ALE | Where Everything Connects

Enabling the Internet of Things and Digital Business

Alcatel·Lucent Enterprise

For the past decade, mobility has been the major story in technology. Internet usage by mobile and tablet devices now exceeds that of desktops worldwide.[1] The forecast for smartphones to be shipped worldwide is expected to reach almost 1.9 billion by 2021, a tenfold increase from the amount of shipments in 2009. This means that by the end of 2017, an estimated 31 percent of the world's population will have a smartphone, a figure that was at less than 10 percent in 2011.[2] However, just as mobility surpassed the number of PCs in use, the number of smartphones in use will be surpassed by the Internet of Things (IoT), "Things" being devices connected to the network, from sensors to sprinklers to lights. Endpoints of the Internet of Things will grow at a 32.9% CAGR from 2015 through 2020, reaching an installed base of 20.4 billion units[3]. That is roughly twice the number of mobile computing devices. And that is just the beginning.

For the enterprise, both these trends will overlap, as most enterprises are only now beginning to catch up with the mobile revolution and move beyond "the carpeted area." The desktop phone and computer have dominated IT since the nineties, but all that is changing. As of March 2017, over 5 million apps were available for download (2.8 million Android and 2.2 Apple). An increasing number of them are enterprise-specific applications. Mobile apps are expected to grow exponentially as they are relatively easier to create than computer apps, as well as their considerable lower price[4]. These numbers give a sense of the increasing interest in using mobile devices, such as smartphones and tablets in the enterprise.

Indications are that the take-up of IoT by enterprises will not be delayed in the same way mobility was. Sensors will be embedded deep in our bodies as well as sent far out into space. We will find connected machines from the factory floor to the warehouse and logistics systems that deliver them to our door. From beacons in retail or sensors and cameras in our transportation systems, there will be few aspects of our lives that will not be sources of digital information. Enterprises will live or die depending on how well they support these initiatives and exploit the big data from all these devices.

What we are seeing is the emergence of a new kind of fluid enterprise that will:

- Embrace mobility
- Equip employees with every kind of device from smartphones to smart eyewear to wireless devices specific to each industry
- Ensure that they are connected everywhere
- Develop task-specific apps that deliver big data analytics on the spot for informed decisions
- Fuel their analytics engines with information from every aspect of the enterprise's multitude of processes and activities, whether it is the heating, ventilation and air conditioning (HVAC) system on their campus or the fuel-injection system on a jet engine at 35,000 feet

Although many of the machine-to-machine (M2M) connections will be across the wide area network, the majority will occur within the local area enterprise network, either on Ethernet or Wi-Fi®, and many other technologies are in development such as low-power wide-area networks (LPWA).

Imagine the issues this raises for IT as every department in the company wants its own M2M network:

- Maintenance wants to monitor and control the HVAC system
- Campus security wants a network for cameras, doors and badge swipes
- Manufacturing wants a network for the factory floor

1 Press release from StatCounter Global Stats, "Mobile and tablet internet usage exceeds desktop for first time worldwide", November 1, 2016.

2 Global smartphone shipments forecast from 2010 to 2021, Statista.com. https://www.statista.com/statistics/263441/global-smartphone-shipments-forecast/

3 Gartner Forecast: Internet of Things – Endpoints and Associated Services, Worldwide, 2016, Peter Middleton et. al., December 29, 2016.

4 Number of apps available in leading app stores as of March 2017, Statista.com. http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

- Logistics wants a network for tracking inventory in the warehouse
- Supply chain wants to link with suppliers to track raw materials to finished goods arriving at the factory door
- Marketing wants to track after-market product use to better understand consumer behavior
- HR wants to monitor the activity data on employees watches to make sure they're getting enough exercise

Each department has an equally good reason to embrace IoT. They can solve real problems, improve productivity, or design new ways to interact with their customers and employees.

