A comprehensive approach to the IoT challenge

Alcatel·Lucent
Enterprise

Table of Contents

Introduction

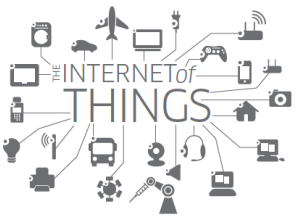
The Internet of Things (IoT) is a hot topic in all industry sectors, including residential and commercial markets. In the enterprise arena, digital transformation is accelerating the number of IoT devices being connected and accessing applications and data.

This whitepaper looks at how IoT is transforming enterprises and how Alcatel-Lucent Enterprise Digital Age Networking manages IoT devices in an automatic and secure manner while enabling seamless integration into business-oriented digital processes.

Discover and classify

Virtual segmentation

Continous monitoring



Exploring the IoT world

What is IoT?

While there are many complex ways to define the Internet of Things (IoT), one of the simplest ways to describe it is "connecting things to the internet." However, the question then becomes, what are the 'things' and why are they being connected to the Internet?

'Things' are physical objects that are embedded with technology such as sensors and actuators, as well as software and network connections. Connecting 'things' to the Internet enables them to interact and exchange data with other devices and systems, as well, they can be controlled remotely.

Why is IoT important?

IoT offers enormous value to businesses undergoing digital transformation. Enterprises must collect and process large amounts of data to understand the health of the business, to identify areas requiring improvement, and to optimize workflows for better outcomes.

IoT devices are autonomous data collection points that can provide instant or historical, up-to-date information. They can interact with other systems in many ways, depending on their function. Some can send data periodically, some can receive commands, while others can trigger actions and alerts. This versatility makes IoT essential to the automation and optimization of business processes.

The IoT explosion

Enterprises are integrating a multitude of devices, from sensors, surveillance cameras, and digital door locks, to industrial machinery and medical equipment. The objective is to streamline building management, improve security and energy savings, and address specific business activities.

Billions of connected devices have already been deployed. According to Gartner, IoT devices are forecasted to grow to 23 billion in 2020, with a projected increase to 56 billion in 2023[1].

1 Gartner, Internet of Things Forecast Database, September 2020

The recent health crisis has impacted IoT technology investment in 2020 across all industries. However, as recovery takes place in the coming years, technology must be ready to support the demand for IoT devices in areas such as people tracking, contact tracing, connected healthcare and 'tap-to-pay' contactless payment.

IoT heterogeneity/complexity

There are many different types of IoT devices to support the many functions they perform – which means dealing with many different technologies. However, the limited processing power of connected objects prevents the devices from having embedded, sophisticated security and management capabilities.

This creates two major problems; devices are hard to manage, and they are easy to hack. The highest security risk is not with the objects themselves, but rather the implications when a compromised object enables access to the enterprise network and data.

When there are hundreds or thousands of devices, management of individual devices is not realistic, and the security risks are enormous.

From connectivity to IoT integration into digital business processes

Digital transformation has been a growing trend and is currently experiencing an unexpected surge in 2020 due to the global pandemic. Enterprises are increasingly aware of the importance of the need to digitalize their operations and processes. The IoT phenomenon cannot be left out of this transformation as IoT becomes a critical foundation and enabler for digital business processes.

As security and management challenges are overcome, enterprises will be tasked with optimizing the business potential from an IoT rich network.

A multi-faceted solution

IoT poses a complex challenge for enterprise networks. It requires connecting many different objects quickly and efficiently without impacting the network performance, for example; speed, latency, and service continuity. At the same time the integrity of company data and business activity must be protected against potential cyberattacks. These requirements must be accomplished and managed with limited IT resources.

Integrating IoT into a company strategy is a complex undertaking that requires putting a great deal of intelligence on the network. Network automation, flexibility, integration capabilities and openness are required for smooth interaction. A multi-faceted solution capable of integrating network equipment, people, objects and applications, working and interacting together safely with optimized workflows provides the components for a successful digital transformation.

IoT network challenges

For a successful IoT operation, the underlying network needs to provide the connectivity, security, and management, all working together seamlessly. As well, an understanding of both the business and the network is paramount to design the appropriate strategy.

As an expert provider of end-to-end enterprise solutions Alcatel-Lucent Enterprise delivers the technology to help address enterprises' business and network challenges. In this section, we will look at IoT challenges and how Digital Age Networking is delivering the solutions that organizations and IT Managers need.

Let's begin with a quick overview of the most common standards and protocols for IoT connectivity.

IoT connectivity technology overview

IoT devices can be either wired or wirelessly connected to the network. **Ethernet** is the leading technology for wired connectivity. It supports high-bandwidth, power is not a problem, and the distance can be either short or long-range, depending on the type of cabling being used: Up to 100 meters in the case of copper cabling, and several kilometers in the case of optical fibre.

