# Table of contents

1 About this document ............................................. 4
   1.1 Purpose ...................................................... 4
   1.2 Scope ......................................................... 4
   1.3 Acronyms ..................................................... 4
   1.4 Related documents ........................................... 5

2 Introduction and use cases ....................................... 6

3 Solution overview ................................................ 8

4 Reference architecture ............................................ 10

5 City net ............................................................. 11
   5.1 Introduction .................................................. 11
   5.3 L2/L3 VPNs and IoT containers .............................. 13
   5.4 Intelligent Fabric in city nets ............................... 14
   5.5 Solution highlights .......................................... 14
   5.6 Why use ALE's Intelligent Fabric for smart city nets? 16

6 Municipal cloud .................................................... 17
   6.1 Introduction .................................................. 17
   6.2 Business drivers and technical requirements .............. 17
   6.3 The virtualized data center .................................. 18
   6.4 End-to-end virtualized hybrid multi-tenant cloud ......... 19
   6.5 Solution highlights .......................................... 20
   6.6 Why use ALE's Intelligent Fabric for smart municipal clouds? 20

7 Municipal Wi-Fi ..................................................... 21
   7.1 Introduction .................................................. 21
   7.2 Business drivers and technical requirements .............. 21
   7.3 Solution overview .......................................... 22
   7.4 Solution highlights .......................................... 23
   7.5 Why ALE's OmniAccess Stellar for smart municipal Wi-Fi? 23
8 Smart transit ................................................................. 24
  8.1 Introduction .................................................................. 24
  8.2 Business drivers and technical requirements ................. 24
  8.3 Solution overview ........................................................ 25
  8.4 Solution highlights ....................................................... 26
  8.5 Why ALE's H2-Automotive+ for smart transit .................. 26

9 Smart civic venue ............................................................. 27
  9.1 Introduction .................................................................. 27
  9.2 Business drivers and technical requirements ................. 27
  9.3 Solution overview ........................................................ 28
  9.4 Solution highlights ....................................................... 29
  9.5 Why ALE's OmniAccess Stellar LBS for smart civic venues . 30

10 Smart roads and highways ................................................. 31
  10.1 Introduction .................................................................. 31
  10.2 Business drivers and technical requirements ................. 31
  10.3 Solution overview ........................................................ 32
  10.4 Solution highlights ....................................................... 33
  10.5 Why use ALE's Intelligent Fabric for a smart roads and highways solution? . 33

11 Security framework ........................................................ 34
  11.1 Securing IOT devices .................................................... 34
  11.2 Securing the perimeter ............................................... 35
  11.3 Securing the network ................................................... 35

12 Conclusion ...................................................................... 38
1 About this document

The purpose of this document is to serve as a reference guide to the solutions that Alcatel-Lucent Enterprise provides to smart city customers. This guide presents use cases, business drivers, technical requirements and a solution overview along with ALE’s value proposition for each solution set.

1.1 Purpose

This guide is intended for Alcatel-Lucent Enterprise’s Business Partner sales and pre-sales staff as well as customers.

1.2 Scope

This document focuses on city nets, municipal clouds, municipal Wi-Fi, smart transit, smart civic venue and smart roads and highways solutions. This document will not provide in-depth product specifications as these are already provided in datasheets.

This document is split into individual modules for each solution set such that the reader can focus on the section that is relevant.

1.3 Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADSL</td>
<td>Asymmetric Digital Subscriber Line</td>
</tr>
<tr>
<td>API</td>
<td>application programming interface</td>
</tr>
<tr>
<td>BLE</td>
<td>Bluetooth Low Energy</td>
</tr>
<tr>
<td>GRE</td>
<td>generic routing encapsulation</td>
</tr>
<tr>
<td>HA</td>
<td>high availability</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>LPWAN</td>
<td>low power wireless area network</td>
</tr>
<tr>
<td>LTE</td>
<td>long-term evolution</td>
</tr>
<tr>
<td>POL</td>
<td>passive optical LAN</td>
</tr>
<tr>
<td>RCD</td>
<td>remote configuration download</td>
</tr>
<tr>
<td>RESTful</td>
<td>representational state transfer</td>
</tr>
<tr>
<td>SDK</td>
<td>software development kit</td>
</tr>
<tr>
<td>SPB</td>
<td>Shortest Path Bridging</td>
</tr>
<tr>
<td>TOR</td>
<td>top of rack</td>
</tr>
<tr>
<td>UNP</td>
<td>universal network profile</td>
</tr>
<tr>
<td>VM</td>
<td>virtual machine</td>
</tr>
<tr>
<td>VXLAN</td>
<td>virtual extensible LAN</td>
</tr>
<tr>
<td>WPAN</td>
<td>wireless personal area network</td>
</tr>
<tr>
<td>WWAN</td>
<td>wireless WAN</td>
</tr>
<tr>
<td>ZTP</td>
<td>zero-touch provisioning</td>
</tr>
</tbody>
</table>
1.4 Related documents


2 Introduction and use cases

According to the Smart City Council, “A smart city uses information and communications technology (ICT) to enhance its live-ability, workability and sustainability. First, a smart city collects information about itself through sensors, other devices and existing systems. Next, it communicates that data using wired or wireless networks. Third, it analyzes that data to understand what’s happening now and what’s likely to happen next.”

Figure 1. Smart city

Table 1 - Use cases and examples

<table>
<thead>
<tr>
<th>Smart Lighting</th>
<th>Save energy with remotely-controlled on-off timing and dimming depending on time of year, weather conditions and motion detection, such as an approaching cyclist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td>Public lighting represents 20% of energy consumed by the Barcelona City Council. Replacing old-fashioned sodium lamps with LED ones provides better lighting and reduces energy use by more than 52%.</td>
</tr>
<tr>
<td></td>
<td>With the addition of remotely controlled, on/off timing and dimming depending on time of the day, or year, weather or other conditions as well as motion detection, such as approaching cyclists, energy savings of up to 72% are possible.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Smart Parking</th>
<th>Reduce parking search time, fuel use, CO₂ emissions, and parking violations by detecting available parking spots and guiding drivers to them with an app.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td>City drivers spend a significant amount of time looking for a parking spot. Sensors detect parking spot availability and a smart parking app can guide drivers to it. In the city of San Francisco, parking search time was reduced by 43% which not only saves time but also reduces fuel use and CO₂ emissions by 30%. In addition, in-app payment makes it easier to pay, resulting in a 23% decrease in the number of parking violations and citations.</td>
</tr>
</tbody>
</table>

| **Smart Transit** | **Improve rider safety and satisfaction as well as ridership** with video surveillance, on-board Wi-Fi and entertainment and real-time schedule information. Real-time vehicle location tracking provides live updates through an app or smart display at the bus stop. |
| **Example** | In Bucharest, visually-impaired riders are alerted that their **bus is approaching**. And bus drivers can be informed that someone may need assistance with boarding at the next stop. |
| **With open data**, real-time location information can be leveraged by **third-party solutions** for wayfinding and more. |

| **Smart Waste Management** | **Reduce waste collection activities, fleets, fuel use and CO₂ emissions** with smart bins that can compact waste and inform their fill level. |
| **Example** | Solar powered smart rubbish bins compact waste, increasing their capacity by a factor of five. Bins use sensors to determine their fill status and communicate it to the management platform. In Australia, smart bin deployment has resulted in a 75% reduction in waste collection activities at Bondi Beach. With real-time access to bin fill-level information, waste collection is optimized with smarter routes, resulting in reduced labor costs, fleets, fuel use and CO₂ emissions. |

| **Smart Metering** | **Reduce water and electricity waste or theft** with smart meters that can measure and report use in near real-time. |
| **Example** | Smart meters measure energy and water use in short intervals and report this data back to the energy or water company. Utilities can set **dynamic use-based pricing** to reduce use at times of peak demand. Smart metering also helps reduce waste and eliminate the need to dispatch technicians for **costly manual meter readings** as well as facilitate trading of excess energy. Smart meters can **detect and alert of energy theft** in public infrastructure such as public lighting. |

| **Video Surveillance** | **Improve public safety** with license plate recognition, vehicle tracking, facial recognition and analytics. |
| **Example** | Cities cannot be smart if they are not safe. Smart video surveillance solutions add features such as license plate recognition, vehicle tracking, and analytics. Facial recognition can identify a suspect, or persons of interest, such as people on a watch list, from a crowd. But it's not just about safety: Facial recognition can be up to 50% faster compared to tap cards when used at metro gates. |

---

3 Solution overview

If we pay close attention to the use cases presented in Section 2, we may notice that they require a network to function. Some use cases are unfeasible without network connectivity (for example, smart metering). Other use cases cannot deliver their full benefits in an offline manner (for example, smart lighting). Figure 2 illustrates a high-level view of a smart city infrastructure.

