

# ALE Networking Solutions Update

A.Doruk Çetinkaya  
April 2017



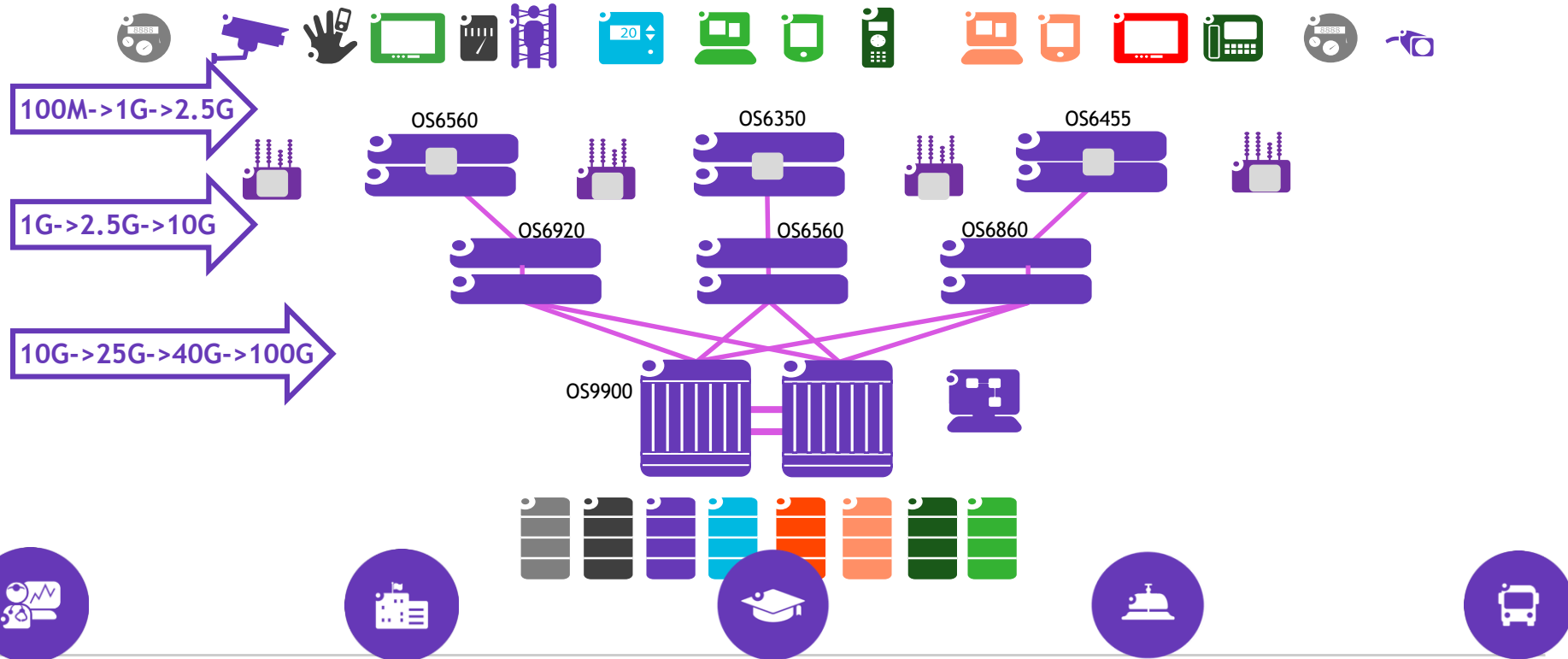
# Our Vision

To deliver the  
customized technology  
experiences our  
customers need.



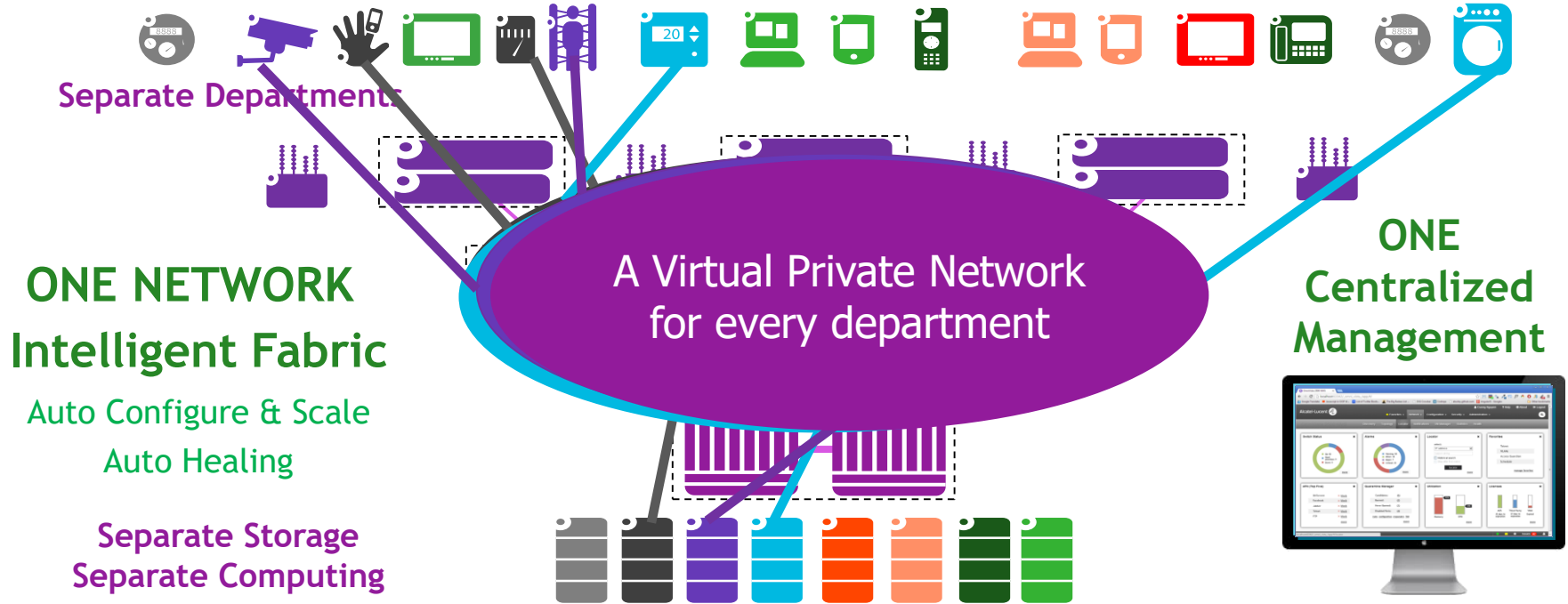
*To Make  
Everything  
Connect*

# Speed increase at all layers of the enterprise



# One Network Infrastructure

## One ALE Private Network for Every Department



The right technology to increase network resiliency and optimize IT operations

# Why SPB?

Network Demands	VLAN/STP (Spanning Tree Protocol)	MPLS (Multiprotocol Label Switching)	SPB (Shortest Path Bridging)
Private Network	Virtual LAN	Virtual Network	Virtual Network
High Availability	Slow fault recovery	Fast Fault Recovery	Fast Fault Recovery
High Performance	Single Active Path	Multi Active Path	Multi Active Path
High Scalability	Small Networks	Very Large Networks	Large Networks
Low Hardware/Operational costs	Low/High	High/High	Medium/Low
	Limited Features	High Cost	Best Option



Consolidation brings cost down

# SPB Applications

## Where to position

### Data Centre: Fabrics

- Large & scalable L2 fabrics
- Active/Active topologies where all links are used - East-West, Server-to-Server traffic
- Free VM mobility

### VPNs

- Enhances scalability and flexibility for L2 VPNs
- Layer-3 VPNs through IETF Draft

### IOT Containment

- Isolate IOT devices in their own container through SPB VPNs

### Campus: Spanning Tree Protocol replacement

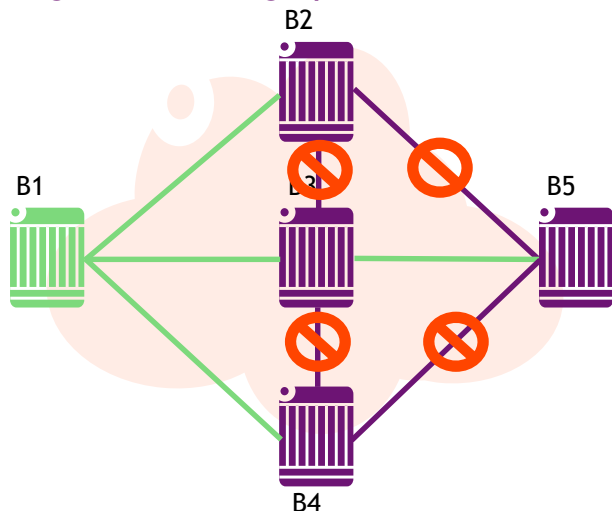
- Better resource utilization, all links used in any topology
- Higher scalability, no MAC learning in the core
- Sub-second convergence & shortest paths

# SPB - High Availability



## Spanning Tree

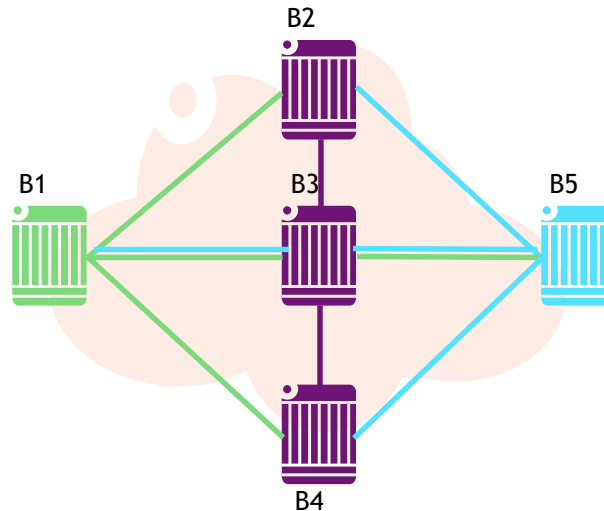
Single Root Bridge per Network/VLAN



Path B5 to B2 = B5 - B3 - B1 - B2

## SPB

Every Bridge is the Root



Path B5 to B2 = B5 - B2

SPB provides Multi- Active Path



# INTERNET OF THINGS...

a proliferation of connected things



**Unified  
Access**

Automated  
secured  
user access

+



**Intelligent  
Fabric**

Automated  
simplified  
network operations

+



**Smart  
Analytics**

Proactive  
IT traffic  
control

=



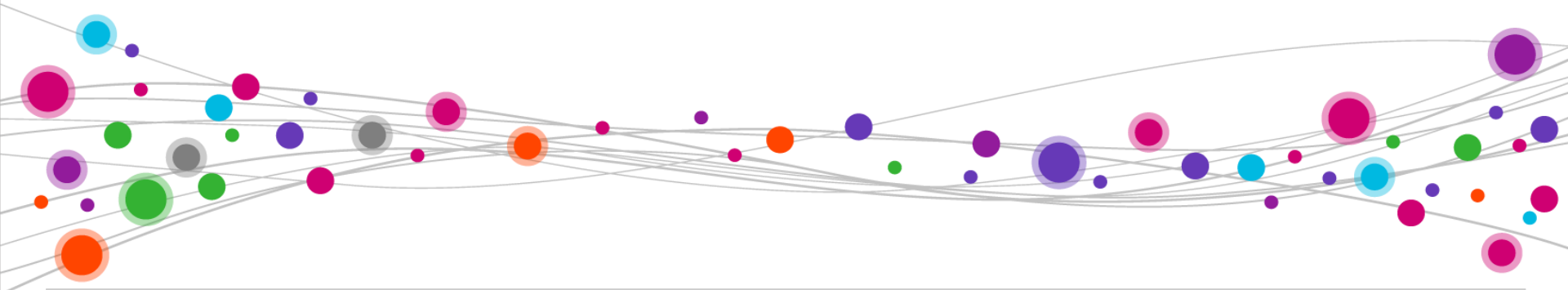
**IoT  
Containment**

Secured  
IoT device  
management



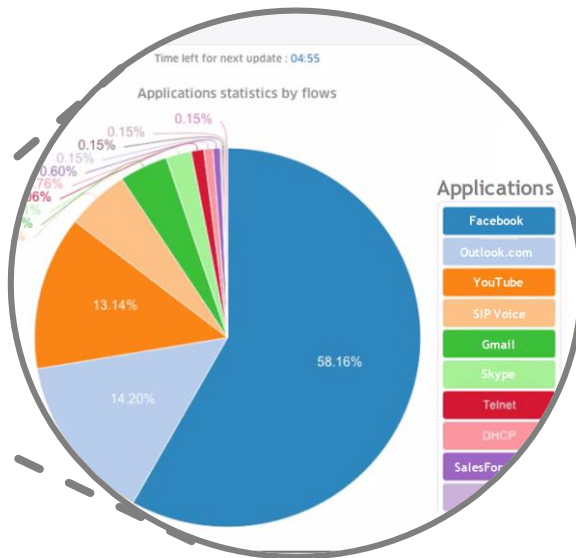
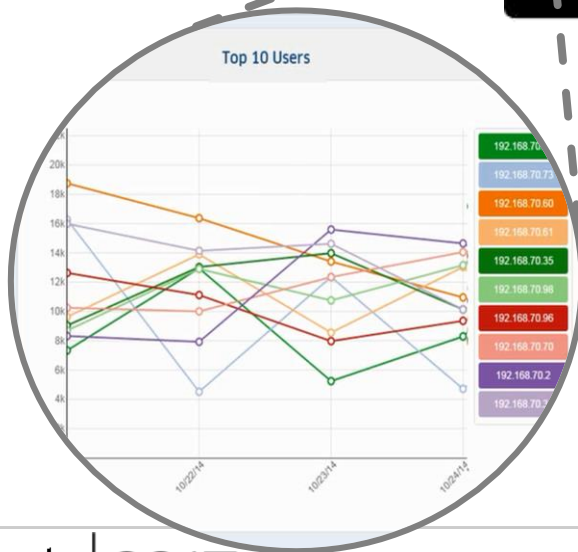
# ALE key technologies

