Torino, 17/01/2024

TIM network

Architecture and management

TIM

LA FORZA DELLE CONNESSIONI

#1 Network architecture

#2 Network management

#3 Current evolution

Network architecture

Requirements
Satisfy the connectivity needs of customer devices and applications:

- Personal computers, mobile devices, enterprise networks, …
- Voice, browsing, video, large data, …
- Security, virtual private networks, …
- Latency, packet loss, availability, …

+

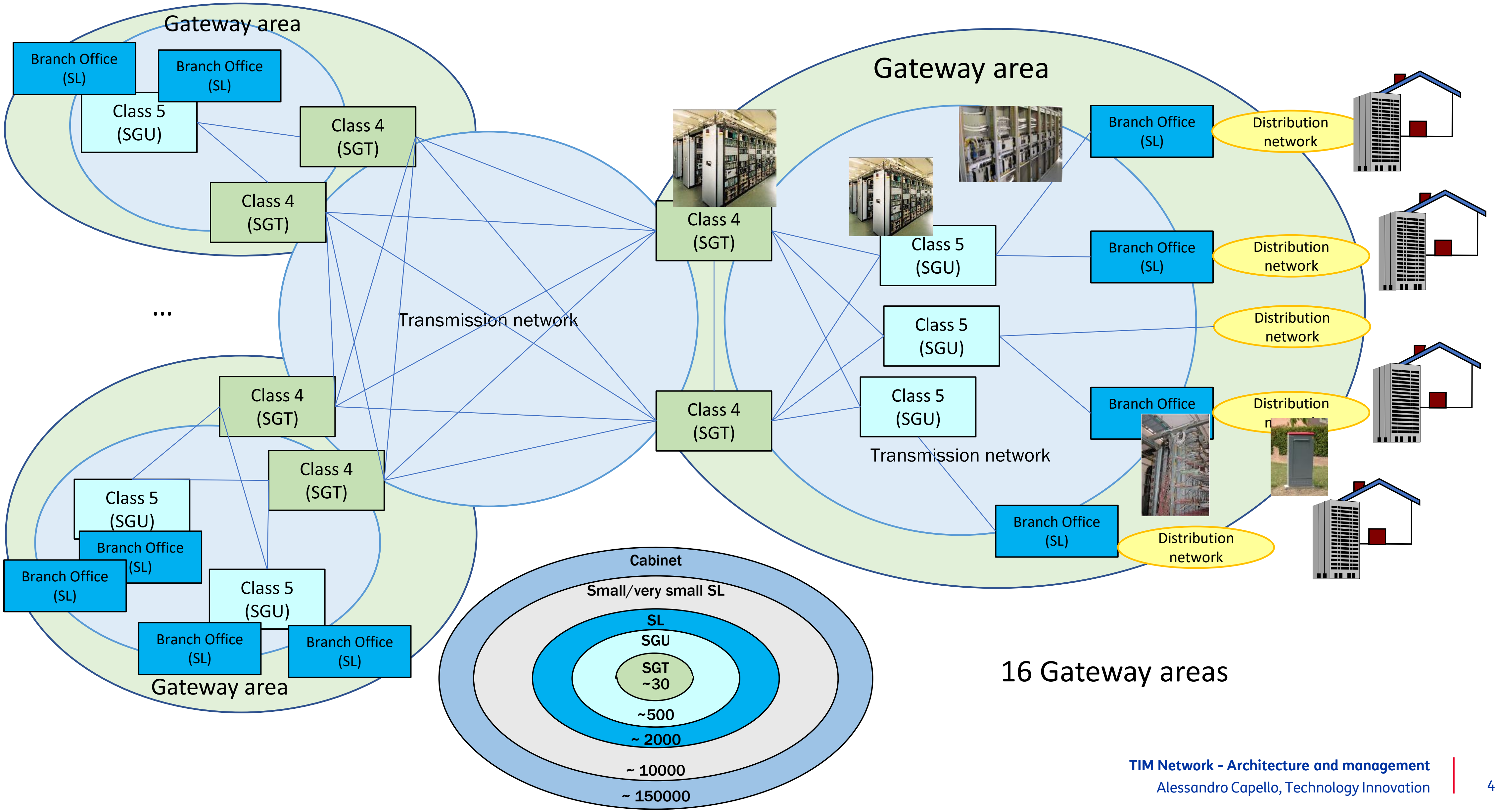
Constraints

- Technology limitations (interface speed, switching performance, fan-out, transmission performance, …)
- Legacy infrastructure (sites, cable ducts, …)
- Budget

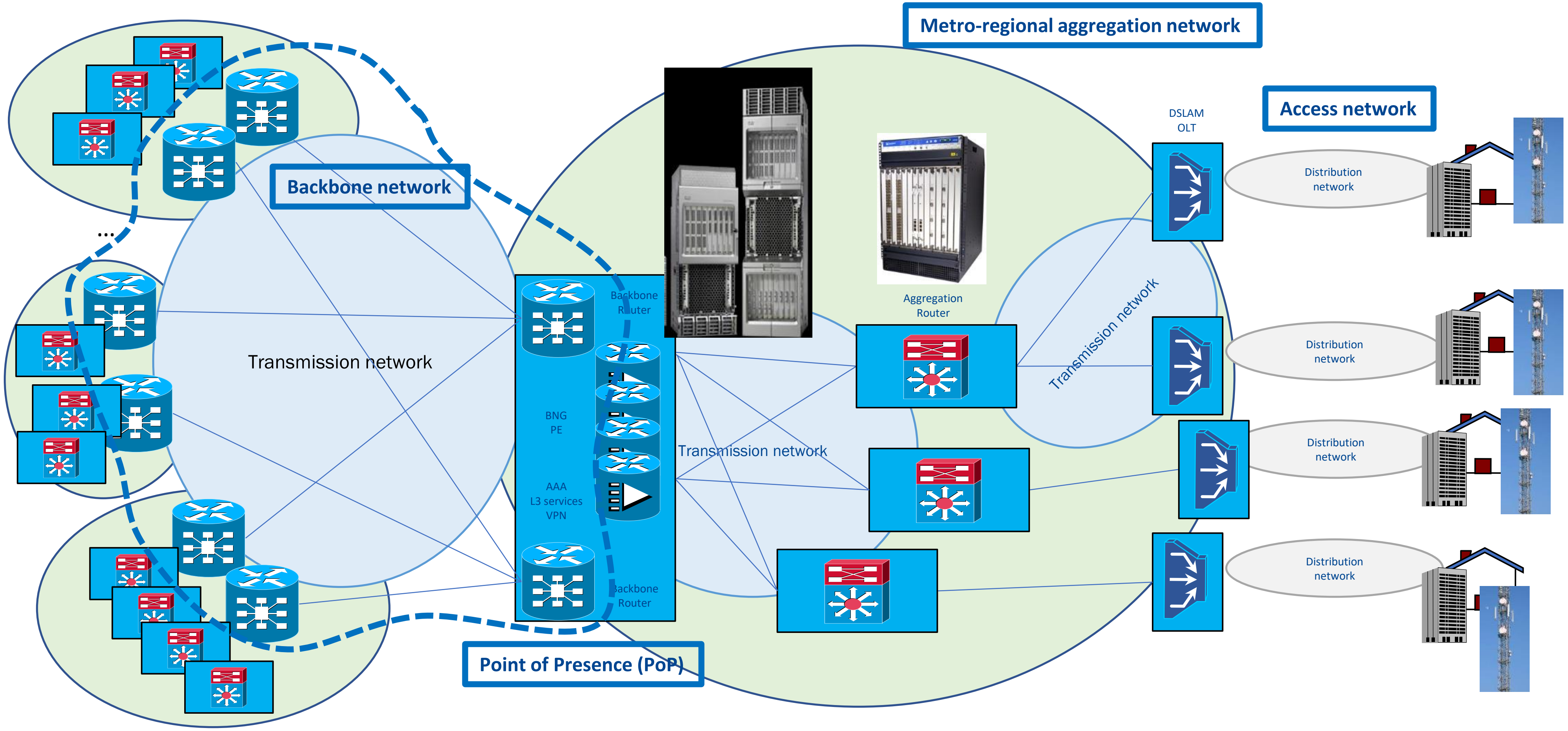
→

The goal is, given the constraints, design the structure of network devices and services in order to satisfy all the requirements at the minimum cost

