucent operating system (AOS) source code
- Address space randomization, which protects the AOS without impacting functionality
- Secure delivery of Alcatel-Lucent OmniSwitch® software, which helps prevent tampering

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

Figure 5. Alcatel-Lucent Enterprise security approach and certifications

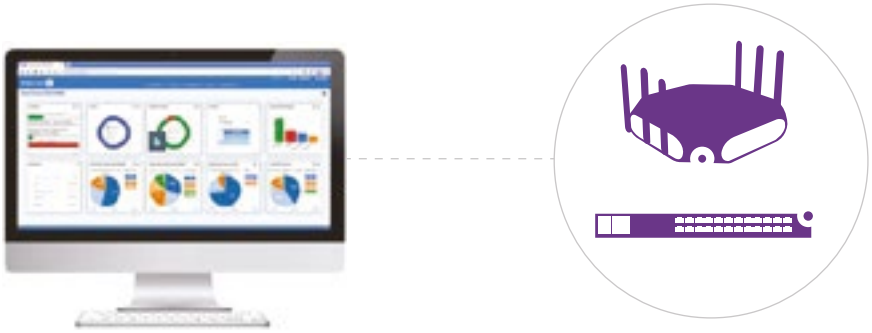


Unified network management

IT departments are facing new pressure to support more and more devices with diverse operating systems, more applications, more multimedia, new BYOD strategies and a consistently high-quality user experience – all while IT budgets remain flat or shrink. You can help your IT department achieve these objectives by deploying a comprehensive, unified network management system (NMS).

The Alcatel-Lucent OmniVista® 2500 Network Management System (NMS) provides a common management experience for access, core and data center networks. This powerful NMS draws on ALE's extensive carrier network management experience to provide end-to-end network and application visibility and carrier-class troubleshooting tools. It can help you manage corporate, branch and home office sites for wired and wireless users, and unify analytics collection and policy enforcement across the wired and wireless LANs.

Figure 6. OmniVista 2500: Unified management for wired and wireless LANs



The OmniVista 2500 provides a customizable dashboard that shows which users and devices are connected to the network, which applications they are using and how much bandwidth they are consuming. Your IT administrators can use this information to create policies that:

- Reserve bandwidth and guarantee a special QoS for business-critical applications
- Limit bandwidth consumption for low-priority applications
- Enforce security by preventing the use of harmful applications
- Tailor experiences for different user profiles

Intelligent Fabric: Simplify network design, installation, and operations

ALE's Intelligent Fabric (iFab) lets you blend agility with automation that speeds up network infrastructure deployments and simplifies network operations. This award-winning technology supports simpler network design, comprehensive interoperability, plug-and-play deployment and automation of moves, adds and changes.

Simple network design

The iFab technology simplifies network design and prevents errors by configuring the L2 and L3 network protocols. Your designers provide input on network equipment locations, the number and type of access ports, interconnection distance and bandwidth. iFab provides feedback that enables them to choose the right Alcatel-Lucent Enterprise technologies for the design. There is no need to provide details on complex network protocols. iFab recognizes the protocols and self-configures to provide the outcome you want.

Straightforward network development

iFab self-configures network equipment using Auto Fabric, which eliminates many manual tasks from the deployment process. The fabric creates itself autonomously after you unpack, mount, connect and power up the systems. By removing manual steps, it shortens time to production for infrastructure and reduces chances for errors in the deployment process.

The iFab technology makes the network components aware of their physical and logical topologies through self-attachment. The fabric can attach itself to adjacent systems, such as access switches (including third-party switches) and servers.

Easy network maintenance

iFab enables you to support seamless operation with a self-healing function that lets your critical networks continue to operate if failures occur. This function detects link or node component failures in real time and automatically re-routes traffic, allowing you to upgrade your network while keeping it in service. This significantly reduces or eliminates your need for disruptive maintenance windows.