## Unified Access



# Unified Access

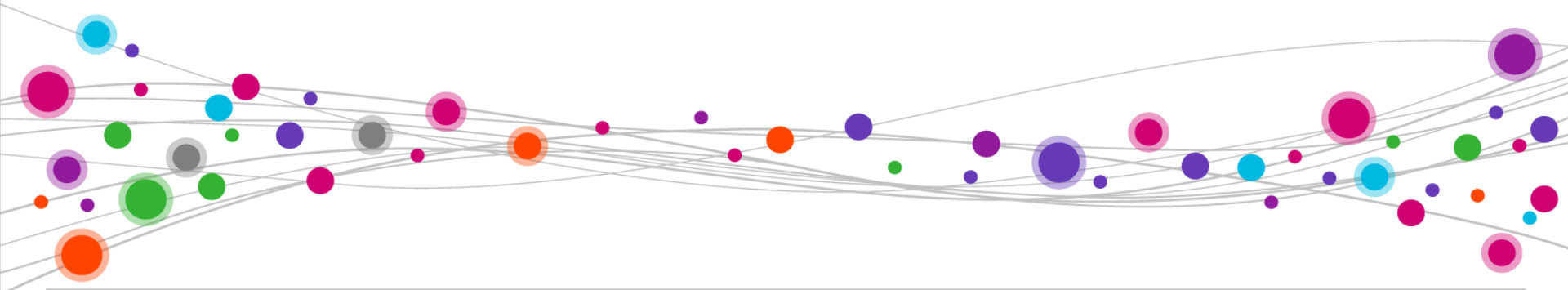
One management system: OmniVista 2500



Unified policy  
Unified topology  
Unified applications visibility  
Licensing management  
Unified alarms and notifications  
Wired and wireless configuration  
Top N reports

# ALE key technologies

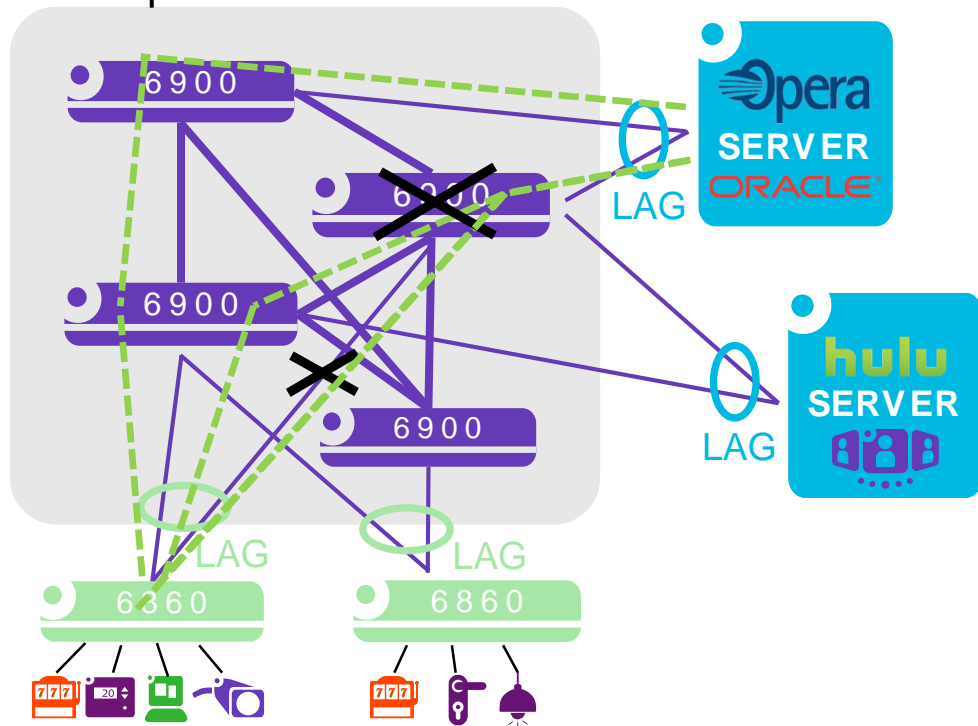
## Intelligent Fabric



# Intelligent Fabric

Simplifying the design, deployment and operation

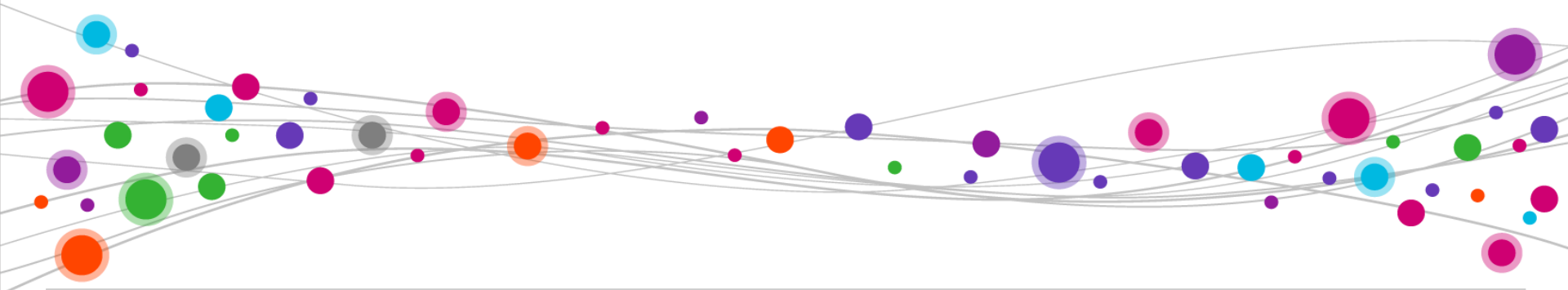
- ✓ Self configuring
- ✓ Self Attachment
- ✓ Simplified moves, adds and changes
- ✓ Self Healing