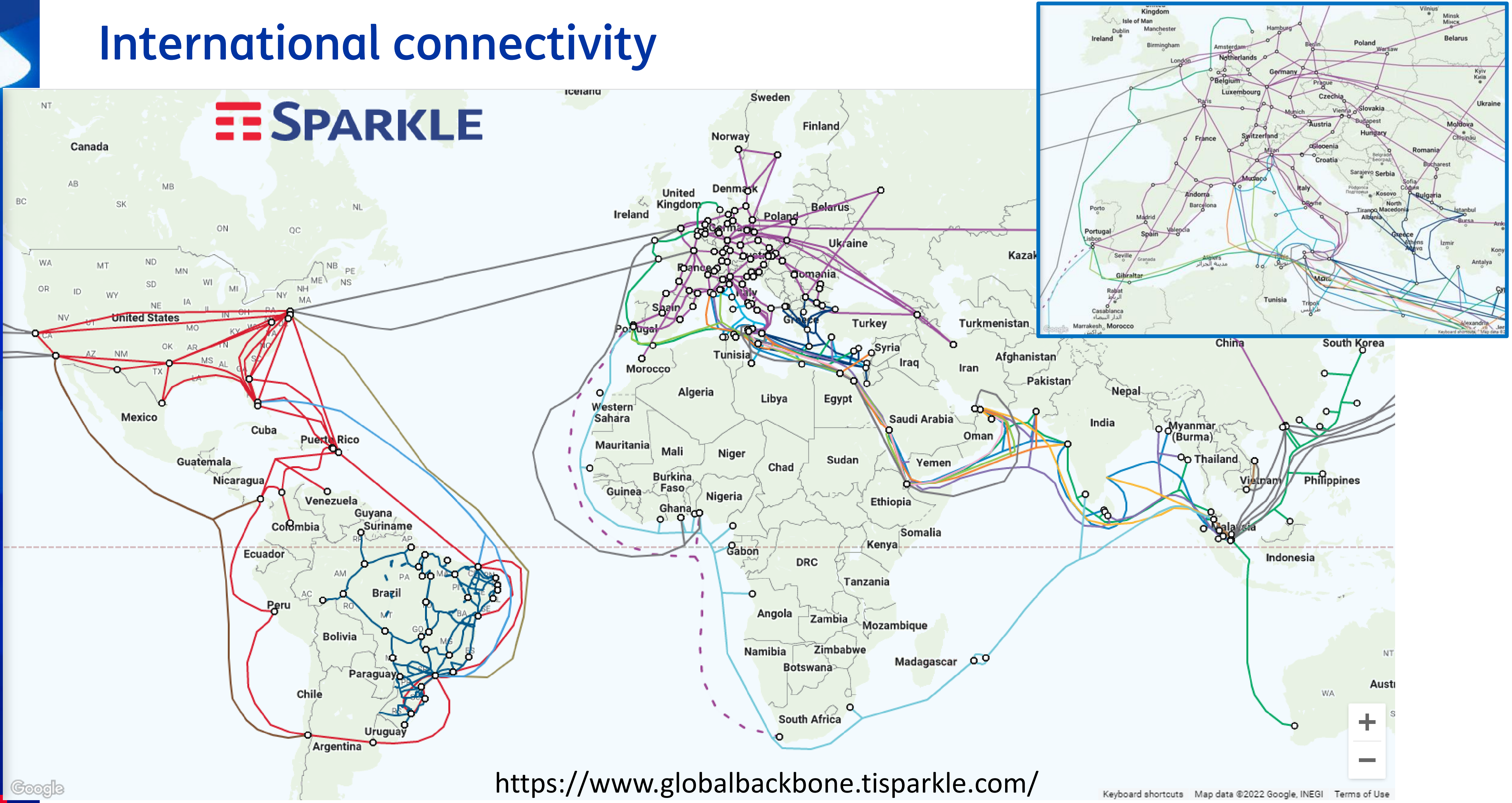
The origins of TIM network



Overview of TIM network

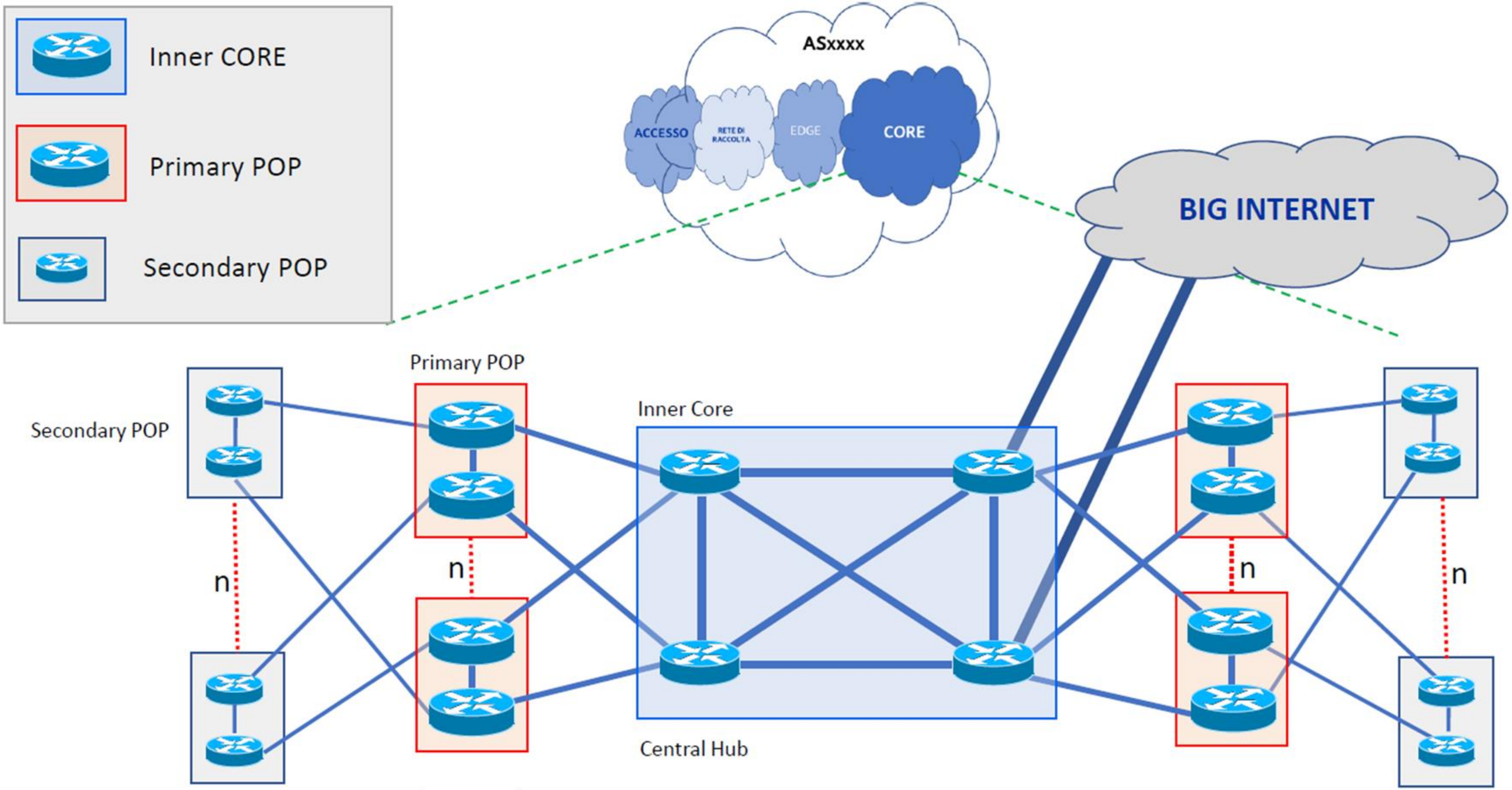


International connectivity



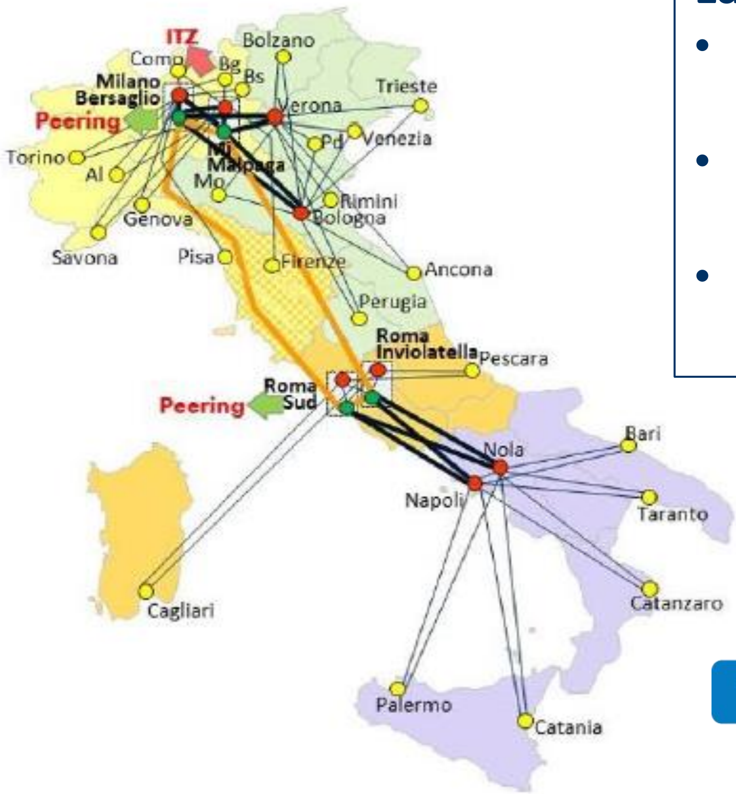
https://www.globalbackbone.tisparkle.com/