Automated moves, adds and changes

Manual moves, adds and changes are important day-to-day activities. But they demand a level of effort that keeps IT departments from achieving their full potential operational effectiveness. The iFab technology provides built-in intelligence that frees your IT team from these manual processes.

iFab uses network profiles to support non-intrusive movement of users, devices and applications. For instance, it automatically detects the addition, movement and deletion of virtual machines and adjusts security, bandwidth and priority without IT involvement.

The Auto Fabric feature supports plug-and-play workflows for adding new infrastructure components. It allows these components to be detected and self-configured based on the physical and logical topology.

Integrated workflow management

Software-defined networking (SDN) supports programmability that enhances your business agility. Your network must be programmable to interact with applications, fit into workflow management and support special customization. iFab addresses these needs by supporting the OpenFlow™ protocol, OpenStack® software and Python® scripting.

Complete virtual private network setup

iFab technology automatically creates the Shortest Path Bridging (SPB) core of the network using previously defined SPB adjacencies. It also creates a dynamic virtual private network (VPN) as an SPB service based on discovered user traffic, and dynamically provides adequate service to user or IoT devices. This technology significantly contributes to secure IoT containment.

iFab uses self-attachment techniques to discover and connect with SPB-capable switches from Alcatel-Lucent Enterprise or other vendors. It then forms an SPB adjacency or SPB core. If at least one SPB adjacency is created on the switch, the SPB uNP will automatically generate the SPB Service and Service Access Point (SAP) based on ingress traffic.

A strong foundation of standard protocols

SPB is built on strong and reliable protocols. For the control plane, it uses IS-IS SPB, a protocol that delivers proven reliability and scalability. The IS-IS protocol has successfully supported IPv4 and IPv6 services for decades. It has now been amended to transport SPB services, which are more accurately called Provider Backbone Bridging (PBB) services. Combining solid IEEE (802.1aq) and IETF (RFC 6329) foundations with ease of deployment, SPB IS-IS goes beyond basic Spanning Tree evolution to usher in a new L2 and L3 VPN era.

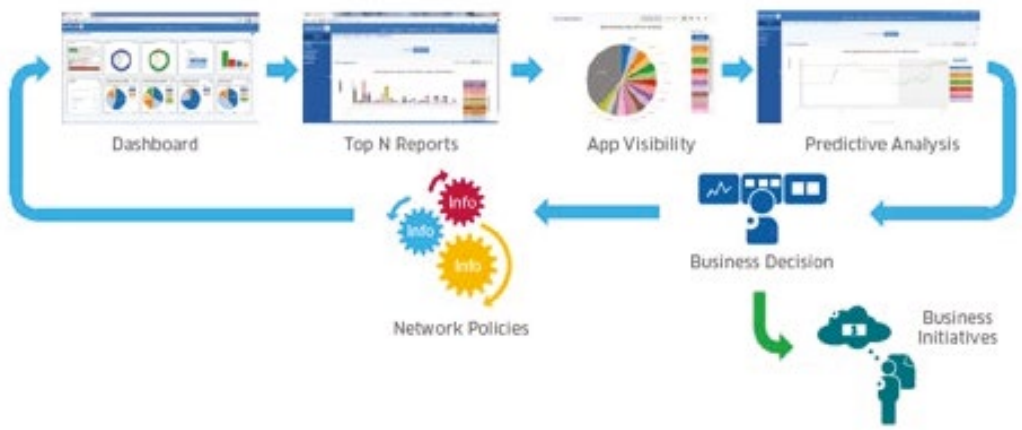
For the data plane, it leverages PBB, based on IEEE 802.1ah standard. PBB initially served with RSTP/MSTP as a control plane. It has since been associated with IS-IS SPB as a control plane. Internet service providers have achieved reliability and scalability with different flavors of PBB (including PBB VPLS and PBB EVPN) over the last 10 years.