Faster deployment, easier support, higher resilience, lower down time

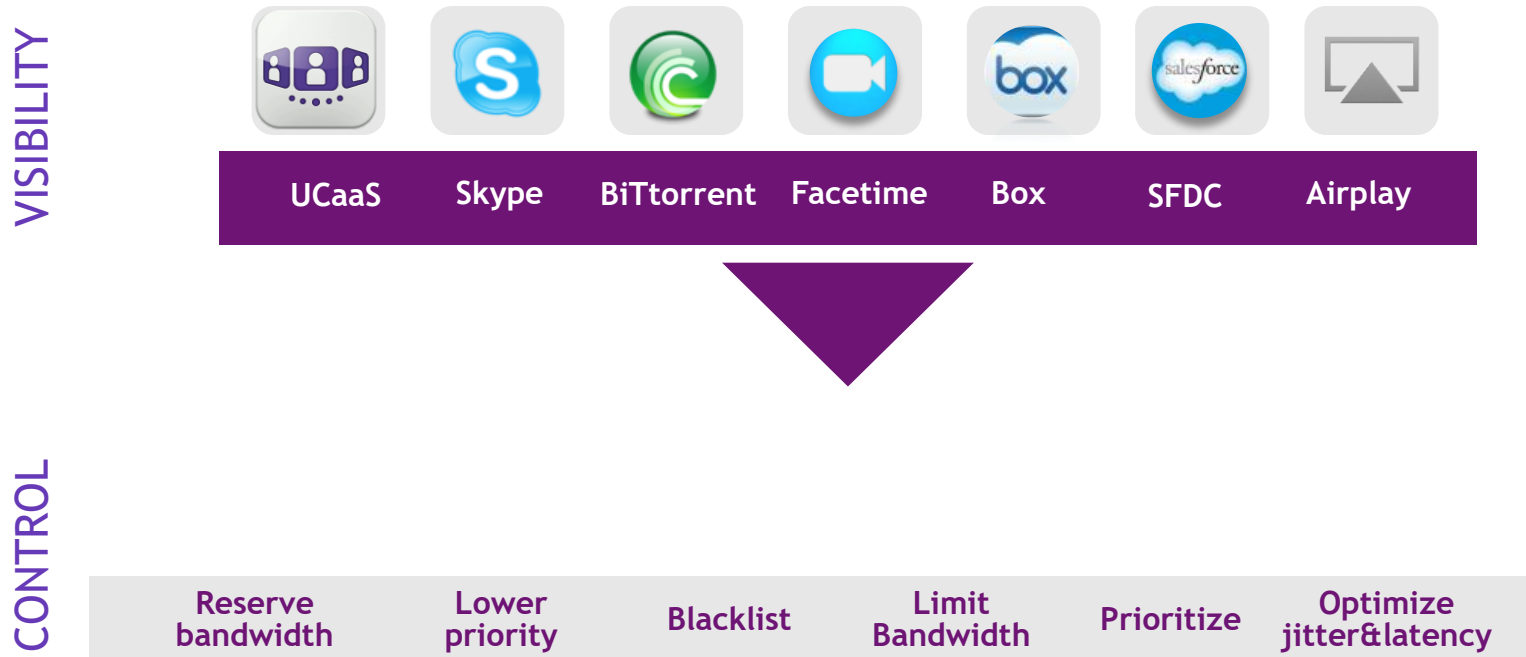
# ALE key technologies

## Smart Analytics



# Application control

Policies per application or application group

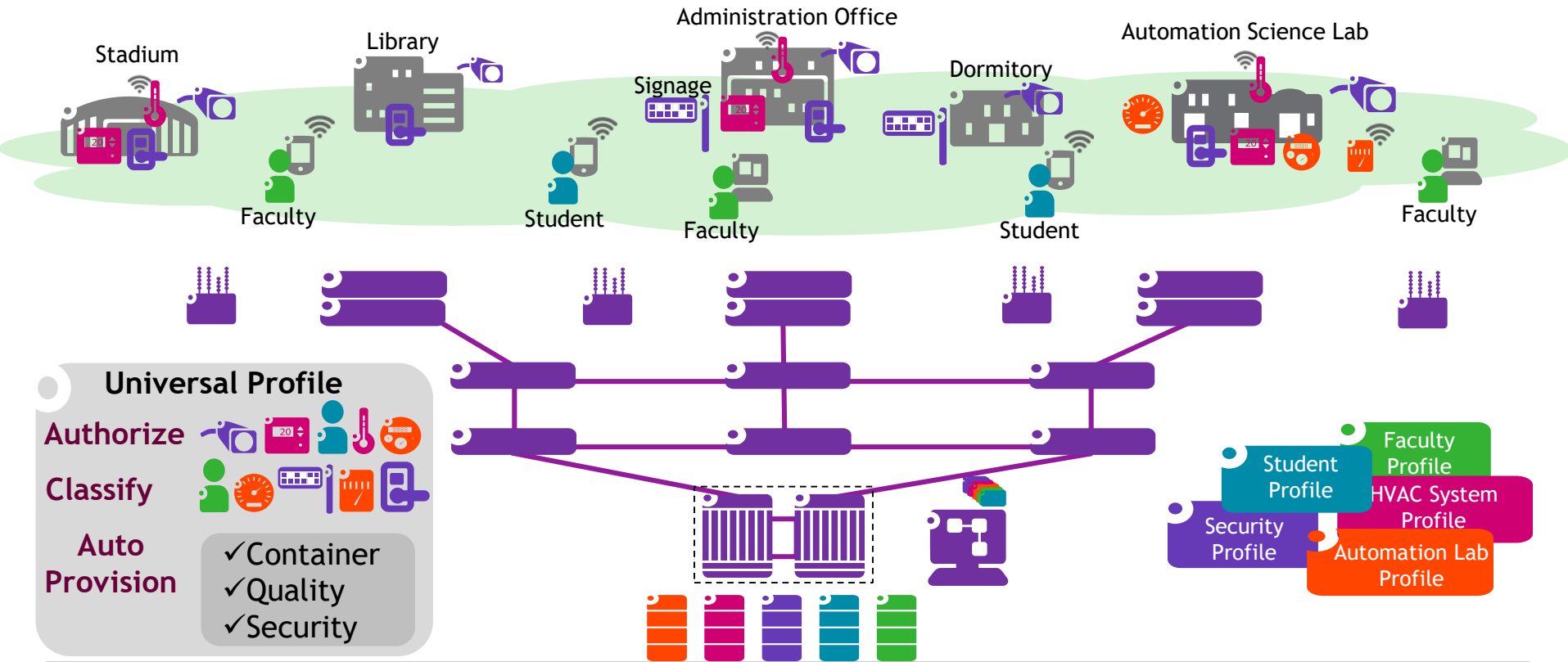


# ALE key technologies

## IoT containment

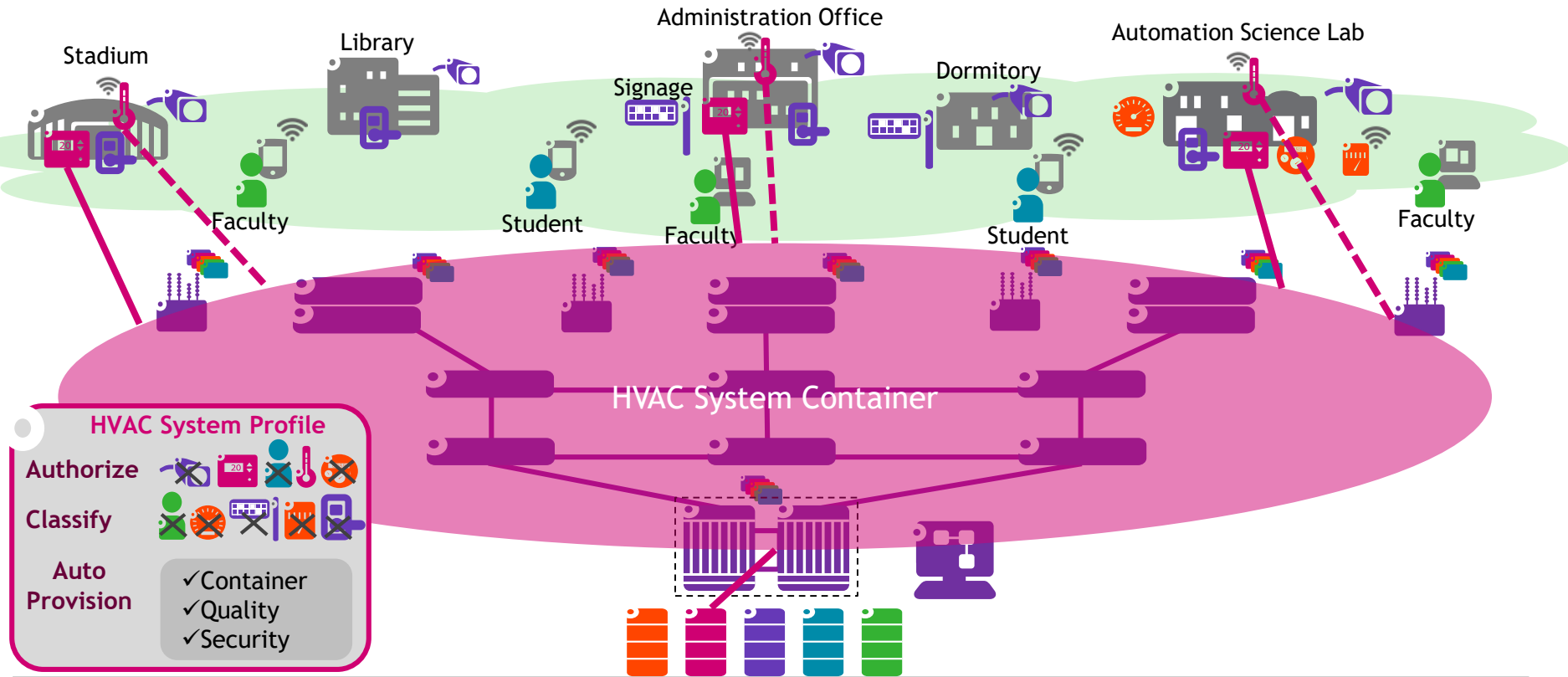


# The connected university campus

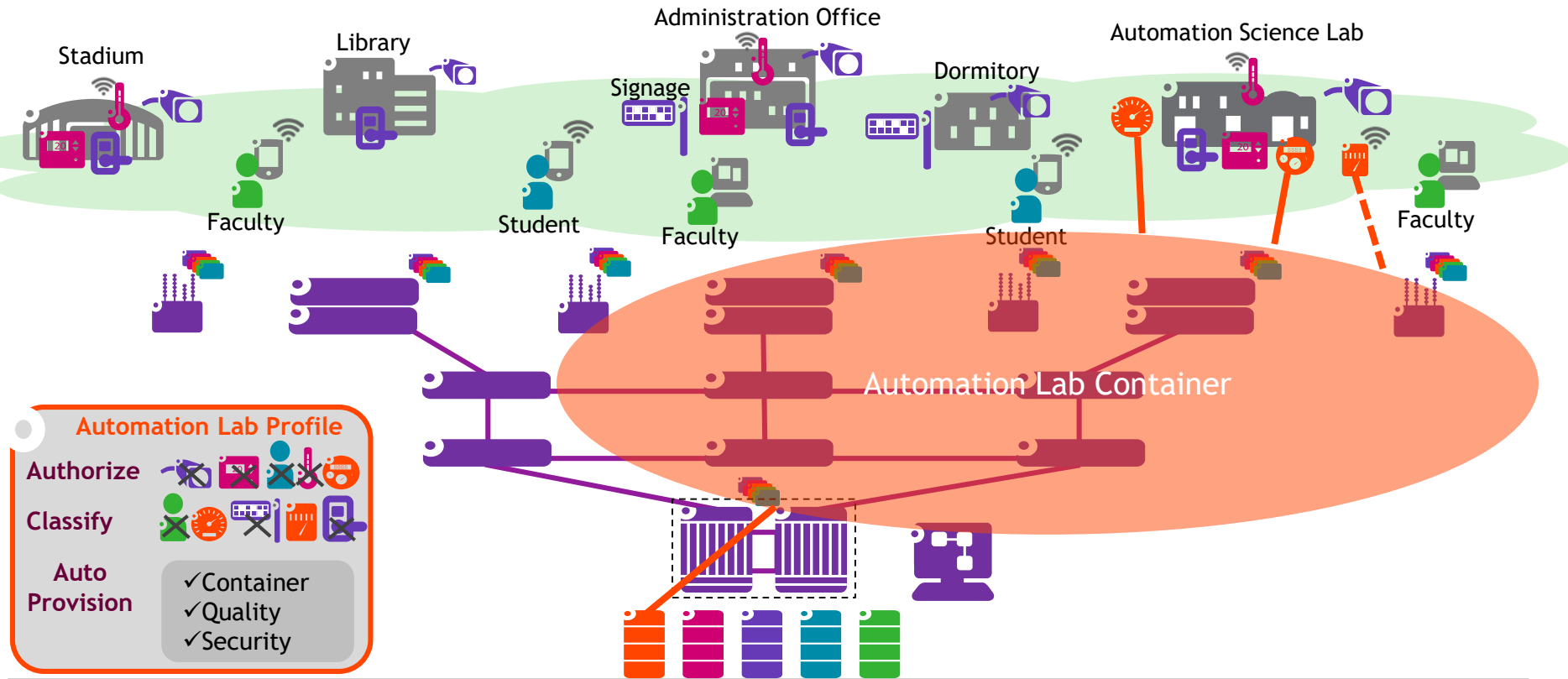




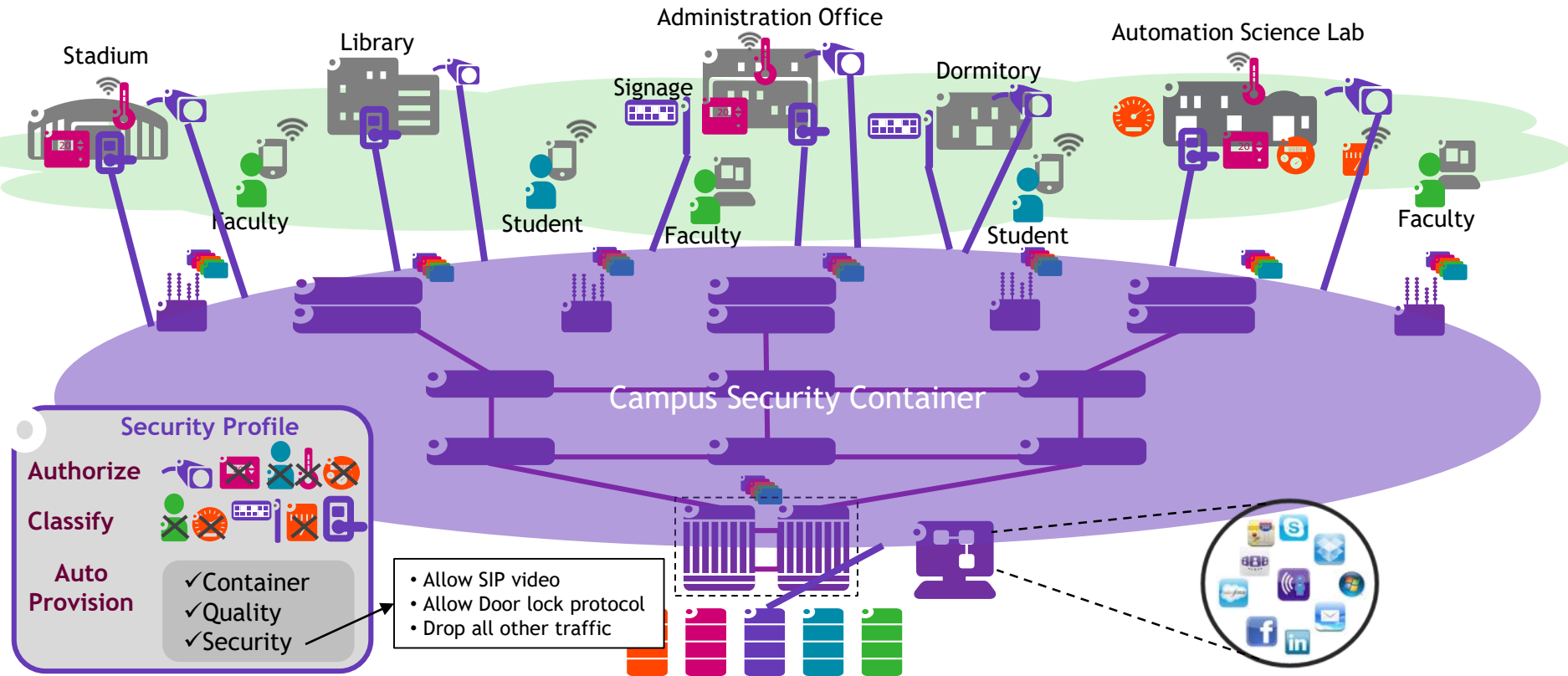
# The connected university campus



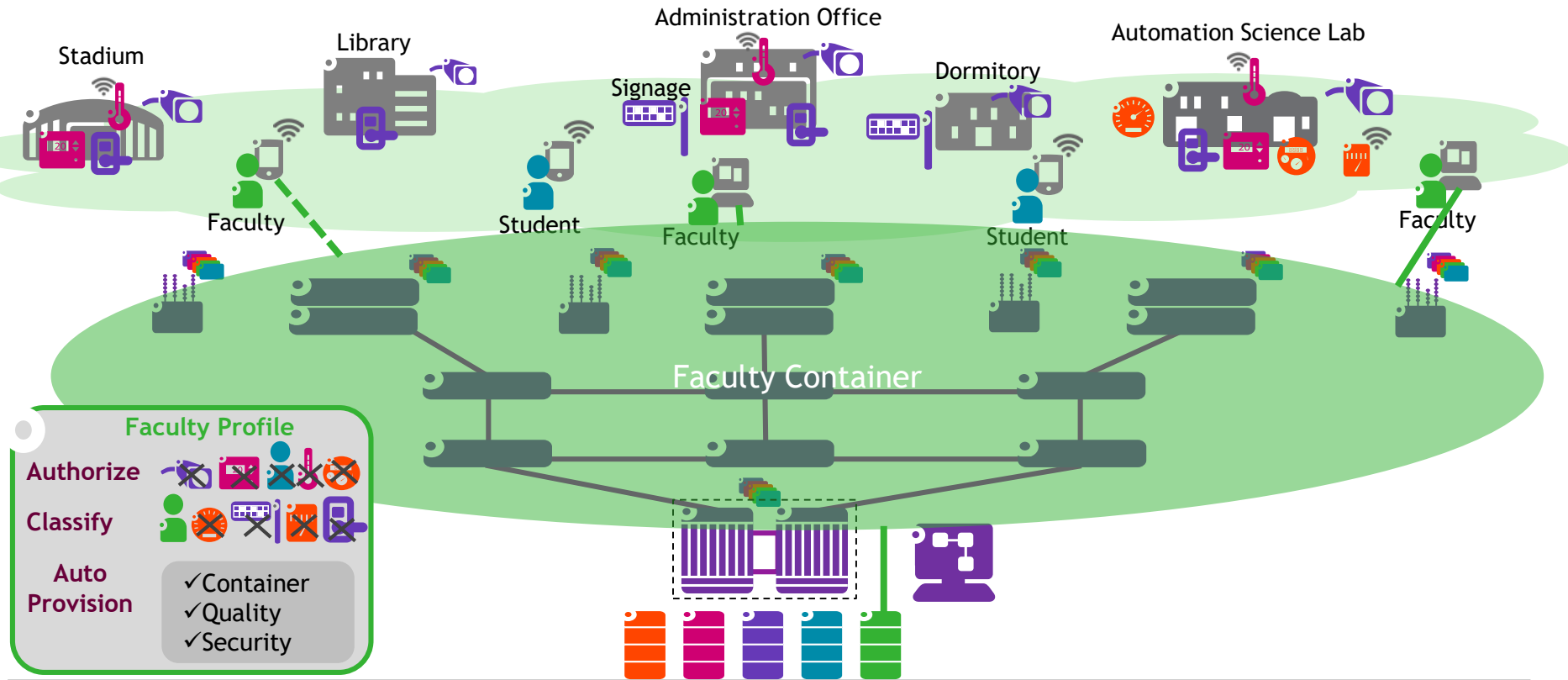
# The connected university campus



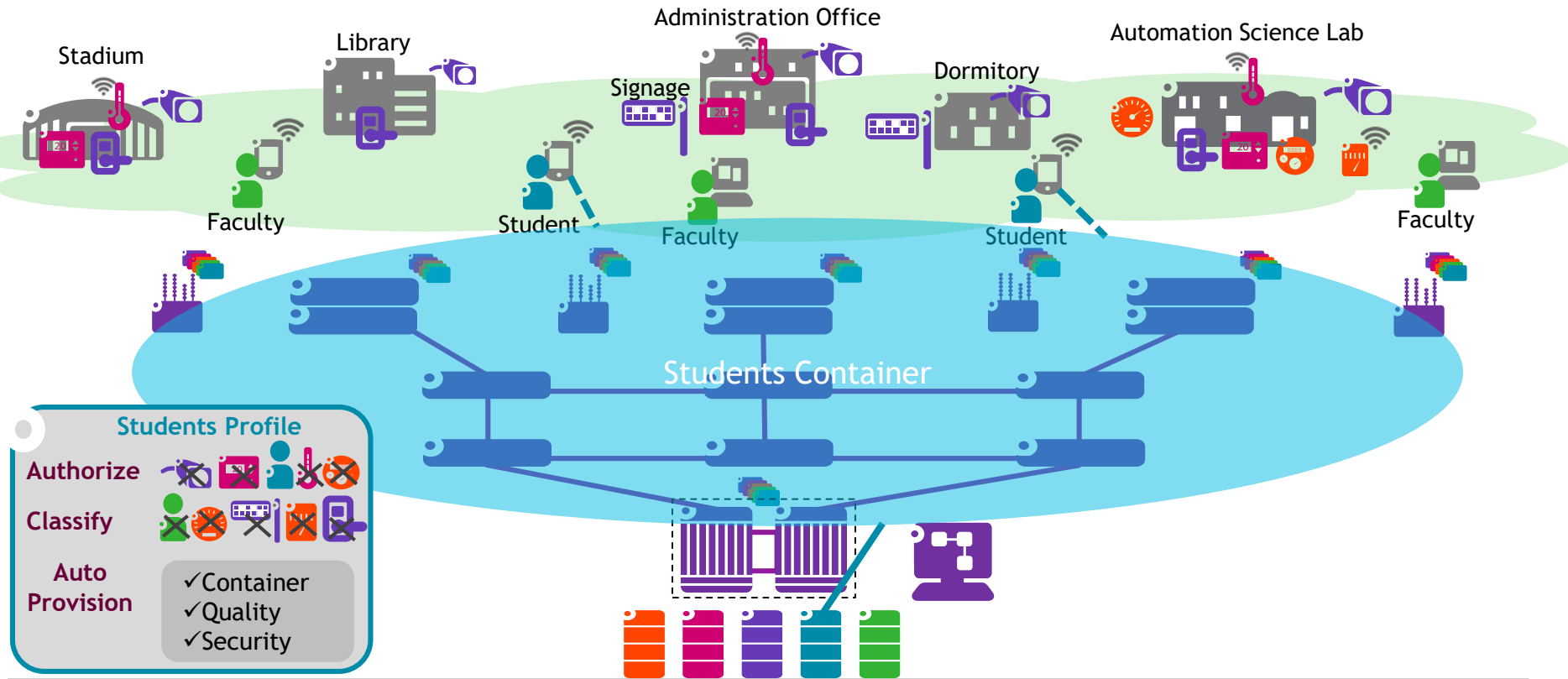
# The connected university campus



# The connected university campus



# The connected university campus



# ALE key technologies

## Security



## DDoS Attacks Affect Major Web Sites

According to Hacker News

(<https://www.dynstatus.com/incidents/nlr4yrr16zt8>, the outage is a result of an attack on Dyn's DNS server. Dyn manages website domains.

The sites that were affected include Amazon, Twitter, Etsy, Github, Vox, Spotify, Airbnb, Netflix and Reddit.



### 3rd Cyberattack 'Has Been Resolved' After Hours of Major Outages: Company

The company at the heart of the attack told CNBC it was hit by "tens of millions of IP addresses" Friday afternoon.