Starting at the bottom of this diagram, we have IoT devices and users. IoT devices are a variety of sensors and actuators, the sensory nerves and the muscles. IoT devices gather data and are commanded by the city’s brain, software and applications running in a municipal cloud and the city’s command and control center.

A smart city leverages its ICT infrastructure to maintain smart interactions with users: residents and visitors. Users consume and produce data as they go about their daily lives using the city’s resources such as public transport, parking, Wi-Fi and so on. Users interact with city agencies directly through official websites and applications, or, indirectly, with third-party websites and applications that access an agency’s open data through APIs. Users connect through fixed (for example, POL or ADSL) or mobile (for example, 4G or LTE) broadband connections or Wi-Fi using a personal device, such as mobile phone, or a city asset, such as an information kiosk.

IoT devices often connect using the same technologies available to users. In other cases, however, other technologies are more appropriate. An IoT gateway may be required to connect such devices to IP-based infrastructure.

Let’s have a look at some of those technologies.

**SCADA:** SCADA is a control technology that is prevalent in many industrial and infrastructure processes. As an example, SCADA may be found in power utilities, water, or wastewater collection and treatment. Modern SCADA devices can connect to an IP network directly. Legacy SCADA devices, however, use a serial interface and require a gateway to connect to the IP network.

**WPAN:** WPAN stands for “wireless personal area network”. These technologies are designed to connect medium-bitrate devices operating on a battery over a short distance (that is, 10 to 20 meters). This distance can be extended by “meshing” to other WPAN devices. Bluetooth and Zigbee are examples of WPAN technologies. WPAN technologies are useful in short-range applications such as those within a “smart building”.

**LPWAN:** LPWAN stands for “Low-Power Wide Area Network”. These technologies are designed to connect low-bitrate devices operating on a battery, such as sensors, over long distances. Examples of LPWAN technologies include Lora/LoRaWAN, Sigfox and NB-IOT. These technologies are useful in low-density, long-range deployments.

The city’s network is the spinal cord linking IoT devices with the software, applications and people that analyze their data and control them. The city’s network delivers network services to government agencies, businesses and users over different technologies. Section 5 introduces ALE’s solution for smart city nets.

The command center is the facility where government personnel manage incident and analyze data for better city planning. The command center also acts as the city’s emergency and disaster management center supporting multiple agencies (for example, law enforcement, public transport, environmental, and more).
ALE’s network solutions enable smart city use cases. In this document, we are focused on six smart city solution sets shown in Figure 3. These solution sets are described in Sections 5 through 10.

**Figure 2 - Smart city infrastructure**

**Figure 3 - Smart city solution sets**

**City Net**
City-wide fabric to interconnect government agencies, residents, visitors, businesses and IoT devices.

**Municipal Wi-Fi**
Municipal Wi-Fi provides amenity to visitors and residents and enables multiple smart city use cases.

**Municipal Cloud**
End2End virtualized and consolidated cloud enables smart city use cases by breaking siloes whilst at the same time achieving economies of scale.

**Smart Civic Venue**
Location and wayfinding enables use cases such as visitor guides, geo-fenced alerts and more.

**Smart Transit**
Dedicated solutions for on-board communications and smart shelters.

**Smart Roads & Highways**
Reducing congestion, improving safety and keeping drivers informed in real time.
4 Reference architecture

Implementing these use cases requires breaking organizational siloes. Information must be shared and budgets must be pooled across multiple government agencies for this to be technically feasible and cost-effective. A siloed architecture in which each vertical use case relies on its own infrastructure, middleware and applications increases complexity and cost.

The ALE reference architecture for smart cities is shown in Figure 4. This horizontal architecture makes common infrastructure and services layers available to use cases and applications.

This approach has the following advantages:
- Facilitates sharing of information across different use cases and applications, a key requirement of smart cities.
- Consolidates network, cloud and services in shared layers which are abstracted from and used by applications, thus simplifying application development.
- Eliminates multiplication of infrastructure and middleware performing similar functions, thus reducing TCO.

The Alcatel-Lucent Enterprise Intelligent Fabric architecture enables this horizontal approach through:
- Automated network node provisioning (ZTP/RCD)
- Automated IoT device provisioning (Access Guardian/UNP)
- Service-oriented architecture (SPB/VXLAN/GRE)
- Northbound APIs (Alcatel-Lucent OmniSwitch®/Alcatel-Lucent OmniVista®)

Figure 4 - ALE smart city reference architecture
5 City net

5.1 Introduction

Smart cities rely on a robust, yet flexible network foundation to interconnect sensors, people and businesses with cloud-based applications. A city net is the cornerstone of a smart city since all use cases are reliant on it.

Figure 5 - Cornerstone of a smart city
Let’s review the three main business drivers of a city net in Figure 6.

**Figure 6 - city net Business Drivers**

We can now translate these business drivers into technical requirements in **Table 2**.

---

**Table 2 - City net technical requirements**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Requirement Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-tenancy</td>
<td>A “city net” provides services to multiple tenants. L3 VPN services are needed for most government agencies, schools and hospitals. L2 VPN services are needed in specific situations such as DC interconnect. IoT devices of different class need to be isolated in their own L2 or L3 container for security.</td>
</tr>
<tr>
<td>Availability</td>
<td>Availability is of utmost importance since the city net provides services to multiple agencies and supports multiple use cases. The city net must implement redundancy at all layers to protect from node or link failure and to facilitate in-service maintenance. In the event of a failure, the network must re-converge in under 1 second.</td>
</tr>
<tr>
<td>Scalability</td>
<td>The city net architecture must be scalable to support the required number of tenants, containers, devices and users as well as bandwidth and multicast flow and more.</td>
</tr>
<tr>
<td>Simple Operations</td>
<td>The city net can be comprised of thousands of network nodes and IoT devices. Because of its size, template-driven automatic provisioning of nodes and devices is necessary to reduce deployment cost, time and errors.</td>
</tr>
<tr>
<td>Security</td>
<td>Because a smart city net supports mission-critical infrastructure, security is even more critical than traditional enterprise security. A multi-layered approach is required including security hardening of nodes and devices, network admission control (NAC) and role-based access, protection of data integrity and confidentiality as well as quarantine and remediation among others.</td>
</tr>
<tr>
<td>Environmental</td>
<td>Smart city net nodes will be deployed in locations such as within a road-side cabinet where they will be subject to extreme temperatures, dust, vibration and shock. The network devices must tolerate such harsh conditions.</td>
</tr>
</tbody>
</table>
5.3 L2/L3 VPNs and IoT containers

Figure 7 illustrates the concept of L3 VPNs for government agencies, schools and hospitals. In this diagram, schools, hospitals and other government agencies are tenants of the city net and each have their own L3 VPN. VPN technology ensures all these different tenants can coexist on the same infrastructure and that tenant data is kept private from other tenants. In a L3 VPN, tenants exchange routes with the city net and the city net routes tenant data from site to site over the most optimal route without traffic tromboning back and forth to a central site for routing. In addition, tenant data is isolated from other tenants and tenant routes are not advertised to other tenants.