Backbone (aka IP Core)



Backbone multi-layer network

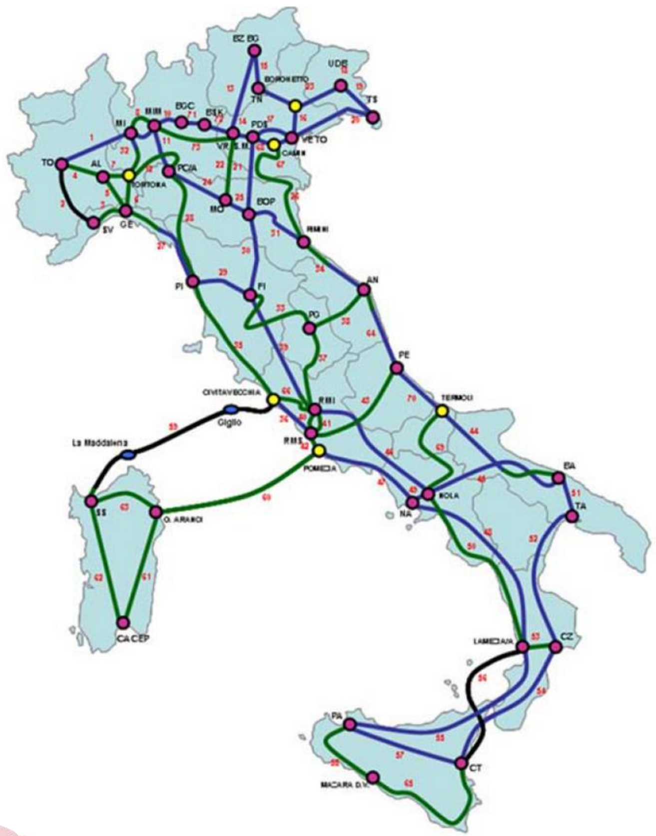
IP network

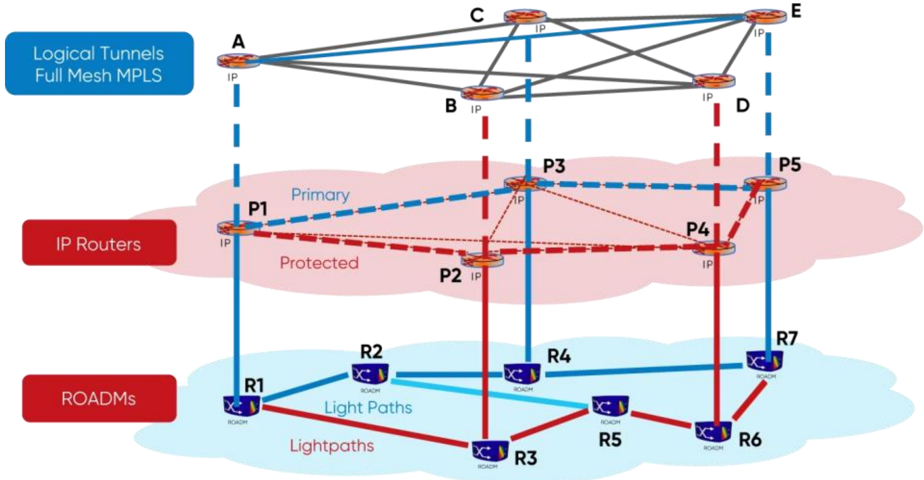


Layers:

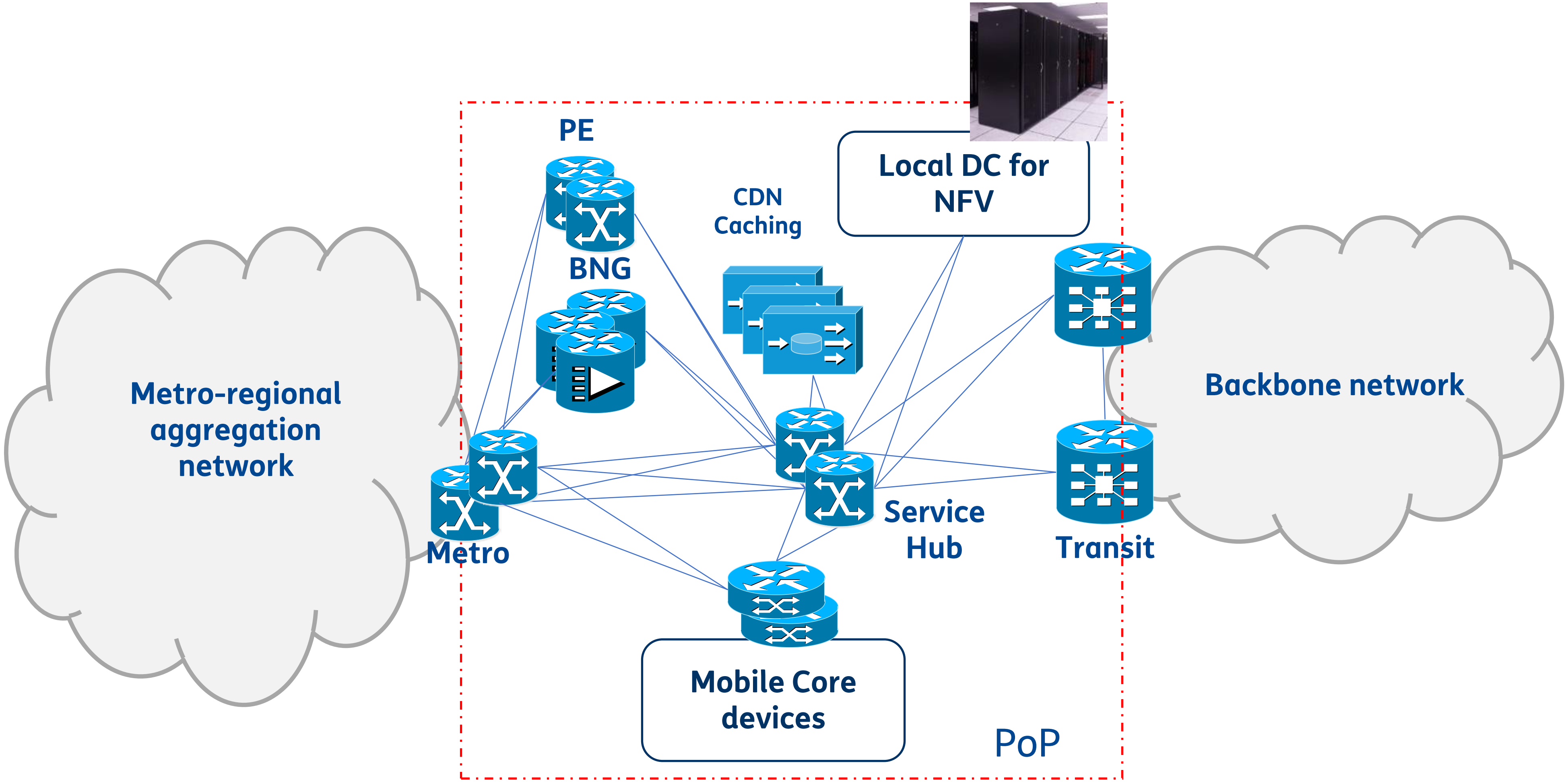
- MPLS: logical full mesh over IP topology
- IP: logical router to router connections over optical network
- Optical: physical connectivity among optical devices