## Healthcare IT News

[TOPICS](#) [SIGN UP](#) [MAIN MENU](#)[Privacy & Security](#)

## Johnson & Johnson issues cyber hack warning for insulin pumps

After a security researcher found that the unencrypted devices could be forced to deliver unauthorized insulin doses, J&J sent patients a letter but also said the probability of such an attack is low.

By [Jeff Rowe](#) | October 05, 2016 | 01:48 PM

SHARE 201



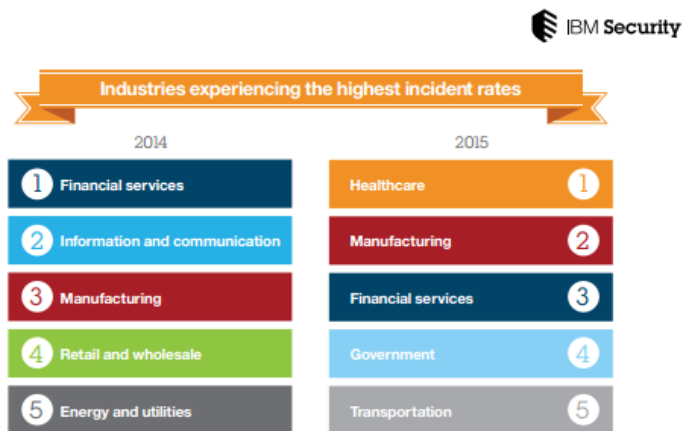
Officials at Johnson & Johnson sent out a letter warning users about the potential for a hacker to program the company's Animas OneTouch Ping insulin pump to deliver a fatal dose of the hormone to a user.



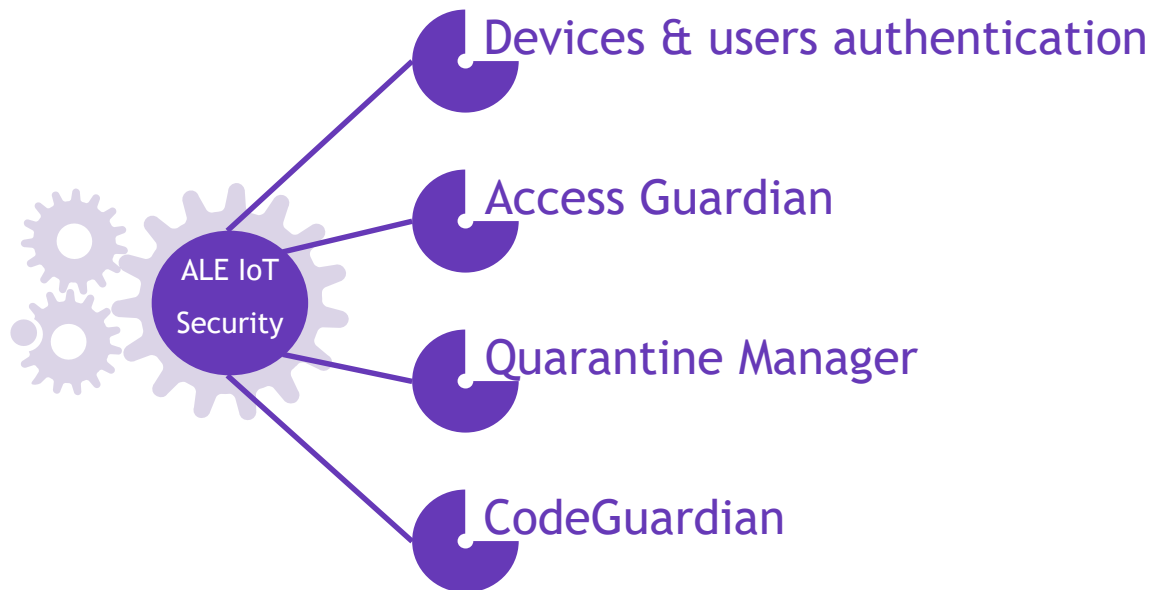
# Botnet

# Rootkit

# ALE Mobility & IoT security



<http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF>

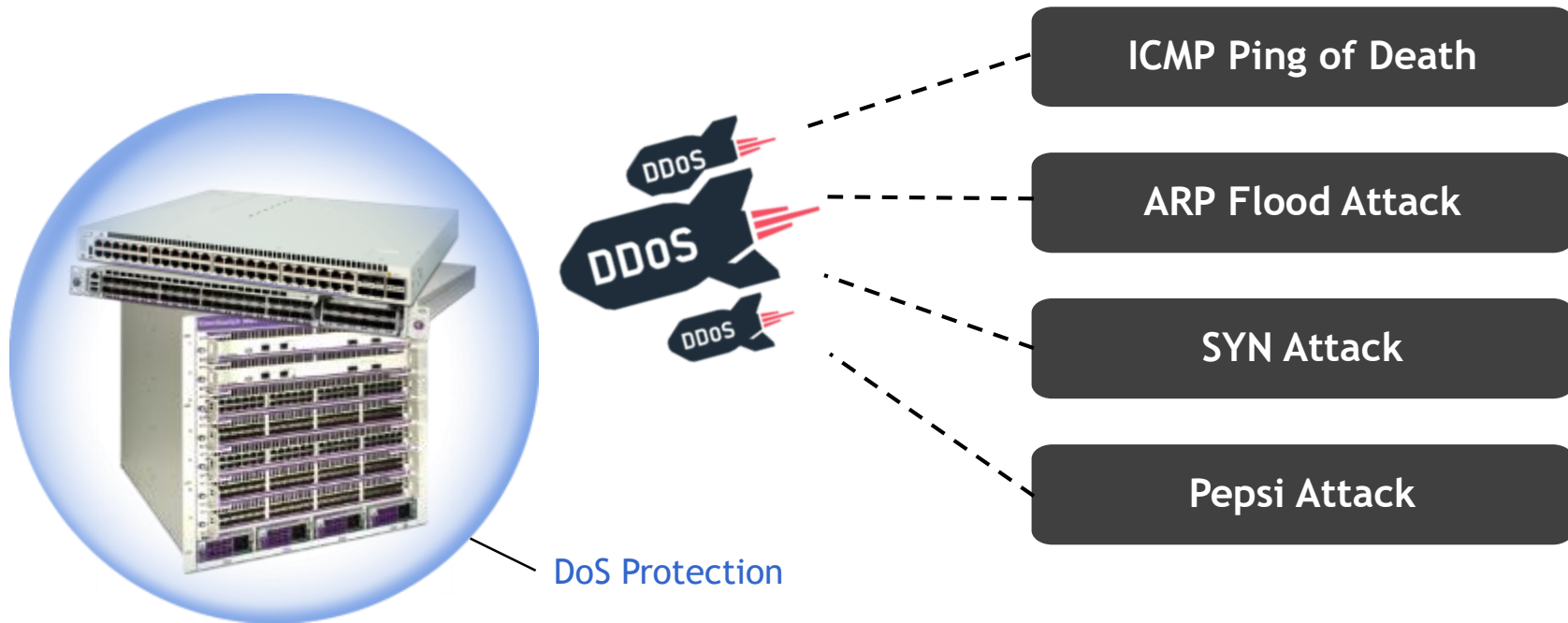


Key elements in your overall network security strategy



# OmniSwitch AOS - hardened by default

## Integrated protection against Denial of Service (DoS) attacks



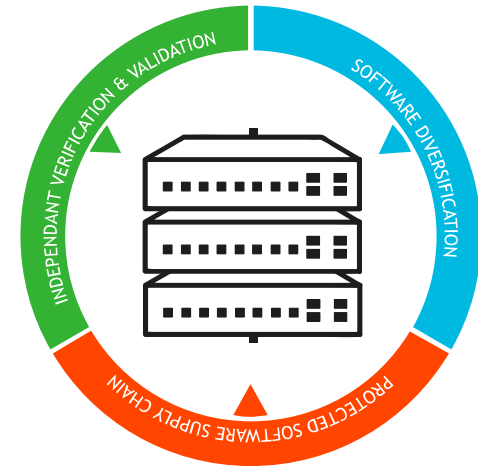
Protecting all connected resources including IoT devices

# What about the network devices themselves?

CodeGuardian is a **unique** technology integrated into ALE switches that differentiates ALE from the competition

Routers and switches are susceptible to the introduction of malware and other attacks!