Figure 7 - City net L3 VPN

Figure 8 illustrates the concept of L2 VPNs for DC interconnect. In this diagram, two DC locations are interconnected by L2 services. These DCs provide services to different tenants. Unlike L3 VPN services, in a L2 service there is no exchanging of routes between tenant and the city net. Any routing is done by the tenant and data is simply bridged across the city net. This L2 communication is a requirement in certain scenarios, such as DC interconnect, because it enables VM mobility an HA across both locations. An L2 VPN also isolates tenant data from other tenant’s data.

Figure 8 - City net L2 VPN
Finally, Figure 9 illustrates the concept of IoT containment. In this figure, multiple different types of IoT devices such as sensors, actuators, cameras and door locks are connected. IoT devices are grouped into different containers: Utility, administration, security, etc. This containerization increases security because a container is isolated from other containers and devices in different containers can only communicate through a firewall. In addition, devices are mapped to containers according to the device type using authentication (MAC or certificate-based 802.1x). Once the device type and container are determined, the device is bound to a profile which will also restrict communication with other devices, even if on the same container, and apply fine-grained QoS policies to the device.

**Figure 9 - IoT Containers**

---

5.4 Intelligent Fabric in city nets

Intelligent Fabric is based on the IEEE standard protocol Shortest Path Bridging. Table 3 compares this technology with legacy protocols such as VLANs, Spanning Tree, and MPLS (Multi-Protocol Label Switching). As we can see, SPB is superior for small to medium-sized city nets because it is much simpler to deploy and operate, resulting in lower total cost of ownership.

**Table 3 - SPB comparison**

<table>
<thead>
<tr>
<th></th>
<th>Legacy (VLAN/STP)</th>
<th>MPLS</th>
<th>SPB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtualization</td>
<td>VLAN</td>
<td>VPN</td>
<td>VPN</td>
</tr>
<tr>
<td>Availability</td>
<td>Slow fault recovery</td>
<td>Fast fault recovery</td>
<td>Fast fault recovery</td>
</tr>
<tr>
<td>Performance</td>
<td>Single active path</td>
<td>Multiple active paths</td>
<td>Multiple active paths</td>
</tr>
<tr>
<td>Scalability</td>
<td>Small networks</td>
<td>Very large networks</td>
<td>Large networks</td>
</tr>
<tr>
<td>Complexity / Operational Costs</td>
<td>Low/high</td>
<td>High/high</td>
<td>Medium/low</td>
</tr>
<tr>
<td></td>
<td>Limited</td>
<td>High cost</td>
<td>Best option</td>
</tr>
</tbody>
</table>
5.5 Solution highlights

Table 4 shows the most relevant ALE products for a smart city net solution and the typical role that they may fulfill along with the key network and environmental features and market-specific certifications that make them a good fit for the role.

Table 4 - City net solution highlights

<table>
<thead>
<tr>
<th>Product</th>
<th>Role</th>
<th>Key environmental features</th>
<th>Key network features</th>
<th>Market-specific certifications</th>
</tr>
</thead>
</table>
| OmniSwitch 6865              | Advanced hardened access or collapsed access + backbone | • fan-less  
• shock, vibration, temperature  
• IP-30 rating* | • ERPv2, SPB  
• OAM  
• POE / POE+ / UPOE*  
• Virtual chassis / ISSU*  
• IEEE 1588v2 | • NEMA-TS2 (Traffic controller assemblies)*  
• CC EAL-2 & NDcPP  
• FIPS-140 |
| OmniSwitch 6465              | Value hardened access       | • fan-less  
• shock, vibration, temperature  
• IP-30 rating* | • ERPv2  
• OAM*  
• POE / POE+ / UPOE*  
• Stacking  
• Alarm replay inputs  
• MACSec*  
• IEEE 1588v2 | • NEMA-TS2 (Traffic controller assemblies)*  
• CC EAL-2 & NDcPP  
• FIPS-140 |
| OmniSwitch 6350 / 6450 / 6565T / 6560 | Value access / Smart building | • Extended temperature range (6465T only)* | • ERPv2  
• OAM*  
• POE / POE+ / UPOE*  
• Stacking  
• MACSec*  
• IEEE 1588v2 | • CC EAL-2 & NDcPP  
• FIPS-140 |
| OmniSwitch 6860 / 6900 / 9900 | Aggregation, backbone, core | | • ERPv2  
• OAM*  
• Virtual chassis / ISSU  
• MACSec*  
• IEEE 1588v2 | • CC EAL-2 & NDcPP  
• FIPS-140 |
| OmniVista 2500 NMS           | Network Management System   | | • Network management  
• Unified access  
• Analytics | |

* Check data sheets for full details
5.6 Why use ALE’s Intelligent Fabric for smart city nets?

Let’s review the key reasons that make ALE’s Intelligent Fabric a great fit for the smart city’s network in Figure 10.

Figure 10 - Why use ALE’s Intelligent Fabric in smart city nets

**Simplicity**
SPB delivers MPLS-like features in a much simpler way, resulting in faster deployments and simpler operations. Further simplification with single OS and management system and plug & play for network nodes and IoT devices.

Simplification reduces costs

**Convergence**
One physical network with multiple virtual containers. Converged electrical and data wiring. Integrates with MPLS and GPON. Standard and harsh environments.

Convergence reduces costs

**Seamless**
VPNs and Containers segregate organizations and IoT devices. Network is protected from attacks. Data is encrypted and protected against unauthorized access or tampering.

Mission-critical security
6 Municipal cloud

6.1 Introduction

The municipal cloud serves two main purposes:

• Hosting the multiple systems, applications, databases, and more powering the various smart city use cases (for example, smart lighting, smart waste management, and more). The smart city’s “brain”.

• Hosting systems, applications, databases and more, for smart city net customers, such as government or private organizations, hospitals and schools.

The municipal cloud may also provide additional services such as email, Web, caching, storage, content delivery network (CDN), voice communications and IP TV.

6.2 Business drivers and technical requirements

Let’s now review the three main business drivers of a municipal cloud in Figure 11.

Figure 11 - Municipal cloud business drivers

![Breaking Siloes]

Breaking Siloes
Sharing information between government agencies and with the public through applications, services and open data initiatives.

![Smarts]

Smarts
Integrate management, analytics, control and applications that power smart city solutions.

![Cost Effectiveness]

Cost Effectiveness
Consolidate budgets and take advantage of economies of scale to lower costs through ownership, bulk buying and wholesale.