Comprehensive Smart Analytics: Understand and control your network

Visibility, monitoring and reporting are the key ingredients of effective infrastructure management. The Alcatel-Lucen Enterprise Unified Access and iFab technologies ensure that your IT organization sees all aspects of the network infrastructure with a single pane of glass: The OmniVista 2500 NMS.

These technologies allow IT teams to examine logical and physical topologies, access and core fabric components, applications and workflows. They also provide complete visibility of overlay technologies such as virtual extensible LAN (VXLAN), which are typically invisible to infrastructure teams. By using OmniVista 2500 to correlate overlay technologies and physical components, your teams better understand application workflows and proactively plan infrastructure requirements.

Figure 7. Smart Analytics



The Alcatel-Lucent Enterprise Smart Analytics technology enables you to analyze infrastructure information in a meaningful way. OmniVista 2500 summarizes vast amounts of data on users, devices, applications, network device status, traffic behavior, warnings and key statistics in a customizable dashboard. You can use this dashboard to create graphs and reports and expand your analysis. This analysis brings vital insights that enable you to fine-tune the network and provide the best possible user experience.

ALE's analytics also provide important insights into user behavior and application adoption. These insights help you make the right company decisions outside the IT realm.

Application visibility and control

Fueled by increasing adoption of cloud applications and BYOD, the number and type of applications used in enterprises are both growing rapidly. Your IT team needs new tools and capabilities to support your business goals and keep your network secure.

The Alcatel-Lucent Enterprise OmniSwitch® 6860 Stackable LAN Switch and Alcatel-Lucent OmniAccess® Stellar WLAN product lines provide application analytics using integrated deep packet inspection (DPI) technology. DPI gives your IT teams detailed visibility into application use and bandwidth consumption. It also allows them to immediately enforce policies to control the prioritization, QoS and security of these applications at the edge of the wired or wireless network.

ALE's application analytics technology empowers you to prioritize business-critical applications, stop non-compliant applications and manage the coexistence of business and personal applications. It also lets you support an open environment where employees can explore new applications, and where IT teams secure and optimize the delivery of key applications to employees and customers.

Powerful reporting

OmniVista 2500 offers an extensive range of reports that help your IT team quickly identify and troubleshoot potential issues. For example, it provides top-N reports that gather information on

the users and applications that generate the most traffic. It also reports on the network nodes and ports that handle the most traffic.

Predictive analysis

OmniVista 2500 provides predictive analysis reports that examine traffic patterns over a long period of time and use machine learning algorithms to forecast future behavior. These reports provide visibility into potential future bottlenecks. They enable you to proactively plan network capacity and expansion. The system also detects abnormal traffic behavior and alert administrators of a potential network security attack.

IoT Containment: Simplify and secure your IoT rollout

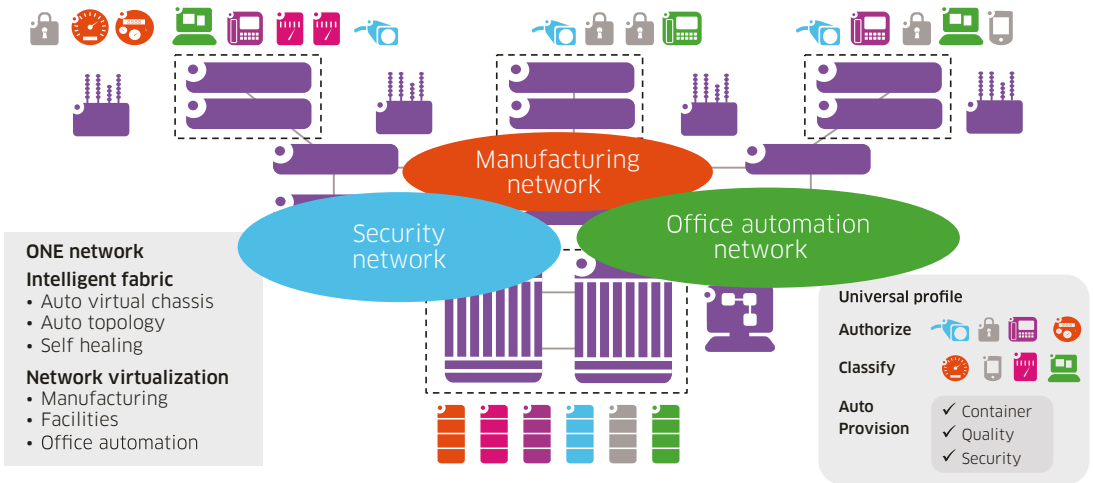
Security will be your biggest challenge as you roll out IoT applications. You need to guard against outside intrusion and provide internal security in the form of firewalls between applications. The seemingly easy answer is to create a separate network for each application. But this can be costly and overly complex to manage.