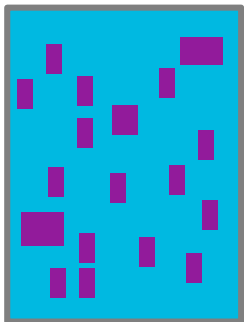
- Independent 3<sup>rd</sup> party (LGS Innovations) white box and black box testing searching for vulnerabilities in external interfaces.
- Object code scrambling to make exploits harder to achieve



CodeGuardian promotes increased security at the network device level

# Software Diversification

Typical network  
node OS



■ Proprietary code

■ Open source code

- bootp
- ntp
- jquery
- libxml2
- net-snmp
- open ssh
- open ssl
- open ldap
- telnet
- traceroute

Most probable entry point for exploitation

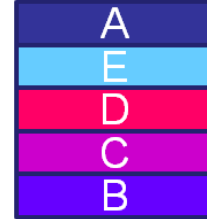
Non-Diversified  
Code



CodeGuardian  
Diversified 1



CodeGuardian  
Diversified 2



Address-based exploits rendered ineffective through software diversification that “shuffles” the AOS memory map of the binary images



# New Products

## Wireless



Alcatel-Lucent  
Enterprise



High-range  
AP1231  
AP1232



Mid-range  
AP1221  
AP1222



Emerging/SMB  
AP1101



Outdoor  
AP1251



# STELLAR WLAN

Controller-less  
architecture

Cloud enabled  
Unified Management

Unified Access  
by design

BYOD

Integrated  
Guest Management

# The Stellar Lineup

## Due out in July



### AP1101

#### 802.11ac: Wave 1

- 2 radios
- 2x2:2SS
- 1.2 Gbps throughput
- No BLE
- 1 GE port
- 248 client devices
- 10 W (802.3af PoE or DC)
- 512 APs(OV2500)/32 APs(web managed)
- Operating Temp: 0°C to 45°C

### AP1221/AP1222

#### 802.11ac: Wave 2

- 2 radios
- 2x2:2 @ 2.4GHz, 4x4:4 @ 5GHz
- 2.1 Gbps throughput
- Optional BLE radio through USB port
- 1 GE Port
- 512 client devices
- <12W (802.3af PoE or DC)
- 512 APs(OV2500)/64 APs (web-managed)
- Operating Temp: 0°C to 45°C

### AP1231/AP1232

#### 802.11ac Wave 2

- 3 radios
- 4x4:4 @ 2.4GHz, dual 4x4:4 @ 5GHz
- 4.2 Gbps throughput
- Integrated BLE radio
- 1xGbE + 1x2.5GbE network interfaces
- 768 client devices
- 40W (802.3at or DC)
- 512 APs(OV2500)/64 APs (web-managed)
- Operating Temp: 0°C to 45°C

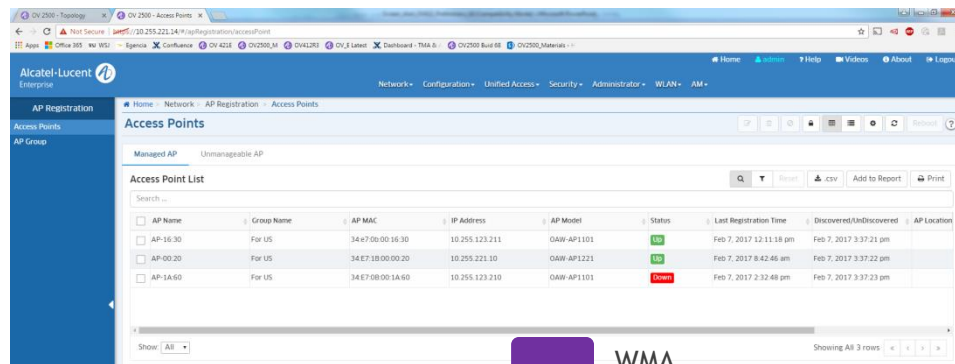
### AP1251

#### 802.11ac Wave 2

- 2 radios
- 2x2:2 @ 2.4GHz, 2x2:2 @ 5GHz
- 1.2 Gbps throughput
- No BLE
- 1xGbE network interfaces
- 512 client devices
- <12W (802.3af PoE or DC)
- 512 APs(OV2500)/64 APs (web-managed)
- Operating temperature : -40 to 65°C

# OMNIVISTA 2500 NMS-E

## WIRED-WIRELESS MANAGEMENT



AP Name	Group Name	AP MAC	IP Address	AP Model	Status	Last Registration Time	Discovered/Undiscovered	AP Location
AP-00-30	For US	34E7 0B 00 16 30	10.255.223.211	QAW-AP1101	OK	Feb 7, 2017 12:11:38 pm	Feb 7, 2017 3:37:21 pm	
AP-00-20	For US	34E7 1B 00 00 20	10.255.223.10	QAW-AP1221	OK	Feb 7, 2017 8:42:46 am	Feb 7, 2017 3:37:22 pm	
AP-1A60	For US	34E7 0B 00 1A 60	10.255.223.210	QAW-AP1101	OK	Feb 7, 2017 2:32:48 pm	Feb 7, 2017 3:37:23 pm	

Up to 512 AP management

WMA

To APs

AP Group

AP Group

AP Group

## Controller-less architecture

- Scaling to 512 APs

## Access Point DPI classification, enforcement and statistics

- Wired and wireless- same ops/features

## OmniVista 2500 is the single platform to provide

- Unified wired-wireless FCAPS
- Access Management (Guest/BYOD)
- mDNS/UPnP policies (Post GA)

## Wireless Management

- Config and visibility of wireless infrastructure
- WLAN topology on building map
- Heat map



# OMNIVISTA 2500 NMS-E

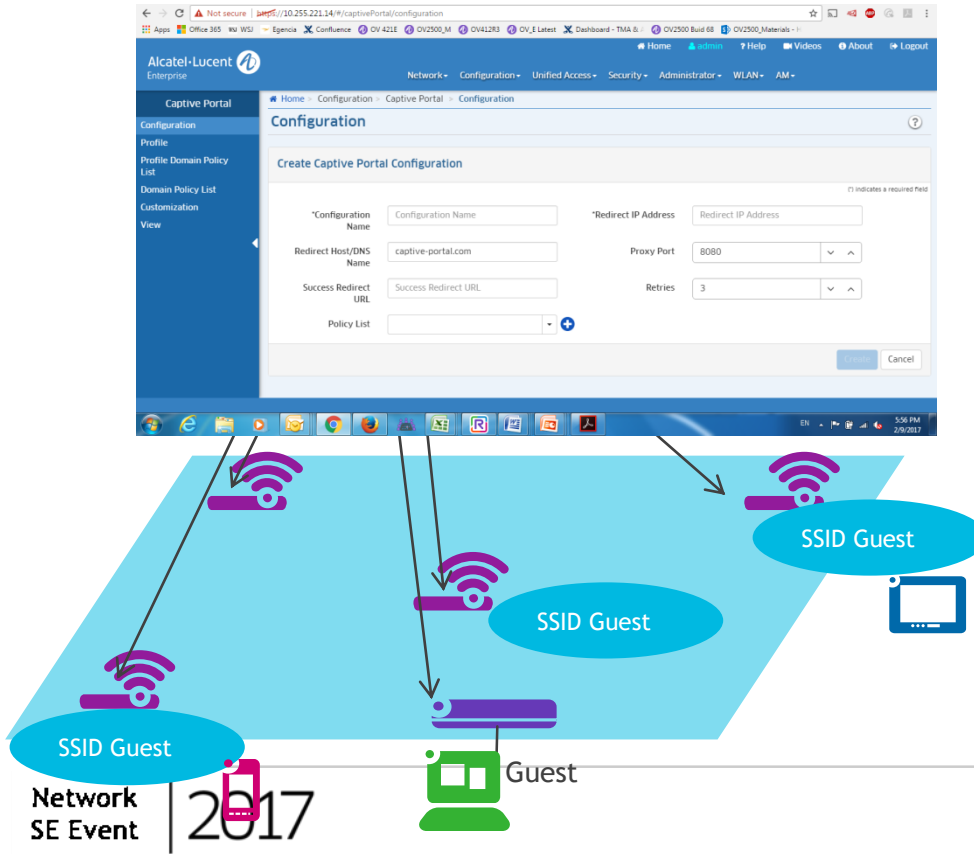
## GUEST MANAGEMENT APPLICATION

### Wireless Services

- Secure Guest Access over wireless and wired network (login and traffic separation)
- Automated credential creation for guest
  - By Guest attendant
  - By Sponsor Employee
  - By Guest itself
  - Pre-set Guest
- Acknowledgement of T&Cs
- Customization of Guest access portal

### Key benefits

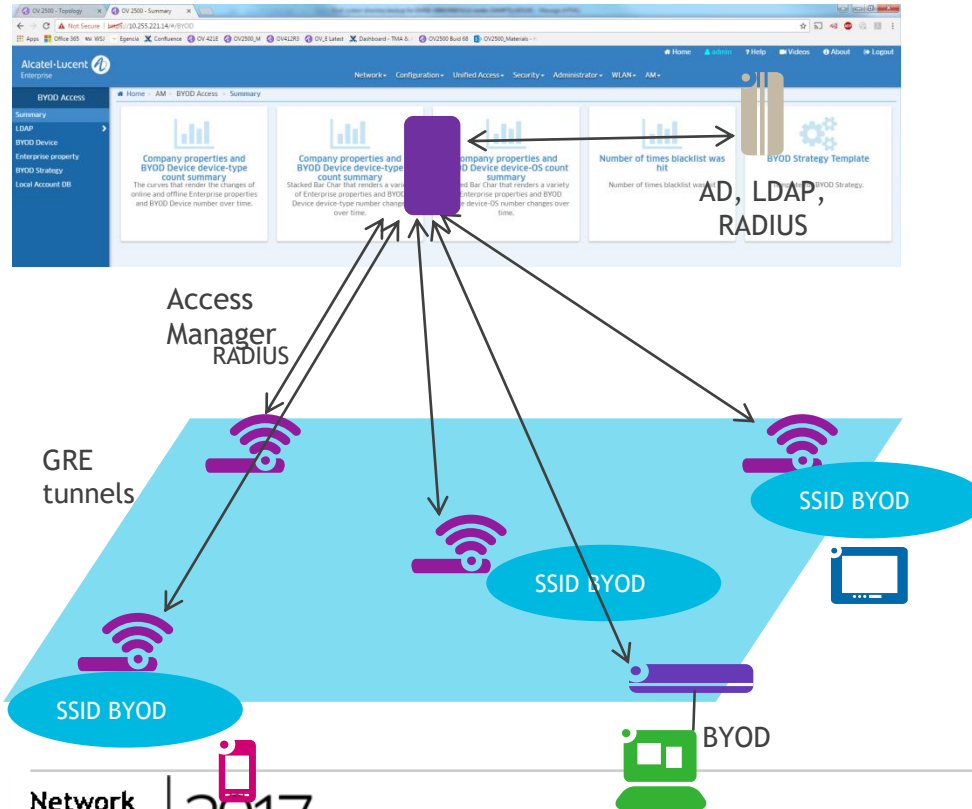
- Highly integrated solution
- Resilient User Database in case of OV failure
- Also compatible with CPPM





# OMNIVISTA 2500 NMS-E

## BYOD



Simple , easy to deploy , less expansive

- Automated Device Registration of Employee devices
  - By Employee through Captive Portal
- Device Registration for secure access
  - By MAC@
  - Ability to revoke a MAC address
- External Database Link for Employee Authentication

### Key benefits

- Highly integrated solution
- **Resilient Device Database** in case of OV failure (Post GA)



## AOS 8

8.4.1.R01 New Hardware Platforms 6865-U12X, 6865-U28X, 6860E-P24Z8

# OS6865 U12X & U28X



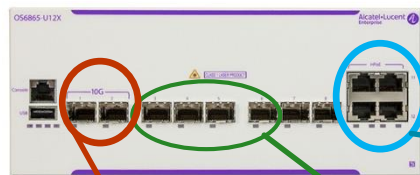
iFab  
Inside

High Surge  
protection  
PSU: 6KV  
Port: 4KV



VC mix-  
n-match

½ RU Clearance  
while mounting



2RU

1/10G  
VC/Uplinks

100FX

HPoE  
(75W)

1588v2  
all  
ports



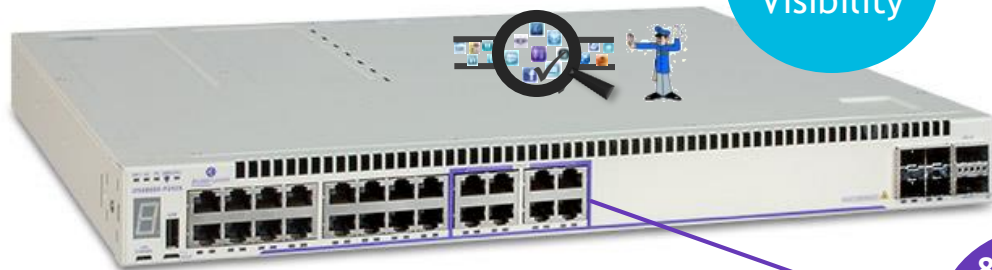
2 x20G  
dedicated  
VC Ports  
on U28x



1RU



# OS6860E-P24Z8



MACSec \*,  
1588v2 \*  
on all ports

App  
Visibility

8 x 2.5G  
Ports,  
HPoE  
(75W)

Power Supplies : Both 600W & 920 W Supported; Default : 600W; No Mix-n-match

Stackable with existing OS6860/E models

Some constraints

Auto-neg supported for 10/100/1000 Mbps speeds only. Manual configuration to choose between 1G & 2.5G speeds

Speed change on 2.5G Ports configurable only in pairs (17, 18), (19, 20) etc

\* HW enabled





# OS99-GNI-U48 Overview

MACSec \*,  
1588v2 \*  
on all  
ports

8 GB  
SDRAM, 32  
MB packet  
buffer



100FX  
Support on  
all ports

96G wire-speed full-duplex

Same transceivers support as OS9-GNI-U24E and OS10K-GNI-U48E

<50W power consumption

Throughput 71.5 Mbps





AOS 8

8.4.1.R02 New Hardware Platform 6560

# OS6560 Multi-GIG Models

MGIG PoE Models	PoE Gigabit/MGIG RJ-45 ports	1G/10G SFP+ ports Uplink/Virtual Chassis	20G Virtual Chassis Ports	Power Supply
Lower cost, less speeds/feeds models				
OS6560-P24Z8	16 (.af/.at PoE) 8 (.bt PoE)	2/2	0	Internal Modular Primary & Backup
Higher costs, more speeds/feeds models				
OS6560-P24Z24	24 (.bt PoE)	4/4	2	Internal Modular Primary & Backup
OS6560-P48Z16	32 (.af/.at PoE) 16 (.bt PoE)	4/4	2	Internal Modular Primary & Backup

Single MGIG family for customers with a healthy or tight budget.