We can now translate these business drivers into technical requirements in Table 5.
Table 5 - Municipal cloud technical requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-tenancy</td>
<td>The municipal cloud will provide services to multiple tenants including government and private organizations. Tenants must be isolated from one another for security reasons and to avoid conflicting IP addressing issues. Tenant traffic must be seamlessly stitched from the city net to municipal cloud, across DC sites and between the private and public cloud.</td>
</tr>
<tr>
<td>Business Continuity</td>
<td>The municipal cloud must recover from multiple failure scenarios without disruption to customers. To accomplish this, active/active intra- and inter-DC redundancy with no single point of failure and sub-second convergence is required.</td>
</tr>
<tr>
<td>Elasticity</td>
<td>Customers must be able to scale their workloads up and down both on-site at the municipal cloud DC sites or off-site across the public cloud.</td>
</tr>
<tr>
<td>Fluid operations</td>
<td>Manual intervention to moves, adds and changes should be minimized. The network must automatically adapt to event such as Virtual Machine Mobility. Operators should be able to perform software upgrades in-service without disruption to customer traffic.</td>
</tr>
<tr>
<td>Performance</td>
<td>The municipal cloud must offer high throughput and low latency, loss-less capability for storage convergence as well as monitoring and optimization of workload performance.</td>
</tr>
<tr>
<td>Sustainability</td>
<td>The municipal cloud must operate within a compact footprint and with low power consumption and cooling requirements.</td>
</tr>
</tbody>
</table>

6.3 The virtualized data center

The municipal cloud also adopts a layered horizontal architecture to break siloes and reduce costs by consolidating and sharing common functions across the board.

The municipal cloud can extend across multiple physical active/active data centers for high availability and load sharing. The municipal cloud can also extend to public clouds for elasticity or to exchange information with those clouds. Containers abstract these aspects such that, to the application and the customer, the container appears to be a virtual DC. Please refer to Figure 12.

Figure 12 - Virtualized municipal cloud
6.4 **End-to-end virtualized hybrid multi-tenant cloud**

City net containers extend deep into the data centers and all the way through the top-of-rack (TOR) switch down to the virtual machine (VM). This deep containerization keeps different organizations applications and data isolated end-to-end. This not only improves security, but also facilitates migration of hardware and applications from on-premises DC to the Municipal Cloud. Regardless of where the application is hosted (primary or secondary DC or even the public cloud) it is mapped to the appropriate container. Secure containerization is maintained seamlessly across DC sites and the public cloud and from the IoT device at the edge of the network all the way to the application that controls it. Refer to Figure 13.

**Figure 13 - End-2-End Virtualized Hybrid Multi-Tenant Cloud**
6.5 Solution highlights

Table 6 shows the most relevant ALE products for a Smart Municipal Cloud solution and the typical role that they may fulfill along with the key network and environmental features and market-specific certifications that make them a good fit for the role.

### Table 6 - Municipal Cloud Solution Highlights

<table>
<thead>
<tr>
<th>Product</th>
<th>Role</th>
<th>Key network features</th>
<th>Specific features</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>OmniSwitch 9900</td>
<td>Modular spine node</td>
<td>• Virtual chassis</td>
<td>• In-line routing</td>
<td>1G / 10G / 25G / 40G / 50G / 100G</td>
</tr>
<tr>
<td>OmniSwitch 6900-C32</td>
<td>Stackable 100G spine node</td>
<td>• SPB</td>
<td></td>
<td>1G / 10G / 25G / 40G</td>
</tr>
<tr>
<td>OmniSwitch 6900-Q32</td>
<td>Stackable 40G spine node</td>
<td>• VM snooping</td>
<td>• VXLAN gateway</td>
<td>1G / 10G / 25G / 40G</td>
</tr>
<tr>
<td>OmniSwitch 6900-V72</td>
<td>Stackable 25G leaf node</td>
<td>• VXLAN</td>
<td></td>
<td>1G / 10G / 25G / 40G</td>
</tr>
<tr>
<td>OmniSwitch 6900-X72</td>
<td>Stackable 10G leaf node</td>
<td>• Openflow</td>
<td></td>
<td>1G / 10G / 40G</td>
</tr>
<tr>
<td>OmniSwitch 6900-X20 / 40</td>
<td>Semi-modular 10G leaf node</td>
<td>• Python programmability</td>
<td>• FC gateway</td>
<td>1G / 10G / 40G / 10G</td>
</tr>
<tr>
<td>OmniSwitch 6900-T20 / 40</td>
<td>Semi-modular 10G copper leaf node</td>
<td>• ZTP</td>
<td></td>
<td>1G / 10G / 40G / 10G-T / FC</td>
</tr>
<tr>
<td>OmniVista 2500</td>
<td>NMS</td>
<td>• VM mobility / snooping</td>
<td></td>
<td>1G / 10G / 40G / 10G</td>
</tr>
</tbody>
</table>

* Check data sheets for full details

6.6 Why use ALE’s Intelligent Fabric for smart municipal clouds?

Let’s review the key reasons that make ALE’s Intelligent Fabric a great fit for the smart city’s municipal cloud in Figure 14.

### Figure 14 - Why use ALE’s Intelligent Fabric for smart municipal clouds

**Service-oriented**
ALE’s Intelligent Fabric technology brings service and container segregation all the way into the DC rack whilst also providing multiple active, low-latency paths.

**Economies of scale**
ALE’s Intelligent Fabric meets the requirements of both DC fabrics and City Nets with a single technology. Operations are simplified with a single OS and NMS across the board.

**Simplification reduces costs**
Simplification reduces costs

**Seamless**
Seamless multi-site HA across the WAN and elasticity towards the public cloud. Network automatically reconfigures on VM moves, adds and changes. In-service upgrades.

**Mission-critical HA**
7 Municipal Wi-Fi

7.1 Introduction

It is assumed that the benefits of Wi-Fi are well understood. Therefore, in this section we will jump straight to the business drivers for Municipal Wi-Fi. That is, the reasons why a City or Municipality may choose to provide this service.

7.2 Business drivers and technical requirements

Let's start by reviewing the three main business drivers of a municipal Wi-Fi service in Figure 15.

Figure 15 - Municipal Wi-Fi Business Drivers

We can now translate these business drivers into technical requirements in Table 7.

Table 7 - Municipal Wi-Fi Technical Requirements

<table>
<thead>
<tr>
<th>Ubiquitous</th>
<th>Municipal Wi-Fi coverage needs to extend to both indoor and outdoor locations.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flexible Deployment</td>
<td>To extend into as many locations as practically possible, Municipal Wi-Fi needs to support deployment over traditional wired Ethernet as well as wireless &quot;mesh&quot; deployments and even mobile or broadband backhaul. Municipal Wi-Fi should support a wholesale model in which a single physical infrastructure can be leveraged by other service providers to offer Wi-Fi services to their customers.</td>
</tr>
<tr>
<td>Scalable</td>
<td>Municipal Wi-Fi must scale up and down. Some locations may require hundreds of Access Points whilst other locations may require only a single AP. The solution must not be constrained by scalability and cost of a hardware controller.</td>
</tr>
<tr>
<td>Performant</td>
<td>Municipal Wi-Fi may be offered in crowded locations where the user density is very high and the user device capabilities can be varied. The Municipal Wi-Fi solution must cater to these environments and provide a good SLA to all users.</td>
</tr>
<tr>
<td>Quality of Experience</td>
<td>The Municipal Wi-Fi must offer a simple registration and authentication experience. The Municipal Wi-Fi must support other network provider's users seamlessly authenticating and roaming into the Municipal Wi-Fi.</td>
</tr>
<tr>
<td>Analytics</td>
<td>The Municipal Wi-Fi must be capable of providing connection information (for example, RSSI) for analysis such as people presence and flow in public spaces.</td>
</tr>
</tbody>
</table>
7.3 Solution overview

Figure 16 illustrates the concept of a municipal Wi-Fi service. The municipal Wi-Fi service is comprised of indoor and outdoor wireless access points connecting to the city net. Municipal Wi-Fi service is offered in locations such as tourist areas, shopping strips, parks, community centers, convention centers and public libraries. Access points use a wired connection whenever possible. When this is impractical however, wireless meshing can extend the municipal Wi-Fi footprint without wires. A captive portal allows users to register for and authenticate to the municipal Wi-Fi service. Users of other approved network service providers (for example, mobile or fixed) can seamlessly roam to the municipal Wi-Fi without need for an additional account thanks to the Hotspot 2.0 feature.

