



Digital Age Networking in Enterprises

Table of Contents

Abstract.....	3
What is Digital Age Networking?	3
Why is it important?	4
Connectivity	5
Service Defined Network	5
IoT	8
IoT containment	8
Augmented intelligence	10
Cloud economics	11
Flexible business models: Network on Demand (NoD).....	11
Location-based services (LBS).....	11
Conclusion.....	13

Abstract

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 organizations 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, is 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 optimizing 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, into a generator of new revenue streams with the lowest operational costs.

What is Digital Age Networking?

Digital Age Networking is the enterprise networking solution that enables businesses and organizations 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).

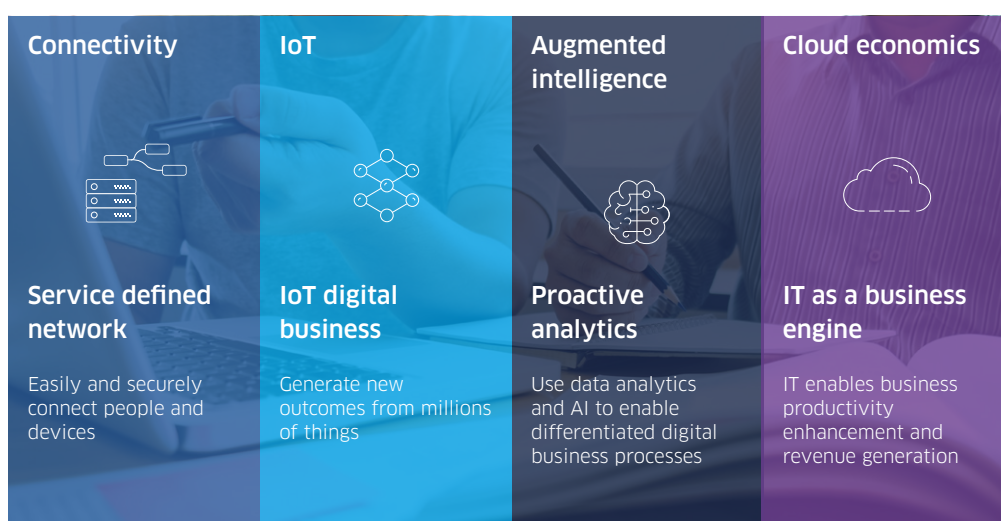
A Digital Age Networking foundation is a high-performance Service Defined Network that automatically provisions network services that guarantee the user Quality of Experience (QoE) and secure IoT onboarding. The solution automatically translates business requirements into network services provisioning, and configures the network to efficiently support the requirements. The solution recognizes and optimizes the QoE of all users, and ensures users do not access unauthorized applications. Digital Age Networking can integrate, onboard, and connect the massive number of IoT devices that are at the foundation of the new enterprise digital business processes.

Why is it important?

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.

Digital Age Networking addresses the key trends in today's enterprises:

1. **Connectivity:** At the foundation of Digital Age Networking is a high availability, Service Defined Network solution that spans from the datacenter, to the access layer. It allows a business to setup and manage network services automatically, to easily and securely connect users, devices, and applications.
2. **IoT:** A rapid increase in the number and types of devices connecting to business networks is creating challenges in the network infrastructure. The network needs to simplify and secure onboarding of these millions of devices. This is critical to generate new outcomes from the connected objects. Digital Age Networking delivers unique IoT fingerprinting, containment, inventory and behavior analysis.
3. **Augmented intelligence:** Enterprise digital businesses, as well as their underlying network architecture need to constantly adapt to be successful. A Digital Age Network can proactively adapt using machine learning and data analytics gathered from application usage, and user quality of experience. Administrators automatically get notifications about potential anomalies, and user or device misconduct. They can also get recommendations for network optimization and suggested changes.
4. **Cloud economics:** Cloud enables transformational new business models in which IT becomes a business engine. The commercial models based on cloud “pay-as-you-go” services help address IT budget constraints. These new business models can address the financial impact of system updates and new technology adoption. New technology can translate into new value-added services and new revenue streams. With Digital Age Networking, the network and cloud can leverage new and innovative services such as location-based services, and it can introduce digital services that can be provided to external businesses for a fee, to help fund the infrastructure.