# New OmniSwitch 6560-P24Z8 model



**OmniSwitch 6560-P24Z8**

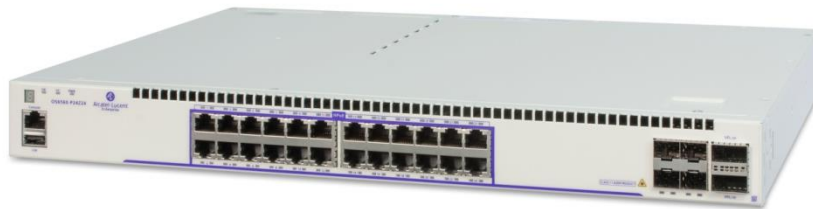
- 16 RJ-45 PoE 802.3af/at ports configurable to 10/100/1000 Base-T (up to 30W on a port)
- 8 RJ-45 PoE 802.3af/at/bt ports configurable to 1000 Base-T or 2.5GBase-T (up to 95W on a port)
- 2 SFP+ 10 Gigabit uplink/stacking, remote stacking
- Wire speed performance and throughput
- Powered by internal modular primary/backup supply option (300W, 600W or 900W), power supply load sharing
- 17.2"W x 13.2"D x 1RU form factor, 2x variable speed fans
- Estimated system power consumption: 85W

Price competitive MGIG model





# New OmniSwitch 6560-P24Z24 model



## OmniSwitch 6560-P24Z24

- 24 RJ-45 PoE 802.3af/at/bt ports configurable to 1000 Base-T or 2.5GBase-T (up to 95W on a port)
- 4 SFP+ 10 Gigabit uplink/stacking, remote stacking
- 2 QSFP 20 Gigabit dedicated stacking ports
- Wire speed performance and throughput
- Powered by internal modular primary/backup supply option (300W, 600W or 900W), power supply load sharing
- 17.2"W x 13.2"D x 1RU form factor, 2x variable speed fans
- Estimated system power consumption: 85W



# New OmniSwitch 6560-P48Z16 model



## OmniSwitch 6560-P48Z16

- 32 RJ-45 PoE 802.3af/at ports configurable to 10/100/1000 Base-T (up to 30W on a port)
- 16 RJ-45 PoE 802.3af/at/bt ports configurable to 1000 Base-T or 2.5GBase-T (up to 95W on a port)
- 4 SFP+ 10 Gigabit uplink/stacking, remote stacking
- 2 QSFP 20 Gigabit dedicated stacking ports
- Wire speed performance and throughput
- Powered by internal modular primary/backup supply option (300W, 600W or 900W), power supply load sharing
- 17.2"W x 13.2"D x 1RU form factor, 2x variable speed fans
- Estimated system power consumption: 85W



# Key takeaways



OS6560 is the first Value Stack product based on Linux 8.x code

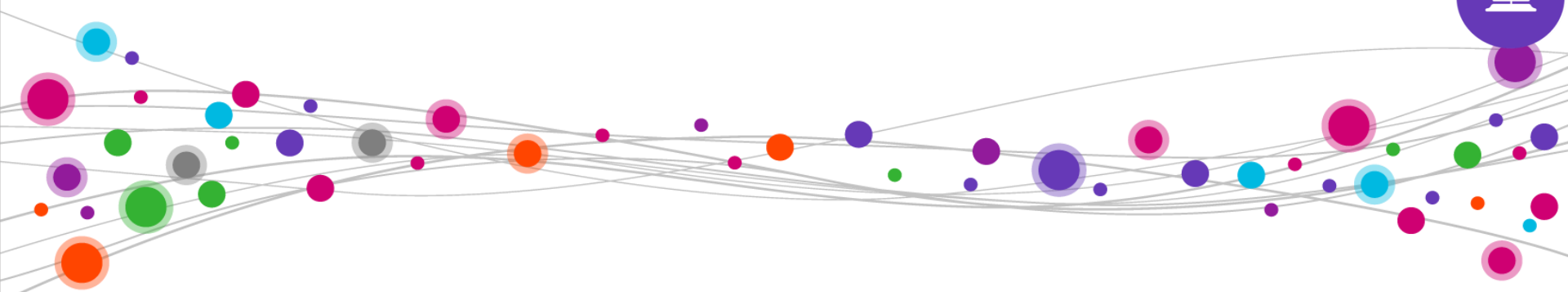
Multigig (1/2.5G) and HPoE (95W) capable

With 2.5GE AP products for a complete 2.5GE solution

Equivalent 6.7.X Metro features not yet available



# Wireless Support in AOS



# AOS support for Stellar WLAN and services

## How

### **AP discovery**

- AOS discovers Stellar APs through UNP (lldp rules enabling trust-tag) to allow tagged traffic from AP dynamically.

### **Guest Management/BYOD**

- AOS using OV UPAM as external Radius.
- **ZeroConf: mDNS/DNLA**
- OS6860/OS6900 acts as mDNS gateway or responder: AOS 841r02
- OS6450 acts as mDNS gateway: AOS 672r02

### **Guest tunneling**

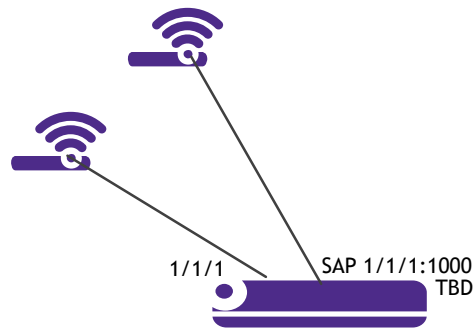
- OS6860/OS6900/OS6560/OS9900 encapsulates guest traffic over L2GRE tunnels to extend guest connectivity directly into the L2GRE gateway located in the DMZ/aggregation layer

Intelligent Fabric operation through UNP smarts

# Zero touch AP Discovery

When a Steller Access Point is detected on UNP port on the switch following actions are taken:

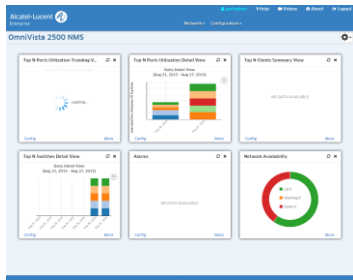
- Send Location information and Management vlan to the AP through LLDP TLV from switch
- An implicit lldp classification rule to recognize AP (similar to ip-phone) is present in the switch and this will assign a special WLAN Access Role Profile (UNP) that is mapped to the management vlan to the AP MAC address
- Trust all the tagged traffic from the AP
- Dynamically create vlan on the switch and propagate the vlan to the LAN network using MVRP



# SSID creation - bringing the LAN into the workflow

OmniVista

SSID / VLAN Manager

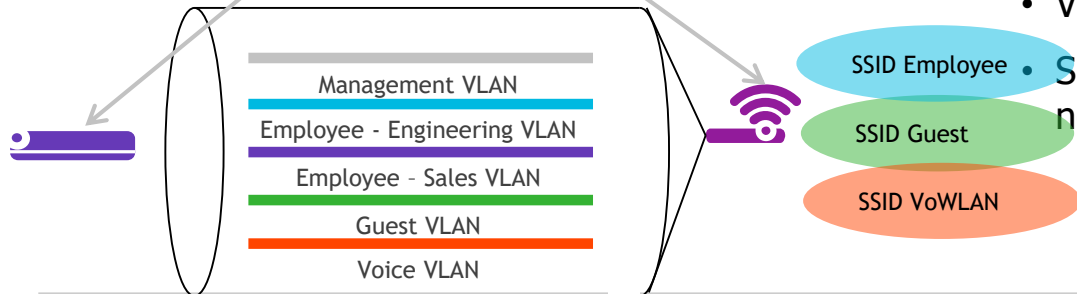


## Customer Challenge

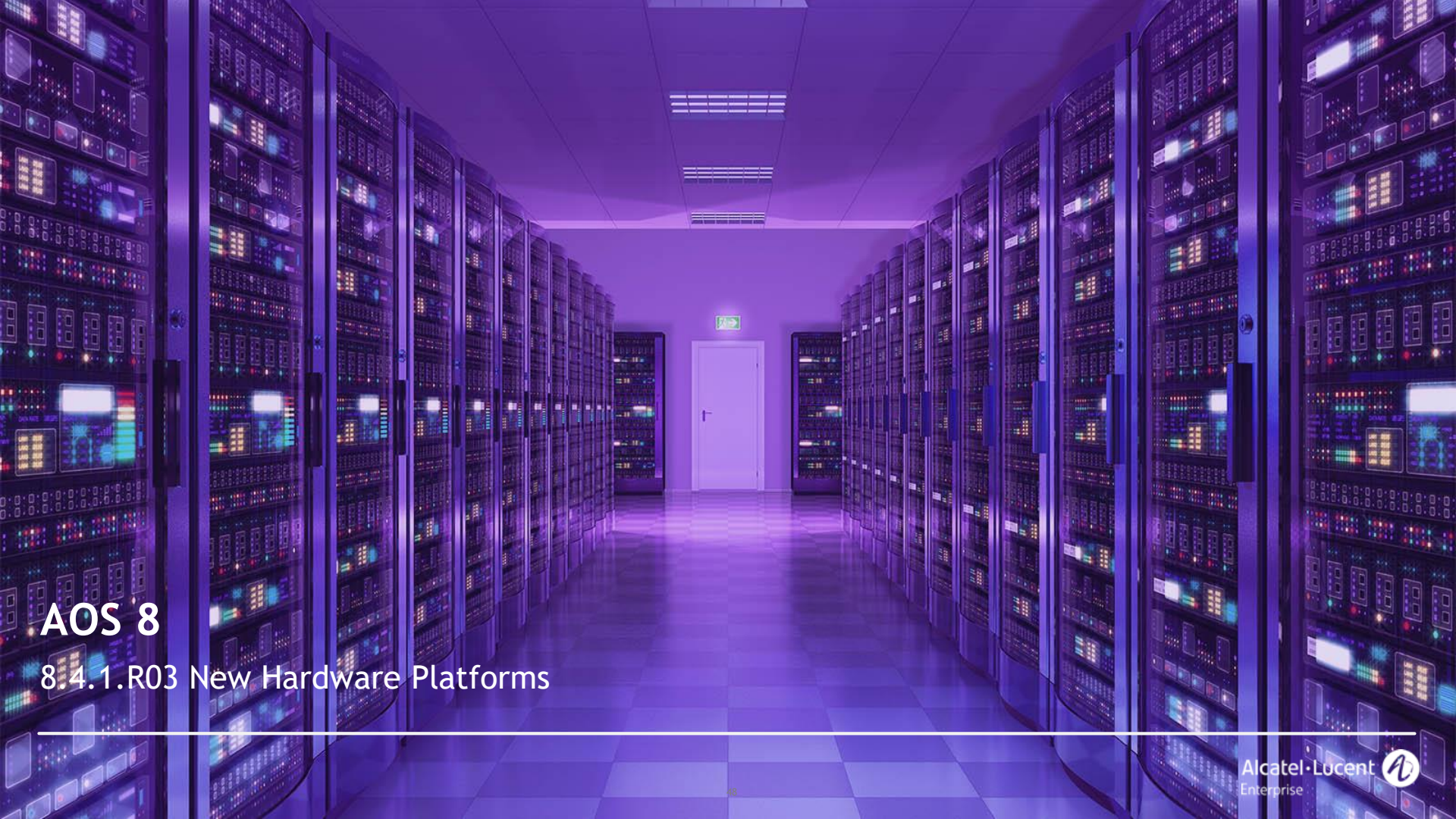
- Distributed AP architecture requires creation of many VLANs at each AP connection point

## Solution / Benefits

- OmniVista automates VLAN definition when SSID is created
- VLAN is instantiated when traffic is sent by AP
- Simplified Deployment, no risk of misconfiguration







# AOS 8

## 8.4.1.R03 New Hardware Platforms



# AOS 841r03 Scope

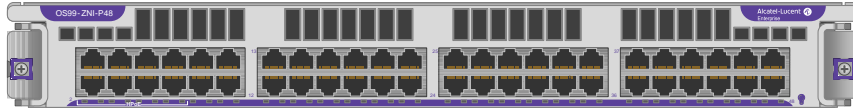
## HARDWARE

- OS6920-CX72
  - Flexible port configuration of 48x 10/25GbE plus 6x 40/100GbE, 12x 50GbE and 24x 10/25GbE.
- OS6920-C18
  - Flexible port configuration of 18x 40/100GbE, 36x 50GbE and 72x 10/25GbE
- OSS99-XNI-P48Z16 (aka OS99-ZNI-P48)
  - Physical: 16 2.5/10G-Base-T + 32 10G-Base-T ports
- OS99-CNI-U8
  - Physical: 8 100G-Base-X QSFP28 ports

## SOFTWARE

- OS9900
  - IPv6 & BFD
    - Advance IPv6 routing - OSPFv3/MP-BGPv4
    - Multicast snooping & routing
    - ACLs
  - SPBM & SPBM IP routing without hairpin
- MACSec support in 6860/E and OS9900
- OV Cloud agent

