Digital Age Networking in Enterprises

Alcatel·Lucent
Enterprise

Table of Contents

Overview

Digital age technologies that help improve efficiency are being adopted by the business world at an increasing rate. To achieve a competitive advantage, enterprises need to integrate the latest mobility, data analytics, cloud and IoT digital innovations into their operations, processes and computing systems. This trend, known as digital transformation, enables organisations to create more efficient processes, differentiate products and services, and better satisfy the needs of customers and employees, while increasing revenues and reducing costs. Companies and institutions embarking on a path toward digital transformation understand that their network infrastructure is the fundamental enabler of this evolution. Alcatel-Lucent Enterprise develops network technology and solutions that help businesses achieve and harness the benefits of their digital transformation.

The latest evolutions in mobility, the Internet of Things (IoT) and data analytics, are directly impacting network infrastructures and driving enterprises to reconsider their network technology choices. Legacy infrastructures are often unable to securely and efficiently support new use cases and business scenarios based on cloud native applications and the massive number of IoT devices in use. Adoption of applications, and IoT-based digital processes, are happening at an unprecedented scale and speed. Manual and static network configurations can no longer address the demand making the need to move to a 21st century network automation imperative.

While in the past it took days to provision a service on the network and configure it – with the potential for errors – today it takes only seconds to provision using error-free automation with Alcatel-Lucent Enterprise Digital Age Networking.

In the Alcatel-Lucent Enterprise vision, the network becomes an enabler for a true digital transformation. It plays an active role in deploying and optimising digital business processes, and proposes productivity and new revenue generating services. This is made possible due to an increase in network operations automation. In this new paradigm, the network evolves from being a complex and costly underlying infrastructure, to a generator of new revenue streams with the lowest operational costs.

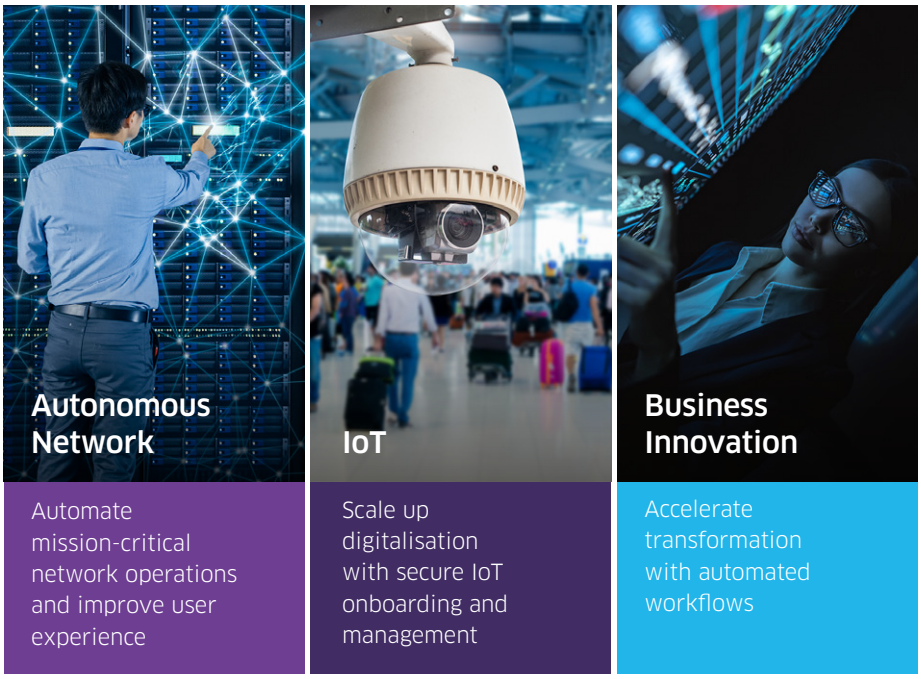
What is Digital Age Networking?