First and foremost, businesses need to provide their digital network users, devices, and IoT, with excellent wired or wireless connectivity.

The foundation of Digital Age Networking is the Service Defined 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. 2019 is the year to deploy real network automation. ALE is at the forefront of this market evolution.

A network service is a secure connection from a user or object to authorized application(s)

Network services are provisioned at the access layer using Universal network Profiles (UnP) to ensure that the right policies (departmental and application access, security, performance and Quality of Service (QoS) parameters) are established for users and devices. User, object, and application policies are applied consistently, regardless of location and type of connection; Ethernet or Wi-Fi. Digital Age Networking simplifies and secures how people, devices, and objects connect, while delivering a performance level that is fine-tuned for individuals, groups, objects, or assets.

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

The ALE Service Defined Network provides a seamless connected experience with the Local Area Network (LAN) and Wireless Local Area Network (WLAN) tightly integrated. New generation enterprise Wi-Fi with embedded WLAN control in access points remove the need for physical centralized 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 center. All of this is supported in even the most extreme and harsh environments.

A single Network Management System provides an additional level of integration between wired and wireless networks. 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).

ALE Service Defined Network technology 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 center 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

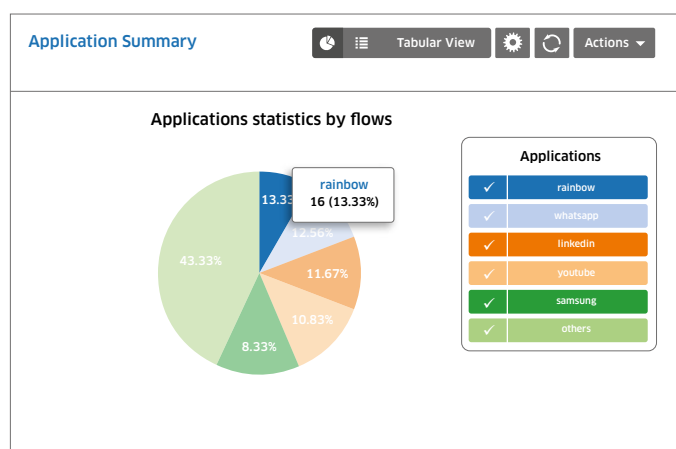
The ALE [Network Management System \(NMS\)](#) provides unified service management and network-wide visibility, which can improve IT efficiency and business agility. It provides a full set of management tools for converged LAN and WLAN campus. The single platform enables operators to easily provision,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

Application visibility

A Service Defined Network collects application usage data from the various network elements (such as access points, and switches), by leveraging the embedded Layer 2 through7 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 prioritization, across the entire network no matter if it is wired or wireless.

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





Customer case study: **Nevada Department of Transportation (NDOT)**

Nevada Department of Transportation (NDOT) wanted to lay the foundations for its next-generation Intelligent Transportation System (ITS), making it easier to connect and manage the growing mesh of Internet of Things (IoT) devices on the state's highways.

NDOT is responsible for the planning, construction, operation and maintenance of the 5400 miles of highway and over 1000 bridges that make up Nevada's state highway system. NDOT's primary goal is "safety first".

One of NDOT's objectives was to increase safety on the state's roads by offering drivers real-time information on road, traffic and weather conditions. To achieve this NDOT needed to harden its data network to withstand the harsh Nevada climate and support a growing number of devices.

Looking to the future, NDOT wanted to lay the foundations for its next-generation Intelligent Transportation System (ITS), making it easier to connect and manage the growing mesh of Internet of Things (IoT) devices on the state's highways.

The ALE solution makes it simpler to provide the best services throughout the 25 billion miles traveled by road users annually, providing the right information for safe travel and ultimately reducing the time spent on the road.



Customer 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.

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. This is just the beginning, however, as IoT increasingly becomes the critical foundation and enabler for digital business processes.