For wireless connectivity, there are a number of possibilities depending on different factors. One of these is the distance to where the IoT devices will be connected. Short-range wireless technologies include **Wi-Fi, Bluetooth Low Energy (BLE), Zigbee, Thread, NFC** and **RFID**, among others. Medium-range technologies include **LTE** and **5G**. Long-range include **LoRaWAN**, **SigFox** and **satellite-based communications**.

According to a recent market analysis of WLAN infrastructure by the 650 Group, the split between the WLAN-based and non-WLAN-based wireless IoT in number of units is about 40% for Wi-Fi and 60% for non-WLAN technologies. Of these, Bluetooth and Zigbee together represent 50%, while LTE, 5G, LoRaWAN and SigFox share the remaining half with others[2].

Wi-Fi and Bluetooth have become the most popular due to their expansion into the domestic and personal environments. These wireless technologies support high bandwidth but have limited range and consume battery quickly. They are suitable for consumer market applications that require continuous data streaming and where user devices can be easily charged. These include devices such as speakers, wireless headsets, fitness bands, among other wearables.

However, in enterprise environments Wi-Fi lacks the necessary range and consumes too much power for many IoT applications. For this reason, Wi-Fi HaLow and Wi-Fi 6 standards have been designed to provide optimized Wi-Fi connectivity for IoT.

Wi-Fi HaLow (802.11ah), designed for low data rate, uses narrow sub 1GHz band, which means that the signal can penetrate tough areas where 2.4GHz and 5GHz signals are absorbed, and can reach up to a distance of one kilometer at low power. Wi-Fi 6 (802.11ax), the latest generation high-efficiency Wi-Fi standard, introduces additional IoT-friendly features providing longer battery duration, better performance in high density and outdoor areas, and higher security.

For Bluetooth standards, BLE is designed for devices that use less data with lower energy consumption, which fit in many industry scenarios. BLE along with Thread and Zigbee are popular mesh networking standards used to add wireless connectivity to home automation, industrial automation, smart lighting, and building automation. BLE is also the technology of choice for indoor location services that require accuracy in the range of three to five meters. All these are low power consumption technologies that can run on small batteries for several years and are suitable for applications that need to send small amounts of data over a limited range.

[2] 650 Group· "Connected Wireless Devices and Internet of Things (IoT) Long-Term Forecast Market Report" June 30, 2020

For medium-range coverage, technologies for mobile networks such as Long Term Evolution Machine Type Communications (LTE-M) and 5G are oriented to IoT applications. LTE-M is a Low-Power Wide-Area Network (LPWAN) based on 4G but with specific energy saving protocols. While 5G with high bandwidth capacity is being heralded by mobile operators as the emerging technology for IoT transformation in many sectors, such as the automobile industry for autonomous cars, and smart cities.

In long-range environments LoRaWAN is designed for large scale networks. LoRaWAN is a LPWAN that can transmit small amounts of data across distances above 10 kilometers while maintaining low power consumption. This makes it suitable for IoT deployments that require low data rates and long battery duration in remote locations. Smart metering to optimize energy consumption in smart cities and industrial environments, weather monitoring in agriculture, or smart logistics in ports are examples of LoRaWAN applications.

IoT challenge #1: Heterogenous standards and protocols

There are many standards for IoT connectivity and the decision about what to select for a particular IoT deployment depends on several factors such as whether:

- The IoT devices are wired or wirelessly connected
- They are battery-powered
- They need to stream large amounts of data frequently, or just send small pieces of information from time-to-time
- They need to transmit over very long distances or a short range

In general, whenever possible, industries prefer low energy consumption technologies. However, some specialized sectors may need IoT networks capable of transmitting a lot of information over very long distances, which requires high energy consumption.

As many different types of IoT may be needed by a single enterprise, the ideal network must be ready to support several standards.

The Alcatel-Lucent Enterprise solution

Digital Age Networking provides multi-standard IoT support to cope with a large variety of enterprise scenarios and deployments.

Ethernet, Wi-Fi, BLE and Zigbee connected objects are natively supported by Alcatel-Lucent Enterprise network equipment. With this support, ALE covers many types of IoT devices and use cases in vertical sectors such as healthcare, hospitality and education.

In the long-range arena, ALE integrates LoRaWAN through a third-party, opening the door to address typical scenarios for smart cities in the government and transportation sectors.

In addition, Alcatel-Lucent Enterprise implements an IoT hub ready to integrate other IoT technologies through standard APIs. The IoT hub is an IoT controller which provides the versatility to adapt to end-customer scenarios through the implementation of gateways and connectors, as required by each project. The IoT hub software platform collects IoT data and models it to deliver advanced services, such as data-driven decision making, IoT-to-human and human-to-IoT services, and automation. Alcatel-Lucent Enterprise has successfully deployed IoT networks including industrial devices that communicate using standards such as MQTT and Modbus, as well as, other network automation and building automation scenarios based on KNX.