The Alcatel-Lucent Enterprise IoT containment technology lets you secure your network in a simpler and more cost-effective way by creating a virtual network for each IoT application. It allows your administrators to use the same underlying network infrastructure to create multiple virtual network slices, or "containers." The containers specify policies related to quality, prioritization, bandwidth reservation, latency and any other capabilities required by the IoT solution. You can specify profiles by container, so that only specified devices – for example, digital security cameras – can authenticate, connect and send traffic.

IoT containment also helps you ensure that devices easily and securely connect to your wired or wireless network:

- When a new device connects, the network automatically recognizes its profile and places it in a VPN. This ensures that the device accesses only the application platform it has permission to use.
- Virtual containers apply QoS and security rules to ensure that the IoT system has the resources it needs to run efficiently and securely.
- You can create, deploy and operate multiple virtual containers on the same network infrastructure by virtually segmenting your physical network.
- By segmenting the network into different virtual containers, you ensure that a breach in one segment does not affect the others.

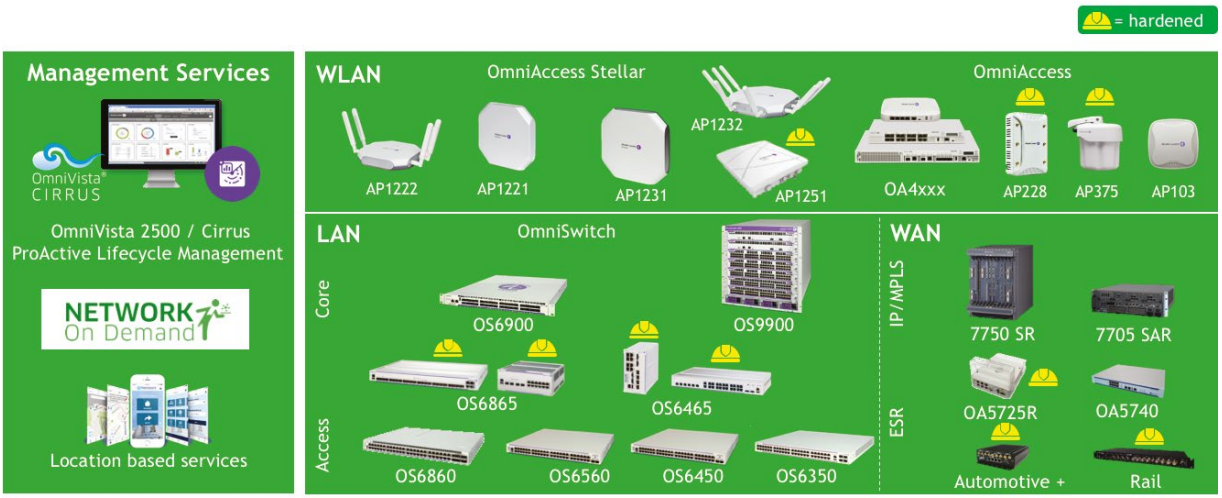
Figure 8. One robust, easy to deploy network with a virtual network for each business unit



Build a complete solution with ALE's comprehensive portfolio

ALE's network portfolio provides all switches, routers, APs and software you need to build a high-speed, resilient and very secure network infrastructure from wireless access to the core and data center. By leveraging the innovations built into the Mobile Campus Network solution, you address changing business demands with pervasive network access, a high-performance core, flexible WAN connectivity, end-to-end network management and adherence to open standards.