IoT containment

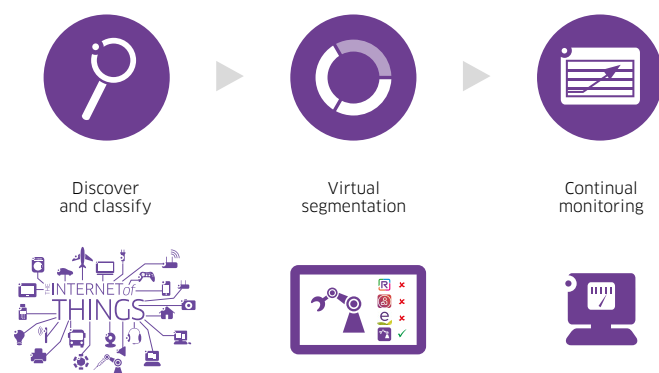
Connected objects' limited processing power prevents devices from having embedded, sophisticated security capabilities. This leads to two major problems; devices are hard to configure, and they are easy to hack. The highest security risk is not on the objects themselves, but rather on the doors they 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.”³

Three major steps to connect, manage and properly control any IoT device, must be followed: discover, segment, and monitor.

“By 2024, at least 50% of enterprise applications in production will be IoT-enabled. By 2021, more than 60% of all IoT devices on enterprise infrastructure will be “virtually segmented” from traditional business applications, up from less than 5% today.”⁴



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, the ALE Digital Age Network provides the ability to access a very large (17 million) device database to immediately identify the object connected

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

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

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.

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.

In the third and final step, the network monitors behavior to ensure that the IoT devices and applications are functioning as desired. Each authorized 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 behavior. 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 authorized 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.



Customer case study: Fortaleza

The Prefeitura de Fortaleza, a city in Brazil with more than 2.6 M inhabitants, has been modernizing its infrastructure to provide better and more efficient service to citizens. After investing in more than 300 kilometers of fiber optic cables, the city wanted to upgrade its network.

The municipality required a solution that offered a quick and easy implementation across its many departments including: administration, schools, hospitals and clinics, local police fire fighters.

The network had to be robust and reliable enough to support more than 9200 Internet of Things (IoT) devices, including CCTV cameras to improve public safety. These devices are currently securely connected, and the network architecture is ready to support many more.

The ALE Service Defined Network, has increased network speed and agility, improving the overall network performance by 10 times. The Prefeitura enjoys simplified, centralized network management that allows the network manager to create and deploy new services in few minutes instead of days.

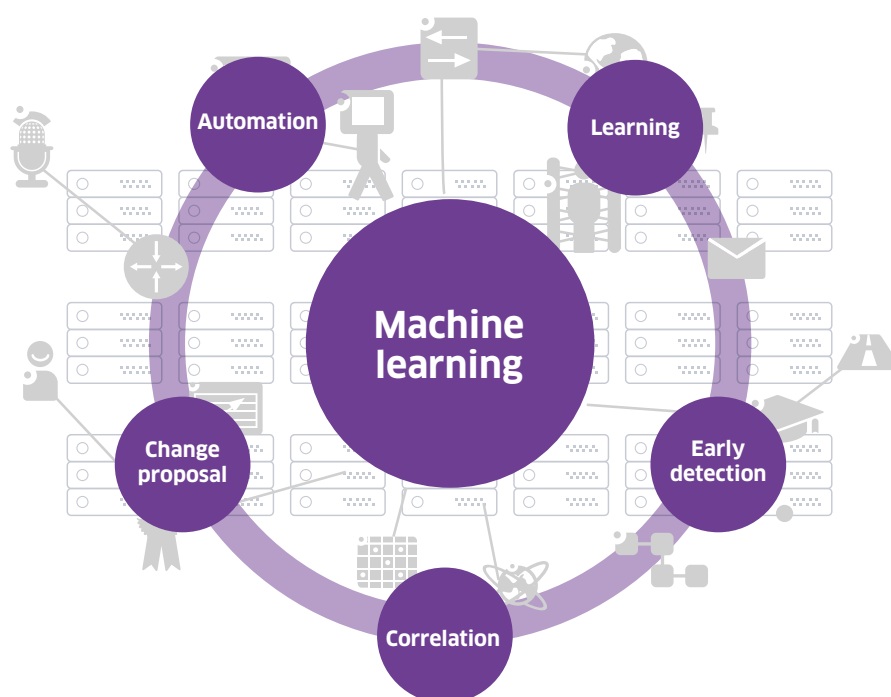
Augmented intelligence

The next level of network intelligence comes from AI, data analytics and machine learning, to enable better correlation among events on the network, user and device behavior. We call this proactive analytics as these elements also provide a deeper correlation between factors to provide a clearer understanding of facts, prevent potential problems, and enable differentiated digital business processes.