Optical network

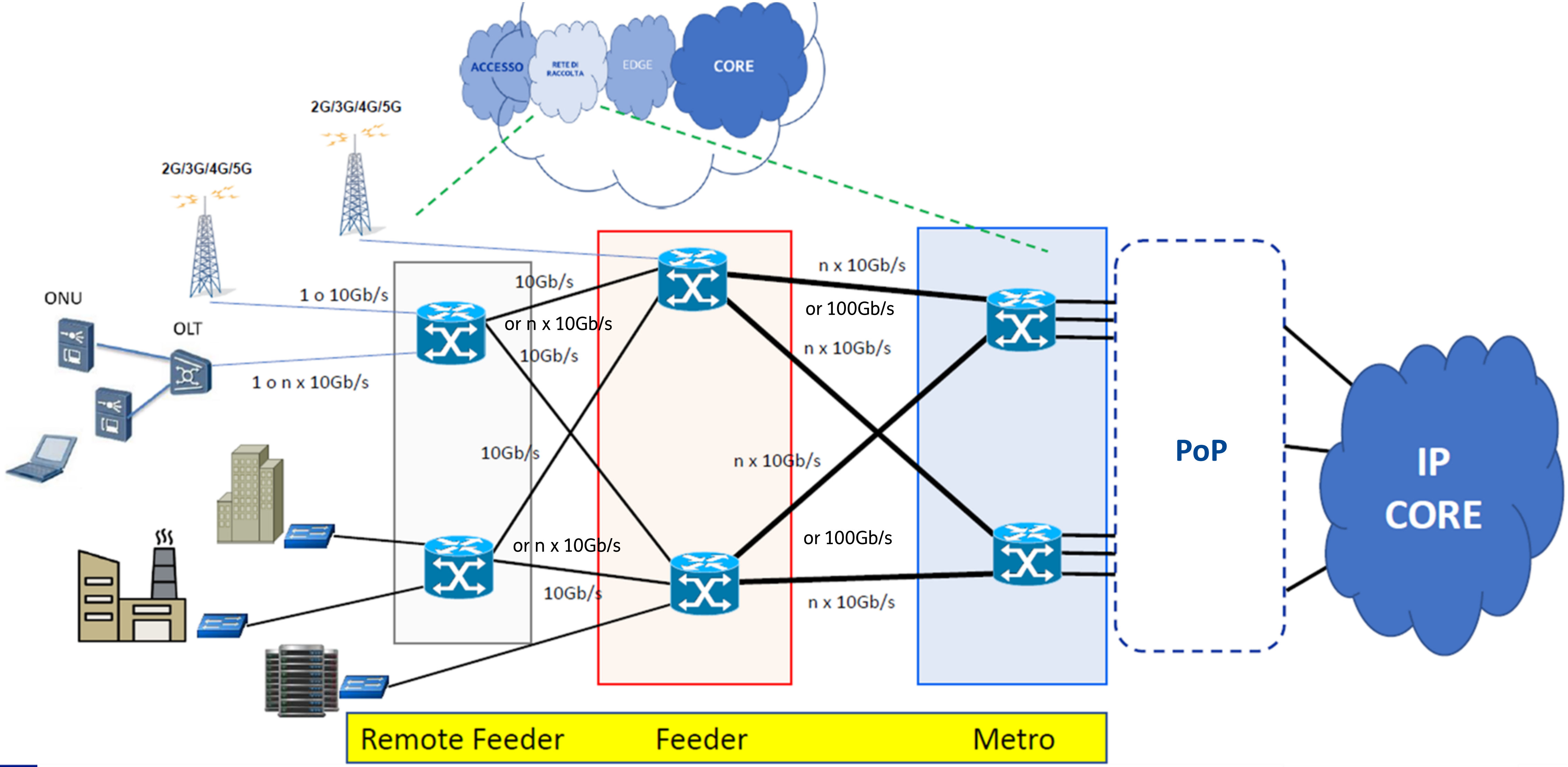




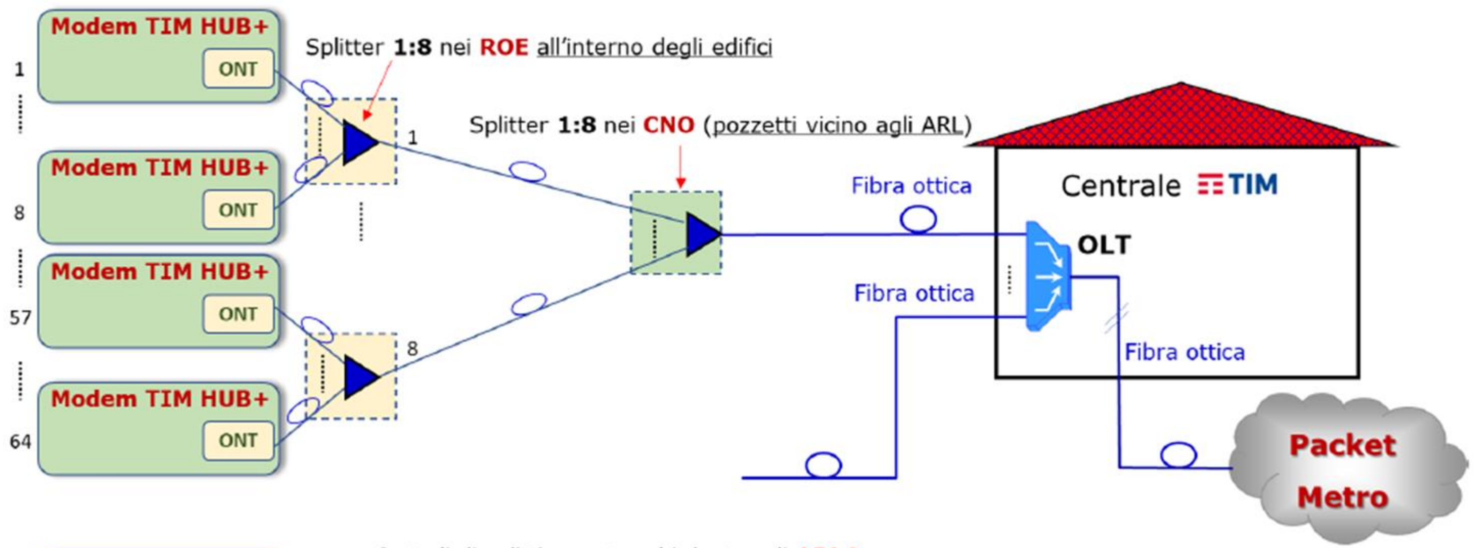
Point of Presence (aka IP Edge)



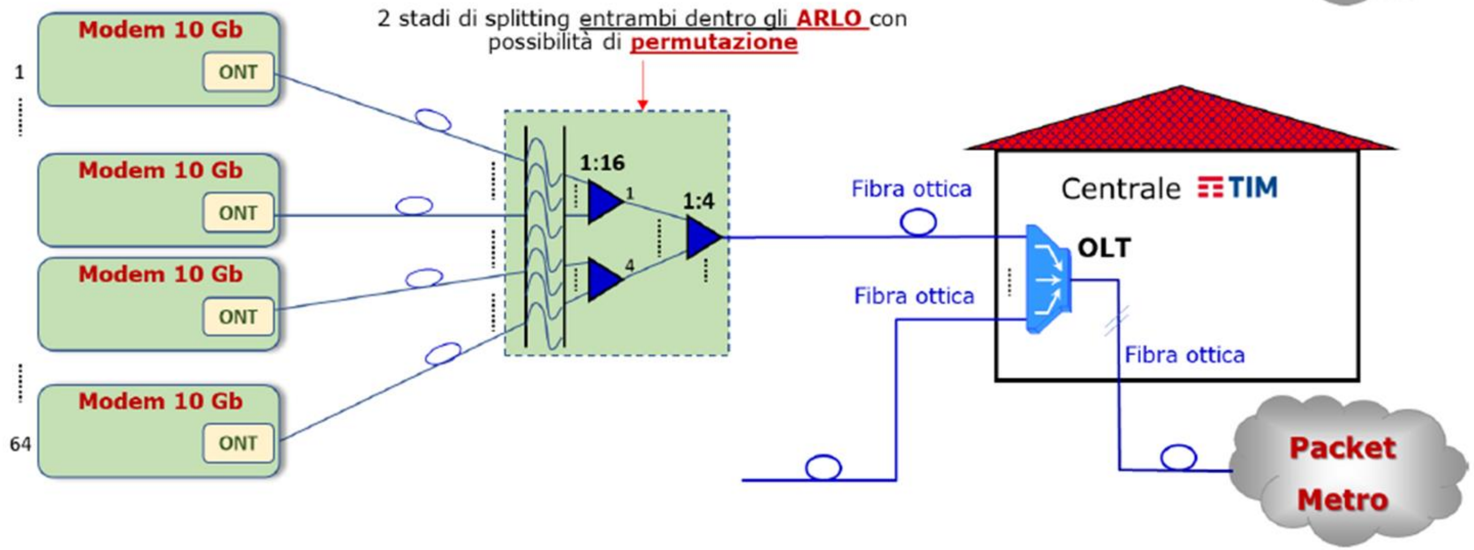
Metro-regional aggregation network



Access network



ROE: Ripartitore Ottico Edificio
CNO: Centro Nodale Ottico
ARLO: Armadio Ripartilinea Ottico