# OS9900: 2 new NI modules



- MultiGE module

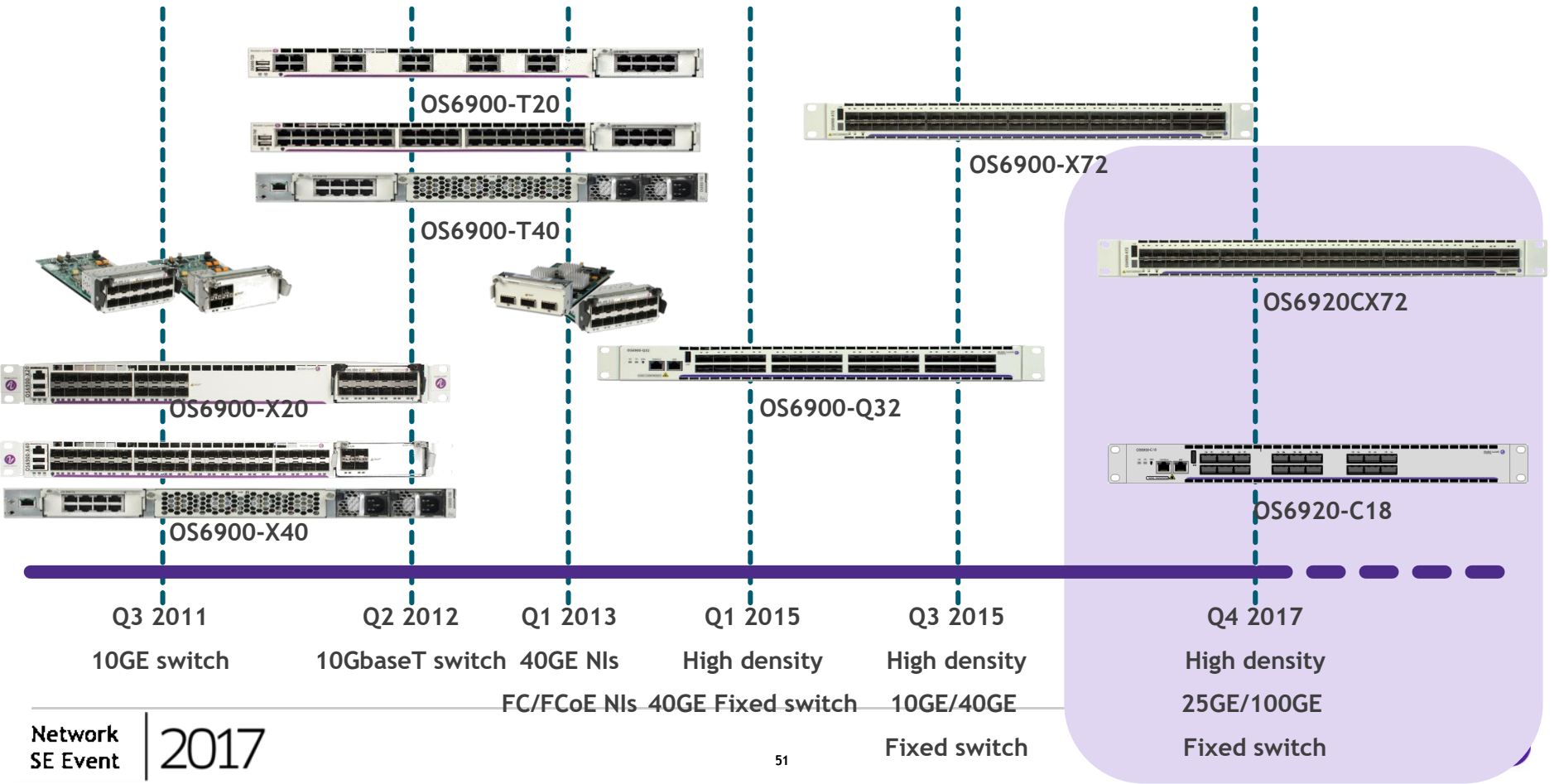


- 100GE Fiber module

- OS99-XNI-P48Z16 (aka OS99-ZNI-P48)
  - Physical: 16 2.5/10G-Base-T + 32 10G-Base-T ports
  - Ports 1-16 Speeds:
    - 10/100/1000/2500/5000/10000 Mbps
  - Ports 17-48 Speeds:
    - 10/100/1000/10000 Mbps
  - PoE:
    - 1-8 ports up to 75W (HPoE) or
    - 9-48 ports up to 30W (at)
- OS99-CNI-U8
  - Physical: 8 100G-Base-X QSFP28 ports
  - Speeds: 10/25/40/100Gbps
  - Max ports: 32 10/25GE with splitter and 8 40/100GE

Increase product competitiveness and completes portfolio

# OS6900 evolution: 25G/100G next generation ethernet



# 100GE OS6920 family



- OS6920-C18

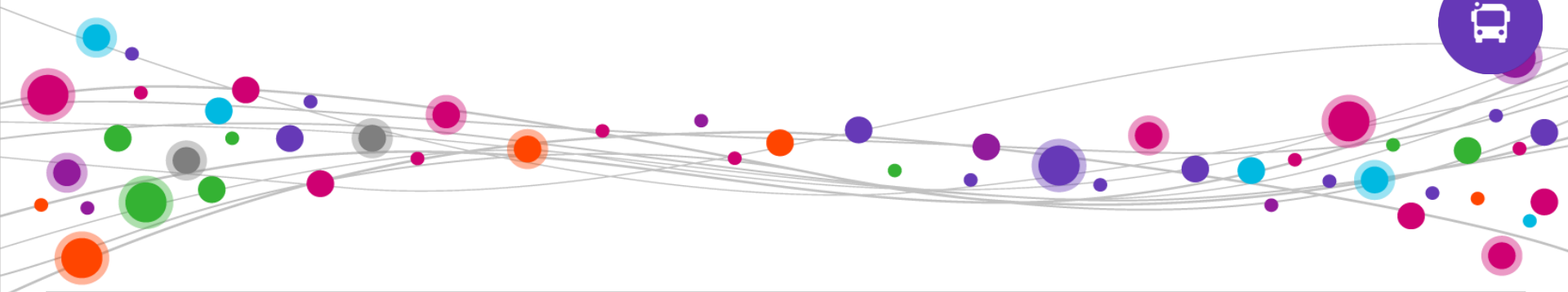
- Single ASIC with 1.8 Tbps I/O switching capacity.
- Multicolored LED front panel data port configuration with 18 QSFP28 slots.
- Flexible port configuration of 18x 40/100GbE, 36x 50GbE and 72x 10/25GbE

- OS6920-CX72

- Single ASIC with 1.8 Tbps I/O switching capacity.
- Multicolored LED front panel data port configuration with 48 SFP28 and 6 QSFP28 slots.
- Flexible port configuration of 48x 10/25GbE plus 6x 40/100GbE, 12x 50GbE and 24x 10/25GbE.

intelligent fabric switches with 100GE support

# MACSec Support



# MacSec support

## What

Provides secure access to network, data integrity, data origin authentication and (optionally) data encryption - all at Layer 2

- (802.1AE-2006) for encryption over Ethernet
- (802.1X-2010) MACSec Key Agreement (MKA) Protocol

## Why

### Key Benefits

- Data encryption at Ethernet layer for IPv4 and IPv6
- Protects network data and integrity
- Works with Intelligent Fabric over SPB or VXLAN

## How

Support phased in. First link encryption (841r03) and future MKA support

- Cryptography used is AES-GCM-128. Implemented in the PHY
- ```
->interfaces {slot <chassis>/<slot> | port <chassis>/<slot>/<port1>[-<port2>]} macsec
    {enable | disable}
->interfaces {slot <chassis>/<slot> | port <chassis>/<slot>/<port1>[-<port2>]} secure-
    channel <sci>{[keychain-tx <tx_key_id>] | rx-mac-address <MAC> keychain-rx <rx_key_id>]}
```

Secured networking @ line rate encryption in PHYs

# MacSec support

## Where

Encryption depends on HW PHY support. Not just SW. Platforms:

- OS6860/OS6860E 10GE uplinks
- OS6860-P24Z8 1GE and 10GE ports
- OS9900 all ports except OS99-CNI-U8. CMM 4x10G supports MACSec, not 40GE

## Phases

**Phase 1: rotating user-configured static key - AOS 8.4.1.r03 Q4/2017**

- User inputs secure keys. Multiple keys can be associated to a port
- Secure Channel (SCI), Security Association (SA), Keys, Key Rotation after Packet Number saturation

**Phase 2: MACSec Key Agreement (MKA) Protocol - Candidate in 2018**

- Keys are managed using a 3<sup>rd</sup> party key manager. Delivers standard operation.
- MACSec Key Agreement (MKA) Protocol, node discovery, SA key generation/distribution, PN synchronization, etc.

## Steps

**In 841r03**

- User creates the keys. Keys can be asymmetrically configured between Tx and Rx
- Keys are associated at physical port level interface configuration

Secured networking @ line rate encryption in PHYs





# AOS 6

## 6.7.2 New Hardware Platform



# OS6455 Models overview

|                       | OS6455-P6   | OS6455-P12  | OS6455-P24          |
|-----------------------|-------------|-------------|---------------------|
| 1Gig RJ45 ports       | 4           | 8           | 22                  |
| PoE+ / HPoE Ports     | 4 / 2       | 8 / 4       | 22 / 8              |
| 1Gig SFP Port         | 2           | 4           | 2                   |
| 10G SFP+ Ports        | -           | -           | 4                   |
| Virtual Chassis       | No          | Yes         | Yes                 |
| Mounting              | DIN-Rail    | Din Rail    | 19" Rack            |
| Form Factor           | Cube/Cuboid | Cube/Cuboid | 1RU, 19" rack width |
| Operating Temperature | -40 to +74C | -40 to +74C | -40 to +74C         |
| Alarm Relay Contacts  | 1In + 1 Out | 1In + 1 Out | None                |
| Power Supply Contacts | Dual, Front | Dual, Front | Dual, Rear          |



# OmniVista NMS 2500 4.2.1 MR1

What's new in OV 2500 4.2.1 on Premises

# OMNIVISTA 2500 NMS-E- R421

## MR1- OBJECTIVES & SCOPE

### ENTERPRISE DEVICE & AOS

Extending OmniVista 2500 NMS certification for Legacy Devices and latest AOS releases with data collection for PALM

### IT OPERATIONS

Closing the features gap for Key apps with usability improvements

- Topology, Notification

### CAMPUS & DATACENTER

#### New Features

- Discovery application with Port Status
- Multi-Vlan configuration
- MS Hyper-V 2016 support for VMM inventory

### FRAMEWORK

Improving VA/VM installation experience & New MS HyperVisor Certification (Hyper-V)

# OMNIVISTA 2500 NMS-E

## MR1- Portfolio Support

### ENTERPRISE DEVICE & AOS

**Certified legacy Devices or newer devices/AOS Releases for OV2500 features set including inventory collection for PALM**

#### Legacy devices

- OS6850 Switches running AOS 6.4.4.743.R01/higher.
- OS9700E & 9800E Switches running AOS 6.4.6.380.R01/higher

#### New software releases

- AOS 6.7.1.R04 on all supported OS6250, OS6350, & OS6450 Switches.
- AOS 8.3.1.R02 on all previously-supported OS6865 , OS6860/6860E, & OS6900 Switches
- OAW 6.4.4 on OAW-4030, OAW-4704, and OAW-4604 devices

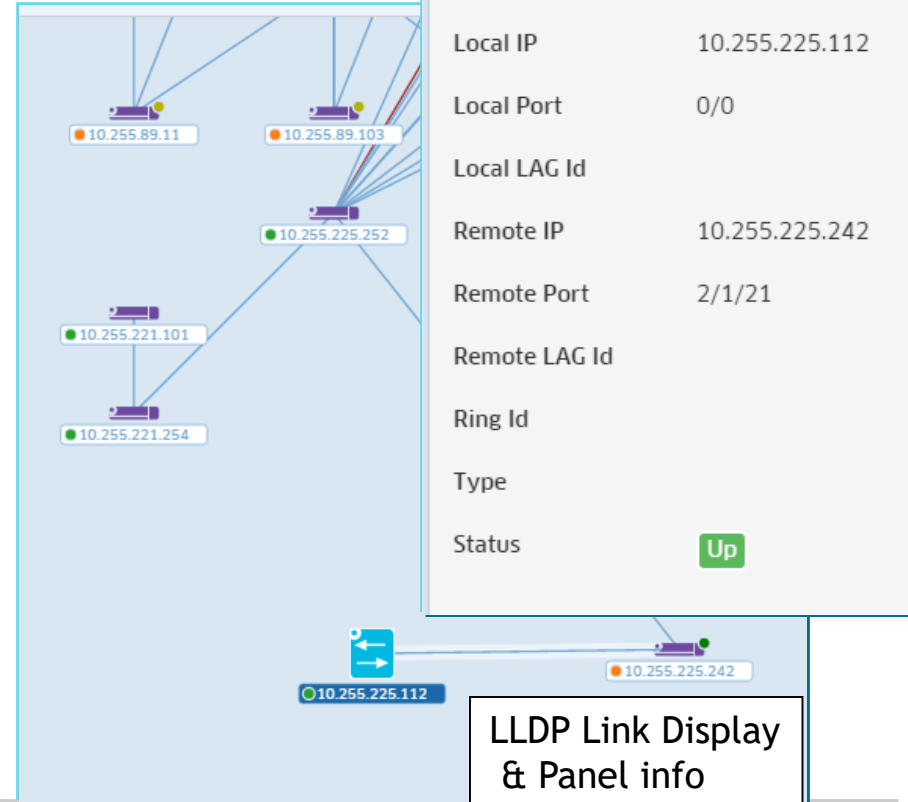
# OMNIVISTA 2500 NMS-E

## MR1- TOPOLOGY- LLDP

### IT OPERATIONS

### CAMPUS & DATACENTER

- Support & Display for LLDP Links for Third-Party Switches
- Support for LLDP Links between AOS and third-party devices
- Support & display for LLDP links between third-party devices