Figure 9. Alcatel-Lucent Enterprise network portfolio



Distributed Intelligent Control: The new way to deliver controller features

ALE's WLAN access points (APs) let you use Distributed Intelligent Control technology to provide Wi-Fi that supports a high density of devices while ensuring high bandwidth.

This technology uses the speed and capacity of the ALE access point processor to distribute a full set of controller features among all APs instead of centralizing them in one physical or virtual location. This feature set includes:

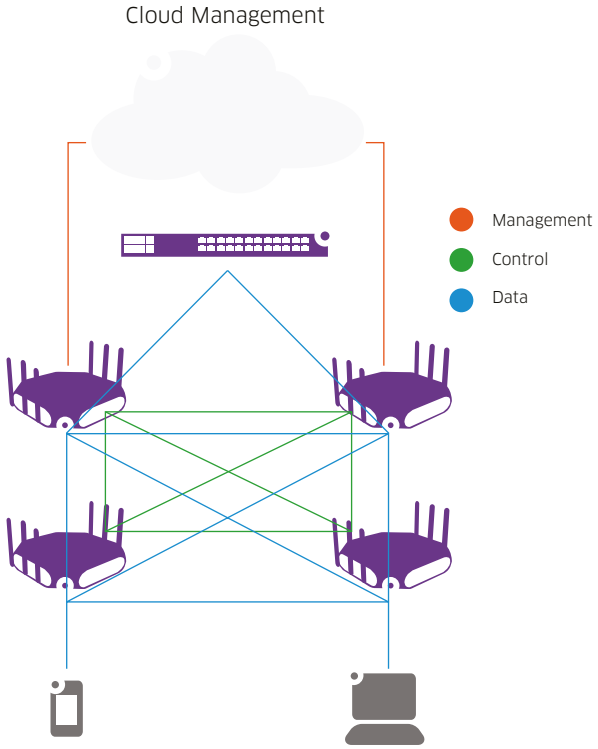
- Automatic radio optimization
- Coordination among neighboring APs
- Band steering
- Smart load balancing
- Airtime fairness

By distributing these features among all APs, the solution supports several key capabilities that are not available with physical or virtual controllers, including:

- Self-healing: If one AP goes down, all the other APs increase their power to counteract its loss and keep services running. These power increases always stay within the limits of the country where the APs are deployed.
- High availability: By distributing controller features across all APs, the solution eliminates the single points of failure typically created by physical or virtual controllers.
- Low latency: Distributed Intelligent Control minimizes latency by ensuring that packets always use the shortest possible route. It also ensures that the flow of traffic always supports the needs of individual users and applications, guaranteeing an excellent user experience for real-time applications like voice and video.
- Easy scalability: When you add an AP, Distributed Intelligent Control configures it automatically.

- Superior traffic control: Avoid wasting bandwidth and maximize security by applying quality of service (QoS), security, application enforcement and firewalling rules at APs located at the edge of the network.
- Low total cost of ownership (TCO): The Distributed Intelligent Control technology eliminates the need to buy, deploy, power up and manage a physical controller.

Figure 10. Distributed Intelligent Control data flows



State-of-the-art wired and wireless network infrastructure

The Mobile Campus Network solution lets you combine wired and wireless equipment to provide the pervasive network access your users demand.