In addition to providing amenity to residents and visitors, the same municipal Wi-Fi infrastructure is leveraged to support connection of various IoT devices powering smart city use cases, such as Wi-Fi enabled smart bins, digital kiosks, smart light poles and video surveillance.

Figure 16 - Municipal Wi-Fi
7.4  Solution highlights

Table 8 shows the most relevant ALE products for a smart municipal Wi-Fi solution and the typical role that they may fulfill along with the key network and environmental features and market-specific certifications that make them a good fit for the role.

Table 8 - Municipal Wi-Fi solution highlights

<table>
<thead>
<tr>
<th>Product</th>
<th>Role</th>
<th>Key environmental features</th>
<th>Key network features</th>
<th>Market-specific certifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP 1101</td>
<td>Value indoor AP</td>
<td></td>
<td>• Wave 1 2x2.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Dual-radio</td>
<td></td>
</tr>
<tr>
<td>AP 1201</td>
<td>Mid-range indoor AP</td>
<td></td>
<td>• Wave 2 2x2.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Dual-radio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Built-in BLE + 802.15.4 (Zigbee)</td>
<td></td>
</tr>
<tr>
<td>AP 122X</td>
<td>High-end indoor AP</td>
<td></td>
<td>• Wave 2 4x4.4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Dual-radio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Built-in BLE support</td>
<td></td>
</tr>
<tr>
<td>AP 123X</td>
<td>Flagship indoor AP</td>
<td></td>
<td>• Wave 2 4x4.4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Tri-radio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Built-in BLE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Dual network ports (1G / 2.5G)</td>
<td></td>
</tr>
<tr>
<td>AP 1251</td>
<td>Outdoor AP</td>
<td>• -40˚ - 65˚ celsius</td>
<td>• Wave 2 2x2.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IP67</td>
<td>• Dual-radio</td>
<td></td>
</tr>
<tr>
<td>OmniVista 2500</td>
<td></td>
<td>Network management system</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>User and policy management</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Check data sheets for full details

7.5.  Why ALE’s OmniAccess Stellar for smart municipal Wi-Fi?

Let’s review the key reasons that make ALE’s OmniAccess Stellar a great fit for the smart city’s municipal Wi-Fi in Figure 17 - Why ALE’s OmniAccess Stellar for smart municipal Wi-Fi.

Figure 17 - Why ALE’s OmniAccess Stellar for smart municipal Wi-Fi

**Distributed Intelligence**
Distributing intelligence on every AP eliminates the controller’s cost, performance bottlenecks and point of failure. ZTP and management from private Municipal Cloud.

**802.11ac and beyond**
Thousands of APs managed from a single pane of glass. Without hardware controllers, the solution can scale from 1 to thousands of APs without the capacity constraints and costs of controllers.

**Scalable**
Simple licensing based on AP count. No hardware controllers. Cost-effective in Small, Medium, Large and Extra Large deployments. Costs are linear with the number of APs.

**City-scale Wi-Fi**
Faster ROI
8 Smart transit

8.1 Introduction

Smart transit solutions make passenger journeys on public buses safer and more pleasant with on-board video surveillance and Wi-Fi. Bus location and live video feeds can be accessed from the operations center and by law enforcement over a cellular link. Bus arrival information is available in real-time on smart displays at the bus stop and smart phones. As a result, ridership figures increase. Smart transit solutions also improve operational efficiency with real-time fleet management and fare collection.

8.2 Business drivers and technical requirements

Let’s start by reviewing the three main business drivers of a smart transit solution in Figure 18.

Figure 18 - Smart transit business drivers

We can now translate these business drivers into technical requirements in Table 9.

Table 9 - Smart transit technical requirements

<table>
<thead>
<tr>
<th>Feature</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardening</td>
<td>On-board and outdoor equipment must tolerate extreme temperatures, vibration, shock and be protected from voltage spikes. On-board equipment must support a delayed-power off feature such that video images can be uploaded when the bus reaches the depot without draining the vehicle’s battery.</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Wi-Fi is required for on-board IoT devices and for passengers. Different traffic types must be segregated in different containers. Wi-Fi radios must support AP mode (for serving passengers and IoT devices) as well as client mode (to connect to an external AP for image and software upload/download).</td>
</tr>
<tr>
<td>WWAN HA</td>
<td>The device must support multiple 4G/LTE radios and SIM cards for load balancing, bandwidth aggregation and high availability.</td>
</tr>
<tr>
<td>Location</td>
<td>Assisted GPS must be supported for fleet tracking. Geo-fencing is required such that the vehicle can use Wi-Fi when it reaches the depot.</td>
</tr>
<tr>
<td>Voice Support</td>
<td>Emergency and driver communications require SIP proxy/gateway with GSM support.</td>
</tr>
<tr>
<td>Cloud Management</td>
<td>Zero-touch provisioning and remote management, tracking and reporting over the WWAN.</td>
</tr>
</tbody>
</table>
8.3 Solution overview

A smart transit solution is depicted in Figure 19. There are two components in this solution: The on-board solution and the smart bus shelter solution.

The on-board solution is comprised of the H2-Automotive+ rugged on-board router. This router includes one or more cellular modules which provide Internet access for passengers as well as secure connectivity to the operations center and cloud-based applications for fleet management, fare collection, location tracking and access to video feeds. Different SIM cards associated to different mobile service providers can be used to increase throughput and reliability. On-board services such as passenger announcement and passenger information also connect to the on-board router. In addition, VoIP or built-in LTE gateway (selected models only) provide emergency phone and driver communication.

A smart bus shelter solution is also comprised of an H2-Automotive+ rugged router supporting similar set of services. Passengers waiting for the bus can enjoy Wi-Fi, live bus arrival time information on smart displays and feel safer knowing emergency phones can connect them to the emergency responders who can monitor the shelter in real time.

Figure 19 - Smart transit solution overview
8.4 Solution highlights

Table 10 shows the most relevant ALE products for a smart transit solution and the typical role that they may fulfill along with the key network and environmental features and market-specific certifications that make them a good fit for the role.

Table 10 - Smart Transit Solution Highlights

<table>
<thead>
<tr>
<th>Product</th>
<th>Role</th>
<th>Key environmental features</th>
<th>Key network features</th>
<th>Market-specific certifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>H2 Automotive</td>
<td>On-board router</td>
<td>• UNE-EN 60068-2 (shock and vibration)</td>
<td>• Up to 2 x 4G/LTE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• -25°C to 70°C celsius</td>
<td>• Up to 2 x WiFi (client/AP modes)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ISO7637-2 (power protection for direct battery power supply)</td>
<td>• GPS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Dual SIM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• IPSEC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 4 x 10 / 100 / 1000Base-T RJ-45</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Load balancing / aggregation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Hotspot</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• GSM gateway</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• SIP Proxy/server</td>
<td></td>
</tr>
<tr>
<td>Colibri</td>
<td>Cloud-based network</td>
<td>• Zero-touch provisioning</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>management system</td>
<td>• Analytics</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Historical location tracking</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Reporting</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Check data sheets for full details

8.5 Why ALE’s H2-Automotive+ for smart transit

Let’s review the key reasons that make ALE’s H2-Automotive+ a great fit for the smart city’s smart transit solution in Figure 17 - Why ALE’s OmniAccess Stellar for Smart Municipal Wi-Fi.

Figure 20 - Why ALE’s H2-Automotive+ for smart transit

Ruggedness
Purpose-built to operate in harsh on-board conditions.

Resiliency
Seamless load balancing and aggregation across multiple LTE/4G radios and providers to protect from service black holes.

Reliability
Always reachable

Faster ROI

Easy Operations
Simple template-based provisioning and fleet tracking from the cloud.