#1 Network architecture

#2 Network management

#3 Current evolution

Traffic management strategies

Capacity planning means adding capacity on the connectivity paths where traffic is growing faster:

- Add optical DWDM channels to transponders and interfaces to routers (pay attention to fan-out limitations)
- Replace interfaces to increase speed if allowed by technology and current devices

Prevent congestion

Traffic engineering means rerouting selected traffic away from paths that are experiencing (or going to experience) congestion:

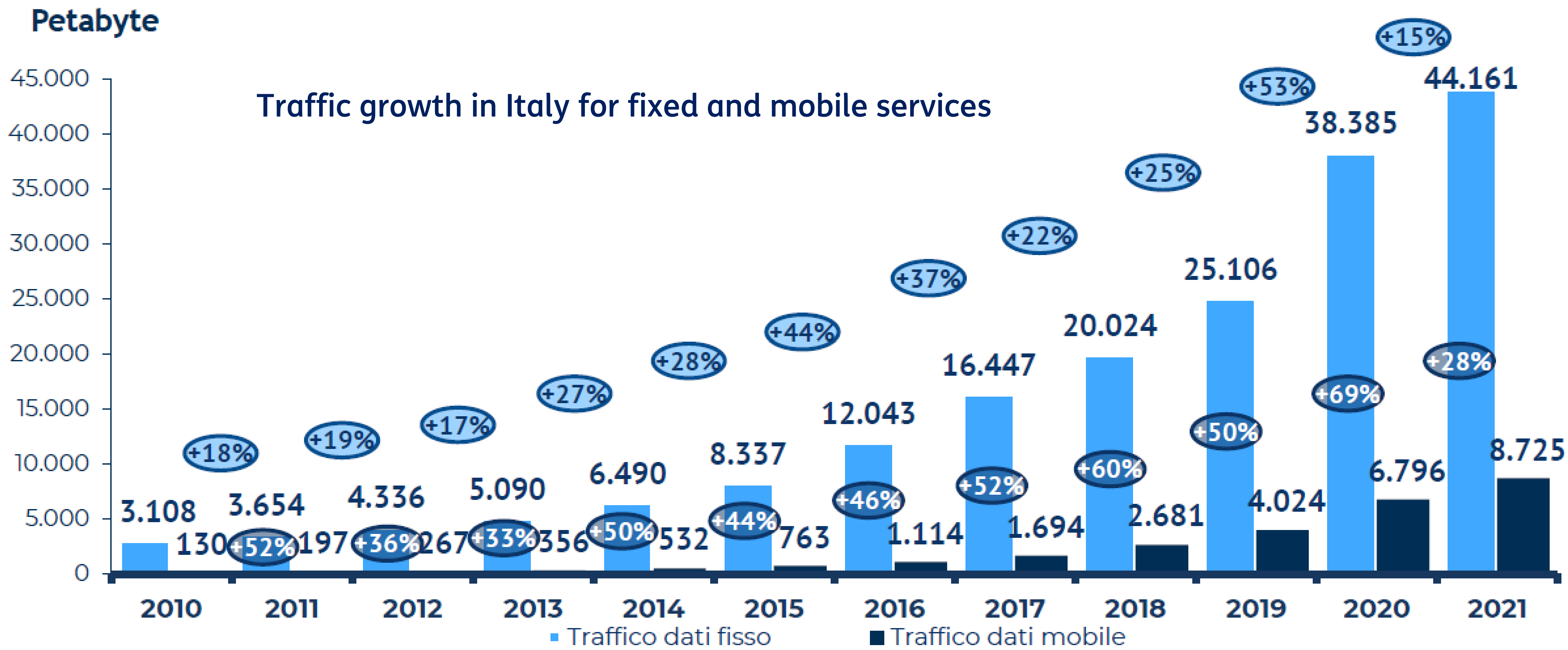
- MPLS Traffic Engineering
- Segment Routing

Avoid congestion

QoS management means differentiating the impact on traffic in case of network congestion

Manage congestion

Current traffic growth



FONTE ELABORAZIONE OSSERVATORI DIGITAL INNOVATION POLITECNICO DI MILANO SU DATI AZIENDALI

TIM traffic management strategy

Traffic measurements and prediction

Continuous monitoring of link load: peak and average traffic rates are collected for all interfaces

Warning thresholds are defined to allow planning for upgrades

Algorithms for traffic prediction must consider both legacy and new services

Unexpected events happen…

Take advantage of topology properties

The network design avoids single points of failure

The symmetry of the topology enables load-balancing of traffic over all equal cost paths

All internal links are dimensioned following the 50% rule: each link can't be loaded more than 50% of its capacity @ peak hour. This protects in case of fault and in case of unexpected traffic surges.

No need for traffic engineering

QoS management with DiffServ

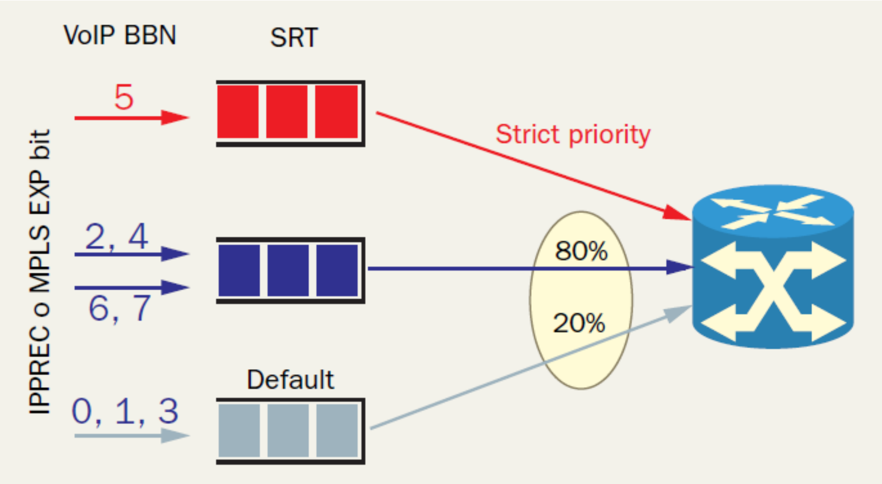
DiffServ

Protect critical traffic in case of multiple simultaneous faults

Classification based on IP precedence, MPLS EXP or Ethernet CoS

3, 4 queues: a strict priority (typically for voice) queue and 2, 3 WFQ for different data classes

Critical point is traffic marking: you can’t trust IP precedence of Internet IP packets… most of the traffic in the backbone is in the Default class



Hierarchical QoS management

Business customers

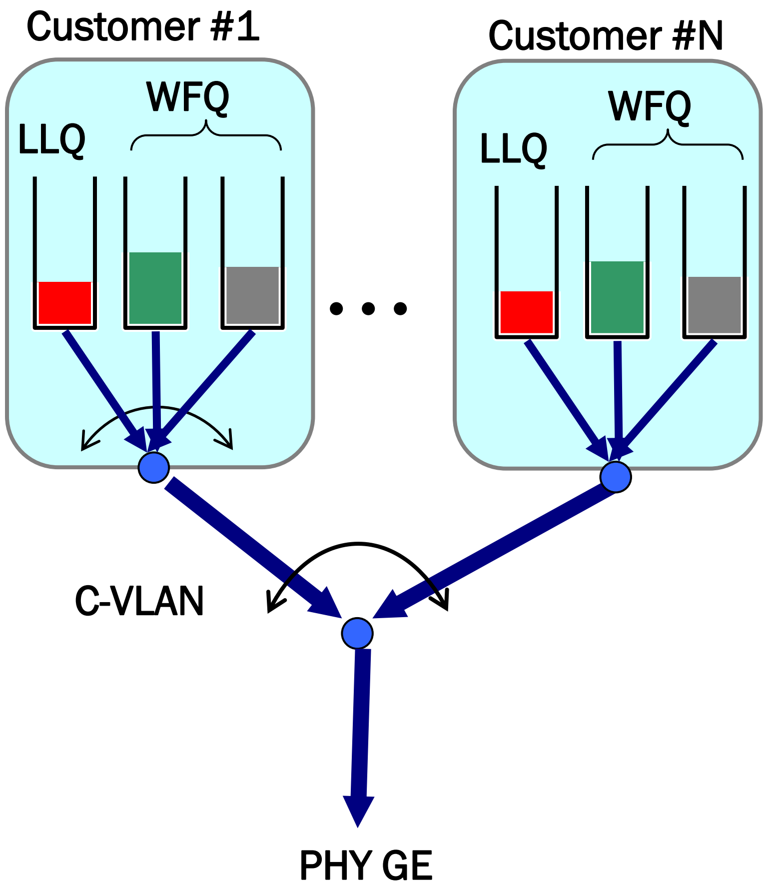
- 3 queues for each customer
  - LLQ + 2 queues with WFQ (Mission Critical and Default)
  - Example of weights is 30:70
- Hierarchical queuing
  - multiple access on a single interface

