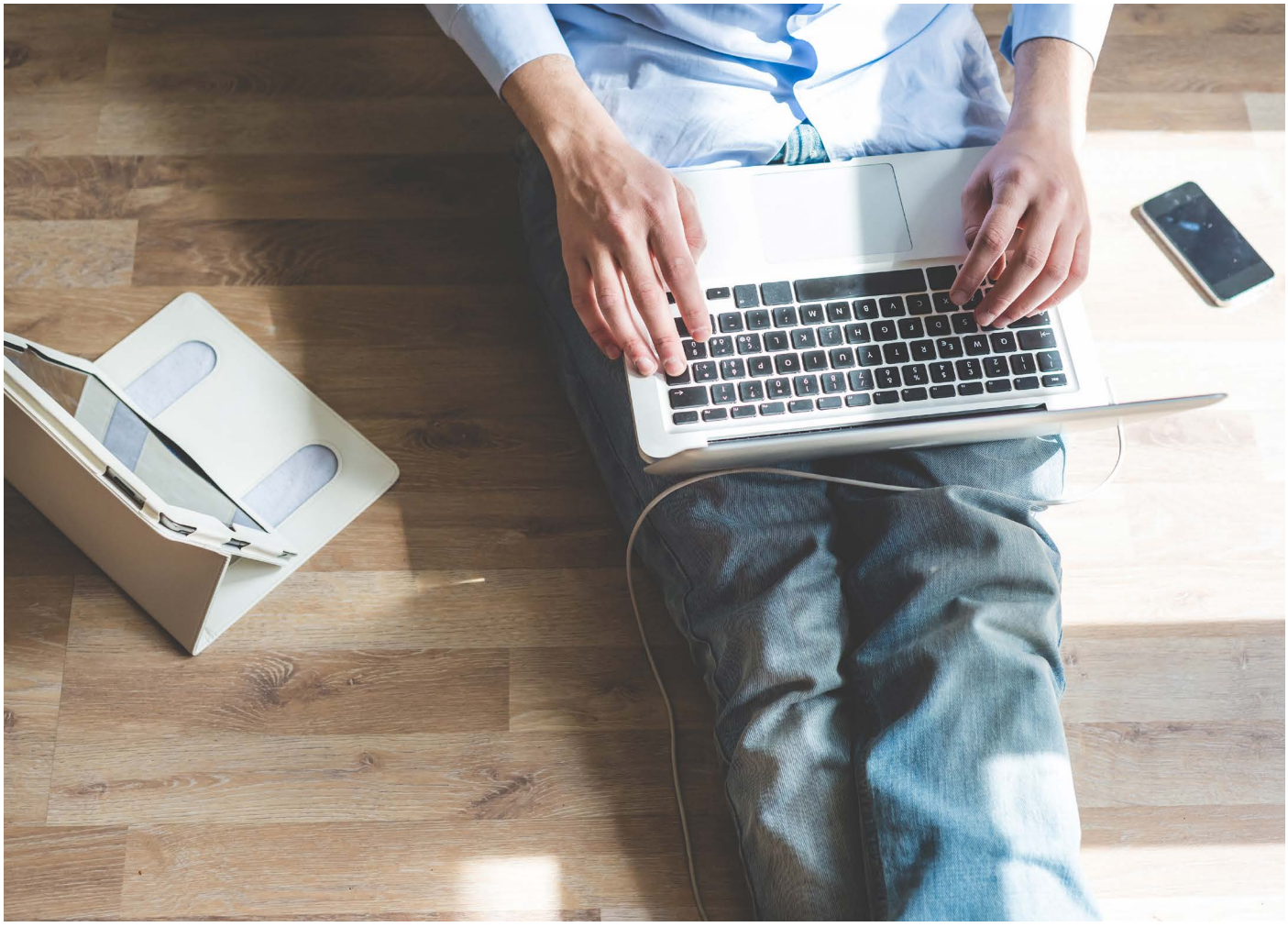
A Layered Approach for Securing “Internet of Things” Devices

A strategic technology perspective



Alcatel·Lucent
Enterprise

Background

Enterprise networks have been pressured to support multiple devices for every user for several years now compared to only one device previously. This phenomenon, known as Bring Your Own Device (BYOD), reflects employees desire for mobility. With that mobility has come security headaches for CIOs. As described in the article "BYOD Was Merely an Appetizer; IoT is the Main Course," the nature of the problem has changed as there is often no user behind IoT connected devices. The scale of the problem is also much bigger with 21 billion objects expected to be connected to enterprise networks by 2020.

Protection against Denial of Service

Network switches should filter denial of service (DoS) attacks by default, which is standard for every Alcatel-Lucent OmniSwitch. A DoS is a security attack aimed at devices that are available on a private network or the Internet. Some attacks seek out system bugs or vulnerabilities, while other types of attacks involve generating large volumes of traffic such that network service is denied to legitimate network users. A recent blog discusses these types of attacks. A network switch should be set to detect various types of port scans by monitoring for TCP or UDP packets sent to open or closed ports.