A Digital Age Network must guarantee an excellent QoE for users and keep them safe against potential security breaches from connected objects.

The ALE Digital Age Network recognizes the QoE of its users and can quickly identify problems on the network. For example, if a device takes too long to connect to the WLAN, the network can rapidly identify the issue based on continuous analysis of the connection times. It will then take remediation actions to solve the problem. The network will then send a notification to the administrator to indicate if the problem can be automatically fixed.

With regard to connected objects, the Digital Age Network automatically disconnects or quarantines devices that act outside of a “reasonable” threshold as that behavior could signify that the device has been hacked. This function is automated to ensure the quickest possible response time. The network administrator can, of course, change this and decide to manage it directly within the NMS.



Gartner believes that “by 2023, 40% of IT teams will use augmented intelligence to automate IT productivity”.⁵

As part of the ALE strategic vision its network management system will be enhanced with machine learning, to analyze network configurations, QoE measurements, and known issues, correlated with network hardware and software version information. The network will then be able to suggest to the administrator, configuration changes and updates. Once approved by the network administrator, the changes can be applied to the network. The goal is for the network to, increasingly, be able to support digital business processes and services on its own.

⁵ Source: Predicts 2019: Artificial Intelligence Core Technologies, November 2018

Cloud economics

Cloud business models are clearly influencing IT economics which can be leveraged to finance network evolutions.

“By 2021, 60% of enterprises will propose economic and procurement models different from today’s, to secure budgets from executive leaders and board of directors.”⁶

Flexible business models: Network on Demand (NoD)

Transforming to a digital business can require significant IT investment, which may not be possible with today’s IT budget constraints. ALE proposes an alternative way to deliver, and finance technology in support of business digitalization using demand-driven models.

ALE has been leading this trend with **NoD**, which is essentially an “Infrastructure as a Service” for enterprise businesses. As an alternative to technology procurement based on a capital expense (CAPEX) model, ALE NoD offers a subscription model based on a monthly fixed operational expense (OPEX) fee.

These types of consumption and subscription models deliver the same solutions and innovative technologies as they would if they were purchased using a traditional (CAPEX) model, without the upfront investment. It is an opportunity for organizations to simply consume network technology, and it provides network configuration automation that allows the business to shift IT employees to focus on value-add digital transformation projects.

ALE supports multiple deployment options to adapt to various requirements for example, public or private cloud, and single or multiple instances. These offers are available through the managed services propositions provided ALE accredited resellers who implement this innovative and disruptive new model.