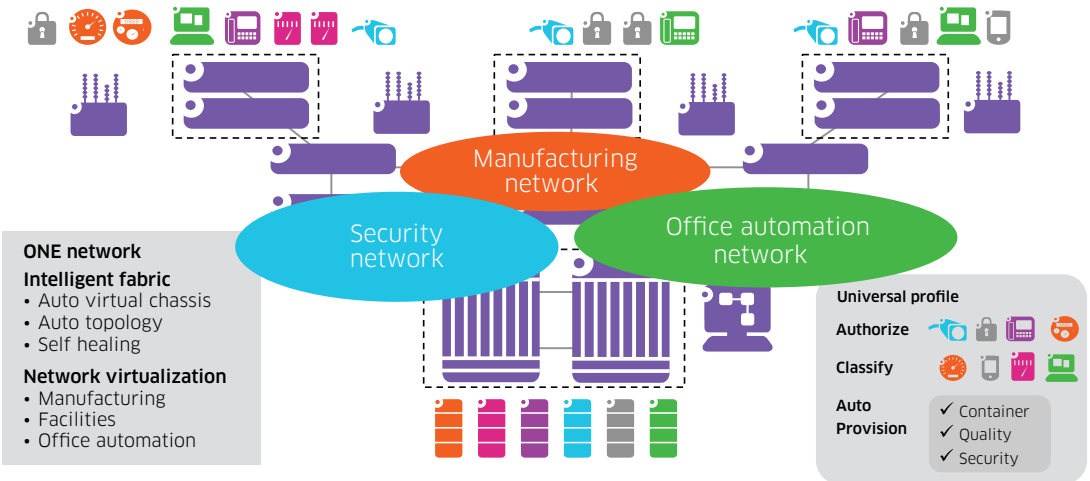
Many of these use cases will require very low latency networks. The proposed specifications for 5G, designed specifically to address IoT, require latencies as low as 1ms. Many IoT devices will also need power over Ethernet (PoE), since sensors will often be installed in locations where there is no power. Different applications will have specific network protocol requirements.

The biggest need will be for security both from outside intrusion, and internally in the form of firewalls between applications. One U.S. retailer, Target, famously had its customer database hacked and thousands of customer credit cards stolen. It was hacked through the HVAC IoT network, which was on the same network as the servers holding their critical customer information.

The seemingly easy answer is to create a separate network for each application. Many of these kinds of M2M overlay networks already exist. Many of them use older serial, synchronous networks. But the trend in the device industry is towards standardization on wireless or Ethernet-based IP. And as they multiply, the number of M2M overlay networks will become far too complex to manage. Each requires its own procedures and employee training for deployment, maintenance, cabling, administration and general operation – even procurement.

The less obvious but far more elegant answer is to create virtual networks for each IoT application. Using the same underlying network infrastructure, administrators can create multiple virtual network slices or "containers". The container specifies the policies related to quality, prioritization, bandwidth reservation, latency and any other capabilities required by the IoT solution. Profiles can be specified by container, so only specified devices can connect and be authenticated, for instance, only digital security cameras.

Figure 1. One robust, easy to deploy network with a virtual network for each business unit



Each container, although running virtually on the same network as all other containers, is logically separated from them and thus invisible to the others. This makes the Target scenario impossible. Many IoT solutions have very light data requirements, but there are still efficiencies to be gained from sharing the bandwidth between many solutions, each with different network usage requirements.

IoT on the University Campus

A university campus application of IoT illustrates some of the common use cases for containerization, but these could be extrapolated to any enterprise. Within a college or university, there is, of course, a clear distinction between students and faculties in terms of their needs and privileges. Although they'd love to have access to them, making exams and student records available to students would not make much sense as they need to be secured. Faculty and administration data and communications, for the most part, need to be kept quite separate from student communication and data services.

As well, facilities, security and other services also may need to be isolated. Containers might be set up for HVAC, CCTV cameras and access control to buildings, including residences and labs. Data centers and labs may require ad hoc containers for secure experiments using sensors and other connected devices as part of the research. Many universities now collaborate with corporate and NGO partners setting up programs and institutes that have their own separate network requirements as well. Even hosted conferences could use a secure container set up for conference administration, communications, delegate badges and mobile access.

The ALE campus solution is fully capable of meeting these requirements. The key technologies for implementing containerization of the network are Unified Access, Intelligent Fabric (iFab) and Smart Analytics.

Unified Access

Although many enterprises and organization have been slow to embrace them, two trends in the last decade have set the stage for IoT on campus: Wireless mobility and "bring your own device" (BYOD). Previously, networks were created to handle predictable, static traffic flows that terminated at wired devices such as the desktop PC and desk phone.

Wireless campus mobility, normally provided by Wi-Fi networks, were initially an overlay on the wired network and required separate sign-on for users. Security policies were often quite different, and levels of access to resources were also different.

This made the user experience anything but seamless. When users began arriving with their smartphones and non-corporate-issued laptops and tablets, BYOD added further complexity and security risks for IT. And yet, as enterprises fully embrace mobility as a strategic tool, they will need to make the movement between the wired and wireless networks more fluid, or what we call unified access. Adding in IoT devices will only make it more urgent.