Residential customers

For a residential access, only a peak bandwidth is defined

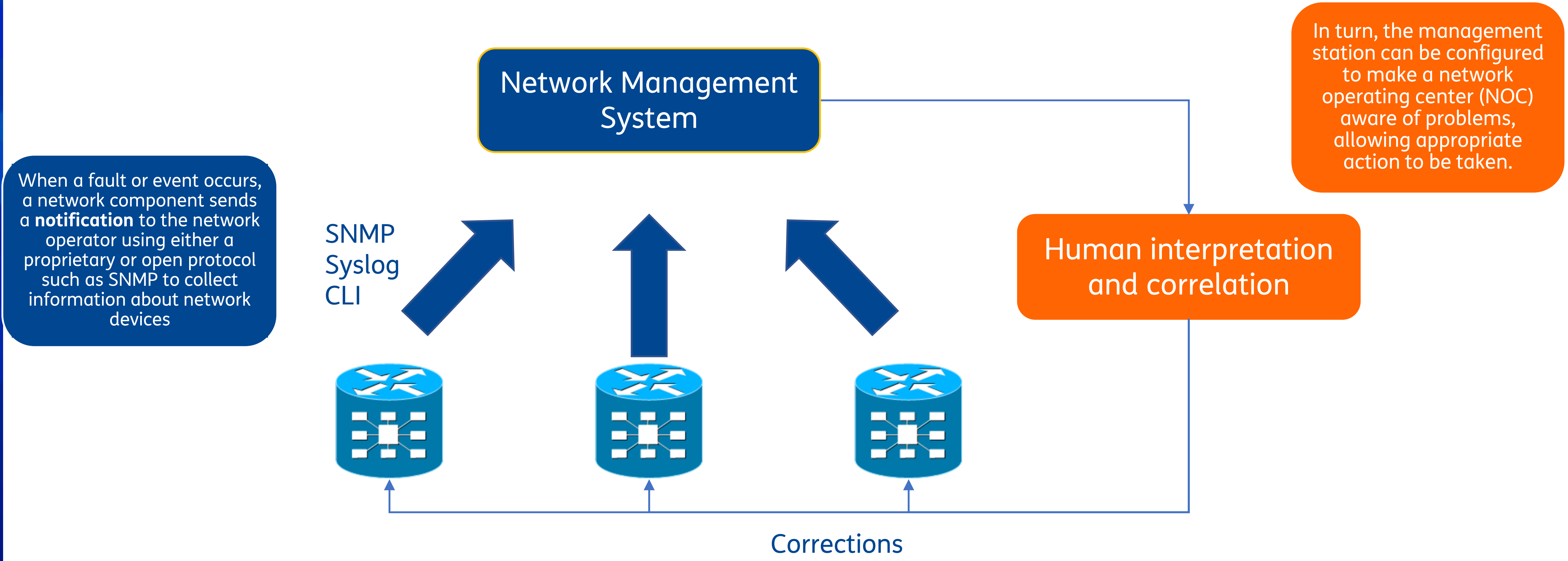
The network applies a limitation of the peak bandwidth at the maximum value defined by the selected offer

For each customer, 1 or 2 queues (LLQ and default) are configured



Fault management

- A fault is whatever event that negatively alter network behavior and performance
- The goal of fault management is to **recognize, isolate, correct and log** faults that occur in the network



Configuration management

- Typical use cases:
  - Deployment of new network devices
  - Upgrade of existing network devices
  - (Re-)configuration of one or multiple devices to add new service instances

- Configuration management is concerned with **monitoring system configuration information**, and any changes that take place.

- This area is especially important, since **many network issues arise as a direct result of changes made to configuration** files, updated software versions, or changes to system hardware.

- A proper configuration management strategy involves **tracking all changes made to network** hardware and software. Examples include altering the running configuration of a device, updating the OS version of a router or switch, or adding a new modular interface card.

Configuration stages

Stage	Actions
Day-0	1. Initial configuration typically applied on power-on, boot-up. 2. Information entered on serial consoles, buttons/switches on device 3. Configurations that need knowledge of physical connectivity, typically entered by operators 4. Configurations that are considered pre-requisite. 5. Configuration required to establish communication between device and network management system
Day-1	Configurations that are common to all network devices (example, NTP, Syslog, SNMP Trap destination etc.)
Day-2..N	Ongoing configurations pushed on the device for day-to-day operations. Configurations pushed to build one instance of a service

Performance management

Performance

- Performance management is focused on **ensuring that network performance remains at acceptable levels**.
- By collecting and analyzing performance data, the **network health** can be monitored. The network performance addresses the throughput, network response times, packet loss rates, link utilization, percentage utilization, error rates and so forth.
- This information is usually **gathered through the implementation of an SNMP management system**, either actively monitored, or configured to alert administrators when performance move above or below predefined thresholds.
- Actively monitoring current network performance is an **important step in identifying problems before they occur**, as part of a proactive network management strategy.

Drawbacks of current network architecture and operations

Network upgrades are expensive considering the current traffic growth

Many weeks to plan changes

Multiple hops to upgrade between source and destination and overlay networks with different provisioning procedures

The introduction of new network services is slow

All network functions are developed as specialized and proprietary network equipment

Need to deploy physical devices

Integration with legacy management systems usually takes time

Network upgrades are expensive considering the current traffic growth

SNMP protocol:

- Poor scalability (pull mode and data organized in static tables)
- Extensibility not managed efficiently by the standard

NMS:

- Per-vendor integration
- Imperative approach
- No service view

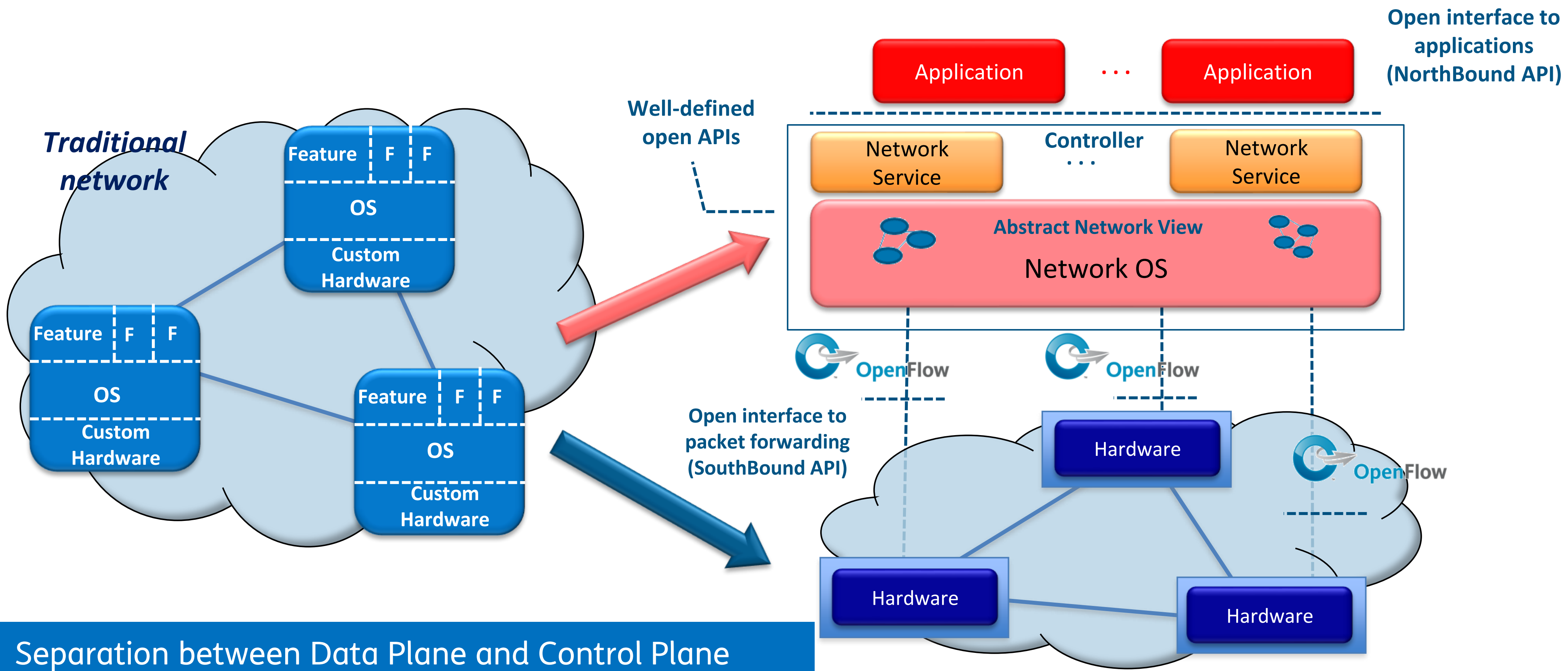
Limited automation and too much dependence on human interpretation