ALE's wired access portfolio includes:

- Stackable gigabit LAN switches such as the advanced OmniSwitch 6860E, the OmniSwitch 6450 and the entry-level OmniSwitch 6350
- Ruggedized layer 3 switches such as the OmniSwitch 6865 Hardened LAN Switch and layer 2+ switches such as the OmniSwitch 6465 Hardened LAN Switch
- Stackable multi-gigabit LAN switches such as the advanced OmniSwitch 6860E and the OmniSwitch 6560
- Core/distribution switches such as the OmniSwitch 6900 Stackable LAN switch
- Core/distribution chassis switches such as the OmniSwitch 9900 Modular LAN chassis

ALE's wireless portfolio includes a variety of high-performance 802.11ac Wave 1 and 2 Wi-Fi access points. ALE embeds Distributed Intelligent Control technology into the OmniAccess Stellar WLAN solution to ensure that it delivers the same level of features of a typical physical controller and exceeds the high availability of a virtual controller. With the ALE wireless portfolio, you gain advantages such as:

- Comprehensive radio coverage
- 802.11ac Wave 2 with MU-MIMO, which allows you to connect and serve as many devices as you need at the same time (up to 125 devices per OmniAccess Stellar AP1231 access point)

- More than 4 Gbps of wireless radio throughput for your devices and applications
- Multi-gigabit connectivity that lets you transport all traffic from the edge of the network to the core
- Real-time application visibility and control, so you can make sure your bandwidth is properly utilized
- Fast roaming between access points, which allows your users to move wherever they want without disrupting their application use
- Smart load balancing to avoid problems with sticky clients

No matter how you combine ALE products in your network infrastructure, you can offer a consistent QoE to users and simplify your IT operations.

A resilient, high-performance core

ALE's portfolio of high-performance 10/25/40/100 GE core network switches provides unparalleled port density and switching capacity. It includes the market-leading OmniSwitch 6900 Stackable LAN Switch family, which comes in a compact 1U form factor, and the OmniSwitch 9900 Chassis LAN Switch.

ALE uses virtualization techniques to eliminate inefficiencies introduced by protocols such as the Spanning Tree Protocol. Instead of disabling all redundant links and using them only if the main link or switch fails, virtualization enables the network to keep multiple links active and to fully use all available resources.

For small networks, ALE recommends using Virtual Chassis (VC) technology to interconnect core switches. This technology allows you to:

- Start with two switches and easily scale up to six OmniSwitch 6900 or eight OmniSwitch 6860 nodes
- Manage the core as one node, even as the network grows
- Use the Link Aggregation Control Protocol (LACP) to connect access layer switches to multiple nodes in the core
- Make all links active to boost bandwidth and redundancy

For medium and large networks, ALE recommends a core based on SPB technology. SPB fulfills all the requirements for large network cores, including:

- Promoting VPN over a single infrastructure that grows up to several hundred nodes
- Fast fault recovery
- Using multiple active paths to avoid L2 loop prevention protocols

MPLS-based cores provide similar capabilities, but SPB offers significantly lower hardware and operating costs.

The iFab technology supports VC- and SPB-based core designs. It helps you achieve your chosen design in a fully automatic way.

Optimized network design

ALE recommends an optimized network design based on a Pod architecture model. This approach makes better use of network resources, guaranteeing high performance and low latency. It virtualizes the transport layer and all the connections between switches in the architecture. A Pod design also allows all the physical connections to be active at the same time. The SPB protocol handles packet forwarding, supporting an extended architecture like the one shown in Figure 10.

ALE's solution uses SPB to ensure that data flows on the shortest path between the two endpoints of the network. This allows you to:

- Support faster convergence by enabling all links to be active through multiple equal cost paths
- Load-share traffic across all paths on a mesh network while ensuring the lowest possible latency at all times
- Scale and simplify network design, configuration and management

Reliable and flexible WAN connectivity

The Mobile Campus Network solution uses the Alcatel-Lucent OmniAccess Enterprise Services Router (ESR) to support branch office WAN connectivity. The ESR provides space and cost savings by combining an integrated WAN router, LAN switch and Wi-Fi access point into a single compact form factor. It supports multiple WAN connectivity options with ample redundancy, comprehensive QoS, security, VPN capabilities and telephony over IP (ToIP) survivability. You can choose from several models to support the needs of small, medium or large branch offices. The ESR series also includes ruggedized models for the industrial and transportation verticals.