Digital Age Networking is ALE's enterprise networking solution that enables businesses and organisations to enter the digital transformation era where their digital business can achieve unprecedented levels of success. Its primary function is as a business enabler to help enterprises generate new outcomes by leveraging the latest technological evolutions in IoT, cloud, and Artificial Intelligence (AI).

Digital Age Networking addresses the key trends in today's enterprises and is comprised of three pillars:

- A high-performance Autonomous Network that can automatically provision network services and automate mission-critical network operations while improving the user experience
- IoT onboarding to enable enterprises to scale-up digitalisation through secure IoT provisioning and management. It can integrate, onboard, and connect a massive number of IoT devices that are at the foundation of new enterprise digital business processes.
- Business Innovation to help enterprises accelerate their digital transformation with new automated workflows, taking the effort out of labor-intensive or repetitive tasks

Networks are now in a perpetual transformation phase. They need to support an always-on, mobile user experience with a proliferation of connected things that need to be securely onboarded and managed. And they need to address the huge increase in data analytics. All this means the network is more mission-critical than ever before. With the need for the network to do more, it is essential to automate as many processes as possible, in order to reduce workloads, increase efficiency and reduce potential human errors.

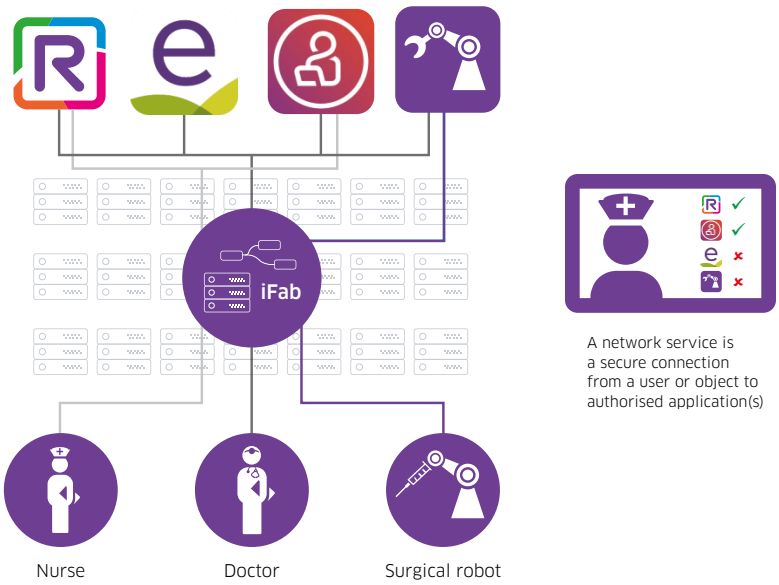


Autonomous Network

The foundation of Digital Age Networking is the Autonomous Network. IT infrastructure has evolved over the last 20 years to where it is now fully automated. Networks unfortunately have not kept up. While it takes minutes to deploy a new application, days if not weeks are needed to manually configure the enterprise network, element by element.

This is now changing. IT leaders are shifting their focus to business transactions rather than building and running the infrastructure as was previously required.

"By 2022, 90% of IT leaders will focus on facilitating transactions, not building or running infrastructure."[1]



The Alcatel-Lucent Enterprise Autonomous Network is configured and provisioned automatically. It ensures mission-critical, secure network operations, while optimising the user experience. As part of the Autonomous Network architecture, Intelligent Fabric (iFab) technology automates the deployment of the network and simplifies moves, adds, and changes, reducing the time and effort it takes to maintain and operate a network. In the future, with the help of machine learning, it will adapt automatically to changing business conditions and provide a secure connection automatically from a user, or object, to an authorised application. By analysing network configurations, Quality of Experience (QoE) measurements, and known issues, correlated with network hardware and software version information, the network management software will be able to suggest configuration changes and updates to the administrator.

