

The background features a complex network diagram with various nodes and connecting lines. A prominent, thick black line forms a large, irregular loop on the left side, while other thinner lines and nodes are scattered across the upper and right portions of the frame.

# Challenges in Infrastructure Services

> **08/12/2016**

CERN openlab Technical Workshop 2016

Stefan Stancu

IT-CS-CE



- › **Commoditization: hardware and software**
- › **Configuration automation**
- › **Fabrics**
- › **Campus connectivity (wired/wireless).**
- › **Security**
- › **IoT**

# HW commoditization – white box switches

## > Network vendors offer similar hardware

- Few vendors continue manufacturing custom ASICs
- Merchant silicon, Differentiator → software

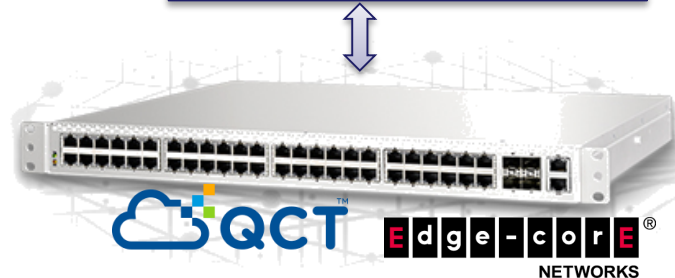
## > White box switch = bare metal device

- Runs a third party Network OS
  - Your entire network could have a common unified interface
- OCP (Open Compute Project):
  - Open HW design and SW of Facebook OCP switches

## > Status and outlook

- Early days, adoption rate difficult to foresee
- Reticence due to network criticality
- Vendors get involved from both directions
- Potentially very disruptive on long term

Network equivalent  
of Linux + x86 server



# SW commoditization – SDN

## › SDN (Software Defined Networking) areas:

- Third-party Network OS on (white box) switches
- Controllers for driving the network
  - Hybrid control
- NFV: replace dedicated network HW with software on servers

## › Status and outlook

- Controllers driven networks: slow adoption
  - hybrid control should give a boost
- NFV: quick adoption (cost effective)
  - Within software performance limitations
- CERN is looking at SDN for contained portions o the network

# Configuration Automation

## > Network device configuration interfaces

- command line, vendor specific
- NETCONF / Vendor specific data models + OpenConfig
- REST / Vendor specific data models

## > Multi-vendor automation alternatives:

- Commercial: mostly vendor specific or vendor-focused
- No uniform configuration management platform (Puppet + Ansible)
- Some open-source modules for device interaction
- No silver bullet, two solutions
  - Home grown solution, possibly leveraging open-source modules
  - Orchestration of multiple platforms
- Need glue code to:
  - Network model database
  - Cloud orchestration platform (e.g. OpenStack)

## Drivers:

- Simplify management
- Provide seamless VM mobility in Data Centres

Fabric type	Scale [end nodes]	Technology	Vendor adoption	Vendor Interoperability
Distributed switch	O(100)	Port extender	All (most)	No
Layer 2 Fabric	O (10k)	TRILL	most	No
		SPB	few	Yes
<u>Layer 3 Fabric</u>	O(100k+)	BGP-EVPN VXLAN/MPLS	most	Yes (- configuration automation)