The key to unified access is knowledge of the device and user. This technology forces authentication and authorization of all users and devices before they are granted access. Once they are identified, a network profile is associated with all the information regarding how the network is going to treat the traffic coming from this device, including what set of policies should be applied. This process ensures the same experience wherever the user is connected and with whatever media (Ethernet or Wi-Fi).

Essential to unified access is a single network management system (NMS) on a single pane of glass. Personnel using this NMS can configure policies and access procedures as well as coordinate and optimize operations across both wired and wireless networks. It eliminates inconsistencies and simplifies the overall operation.

This solves many of the headaches of BYOD and enables a seamless experience for users, wherever they are on the network. It also vastly simplifies the discovery and onboarding of IoT devices, which are often installed by personnel unfamiliar with IT procedures.

Intelligent Fabric

iFab, or Intelligent Fabric, allows for automation of many tasks that are normally time consuming for IT, including the deployment and moves/adds/changes of the network. iFab also leverages Shortest Path Bridging (SPB) to create a robust network fabric. With SPB it is very simple to create virtual isolated networks, or containers, that share the same physical infrastructure. SPB has also many advantages when compared to STP (spanning tree) as it provides faster recovery on failures, better throughput (as it uses all links) and in many cases lower latency. These are all aspects that are important for IoT, making sure that the proper quality and security conditions are provided for the IoT solution to run properly.

iFab simplifies many operational tasks of IT. It enables:

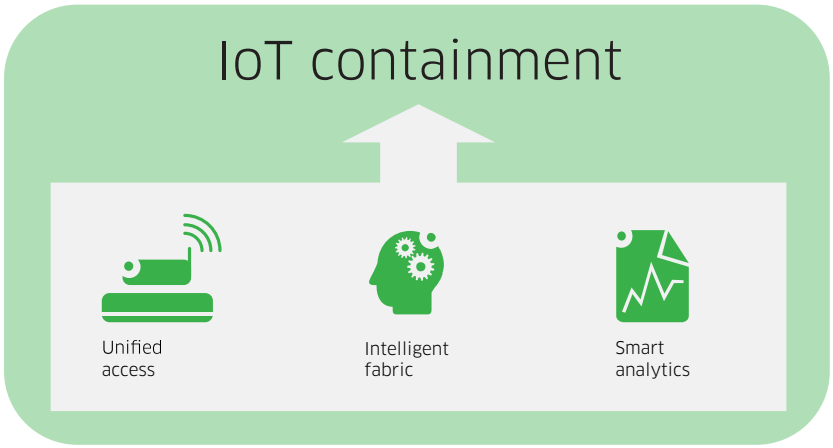
- Simpler network design
- Plug-n-play deployment
- Comprehensive interoperability
- Self-attachment to existing switches and wireless access points
- Dynamic attachment to virtual machines
- Automation of moves, adds and changes
- Remote configuration loads (RCL)
- Self-healing capability, where any component failure, link or node, is detected in real time with automated re-routing of the network traffic
- Network upgrades while in service

Smart Analytics

The last piece of the puzzle is the Alcatel-Lucent Smart Analytics capability, which can monitor these containers and apply policies to them automatically. In the context of IoT, it increases security and monitors the status of the network for potential performance problems, which might, for instance prevent the network of delivering the needed quality of service (QoS).

For enhanced security, it leverages the application's analytics capability. For example, IT could set up a policy for a container with surveillance cameras to only accept SIP video traffic. If any other traffic is detected (for instance a hacker spoofing the MAC address of a surveillance camera), this traffic is discarded.

Figure 2. One network with virtualization capability



The ALE IoT Solution

As we have seen in our campus IoT example, beyond the needs of campus users, IoT requires reliable, secure and scalable networks to handle both users and M2M or IoT traffic coming from cameras, sensors, HVAC and a diverse array of devices that might be deployed in research or elsewhere. Containerization of these divergent networks using policy-based and virtual networks provides an elegant solution. In this section, we will discuss the ALE products and technologies that make this possible.

Persistent network access

IoT network access includes the need for both wireline and wireless equipment. Alcatel- Lucent Enterprise Stackable Gigabit LAN switches provide wireline access, with wireless access delivered by a variety of high-performance 802.11ac Wi-Fi access points (APs).

The Alcatel-Lucent OmniSwitch® 6860 Stackable LAN Switches (SLS) are compact, high-density Gigabit Ethernet (GigE) and 10 GigE platforms designed for the most demanding converged networks. In addition to high performance and availability, the OmniSwitch(OS) 6860(E) offers enhanced QoS, user authentication, deep packet inspection (DPI), and comprehensive features to securely accommodate users and devices with a high degree of integration between the wired and wireless LAN.