The Autonomous Network provides a resilient and seamless connected experience with the Alcatel-Lucent OmniSwitch®LAN and Alcatel-Lucent OmniAccess®Stellar WLAN with ultra-fast convergence, secure network access control, assured QoS, and secure diversified code to ensure an OS hardened switch. New generation enterprise Wi-Fi with embedded WLAN control in access points removes the need for physical centralised controllers. This distributed architecture delivers the best performance and scalability, and ensures high-availability, with operational simplicity and low total cost of ownership (TCO). The WLAN solution is coupled with a comprehensive wired LAN that support deployment requirements ranging from access, to core, and data centre. All of this is supported in even the most extreme and harshest environments. A single Network Management System (NMS) provides an additional level of integration between wired and wireless networks.

1 Source: Gartner Report: 2018 Strategic Roadmap for I&O Automation, May 2018

This reduces the IT manager workload as they no longer have to handle two management systems with two sets of policies and configuration rules (one for the LAN, and another for the WLAN). The NMS provides unified service management and network-wide visibility, which can improve IT efficiency and business agility.

The Autonomous Network allows enterprises to automatically provision the network to properly support services to provide value for businesses, regardless of the type of connectivity that is required. A dedicated route can be set up from a data centre application to a user, or to an IoT device; a high-speed connection can be provided on the fly for a specific application need; a secure connection from an IoT device to a cloud application with dedicated encryption can be established from a user to a virtual machine. Every type of network service can easily be created and deployed on the network.

Unified Service and Network Management

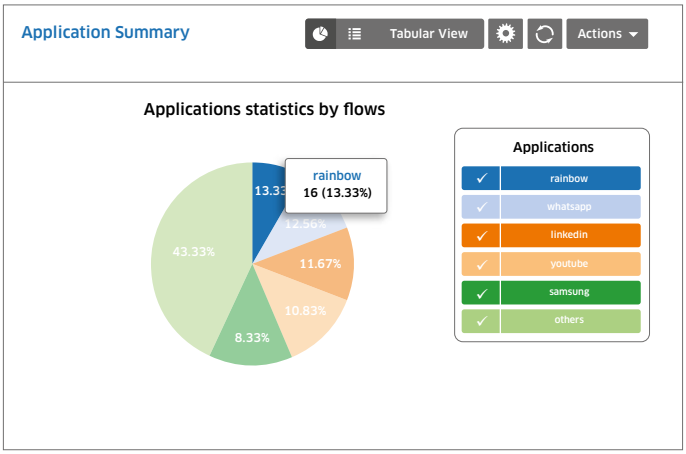
The ALE Network Management System (NMS) provides unified service management and network-wide visibility, which can improve IT efficiency and business agility. It provides a full set of management tools for converged LAN and WLAN campus. The single platform enables operators to easily provision, manage, and maintain a network infrastructure with its network elements, alarms, unified access security policies, and virtualisation. It also provides advanced network analytics for full visibility into wireless, devices and applications, as well as predictive analysis for forward planning.

Application visibility

The Autonomous Network collects application usage data from the various network elements (such as access points, and switches), by leveraging the embedded Layer 2 through 7 Deep Packet Inspection (DPI) capabilities.

Every application can be controlled centrally by the administrator. Rules and roles are set up by applying QoS policy enforcement such as, rate limiting, blocking, and application prioritisation, across the entire network no matter if it is wired or wireless.

The information collected can then be analysed to assess business outcomes, and to improve user experiences. The embedded analytics engine provides in-depth application usage reports and key measurement indicators.



Case study:
University of Technology Sydney

University of Technology Sydney (UTS) is one of Australia's largest universities, and a leading provider of technical education. UTS have provided a comprehensive educational curriculum to students since its inception in 1988 and are recognised worldwide as an outstanding example of expertise in technology education.

Communications and collaboration are fundamental to the UTS educational offering. UTS use technology to enhance teaching and learning through social media, audio, and electronic communications with students resulting in increased demand on the Wi-Fi network.

Challenges:

- UTS required a robust, high-performance network infrastructure to support a billion-dollar campus expansion plan
- Wireless access to multiple devices, to support students and faculty, throughout campus and housing developments
- Building a secure WLAN network in a high-density urban environment with large volumes of non-university device interference was also taken into account

Alcatel-Lucent Enterprise deployed a solution that was easy to configure across the network including wired and wireless, local, as well as branch integration with LDAP, AD, RADIUS. The solution helped with the end-to-end network configuration making sure the new application functioned properly. Once the application bandwidth and priorities are set configuration becomes automatic.