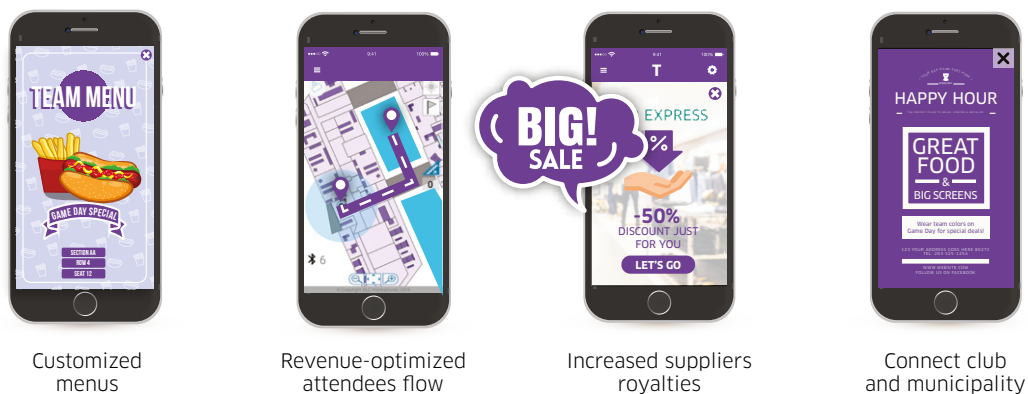
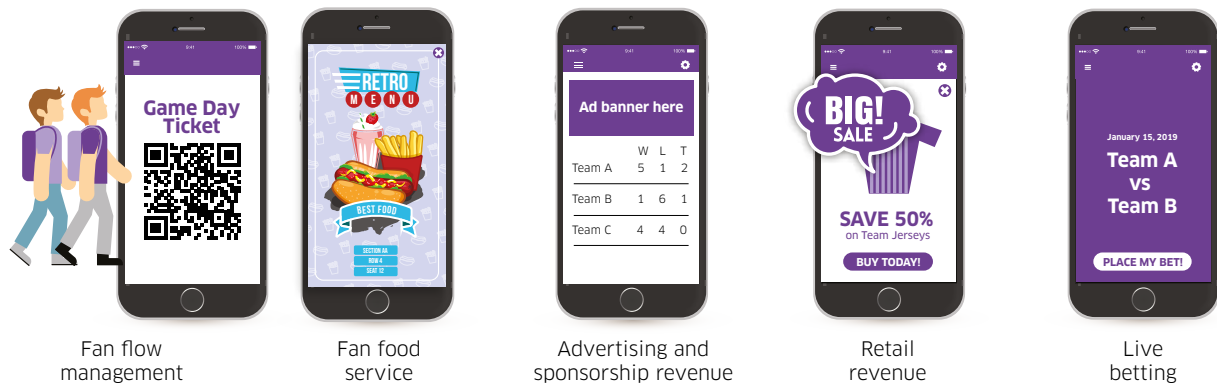
Location-based services (LBS)

According to Gartner, the fast path to digital business transformation will be to convert internal capabilities into external revenue generation opportunities.⁷ Some businesses do not have the budget to fund the necessary network infrastructure investment that may be required to deliver the next generation customer or consumer services. Subscription OPEX-based models can help, but sometimes even that is not enough, and an organization may need to obtain funding from other lines of business such as, marketing or business partners. An example would be a stadium that does not have the budget to refresh its Wi-Fi infrastructure to offer an enhanced fan experience. However, geolocation technology, which provides many use cases to generate revenue, can help the stadium fund the Wi-Fi refresh.

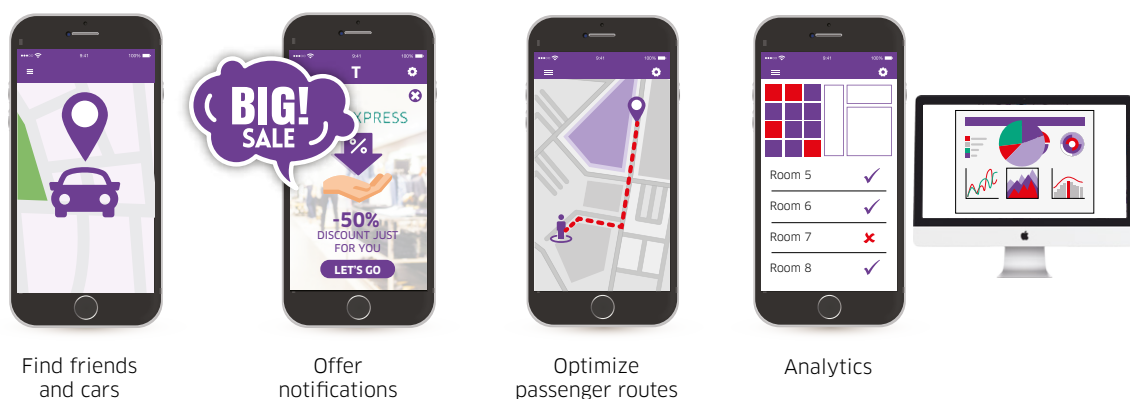
With geolocation, if one of the stadium entrances is crowded, fans can be redirected to another entrance via the stadium app. If fans move through security quickly, they have free time to visit a retail shop or stop for a meal. The stadium can deliver value-added services such as serving meals and drinks to fans at their seats. The app, which delivers team news and game stats, can also be used to generate advertising revenue. Pushing promos for goods and services, and directing fans to the retail area can significantly increase revenues. These new revenue streams are poised to deliver a strong return on investment (ROI) that will enable the stadium to finance a new ALE state-of-the-art network.