Network vendors usually have ways of protecting against DoS attacks. An important difference that ALE offers are DoS filtering features which are enabled by default. From the moment a switch is turned on, network access is secure. These basic DoS filtering features strengthen the foundation for secure connectivity and operation of IoT devices.

Secured network

ALE provides a unique network architecture design that offers a single layer (called a POD/MESH) that provides a unique, nearly linear scalability from 50 to 14,000 10GigE ports. Moves, adds and changes are fully automated, which dramatically reduces the potential of human configuration errors. Such errors are leading causes of security vulnerabilities. This unique capability is called iFab (Intelligent Fabric).

iFab is based on the IEEE 802.1aq Shortest Path Bridging standard (SPB), which provides multi-link topology. This means that all links are active with load sharing. SPB enables large Layer-2 topologies with a shorter convergence time.

SPB is not new. It is an amendment to IS-IS, which is a mature protocol used by carriers for the past 25-30 years. IS-IS is built over Ethernet, and not over IP over Ethernet. Consequently, SPB does not need an IP address. This means it's possible to build a network backbone of 100 switches without an IP address, so core switches are invisible from hackers. IP-based attacks are therefore impossible. Only Ethernet-based attacks are possible, but they are complex to execute, and more importantly they have an effect on only one hop in the network.

SPB should be deployed in a service-based approach. Each service is created and IS-IS distributes the service information and automatically builds the topologies to connect all the endpoints (IoTs) to the service. Each SPB service represents a single Layer-2 virtual network, and the protocol can scale up to 16.7 million separate services using a 24 bit service description field. This easily enables highly virtualized networks that far exceed the 4K limit of the traditional VLAN tag format. This is what enables the creation of "containers," separating traffic from HVAC sensors to CCTV for example. This is why an attack on one object type will affect a very limited portion of the network, thus limit network downtime and in most cases, eliminate many unplanned network outages.

Secured service

Additional security measures ALE provides are at the service level, meaning the IoT level.

IoTs are authenticated via IEEE 802.1X network-based authentication, MAC-based authentication or other mechanisms. The object is then automatically assigned to a specific "HVAC" or "CCTV" profile, for example. These profiles contain parameters such as Access Control Lists (ACLs), VLAN, QoS, and bandwidth limitations. This ensures that only multicast CCTV type of traffic is forwarded on the network from an object authenticated as "CCTV". Any other type of traffic from such an object will be automatically discarded even before entering the network. This is configurable and several types of traffic can be defined in a very granular manner.

Such authorized traffic will only enter the right "container," meaning only the SPB virtualized portion of the network. In essence, the right object will be in the right container.

When coupled with access switches, a Layer 2-7 deep packet inspection at wire-speed knows the exact traffic status, per object and per user. This should be presented in an easily readable manner for managers. Managers are then able to make the right decisions on network upgrades. Of course, this provides user and object data, which is today's gold mine.

Embedded software – Ethernet switch security

Intelligent networks now require an increasing number of software capabilities that every piece of network equipment must support. And of course, the larger and more complicated the software program, the more likely it is to have vulnerabilities and backdoors.

One way that ALE (operating under the Alcatel-Lucent Enterprise brand) addresses this situation is to have the Alcatel-Lucent Operating System (AOS) software, which is embedded in all ALE network switches, hardened to provide network-level integrity. The AOS software is checked and guaranteed by LGS Innovations, an independent organization.

LGS provides:

- Independent code checking to remove backdoors and vulnerabilities
- Code diversification reduces the risk of hacking via scanning of well-known maps by compiling code multiple times using different memory maps. Each time an ALE integrator downloads a new firmware version from a support site, the user receives a randomly generated version.
- A secured supply chain (available in the USA only) guarantees non-alteration of the code when downloaded by a partner or customer.

Network securing technology is here today

Although ALE is not a security vendor providing firewalls or Unified Threat Management (UTM) solutions, it actively participates in the security effort – something every business should do.

ALE has always been at the forefront of embedding and offering the right security features in LAN and WLAN network infrastructure products. 15 + years of innovations are now resonating with businesses as tomorrow's world of billions of connected objects on enterprise networks increasingly become a challenge. Alcatel-Lucent Enterprise LAN and WLAN solutions with their embedded security functionalities make them ideal for multi-level IT security:

- Embedded security firmware in network switches
- Embedded protection against Denial of Service (DoS)
- Secured network at both the core and access layers
- Secured network service for IoT

Enterprise or public organizations can now simplify deployment of IoTs while providing a good secure base. ALE enables businesses to manage deployments themselves as long as the businesses' IT department provides the right network profile and the right network container.

Alcatel·Lucent Enterprise