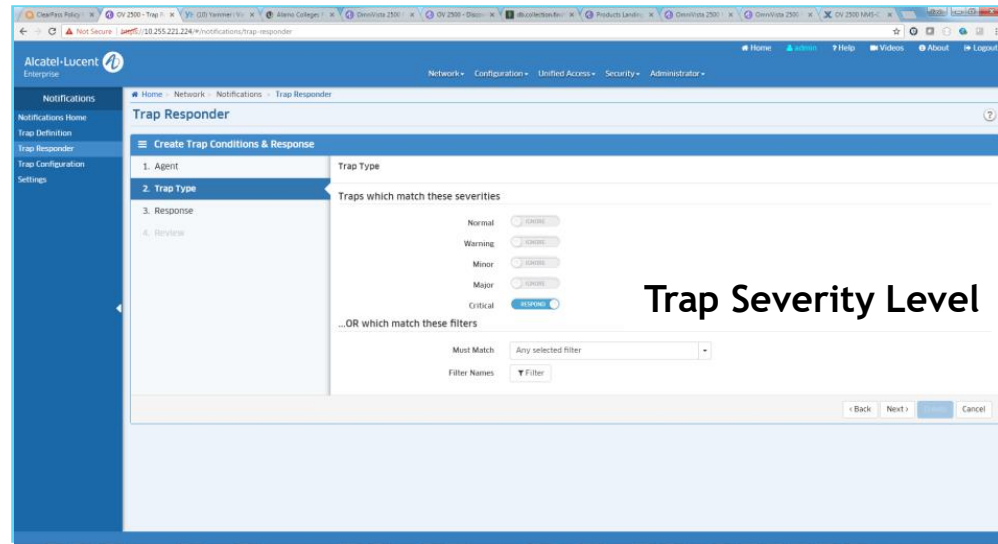


# OMNIVISTA 2500 NMS-E MR1- NOTIFICATION

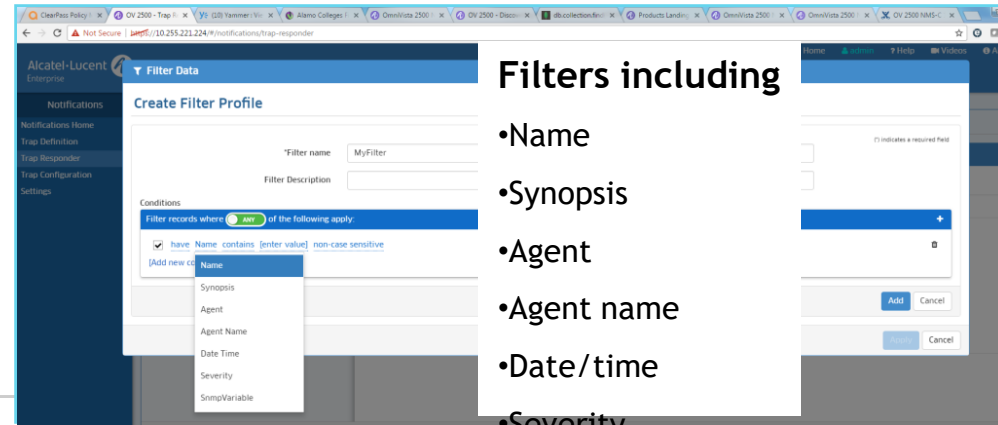
## IT OPERATIONS CAMPUS & DATACENTER

### Trap Responder extended now with:

- Multiple email addresses for Responder notification
- Trap Responder with Trap Severity level or trap conditions using Filters



### Trap Severity Level



### Filters including

- Name
- Synopsis
- Agent
- Agent name
- Date/time
- Severity
- Acknowledge

# OMNIVISTA 2500 NMS-E

## MR1 - SUPPORTED PATHS

**No License Key change Same license keys as OV421**

### **Supported Installation Paths**

- **New Installation** starting with MR1 images for new fresh installation
- **MR1 Update** for OV421 GA installed base
- **Update directly from Installation from Release 4.2.1 GA**
  - Automatic upload from Repository (OV Repo) , implying external internal access)



# OMNIVISTA 2500 NMS-E

## MR1- PLATFORM & INSTALLATION

### Available as Virtual Machine / Virtual Appliance for all HyperVisors

Certified OS (64-bit version only) with hypervisor support

- Microsoft Windows™ Server Hyper-V 2012 R2
- **Microsoft Windows™ Server Hyper-V 2016**
- Microsoft Windows 8.1 Pro & Enterprise Editions (with Hyper-V installed- Windows Features)

Supported OS with  
VirtualBox 5.0.12min installed

- Red Hat® Enterprise Server 6.5 or higher
- SUSE® Linux Professional v12.0

Certified hypervisors

VMware ESXi™ 5.5 and 6.0  
Microsoft Hyper-V 2012, **2016**  
VirtualBox v5.0.12 min

Certified Web Browsers

- Chrome - min version 26+
- Firefox- Min version 26+
- Internet explorer Min 10+
- Safari & Edge Not certified at this stage

SIZING & CONFIGURATION GUIDELINES SAME AS OV421R01- GA



# OMNIVISTA 2500 NMS-E- R421

## MR2-OBJECTIVES & SCOPE

**PRELIMINARY**  
Candidates  
Features

**ENTERPRISE  
DEVICE & AOS**

ESR 57xx series (Teldat) - Data collection from OV for PALM analysis

**IT OPERATIONS**

Usability improvements for Key Web 2.0 apps

**CAMPUS**

**&**

**DATACENTER**

- Topology- functional improvements & ergonomics (ie. Snap to Grid)
- Key Web apps - Usability optimization /Ergonomics Improvements

**Closing the Gap for Web Applications**

- Statistics (Live monitoring) – back in MR2

**FRAMEWORK**

Enhancements to OV2500 VM/VA Backup



# OmniVista 2500 NMS 4.2.2R01

What's new in OV2500 on Premise

# OMNIVISTA 2500 NMS-E

## R4.2.2 - CONVERGED MANAGEMENT

### INFRASTRUCTURE NODAL

- Latest AOS Portfolio support extension (AOS 841R02)
- New Stellar AP family Portfolio support (AP1011/1221/1231/1251)
- Network admin Credentials- extended (wireless roles w/ Guest Management)
- Span of control extended for Wireless apps & common Wired/Wireless Services

### ADMIN CREDENTIALS

### INFRASTRUCTURE PROVISIONING & MANAGEMENT

- Wireless Registration & Single Inventory view & unified topology
- WLAN Services (SSID configuration) & RF management
- Unified Life Cycle ops with Resource Manager

### TROUBLESHOOTING

- Single Event Mgt with Notification Manager
- Locator extended to bring wireless user knowledge ( BYOD attributes & Locations)
- WiPS (Wireless Intrusion Prevention System)

### FRAMEWORK

- Simplified installation for all solution components
- Single UI entry point and Licenses workflows for Wired/Wireless features support

# OMNIVISTA 2500 NMS-E

## R4.2.2- WIRED/WIRELESS USER SERVICES

### USER/ROLE PROFILES

- Access Guardian - UNP / Unified role based Workflow across Wired & Wireless
- Common Policy criteria through same UI operations

### SMART ANALYTICS

- Converged Wired/Wireless Dashboard with Wireless widgets
- Smart Analytics support extended to Wired/Wireless
- Application Visibility key features extended to Wireless (Appmon/DPI/Stats)

### BYOD

- BYOD- Automation - Captive Portal Registration
- Device Registration
- Authentication Servers for Employee

### GUEST ACCESS

- Captive Portal - Admin credentials managed & maintained from OV
- Guest account generation & Guest Portal Customization
- Guest Tunneling (Post OV422 R01 GA)

### SERVICE SHARING

(POST GA)

- Policy Based for DLNA/UPNP Management-
- Discovery & Configuration for Service Sharing Devices (Printers & Media Players)

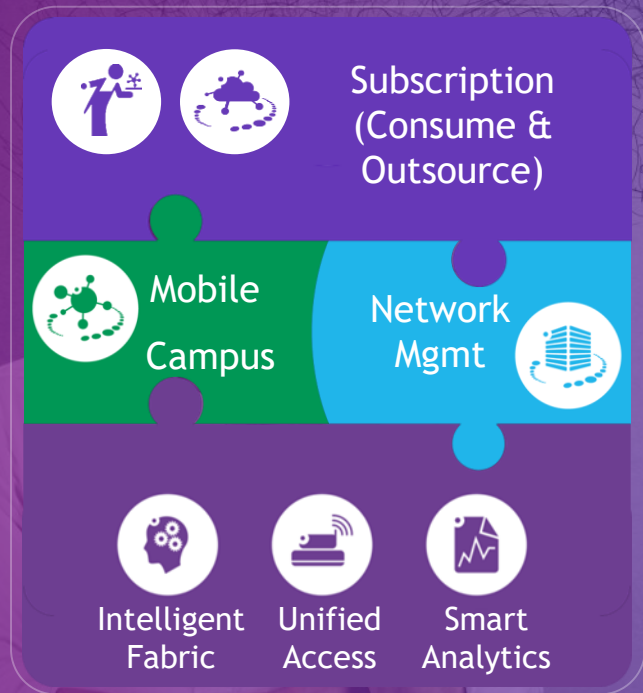


# Network As A Service

NaaS

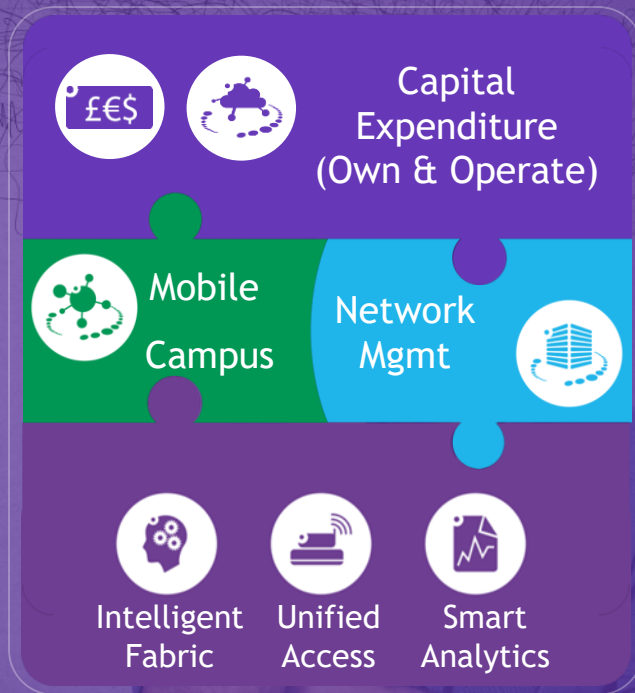


# NETWORK ON DEMAND



Same

Same







# E-Demo

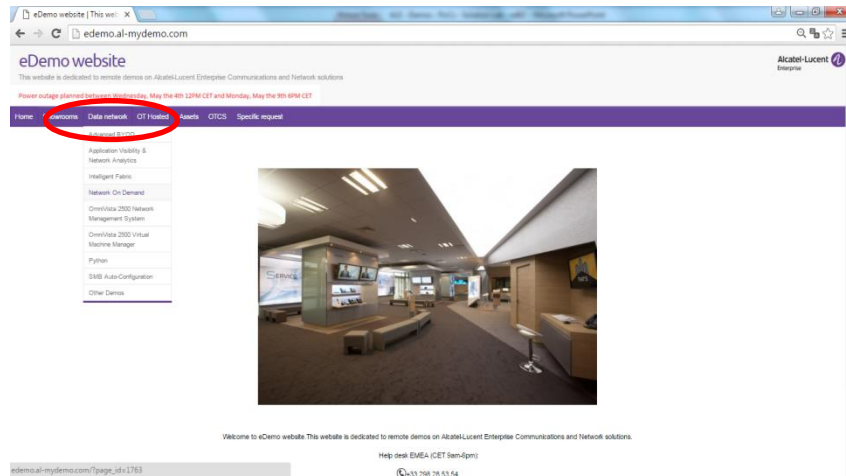
## Remote Demo Catalogue



# Remote demonstrations (eDemo)

Remote demonstrations have been designed and deployed in ALE's Brest datacenter for a world wide availability

- A remote demonstration may be requested by a pre-sales engineer from ALE or a Business Partner through a web portal:



<http://edemo.al-mydemo.com/>

# Remote Demos - catalogue

OV 2500  
NMS

Python

SPB

Application  
Visibility

Networks  
Analytics

OV VMM

NoD

Auto-config

iFAB

PALM

AP1101

Advanced  
BYOD

OV3600  
Air Manager

VxLAN

Follow us on:



[Twitter.com/ALUEnterprise](https://twitter.com/ALUEnterprise)



[Facebook.com/ALUEnterprise](https://Facebook.com/ALUEnterprise)



[Youtube.com/user/enterpriseALU](https://Youtube.com/user/enterpriseALU)



[Linkedin.com/company/alcatellucententerprise](https://Linkedin.com/company/alcatellucententerprise)



[Slideshare.net/Alcatel-Lucent\\_Enterprise](https://Slideshare.net/Alcatel-Lucent_Enterprise)



[Storify.com/ALUEnterprise](https://Storify.com/ALUEnterprise)

[enterprise.alcatel-lucent.com](http://enterprise.alcatel-lucent.com)