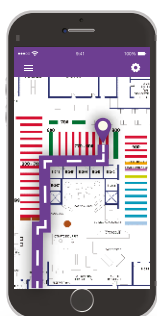
⁶ Source: Predicts 2019: Artificial Intelligence Core Technologies, November 2018

⁷ Gartner Unveils Top Predictions for IT Organizations and Users in 2019 and Beyond, OCT 2018

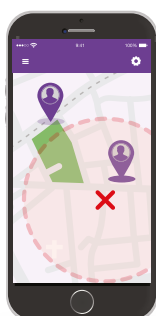


ALE LBS based on Wi-Fi and Bluetooth technologies, provide the location of users or objects, in indoor facilities. This information allows businesses to increase productivity and enhance user experiences. In addition to the products or services that the business normally sells, it can also boost revenues. LBS includes self-navigation through a hotel, an airport, a hospital, or a university campus, similar to using turn-by-turn direction apps in a car. LBS also provides push marketing notifications and the ability to set up virtual boundaries, or geo fences, where crossing those boundaries can initiate an action to a nearby consumer or employee, such as pushing a sales offer, point of reference information, a security alert, or enforcing a policy such as hand hygiene in a hospital.





Asset optimization



Security and safety



Optimize workforce

LBS can help businesses engage with customers and consumers, whether they are students, patients, visitors, or travelers in an airport. The additional value for the business is understanding user (anonymously) behaviors and patterns. Businesses can use analytics to measure and analyze data patterns to optimize workflows, offers, and services, based on the behaviors that they discover.

The use of badges or tags, make it possible to locate people or objects such as wheel chairs and beds in a hospital, luggage and electric carts in an airport, and projectors and monitors at a university. These services are important for improving productivity.

For example, if a person with reduced mobility requires assistance, the nearest wheelchair can be quickly located, and the nearest staff can be notified to assist the passenger. When security personnel need to be mobilized, knowing who is closest to an incident can reduce response time.

From an operations perspective, misplaced or lost equipment can incur a heavy cost to businesses every year. Knowing where assets are in a real-time, or where they were last seen, as historical location information, can help businesses keep equipment costs under control. The projector that went missing from a classroom, or the luggage that was sent to the wrong gate, or the wheel chair that can't be located in a hospital are just a few examples of scenarios that can be avoided with the ALE LBS solution.

The goal for a business is to boost revenues, reduce costs, or both. The ALE LBS solution can help achieve these objectives, and turn IT into a business engine.

Conclusion

Digital Age Networking is the ALE vision and strategy that enables businesses and organizations to enter the digital era and grow their digital business to unprecedented levels.

The Service Defined Network foundation easily, automatically, and securely connects people, processes, applications, and objects, which enable digital business transformation to generate new outcomes. This foundation supports the services that enterprises need to grow their business.

Digital Age Networking enhances security and can automatically onboard the IoT devices required to help the business succeed. Fingerprinting and classification simplify IT tasks. Segmentation keeps the devices in their dedicated containers and minimizes the risk of having the device and network hacked. IoT containment can help businesses easily and automatically understand if the device is behaving properly, or not, and help to keep the network safe.

Augmented intelligence maximizes network configurations and simplifies troubleshooting. It can also be proactive and send notifications about potential problems. With augmented intelligence the network is smarter and can understand the QoE and identify problems when operations degrade below a specified threshold.

Digital Age Networking relies on cloud technologies to provide value-add services to improve productivity and generate new revenues. Cloud solutions offer optimum financial models, with the option to choose between CAPEX and OPEX.

Alcatel-Lucent Enterprise is committed to developing network technology and solutions that help businesses realize their digital transformation.