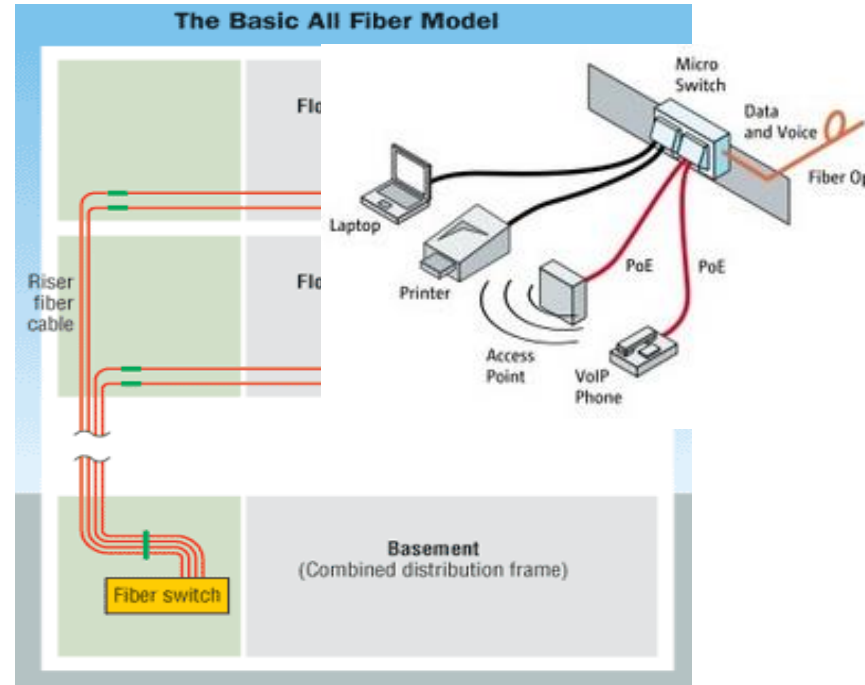
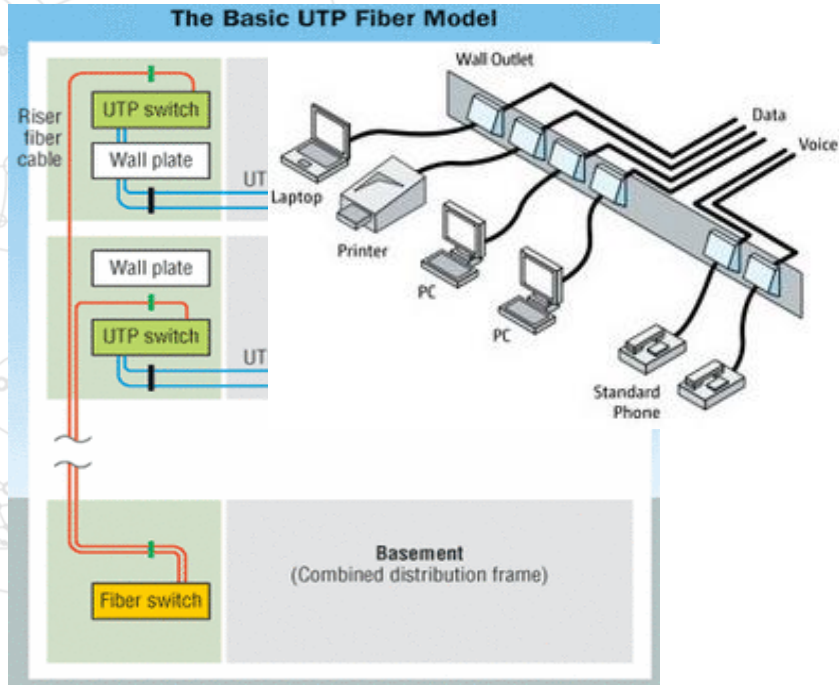
## Challenges for L3 fabrics

- configuration automation for multi-vendor devices
- integration with Cloud orchestration platform (OpenStack.)

# Campus connectivity: wiring

## SCN (Structured Cabled Network)

## FTTO (Fibre to the office)



# Campus connectivity: wiring

## SCN (Structured Cabled Network)

- › Strict lengths limitations (90 m)
- › Thick cable trunks, EMI susceptibility
- › Speed dependent cable technology
- › Many wiring cabinets for cable consolidation
- › Core switches + floor switches
  - Maintenance and possible cooling per floor
  - ~24/48 users aggregation factor
- › For small and mid size installations

## FTTO (Fibre to the office)

- › Almost no length limitations
  - 500m/MM, 10km/SM
- › No cable trunks, no EMI concerns
- › Future-proof for higher speeds
- › Few wiring cabinets needed
- › Core switches + office FTTO small switches
  - Better PoE efficiency
  - Smaller user aggregation factor
- › For large, spatially distributed facilities