Solution guide
Smart City Solution Guide
9 Smart civic venue

9.1 Introduction

Civic venues such as museums and conference centers can become smarter with the aid of ALE's Location Based Services. Precise visitor positioning information is leveraged by visitor guide applications to enhance the visitor’s experience providing navigation through stands, museum pieces, augmented reality and more. Visitors can easily meet up with their friends and colleagues. Security is improved in various ways: visitors can easily locate and be routed to emergency exits and security staff can be located and quickly mobilized where needed. Finally, location information can be used for marketing (for example, vouchers and discounts) and visitor analytics.

9.2 Business drivers and technical requirements

Let’s start by reviewing the three main business drivers of a smart civic venue in Figure 21.

**Figure 21 - Smart Civic Venue Business Drivers**

- **Tourism and Events**: Contextual visitor experience. Geo-push when in proximity to POI. Assisted navigation and improved flows.
- **Safety**: Pinpointing accurate location of 911 caller. Routing to nearest exit. Reporting safety hazards.
- **Indoor Navigation**: Improving people flow in busy locations. Helping the visually challenged find their way around.

We can now translate these business drivers into technical requirements in Table 11.

**Table 11 – Smart civic venue technical requirements**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td>Location accuracy within a few meters is required for positioning and wayfinding.</td>
</tr>
<tr>
<td>Low Maintenance</td>
<td>Battery-powered standalone beacons must last 5 years or more without signal degradation or need to recalibrate to keep TCO low.</td>
</tr>
<tr>
<td>Multiple BLE Options</td>
<td>Multiple BLE options such as standalone battery-operated beacon, USB dongle, and built-in into an Access Point are required for deployment flexibility.</td>
</tr>
<tr>
<td>People Tracking</td>
<td>Employee tracking must be supported with dedicated application.</td>
</tr>
<tr>
<td>Analytics</td>
<td>The solution must provide visitor analytics such as duration of the visit per day/week, heatmaps, OS, returning visitors, etc.</td>
</tr>
</tbody>
</table>
9.3 Solution overview

Figure 22 provides an example of a smart civic venue application and its benefits.

The smart civic venue solution uses positioning and way-finding to enhance a visitor’s experience and safety. A location SDK (Software Developer Kit) is leveraged by the smartphone application to compute the visitor’s location by triangulating signals received from BLE (Bluetooth Low Energy) beacons and combining this information with compass, accelerometer and GPS data to increase accuracy. The SDK also includes geo-fencing to notify visitors when entering/exiting a specific zone. BLE beacons are installed throughout the venue such that visitors are always within range of 3 or more beacons. BLE beacons are available as standalone (battery-operated), USB dongle (powered through an USB port, such as the USB port on a Wi-Fi AP or desk phone) or natively built-in into an OmniAccess Stellar Wi-Fi AP. The OmniAccess Stellar LBS installer application is used for beacon installation and calibration. The OmniAccess Stellar LBS Cloud Manager is a cloud-based application which provides beacon management, geo-notification campaign management, analytics as well as people tracking (staff only). Lastly, the OmniAccess Stellar LBS Tracker is an android-based application which is installed on staff’s smart phones and always runs in the background to track their location.

Figure 22 - Smart Civic Venue Solution Overview

1. Visitor enters venue such as a museum or convention center and launches the smart venue application. Their location is identified on the map.

2. Visitor shares their Group ID with other members in their party so they can keep track of their location.

3. A specific GEO tag is assigned to children or elderly members so geo-fencing alerts will alert the user when they exceed their allowable perimeter.

4. Looking for a stand, booth or restroom? Select point of interest to get directions and associated wait times so the user can optimize their time at the venue.

5. As the user passes restaurants or shops, they receive advertising such as discounts and specials which will help drive additional revenue for their venue.

6. In case of an emergency, you will be alerted and the quickest path to an exit will be highlighted on your map.

7. Venue security administrators can use the tracker to locate and mobilize security staff quickly, and ensure all visitors are evacuated.
9.4 Solution highlights

Table 12 shows the most relevant ALE products for a smart civic venue solution and the typical role that they may fulfill along with the key network and environmental features and market-specific certifications that make them a good fit for the role.

Table 12 - Smart Civic Venue Solution Highlights

<table>
<thead>
<tr>
<th>Product</th>
<th>Role</th>
<th>Key environmental features</th>
<th>Key network features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standalone beacon</td>
<td>Battery-operated BLE</td>
<td>• 5+ years battery life</td>
<td>• Transmit only</td>
</tr>
<tr>
<td>BLE dongle</td>
<td>USB BLE</td>
<td>• USB powered</td>
<td>• Transmit only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Compatible with Stellar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>and 3rd party</td>
<td></td>
</tr>
<tr>
<td>AP 1230 and AP 1201</td>
<td>Integrated BLE</td>
<td></td>
<td>• Transmit and receive* (1201)</td>
</tr>
<tr>
<td>OmniAccess Stellar LBS Installer</td>
<td>Beacon deployment and calibration</td>
<td></td>
<td>• Calibrate the indoor location service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Evaluate location accuracy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Test geonotifications</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Indicate beacons locations</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Check beacons life status in real-time</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• (Re)configure beacons</td>
</tr>
<tr>
<td>OmniAccess Stellar LBS Cloud Manager</td>
<td>Solution management</td>
<td></td>
<td>• Beacon management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Sync positioning database</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Geonotification campaigns</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• People and asset tracking</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Location analytics</td>
</tr>
<tr>
<td>OmniAccess Stellar LBS SDK</td>
<td>Location computation</td>
<td></td>
<td>• 3D location</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Geonotifications</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Data sync with Cloud Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Sensor management</td>
</tr>
<tr>
<td>OmniAccess Stellar LBS Tracker</td>
<td></td>
<td></td>
<td>• Background Android app</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Automatic start-up at boot</td>
</tr>
</tbody>
</table>
9.5 Why ALE’s OmniAccess Stellar LBS for smart civic venues

Let’s review the key reasons that make ALE’s OmniAccess Stellar LBS a great fit for smart civic venues in Figure 23.

**Figure 23 - Why ALE’s OmniAccess Stellar LBS for smart civic venue**

- **Accuracy**
  Fusion algorithm combines multiple sensors (BLE, compass, accelerometer, barometer) to improve accuracy with lower beacon density.

- **Reliability**
  Long-lasting military-grade batteries and steady output power levels for accurate location without need for recalibration.

- **Easy Operations**
  Over-the-air maintenance and crowd-sourced beacon monitoring. All operations (monitoring, geofencing, analytics) in a single application.

- **Low TCO**

**Location, not just “proximity”**
10  Smart roads and highways

10.1  Introduction
Smart roads and highways use communications technologies to prevent accidents and reduce congestion. Wired and wireless networks handle the communications for all ITS systems and subsystems. They link cameras, sensors, signage, signaling and vehicles to remote traffic operations centers where the vast amounts of data that will be produced by these systems are monitored and acted upon to reduce vehicle congestion, monitor and respond to incidents and otherwise ensure the smooth running of roads and highways.

10.2  Business drivers and technical requirements
Let’s start by reviewing the three main business drivers of smart roads and highways in Figure 24.