#1 Network architecture

#2 Network management

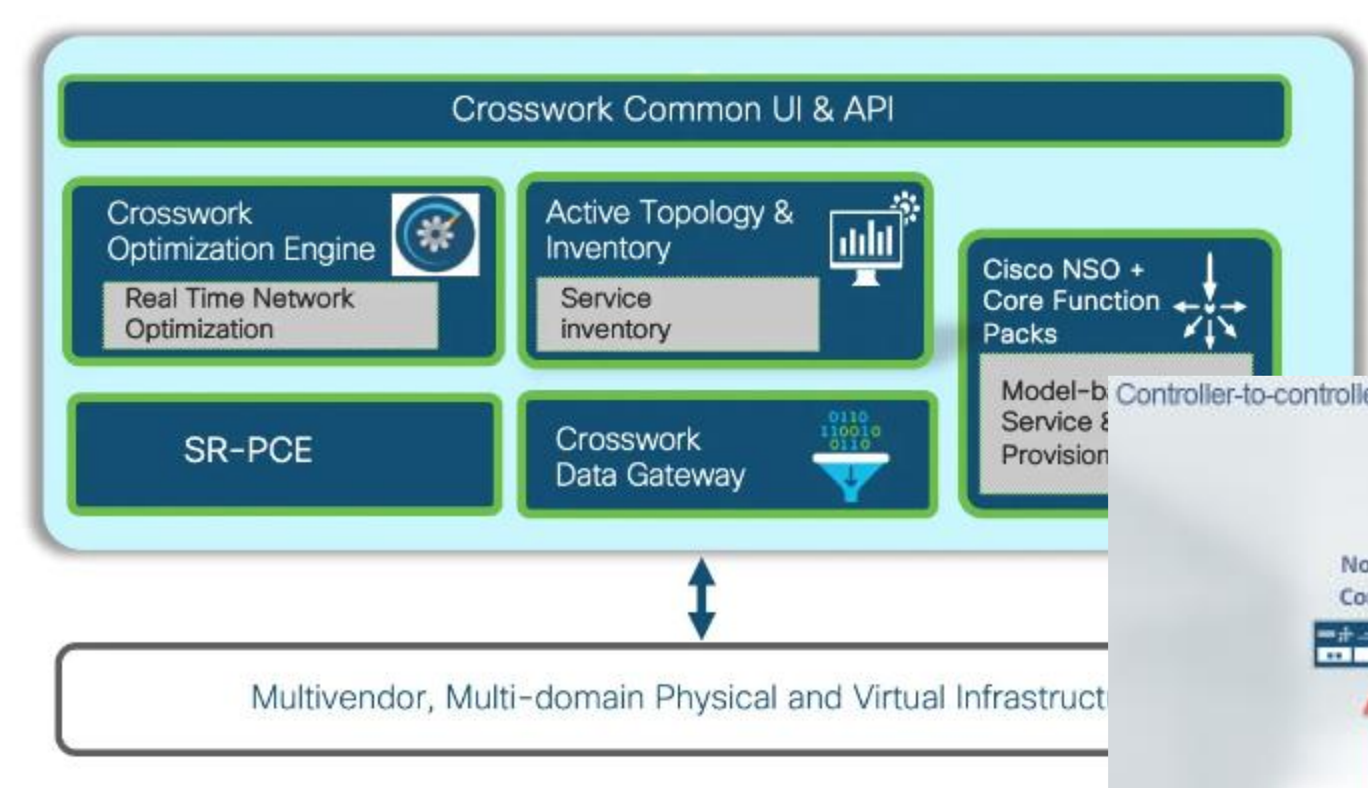
#3 Current evolution

Software Defined Network: the original concept

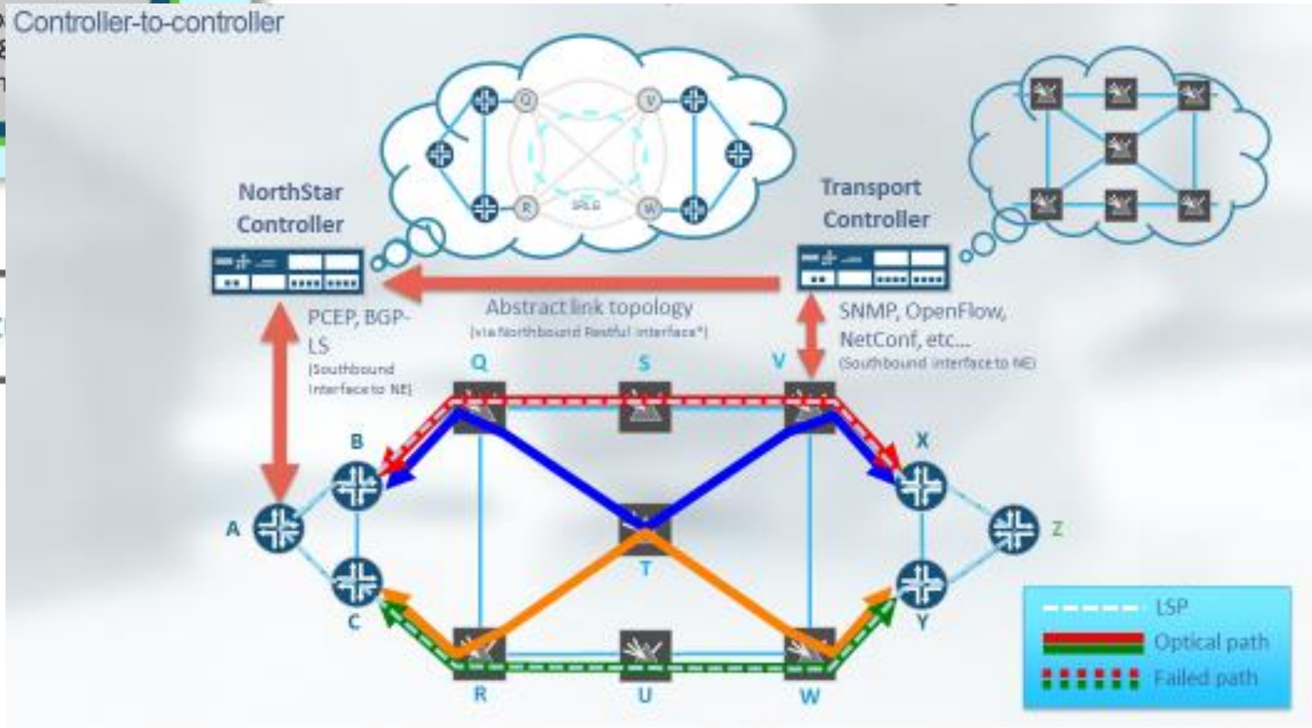


- Separation between Data Plane and Control Plane
- The Control Plane is logically centralized
- The Data Plane is "programmed" by the Control Plane
- Open APIs towards applications