IoT challenge #2: Managing network access

Enterprises will usually have wired and wireless IoT objects connecting to the network. Therefore, both the LAN and WLAN must be ready to comply with the necessary connectivity and security requirements. The network must also cope with onboarding a huge variety of heterogeneous devices from many different vendors, and with many different capabilities.

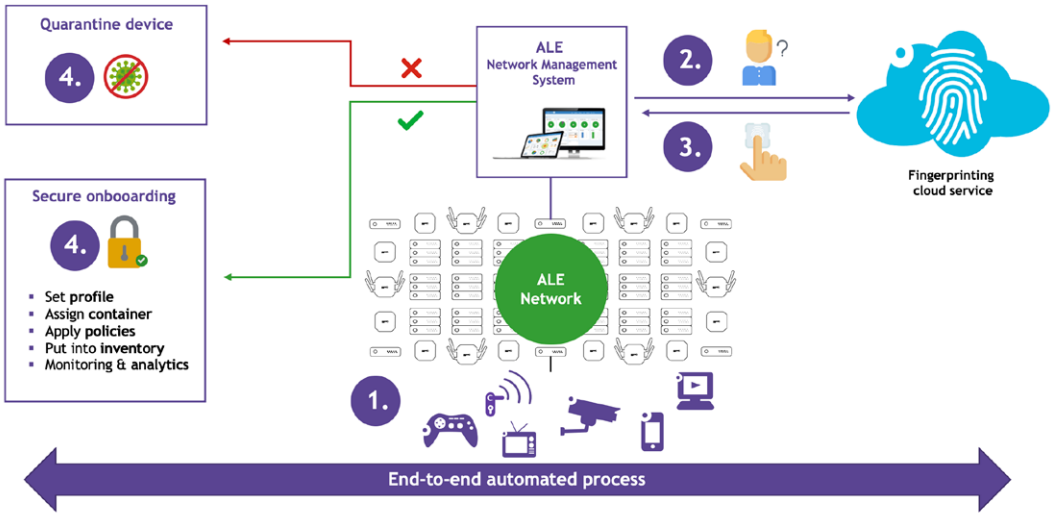
Under this premise, implementing unified access and centralized security policies for wired and wireless networks becomes paramount to simplify the complete procedure and minimize security risks.

As the number of devices moves into the thousands, automation of access procedures becomes a priority for IT managers.

The Alcatel-Lucent Enterprise solution

The Alcatel-Lucent Enterprise network fabric can onboard both wired and wireless IoT objects in a consistent and secure way, based on centralized security polices, unified access and Universal Network Profiles (UNP) implemented in access switches and access points.

How do IoT devices connect to an ALE network? Whenever a new IoT device tries to connect to a switch or access point, the Network Management System (NMS) will collect the object's data and ask a cloud-based fingerprinting service to identify the object by its unique fingerprint. Once the object is identified it is automatically classified and assigned a UNP with specific requirements for security, bandwidth and Quality of Service (QoS). The discovery, classification and profiling of IoT objects is totally automated in Alcatel-Lucent Enterprise Digital Age Networking.



IoT challenge #3: Mitigating the security risks

With the surge of IoT devices, the classic network security methods based on firewall rules, ACL, VLANs, and VPNs are growing more complex, cumbersome and expensive by the minute. The paradigm shift introduced by IoT and its interaction with business applications requires approaching network security from a segmentation angle.

As IoT becomes integral to business processes, more enterprise applications and the associated data, will interact with IoT devices. This makes it increasingly important to reinforce security measures and create contained areas in the network to ensure that any potential security breach does not impact the business processes or data.

The Alcatel-Lucent Enterprise solution

Digital Age Networking is totally aligned with the segmentation approach. Alcatel-Lucent Enterprise networks implement an IoT containment solution that virtually segments the physical infrastructure into micro-segments called "containers". Each connected object is automatically assigned to the correct container according to its profile.

A container is described by the services that the devices can access. The traffic among devices is contained to their virtual micro-segment and blocked from communicating with other micro-segments of the network. This is a strong security mechanism as it ensures that a potential cyberattack through a compromised device cannot impact the entire network.

IoT challenge #4: Preserving network performance

The ongoing adoption of IoT devices means networks must be ready to cope with an increase in processes and data, while maintaining performance. Thousands of devices may be connected to the network which will require higher capacity and more efficient equipment to provide more bandwidth, as well as the ability to connect more devices simultaneously, and powerful management tools.