# Campus connectivity: wireless

## > Wireless

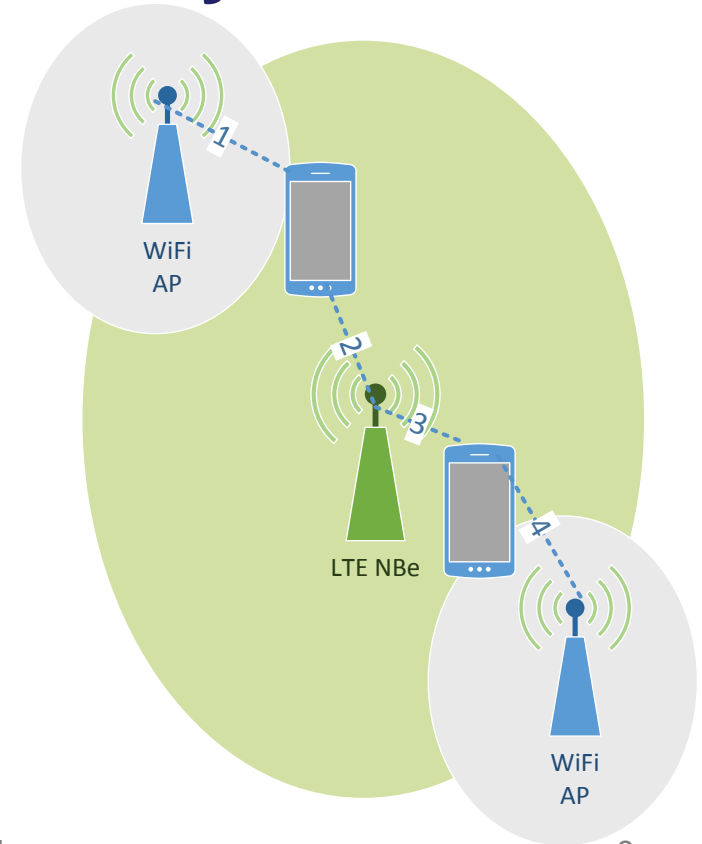
- Convenient, easy to use
- Suitable for most applications

## > Controller based WiFi solutions

- significant user experience improvement
- Simplified management

## > Can further improve: WiFi+LTE

- No WiFi coverage → LTE
  - True seamless roaming
- WiFi coverage → LTE offload



# Security (AAA)

## > Port-based access control: 802.1X

- Supported in modern OSES (user authentication)
- MAC Authentication Bypass → for “dumb” devices

## > Controller based access network

- Role-based
  - network access enforcement
  - QoS
- Already available in controller based WiFi solutions
  - proprietary technology
- Will become available on wired switches
  - unified campus network access policy

## > Challenges

- Management of users and their roles / privileges
- Accounting: role-to-MAC mapping for every authentication

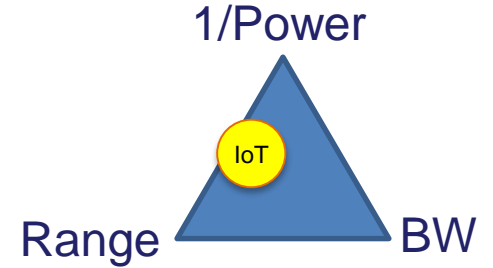
## > Scale – coverage:

- Wireless for most devices
- High range / low power / low bandwidth
- Licensed spectrum 3GPP technologies
  - Deterministic performance at a cost
- Unlicensed spectrum technologies (LoRa, HaLow)
  - “Free”, but risk of collapse in dense areas

## > Scale – addressing: OK with IPv6 or IPv4+NAT

## > Security:

- Access control
- Apply latest security patches ... if available...
- Compromised devices
  - high local impact (control devices)
  - DDoS attack platform



# Summary

<b>Commoditization: HW and SW</b>	<ul style="list-style-type: none"><li>• White-box switches</li><li>• 3<sup>rd</sup> party OS</li><li>• SDN Controllers.</li></ul>
<b>Configuration automation</b>	<ul style="list-style-type: none"><li>• No true multi-vendor solution</li><li>• Growing open-source eco-system</li></ul>
<b>Fabrics</b>	<ul style="list-style-type: none"><li>• VM mobility across large L3 Data Centers</li><li>• Unified management for multi-vendor fabrics</li><li>• Integration with Cloud Orchestrator</li></ul>
<b>Campus connectivity (wired/wireless).</b>	<ul style="list-style-type: none"><li>• FTTO for large scale dense deployments</li><li>• Uniform of user experience</li><li>• Wired/WiFi/LTE convergence</li></ul>
<b>Security</b>	<ul style="list-style-type: none"><li>• Role based access control</li></ul>
<b>IoT</b>	<ul style="list-style-type: none"><li>• Coverage and Interference</li><li>• Security</li></ul>