Case study:
Inspira Health Network

Inspira Health Network operates throughout southern New Jersey. It is the region's leading network of health care providers, delivering the full continuum of primary, acute, and advanced care services, with more than 60 clinical access points (hospitals, clinics, labs).

There had been multiple assessments involving the wired and wireless network, nurse workflow, and the overall IT environment. In each case recommendations were made and a roadmap was developed and implemented at a pace that made the most sense.

Challenges included:

- Growing network of facilities, including a merger with major hospital
- Federal mandates for use of electronic medical records and improving patient satisfaction
- Making clinical staff more effective for cost control as well as making their jobs easier

The ALE broad portfolio of solutions and ability to interoperate with existing infrastructure provided the solution Inspira Health Network was looking for.

Internet of Things (IoT)

Billions of connected devices are already deployed and this surge in IoT is not going to slow down any time soon.

The importance of these devices is undeniable. They are changing our lives, the world we live in, and the way we do business. However, this is just the beginning as IoT increasingly becomes the critical foundation and enabler for digital business processes.

IoT containment

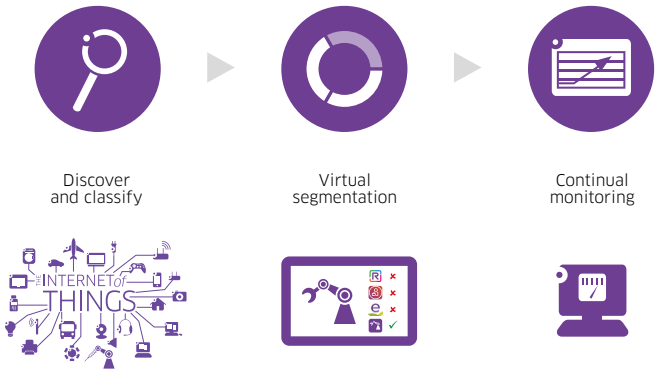
Connected objects' limited processing power prevents devices from having embedded, sophisticated security capabilities. This leads to two major problems; devices are hard to configure, and they are easy to hack. The highest security risk is not on the objects themselves, but rather on the doors they open to other network segments. Once the object is compromised and hacked, the whole enterprise network becomes vulnerable to attack vectors such as a trojan horse or other virus. When you consider the fact that enterprises connect thousands, if not millions, of these objects, the challenge becomes clear; configuration and management of individual devices is totally unrealistic, and the security risks are enormous.

The ALE IoT containment solution is designed to provide an automated solution to securely onboard IoT devices while protecting the network at the same time.

According to Gartner, in the next 5 years, "more than 50% of enterprise applications will be IoT-enabled. Within 2 years, 60% of all IoT devices will be virtually segmented, between themselves, and separated from traditional applications."[2]

Three major steps to connect, manage and properly control any IoT device, must be followed: discover and classify, virtual segmentation, and continuous monitoring.

"By 2024, at least 50% of enterprise applications in production will be IoT-enabled."[3]



Discover and classify: As a first step, each object connected to the network must be discovered and classified. Identifying the IoT device is the key to defining related network requirements and policies such as, quality of service, security and bandwidth. These parameters are added to a profile, in order to easily manage the service that is automatically created by the network.

To simplify network configuration steps, Digital Age Networking provides the ability to access a very large (29+ million) device database to immediately identify the object connected to the network and automatically provision a configuration associated with a specific device. There is no need to manually search for devices on the database, this becomes automatic.