Figure 24 - Smart roads and highways business drivers

We can now translate these business drivers into technical requirements in Table 13.
### Table 13 – Smart roads and highways technical requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>High availability is a fundamental requirement for a network carrying mission-critical system traffic. Redundancy without single point of failure (SPOF) is required at the network and system level such that recovery upon a failure event is automatic and maintenance tasks can be performed in-service.</td>
</tr>
<tr>
<td>Virtualization</td>
<td>One network will carry traffic for multiple systems over a common infrastructure. These systems will communicate various disparate, often proprietary, devices and applications that may be operated and maintained by different groups or vendors and may require communication with third parties. The network must be able to support multi-tenancy and virtual segregation such that systems and tenants do not interfere with one another. Virtual private networks (VPN) enable secure separation and bandwidth allocation for system and tenant traffic.</td>
</tr>
<tr>
<td>Scalability</td>
<td>The network must be capable of scaling to support the required number of systems and tenants, IoT containers, end devices, multicast flows, bandwidth and so on.</td>
</tr>
<tr>
<td>Performance</td>
<td>Not all systems are critical to the same extent and different systems have different performance requirements. The ability to prioritize certain systems over others will be important when the network is congested or when traffic is re-routed around a failure. When these conditions occur, the network will need to manage the congestion by allocating bandwidth and prioritizing traffic.</td>
</tr>
</tbody>
</table>
| Security             | Security is paramount to networks supporting critical transport infrastructure. In addition to segregation of system traffic into VPNs or containers, the following security requirements must be catered for:  
  • Network node security: Network nodes must be hardened and protected from attacks such as DDoS attacks.  
  • Network admission control and role-based access: access to network resources will only be granted upon successful user or device authentication and privileges will be set according to user or device role.  
  • Quarantine: The network must be capable of isolating a compromised device.  
  • Integrity: Accuracy, consistency and trustworthiness must be protected while in transit through the network. Data must be protected from modification by unauthorized parties.  
  • Confidentiality: Data must be protected from access by unauthorized parties while in transit through the network. |
| Environmental        | Roadside equipment will be subject to harsh conditions such as extreme temperatures, vibrations and dust. Roadside equipment must be compliant with NEMA TS-2 standard to be mounted in NEMA roadside cabinets. |

### 10.3 Solution overview

Figure 25 depicts the smart roads and highways solution. An OmniSwitch network communicates the array of video cameras, sensors and signage and more, at the roadside, with the applications hosted at the data center. VPN containers keep different system, tenant and IoT device traffic isolated from one another to increase security.

![Figure 25 - Smart Roads and Highways Solution Overview](image-url)
10.4 **Solution highlights**

Table 14 shows the most relevant ALE products for a smart roads and highways solution. The table shows the typical role that the ALE solutions fulfill along with key network and environmental features and market-specific certifications that make them a good fit for the role.

**Table 14 - Smart roads and highways solution highlights**

<table>
<thead>
<tr>
<th>Product</th>
<th>Role</th>
<th>Key environmental features</th>
<th>Key network features</th>
<th>Market-specific certifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>OmniSwitch 6865</td>
<td>Advanced roadside access or collapsed access+core</td>
<td>• fan-less&lt;br&gt;• shock, vibration, temperature&lt;br&gt;• IP-30 rating*</td>
<td>• ERPv2&lt;br&gt;• OAM&lt;br&gt;• POE / POE+ / UPOE*&lt;br&gt;• Virtual chassis / ISSU*&lt;br&gt;• IEEE 1588v2</td>
<td>• NEMA-TS2 (Traffic controller assemblies)*&lt;br&gt;• CC EAL-2 &amp; NDCPP&lt;br&gt;• FIPS-140</td>
</tr>
<tr>
<td>OmniSwitch 6465</td>
<td>Value roadside access</td>
<td>• fan-less&lt;br&gt;• shock, vibration, temperature&lt;br&gt;• IP-30 rating*</td>
<td>• ERPv2&lt;br&gt;• OAM*&lt;br&gt;• POE / POE+ / UPOE*&lt;br&gt;• Stacking&lt;br&gt;• Alarm replay inputs&lt;br&gt;• MACSec*&lt;br&gt;• IEEE 1588v2</td>
<td>• NEMA-TS2 (Traffic controller assemblies)*&lt;br&gt;• CC EAL-2 &amp; NDCPP&lt;br&gt;• FIPS-140</td>
</tr>
<tr>
<td>OmniSwitch 6350 / 6450 / 6465T</td>
<td>Value access</td>
<td>Extended temperature range (6465T only)*</td>
<td>• ERPv2&lt;br&gt;• OAM*&lt;br&gt;• POE / POE+ / UPOE*&lt;br&gt;• Stacking</td>
<td>• CC EAL-2 &amp; NDCPP&lt;br&gt;• FIPS-140</td>
</tr>
<tr>
<td>OmniSwitch 6860 / 6900 / 9900</td>
<td>Aggregation, backbone, core</td>
<td></td>
<td>• ERPv2, SPB&lt;br&gt;• OAM&lt;br&gt;• Virtual chassis / ISSU&lt;br&gt;• MACSec*&lt;br&gt;• IEEE 1588v2</td>
<td>• CC EAL-2 &amp; NDCPP&lt;br&gt;• FIPS-140</td>
</tr>
<tr>
<td>OmniVista 2500 NMS</td>
<td>Network management system</td>
<td></td>
<td>• Network management&lt;br&gt;• Unified access&lt;br&gt;• Analytics</td>
<td></td>
</tr>
</tbody>
</table>

* Check data sheets for full details

10.5 **Why use ALE’s Intelligent Fabric for a smart roads and highways solution?**

Let’s review the key reasons that make ALE’s Intelligent Fabric a great fit for the smart city’s roads and highways in Figure 26 - Why ALE’s OmniAccess Stellar for smart municipal Wi-Fi.

**Figure 26 - Why get ALE’s Intelligent Fabric for smart roads and highways**

Simpler

SPB delivers MPLS-like features in a much simpler way, resulting in faster deployments and simpler operations. Further simplification with single OS and management system.

**Simplification reduces costs**

Converged

One physical network with multiple virtual containers. Converged electrical and data wiring. Integrates with MPLS and GPON. Standard and Harsh environments.

**Convergence reduces costs**

Secure

VPNs and Containers segregate organizations and IoT devices. Network is protected from attacks. Data is encrypted and protected against unauthorized access or tampering.

**Mission-critical security**
11 Security framework

Securing mission-critical city infrastructure requires a layered “defense-in-depth” approach that combines both proactive and reactive defense mechanisms. Please refer to Figure 27 for a snapshot of the various applicable mechanisms.

Figure 27 - Layered security framework

Let’s examine these mechanisms in more detail.

11.1 Securing IOT devices

IoT devices are vulnerable to security threats just like other IT assets. A compromised IoT device can also become an attack vector into other devices and systems. Because of the high number of IoT devices, the impact of such attacks can be very high.

These devices must be securely configured and managed. The exact measures will depend on the device capabilities and manufacturer recommendations, but some of these are listed.

- Passwords: Password complexity, renewal and authentication against a central database.
- Certificates: X.509 certificates can be installed on IOT devices allowing for mutual authentication between the IOT device and the server. Certificates can also be used for Network Admission Control (NAC).
- Encryption: Secure protocols such as Transport Layer Security (TLS) must be used when managing these devices and any unsecure protocol must be disabled.
- OS updates: IOT devices must be updated and patched according to manufacturer specifications to prevent exploitation of known vulnerabilities.
11.2 Securing the perimeter

When communication between different containers is required, it must only be allowed through Firewalls and controlled by fine and specific policies. Different systems may have physical or virtual firewalls of their own if operated by different organizations. Please refer to [4] for an explanation of how integration between Alcatel-Lucent Enterprise’s Unified Access solution and Palo Alto Networks firewall can be used to create dynamic fine-grained policies that take the user’s identity, device, application, location and other situational factors into consideration.

11.3 Securing the network

Several steps must be taken to secure the network infrastructure itself. An overview of network security mechanisms is given below.