For use on the factory floor or outdoors, the OmniSwitch 6865 Gigabit Ethernet LAN Switch is an industrial grade, Layer 3, Gigabit Ethernet switch designed to operate reliably in all kinds of harsh environments. It can operate at wider operating temperatures (-40 to +167˚F or -40 to 75˚C), variable power conditions (90 – 260 VAC and 20 – 60 VDC), and can withstand electromagnetic fields, high vibrations, dust/dirt and high humidity. It has an optimized feature set for high security, reliability, performance and easy management.

Both the OS6860 and OS6865 support Shortest Path Bridging MAC (SPB-M), which can deliver containers, VPN services and eliminate spanning tree from the network. Both have Gigabit optical backbone connectivity, allowing up to 10 Gigabit uplinks and support for a variety of optical fiber types including single-mode, multi-mode, short and long-haul optics allowing for the linking of satellite campuses or devices at distances of up to 50 miles.

Both have Power over Ethernet (PoE) support for connecting security cameras, wireless access points and sensors, and High Power over Ethernet (HPoE) for up to 75W support for applications such as heated, pan-tilt-zoom (PTZ) cameras. They support advanced quality of service (QoS)

to support the special demands of video and voice applications, as well as integrated security features for controlling access to the network, policy enforcement and network security attack containment. Operationally, both have intelligent fabric technology (iFab) to support cost-effective installation and deployment using automated switch setup and configuration.

A resilient and high-performing core

Although IoT planners and architects will be primarily focused on the access network, which links all the sensors, cameras, HVAC and other IoT devices, these access switches will also need support from the core fabric to aggregate their traffic and ensure that the network can scale to meet the specific network requirements of all the users and devices on the network, including IoT containers.

The core fabric is built around high-performance wire-rate 10 Gigabit Ethernet/40 Gigabit Ethernet network switches that provide unparalleled port density and switching capacity to grow and scale the network inexpensively. This includes the Alcatel-Lucent OmniSwitch 6900 Stackable Ethernet LAN Switch family, and the OmniSwitch 9900 and OmniSwitch 10K Modular LAN Chassis.

All Alcatel-Lucent OmniSwitches have the virtual chassis (VC) feature, which enables up to six switches to be combined and behave as a single fully redundant unit. In many cases, this can replace an expensive chassis, requires less space and power, and can be delivered at a lower cost. It allows for rapid expansion of the core fabric, and the VC provides fast re-convergence if equipment fails, without impacting real-time applications and user experience, such as voice and video.

The core products incorporate the award-winning Intelligent Fabric (iFab) technology offering a set of capabilities, including containerization and automation techniques that simplify the design, deployment and operation of the network.

End-to-end network management

The management suite includes all the tools needed to provision, monitor, analyze and troubleshoot the network. The Alcatel-Lucent OmniVista® 2500 Network Management System (NMS) can manage the LAN, WLAN, core, WAN, and data center from a centralized single pane of glass. It is an essential component of our iFab technology and is used to manage containers and the policies that define them.

The Alcatel-Lucent Smart Analytics technology enables technical staff to analyze the network information in a meaningful manner. The OmniVista 2500 uses a customizable dashboard to summarize and display the vast information available from the network. From this dashboard, staff can expand the analysis in more detail through multiple graphs and reports. The data collected includes information for the users, devices and applications traversing the network. It also includes network device status, network traffic behavior, warnings and key statistics.

The OmniVista 2500 has the unique ability to offer predictive analysis reports. It analyzes network traffic patterns over a large period and uses sophisticated algorithms to predict future behavior. It provides visibility into potential future bottlenecks, enabling proactive planning of the network capacity and expansion. The system can detect abnormal network traffic behavior and alert administrators to network security attacks.

IoT ready

As we have seen, the Internet of Things offers important opportunities for enterprises, while posing some unique challenges. However, the challenges of IoT have already been anticipated in the ALE network design, because they are very similar to the kinds of challenges posed by implementing wireless mobility and BYOD. If anything, IoT pushes us farther and faster towards network virtualization and the use of network containers. But there are many other business trends, besides IoT, that will use these capabilities.

The modern enterprise is itself becoming more virtual and its boundaries more fluid. Responsiveness to markets, collaboration opportunities, joint ventures and the growth of the “gig” or temporary work economy will require highly responsive, policy-driven networks that allow for the onboarding of new organizations, workers and “things” in a highly automated, secure way. In this emerging world, an ALE network can be a critical foundation for the evolution of your business, not only to IoT, but as well, to the many new business models it will bring with it.

Alcatel·Lucent
Enterprise