2 Source: Predicts 2019: IoT Will Drive Profound Changes to Your Core Business Applications and IT Infrastructure, December 2018

3 Source: Gartner Report: IoT Solutions Can't Be Trusted and Must Be Separated From the Enterprise Network to Reduce Risk, May 2018

Virtual segmentation: As a second step, it is critical to segment single physical network infrastructures into separate virtual networks, or containers, to ensure that each service, or application, has its own dedicated segment, ensuring proper function and secure operations. With this step, the traffic of a specific IoT device is contained to a single instance and can be easily blocked from communicating with other portions of the network, in the event of a security issue. Segmentation is created for the application to which the device needs to connect and is automatically provisioned into the network.

Continuous monitoring: In the third and final step, the network monitors behaviour to ensure that the IoT devices and applications are functioning as desired. Each authorised object is stored in an inventory. This enables IT to know exactly and instantly, how many devices are connected on the network, along with the vendor device type and serial number, exact location in the facility, and status on the network. Valuable IT staff time is no longer wasted looking for objects in the enterprise facility in order to update IoT inventory. The ALE strategic vision is to be able to indicate when a device has to be serviced by connecting to the device vendor inventory management system. Ensuring that all network-connected assets are clearly identified in a database, and maintained or upgraded, based on a predetermined timeline, improves global information system security.

It is important to continuously monitor a connected object on the network to take immediate action in the event that there is a deviation from usual behaviour. For example, if a device that usually sends a few kilobytes of data per second suddenly starts sending a large amount of data, or sends multiple Domain Name Services (DNS) requests, the network immediately knows that something is wrong. The network can take actions such as, disconnecting the faulty device, sending a notification to the network administrator, or changing the destination of the dedicated container for further verification. All these processes and actions can be automated, or network administrators can choose to receive notifications and take the actions themselves.

The ALE IoT containment solution delivers substantial benefit. Once authenticated and profiled in terms of an authorised related application, the solution virtually segments the physical infrastructure to make sure each object connected to the network receives the right quality of service (QoS), bandwidth, and security. The network leverages the user, object, and application profiling capabilities to easily and automatically create and assign virtual networks to each IoT device, making sure only the right application(s) can run within a container. The ALE IoT containment solution has enabled many enterprise customers to turn a single physical network into a multi-service network, capable of supporting the digital business needs of today and tomorrow.

Case study

ALE addresses network needs at one of SEA's busiest airports

An increase in passenger traffic at a renowned state-owned facility responsible for managing airport operations and service providers was causing strain on the organisation. The increase in daily traffic prompted the organisation to scale-up operations to provide better stakeholder connectivity. Adding resources on the ground and in the network was essential to ensure successful operation and collaboration between staff. The result is an improvement in the management of network infrastructure, bandwidth allocation and connectivity.

Challenges:

- Increased passenger capacity at the airport which doubled after the terminal was opened
- Unprecedented flows of data, as well as operational and management challenges to the network infrastructure, and increased security risks from all end-points
- Creating a network design to provide the intelligence, automation and security to meet the increased demand

Alcatel-Lucent Enterprise offered a multi-level security approach with a combined LAN/WLAN and IoT containment solution. For example it included: Network switches for efficient bandwidth distribution; controller-based access points for Wi-Fi connectivity with multiple devices; network infrastructure for secure connection to take advantage of the benefits and mitigate the risks of IoT deployment.

The IoT containment strategy helped to simplify and secure device onboarding and deliver the right network resources to efficiently operate the system in a secure environment to safeguard against cyber attacks.

Business Innovation

New business processes are optimised when they leverage user, application, and IoT metrics in real-time. Digital Age Networking can help businesses optimise processes and services. This is the key to innovation, improved productivity, workflow optimisation, and an enhanced user experience.

Technology innovations including IoT, location services, and collaboration platforms are at the forefront of business process and services automation. Alcatel-Lucent Enterprise is leading the way by integrating these components to help enterprises reap the benefits of their technology investments.

Alcatel-Lucent OmniAccess Stellar Location Services, which include asset tracking and location-based services, can help increase safety and reduce both operational and asset-related costs.

Alcatel-Lucent OmniAccess Stellar Asset Tracking provides real-time and historical location of users or objects, in indoor facilities, using Wi-Fi and Bluetooth technologies.