11.3.1 Authenticated switch access and logging

Switch security features increase the security of the basic switch login process by allowing management only through specific interfaces for users with particular privileges. Login information and privileges should be stored on an external server such as Radius or LDAP. External servers should also be used for accounting, which includes logging statistics about user sessions. Admin authentication against the local database may be allowed on the console port only as a failover mechanism in case the external servers become unavailable or in case of misconfiguration.

11.3.2 Management plane protection

Management protocols must be secured, as detailed below:

- Unsecure protocols such as Telnet, FTP/TFTP and SNMP must be disabled
- SSHv2 should be used with keys larger than 2048 bits
- HTTPS can be used if required for RESTful API/WebServices access and if so, it should be setup with X.509 certificates for mutual authentication between network nodes and server.
- SNMPv3 with authentication and privacy options should be used for monitoring
- TLS 1.1. or 1.2 (preferred) should be used when connecting to remote RADIUS, LDAP or Syslog servers.

11.3.3 Denial of service (DoS) filtering

By default, an OmniSwitch filters denial of service (DoS) attacks. Some DoS attacks aim at system bugs or vulnerability, while other types of attacks involve generating large volumes of traffic so that network service is denied to legitimate network users.

11.3.4 OS hardening – CodeGuardian

CodeGuardian is a technology which mitigates risks at the source, enabling an enhanced security profile through:

- Independent verification and validation of OmniSwitch source code
- Software diversification of OmniSwitch object code to prevent exploitation
- Secure delivery of OmniSwitch software

CodeGuardian protects networks from intrinsic vulnerabilities, code exploits, embedded malware, and potential back doors that could compromise mission-critical operations. The CodeGuardian technology is continuously applied on every new AOS release, therefore it addresses both current and future threats.

11.3.5 Data plane protection - MACSec

Data integrity and confidentiality must be protected whilst in transit through the network. MACSec is an IEEE standard (802.1AE) which provides point-to-point authentication and optional encryption between MACSec-capable devices such as switches. MACSec can prevent various threats such as man-in-the-middle, sniffing, spoofing and playback attacks.

Because MACSec operates at the MAC layer, it transparently secures all upper layer traffic transiting through MACSec-enabled links. This includes both application-layer data as well as control-plane and management-plane communication. In addition, unlike IPSec, MACSec is implemented in hardware at wire-speed and does not introduce additional latency or bandwidth limitations.

In a smart city, the main application for MACSec is protecting data integrity and confidentiality whilst transiting over public spaces outside of the physical security perimeter, where it can be subject to tapping and other malicious activity.

11.3.6 Independent certification

OmniSwitch products have been independently certified to comply with rigorous security standards. Compliance with these standards is mandated in the public sector, but is valuable beyond. Independent certification is an objective benchmark to compare security features in different products.

OmniSwitch products are certified to comply with the following standards.

**Figure 28 - Security certifications**

11.3.6.1 Common Criteria

The Common Criteria for Information Technology Security Evaluation, normally referred to as Common Criteria for short, is a set of specifications which serves as a framework in the evaluation of security products.

There are two important aspects in the Common Criteria certification:

- The protection profile: This defines the specific security requirements which are relevant to a particular device class such as a network device or a firewall.
- The Evaluation Assurance Level (EAL): This is a number from 1 to 7 representing how thoroughly the product has been tested. Higher EAL levels do not necessarily mean more secure products but rather more thorough testing.

OmniSwitch products 6250, 6350 and 6450 with AOS 6.7.1.79R04 and 6860, 6865, 6900, 9900 and 10K with AOS 8.3.1.348.R01 are EAL-2 (Structurally Tested) against the Network Device Collaborative Protection Profile (NDcPP) set of requirements. Please refer to [9] and [10] for the EAL-2 and NDcPP certificates, respectively.
11.3.6.2 FIPS 140-2
The Federal Information Processing Standard 140-2 (FIPS 140-2) is a US and Canadian security standard focusing on hardware and software solutions using cryptography.

FIPS 140-2 certificates for AOS 6.7.1R04 (used in OmniSwitch 6350 and 6450) and AOS 8.3.1R01 (used in OmniSwitch 6860, 6865, 6900 and 9900) can be found in [11] and [12] respectively.

11.3.6.3 JITC
The Joint Interoperability Test Command (JITC) is the US Department of Defense’s Joint Interoperability Certifier and only non-Service Operational Test Agency for Information Technology (IT)/National Security Systems. JITC provides risk based Test, Evaluation and Certification services, tools, and environments to ensure Joint Warfighting IT capabilities are interoperable and support mission needs. OmniSwitch 6860, 6865, 6900 and 9900 are certified. Please refer to [13].

11.3.7 Network Admission Control – Access Guardian
Physical devices attached to a LAN port on the switch can be authenticated using port-based network access control. The following options for authentication are available:

- 802.1X authentication for supplicants.
  Uses Extensible Authentication Protocol (EAP) between an end device and a network device (NAS) to authenticate the supplicant through a RADIUS server.
- MAC-based authentication for non-supplicants.
  MAC-based authentication does not require any agent or special protocol on the non-supplicant device; the source MAC address of the device is verified through a RADIUS server. The switch sends RADIUS frames to the server with the source MAC address embedded in the username and password attributes.
- Internal or External Captive Portal
  Captive Portal authentication enables web-based authentication for guest and BYOD users.
  The authentication server may return a User Network Profile (UNP). UNPs map devices to VLANs or services and may contain security and QoS policies. If no UNP is returned, a default UNP is applied.

11.3.8 Containerization
Containers are virtual network segments where IoT devices and applications that control them are isolated from other devices and applications. This segmentation facilitates enforcement of security policies and limits the damage in the event of a security breach.

SPB intrinsically segments IOT devices into containers by way of MAC-in-MAC tunneling and the ISID field designates the container. Any communication outside of the container will be controlled by a firewall.

11.3.9 Threat mitigation and remediation
So far, we have focused on best practices and preventive measures that can proactively stop a security incident from happening in the first place. But due to the fast-evolving nature of security threats, no security strategy is complete without reactive mechanisms to thwart or dampen the effect of those threats that cannot be proactively avoided.
OmniVista 2500 NMS can be integrated with external Intrusion Detection Systems (IDS) through Syslog. When intrusion or malware attacks are detected by the IDS, a Syslog message is sent to OmniVista. The Syslog message includes the intruder’s or attacker’s address. OmniVista can use this information to locate the switch and port or AP that the device is connected to and quarantine it by shutting down the port or applying a quarantine profile (restrictive VLAN and ACLs) such that the malicious activity is stopped and remediation activities (for example, OS patching and cleanup) can be performed.

An additional DDoS mitigation method is described in [6] InMON sFlow-RT collects sFlow data from switches and detects DDoS attacks in real time. InMON notifies the DDoS Mitigation SDN Application which in turn instructs the SDN controller to push the necessary rules to drop traffic associated to the attack.

### 11.3.10 Analytics

Smart Analytics in OmniVista 2500 brings unprecedented visibility into the network status and use patterns up to the application level. Understanding patterns assists in fine tuning and enforcing security policies to drive compliance.

OmniVista 2500 collects data from all OmniSwitch products through SNMP and SFlow. Various reports transform this data into valuable information.

Application Visibility extends this view to the Application Layer through Deep Packet Inspection. This means applications can be detected even if running on standard Web ports such as TCP ports 80 and 443.

When using the OmniSwitch 6860E as a site access node, application visibility and policy enforcement can be enabled on standard (VLAN) access ports.

### 12 Conclusion

Alcatel-Lucent Enterprise’s offers a comprehensive set of solutions that allow smart cities to optimize investment while bringing new services that enhance the city’s livability, sustainability and competitiveness. Alcatel-Lucent Enterprise’s multi-layered security protects the city’s mission-critical infrastructure from cyberthreats.