It is expected that the majority of the networking devices will be wireless IoT in the next few years. Based on this fact, Wi-Fi standards are evolving to better support the impending IoT proliferation. Wi-Fi 6 includes technical improvements to deal with the IoT phenomena more efficiently. For example, Orthogonal Frequency-Division Multiple Access (OFDMA) together with an improved Multi-User, Multiple Input, Multiple Output (MU-MIMO) provide better network resource usage allowing more devices to connect simultaneously to one access point and drastically improving performance in high density environments.

As well, Target Wake Time (TWT) reduces connected devices energy consumption as they only need to wake when they receive the TWT, enabling batteries to last longer.

To avoid bottlenecks, an increase in WLAN capacity must be accompanied by an enhanced underlying LAN capable of complying with network requirements including bandwidth, powering, port density and ubiquity demanded by the connected IoTs.

The Alcatel-Lucent Enterprise solution

The Alcatel-Lucent Enterprise network portfolio provides support for IoT with Wi-Fi 6 access points, a wide range of access switches to address varied IoT deployment scenarios, as well as a powerful NMS that integrates IoT management tools and automation.

From a LAN perspective, the access switches provide 1G and Multigig, PoE/PoE+/HPoE ports to support and power up any type of IoT device, whatever the bandwidth and energy consumption requirements. Customers can choose from a range of switches, along with stacking and virtual chassis options, that span from a few IP ports up to very high-density configurations. As well, ruggedized access switches and access points enable IoT connectivity in outdoor and harsh environments.

In addition to automation of the IoT on-boarding process, the NMS embeds an IoT inventory tool that enables monitoring of the connected devices as well as comprehensive reporting information about each device including, MAC address, IP address, port or access point status, category, and manufacturer, among others.

The entire process, from IoT discovery to registration into inventory, is done automatically, which minimizes manual intervention and helps IT administrators manage and see 'at-a-glance' the objects connected to the network.

IoT solution applications

Following are a number of real customer examples that showcase Digital Age Networking support for IoT deployment.

Digital door lock centralized records

A regulation of the Security Industry Regulatory Agency for hotels **in Dubai (UAE)** requires installation of digital door locks in guestrooms, as well as a centralized database record of all lock and unlock actions performed, for at least six months.

To assist hospitality customers in Dubai in complying with this regulation, Alcatel-Lucent OmniAccess® Stellar WLAN provides a Zigbee interface in the access points which obtains the lock/unlock information from the digital locks. The NMS collects and centralizes the data from all the access points and sends it to the digital door lock system manager through a standards-based API.

In-room automation remote control

To be recognized as a high technology hotel and differentiate from their competition, a luxury resort **in South Korea** was required to provide VIP room guests with remote control room automation including: lightning, heating, and air conditioning.

Since the hotel's in-room devices did not support the standards currently provided by Alcatel-Lucent Enterprise networking, ALE developed an IoT hub to interface between room devices and the touch-screen smart IP phones which features a guest application to control room automation.

Visitor location services

An oceanographic park **in France** required an app to help customers make the most of their visit. It included capabilities such as:

- Wayfinding
- Points-of-interest
- Contextual multi-media, for example an explanatory video about sharks
- The ability to locate family members and friends
- Dynamic marketing for restaurants and shops

In another example, a large European legal institution **in Luxembourg** required an app for citizens to access a variety of information including:

- Directions to a courtroom, or lawyer's office
- Dedicated routes for people with reduced mobility
- Multi-media content pop-ups for users getting close to a point-of-interest such as a courtroom entrance, or notable artwork
- Accurate position information in emergency situations
- Visitor location data to assess the visitor flow
- Cafeteria menus

Alcatel-Lucent Enterprise Location Services solution provides the visitor app with the required functionality. Using BLE technology embedded in the OmniAccess Stellar access points and BLE beacons, the app calculates the exact location of the visitor's smartphone, enabling the wayfinding and geofencing notifications to execute the required features.

Valuable lab equipment and IT staff tracking

A university **in Colombia** identified three requirements related to location services. These included:

- Knowing where expensive electronic lab devices were located, as well as laptops lent to university students
- Keeping a record of IT on-site interventions; knowing when IT staff are on-site and for how long
- Implementing an app to guide students and visitors within the university buildings

Adding BLE tags to the location solution based on OmniAccess Stellar BLE-enabled access points and beacons, means Alcatel-Lucent Enterprise delivers a complete solution to track lab equipment and maintenance staff, and provide wayfinding for students and visitors.

Conclusion

IoT adoption is growing rapidly within enterprise environments. And, while IoT can help CEOs leverage the benefits of the technology to improve workflows and business processes it also presents challenges for CIOs and CFOs who must deal with technological evolutions and limited budgets.

Digital Age Networking provides the networks that enterprises need to address the increasing adoption of IoT. These autonomous networks seamlessly and automatically integrate IoT into the enterprise digital transformation, minimizing risks, keeping costs contained, and supporting digital business needs for today and tomorrow.

Alcatel·Lucent Enterprise