End-to-end network management

ALE's management suite provides all tools you need to provision, monitor, analyze and troubleshoot your network. The OmniVista 2500 lets you manage your LAN, WLAN, core, WAN and data center from a centralized single pane of glass. This platform delivers ALE smart analytics technology. It is also an essential component of ALE's Unified Access and iFab technologies.

The management suite also expands the network services provided by the campus network solution. For example, it provides authentication, authorization and accounting (AAA), BYOD-related services, premium guest access and advanced policy services.

Investment protection through open standards

The Mobile Campus Network solution supports open standards and interfaces, including SDN support that spans the entire campus portfolio. Open standards help you ensure interoperability, support future alternative network architectures and protect your investment.

Enjoy the advantages of a mobile campus network

Deliver a high-quality user experience

- Use application analytics to guarantee QoS for business-critical applications and allow employees to explore new business or personal applications
- Dynamically tune network performance to ensure a high quality of experience for real-time multimedia applications
- Support comprehensive BYOD network services that give employees the freedom to use their personal wired or wireless devices for work
- Ensure a consistent and seamless user experience by using Unified Access to extend the same policies and network services across wired and wireless networks
- Rely on market-leading resiliency to recover from switch and link faults before they impact real-time applications such as voice and video
- Deploy end-to-end security that protects corporate information and keeps network infections from compromising performance or causing downtime

ALE's Mobile Campus Network solution reduces total cost of ownership by up to 60 percent compared to network solutions from other vendors.

Streamline your IT operations

ALE's Mobile Campus Network solution reduces total cost of ownership by up to 60 percent compared to network solutions from other vendors.

- Embed security at the network edge to increase user, device and corporate security without adding operational complexity
- Spend less time on network support with a solution that automates provisioning of edge switches and endpoints and integrates carrier-class troubleshooting tools
- Simplify core fabric design and deployment with automation embedded in the iFab technology
- Reduce your IT workload with automated end-user device connectivity and guest self-registration
- Avoid provisioning duplication and minimize inconsistencies between networks by unifying wired and wireless management
- Use smart analytics to gain visibility of critical points in the network and accelerate time to troubleshoot
- Ease expansion planning and avoid trouble tickets by using predictive analysis to detect potential problems before they before they impact network performance

Reduce network infrastructure costs

- Lower equipment and capital costs by using virtualization to flatten your network architecture and make better use of switch and network links
- Reduce operating costs with network equipment that combines market-leading power efficiency with self-healing capabilities and MAC automation
- Consolidate routers, switches and wireless APs into a single device with all-in-one branch routers

Protect your investment

- Scale your WLAN infrastructure up to 64 APs using intelligent distributed control – or remove scalability limits by deploying OmniVista 2500
- Buy only the number of licenses you need for the employee (BYOD) and guest devices that actually connect
- Protect your investment and choose the best financial option for you: CAPEX or OPEX (Network on Demand or Network as a Service)
- Extend SDN support to all LAN switches and the WLAN so you can continue to use the same equipment for future SDN architectures

Network on Demand: Network infrastructure with flexible financing

Alcatel-Lucent Enterprise Network on Demand offers an alternative to purchase and operate your own network. This solution combines an on-premises network backbone with LAN and Wi-Fi access and comprehensive management, reporting and support services. It can be tailored to provide the exact service levels your business needs.

Network on Demand is an infrastructure-as-a-service (IaaS) offer available through authorized resellers as a managed service. ALE resellers have the knowledge and operational expertise to seamlessly integrate the solution into your IT organization.