This information allows businesses to better understand workflows, increase utilisation of equipment, significantly reduce the time it takes to find someone or something, avoid lost or stolen assets, and increase productivity, while enhancing user experiences. From an operations perspective, misplaced or lost equipment incurs heavy costs to businesses every year. Knowing where assets are in a real-time, or where they are stored, can help businesses keep equipment costs under control. Other key OmniAccess Stellar Asset Tracking features include real-time hot spot tracking and historical contact tracing which can help identify areas where crowd restrictions are being exceeded, or allow follow-up notifications with individuals in the event of an incident such as, possible exposure to harmful chemicals or infectious diseases.

Alcatel-Lucent OmniAccess Stellar Location-based Services (LBS) includes wayfinding (self-navigation indoors), and geonotifications (push messages) based on geolocation, all managed from a cloud application. Wayfinding enables turn-by-turn directions to offices and conference rooms, as well as other points of interest such as, the cafeteria and restrooms. Geonotifications are messages relevant to the location, which can be sent to employees' and visitors' mobile devices. LBS enables businesses to understand user behaviours and patterns. The LBS cloud application captures the data and provides analytic dashboards that can be used to optimise people, assets, and operational workflows. This information can help businesses and facilities run more efficiently, enable indoor navigation, and generate revenue by offering customer promotions and services based on the customer's location.

Real-time and historical data with a geolocation context enable the development of new innovative digital business processes and services. Integrating data from the OmniAccess Stellar Location Services with a business collaboration tool like Rainbow™ by Alcatel-Lucent Enterprise enables automation of simple or repetitive tasks. It also enables the development of workflows that can be automated using triggers, rules, and actions.

Case study

Cambodian educational institute adopts ALE solution to address growing user demand

An educational centre of excellence based in Cambodia that delivers higher learning for the student community was experiencing an increase in the number of students bringing their own devices to school. As well, digital assessments were becoming standard.

With new methods of online learning being introduced into the education curriculum, and demand for high-performance networking everywhere, the organisation and the existing network infrastructure were both being strained.

Challenges:

- An increase in the user base and the number of devices on campus
- Traditional network management features, as well as limited access to guest and BYOD support
- Delivering the right integrated security at every layer of the network

The Alcatel-Lucent OmniVista® Cirrus Network Management as a Service solution was implemented to address the challenges. It offers a high-performance network infrastructure that is simple to deploy, operate and maintain. OmniVista Cirrus is a scalable network solution with unified cloud-based management and on premises LAN switches and Wi-Fi access points. Because it's cloud-based the organisation never has to worry about servers, maintenance, or software upgrades. OmniVista Cirrus goes beyond traditional network management functions with integrated guest access, BYOD support and analytics at no additional cost.

Conclusion

Digital Age Networking is the Alcatel-Lucent Enterprise blueprint that enables businesses and organisations to enter the digital era and grow their digital businesses.

ALE digital transformationew3 is based on three pillars:

- An **Autonomous Network** that easily, automatically, and securely connects people, processes, applications, and objects: The ALE Autonomous Network is based on a streamlined portfolio complete with a true unified management platform, delivering common security policies across our LAN and WLAN. The Autonomous Network also provides deployment flexibility indoors, outdoors, and in industrial environments. Network management can be delivered on premises, in the cloud, or in a hybrid deployment, depending on the customer preference.
- Secure and efficient onboarding of **IoT** devices: Segmentation keeps devices in their dedicated containers and minimises the risk of having the device and network compromised. IoT containment can help businesses easily and automatically understand if the device is behaving properly, or not, and help to keep the network safe.
- **Business Innovation** through workflow automation: Integrating user, applications, and IoT metrics in real-time, with geolocation data, into Rainbow workflow capabilities, simplifies the creation and roll-out of new automated digital business processes and services. This is the key to business innovation, enhanced productivity, and enabling new revenue streams.

Alcatel-Lucent Enterprise is committed to developing networking technology and solutions that help organisations realise their business potential through digital transformation.