ALE offers two options for Network on Demand:

- Universal Network on Demand, an OPEX model that provides consumption-based operational expenditures. It 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. It matches monthly expenditures with the actual size of the network infrastructure.

With Network on Demand, you can:

- Pay only for what you use and avoid capital investment
- Minimize payments for unused infrastructure and align your infrastructure costs with your business revenues
- Refocus your IT staff on business applications and communications

Figure 12. Network on Demand financial models

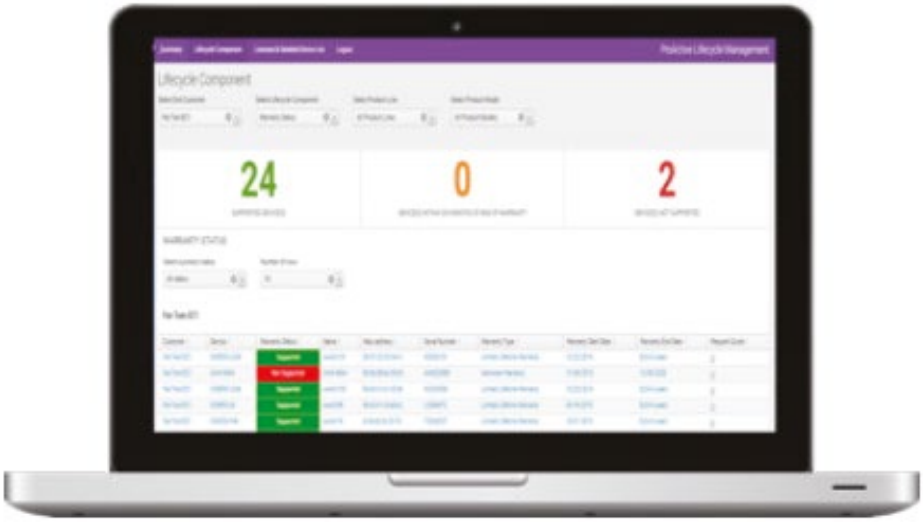
	Traditional	Universal NoD	Flex NoD
Expenditure	CAPEX	OPEX	OPEX
Payment base	Equipment	Daily connections	Equipment
Payments	Cash on delivery	Monthly post-paid	Monthly pre-paid
Duration	Lifetime	24-72 months	24-72 months
Elasticity	Up	Up & down	Up & down
Service & Support	Sold separate	Included	Included
Network Management	Sold separate	Included, mandatory	Included, optional

ProActive Lifecycle Management

ALE's cloud-based ProActive Lifecycle Management (PALM) service provides a dashboard that gives you a real-time service status view of the network. With PALM, you can:

- Automatically track physical equipment inventory, software licenses and warranty information
- Reduce risk by identifying non-compliant infrastructure
- Use new artificial intelligence and machine learning algorithms to predict potential risks relating to specific network configurations and block incorrect configurations

Figure 13. ProActive Lifecycle Management dashboard



A campus network that's ready for tomorrow's digital business

The Alcatel-Lucent Enterprise Mobile Campus Network solution enables you to build a simplified, virtualized network that delivers industry-leading performance, intelligent automation, maximum security and a consistent, high-quality user experience across wired and wireless. This solution combines Unified Access, Intelligent Fabric, Smart Analytics and IoT Containment technologies. It lets you provide an open and engaging environment for employees, create new operational efficiencies, reduce costs, improve productivity and differentiate from your competition. These capabilities help you reach your business objectives faster.

ALE's campus network provides innovations that allow you to address your immediate needs and prepare for the future by gradually increasing mobility, BYOD and IoT containment. It eases this transformation by enabling you to continue using the same hardware and by protecting your existing investments. ALE backs the solution with support services that preserve the continuity of your business.

Visit the Alcatel-Lucent Enterprise website to learn more about how ALE can help you deploy a sustainable campus network that will bring an outstanding return on investment for years to come.

Alcatel·Lucent Enterprise