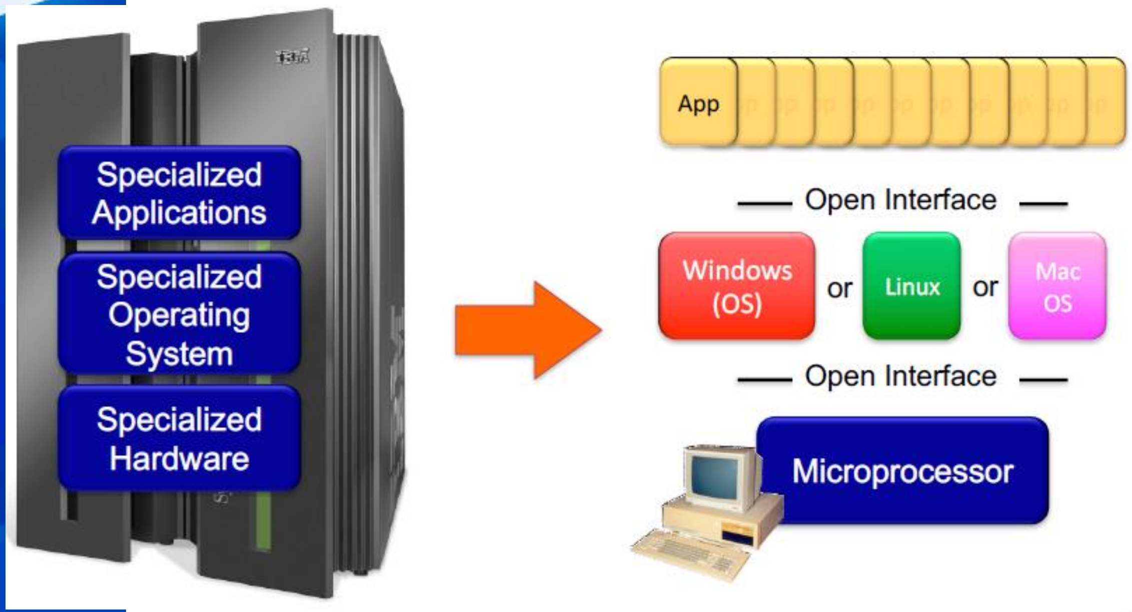
Software Defined Network for traffic engineering



New protocols (Path Computation Element Protocol, PCEP) or extensions to existing ones (BGP-LS) can be used to delegate to an external controller the calculation of optimal traffic engineering paths

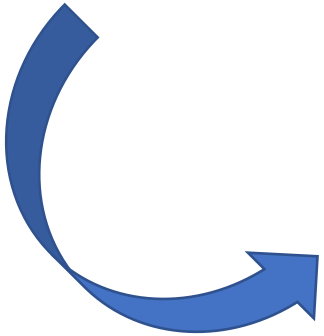


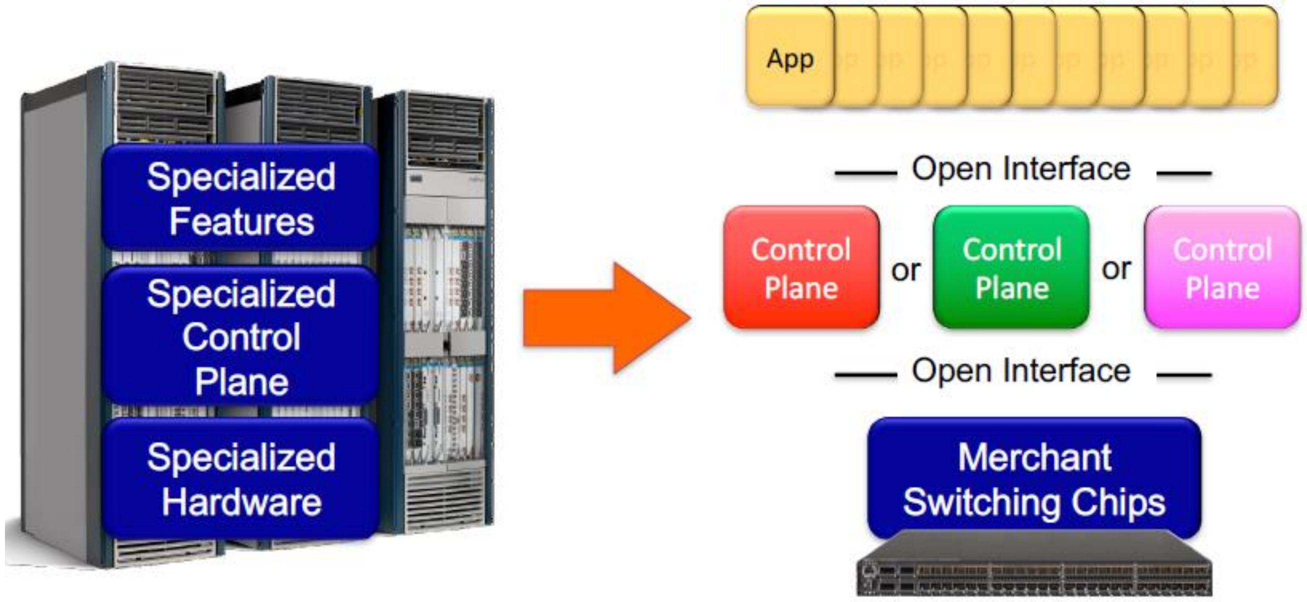
Disaggregation of network devices



Enabled by the availability of networking ASIC with open programming interfaces

Disaggregation replicates in networking technology what happened in IT technology with the migration from proprietary mainframe systems to microprocessor systems and operating systems from third parties



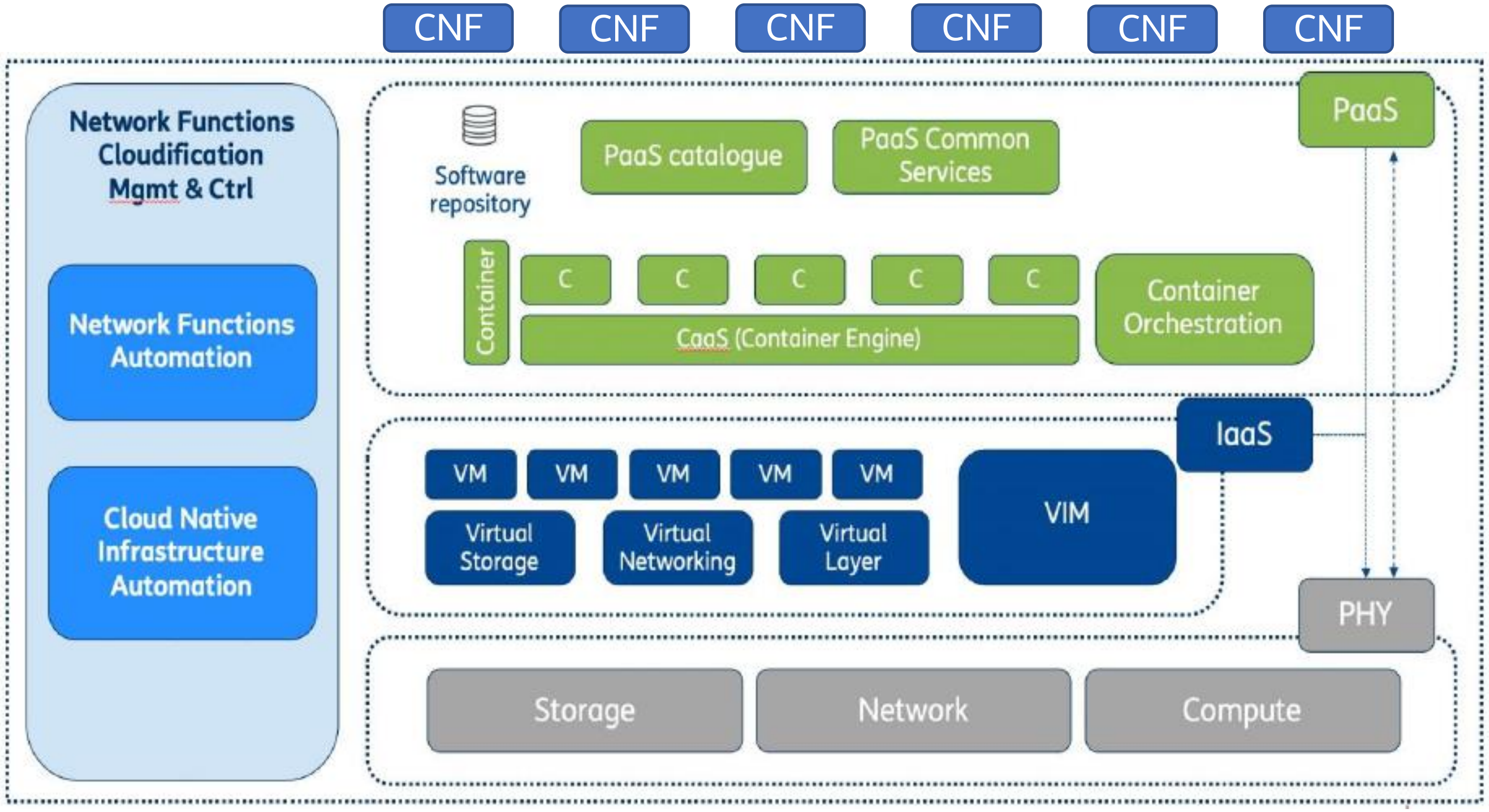


Images from Nick McKeown, Stanford University

Disaggregation + virtualization -> Network Function Virtualization

NFV: Network Function Virtualization

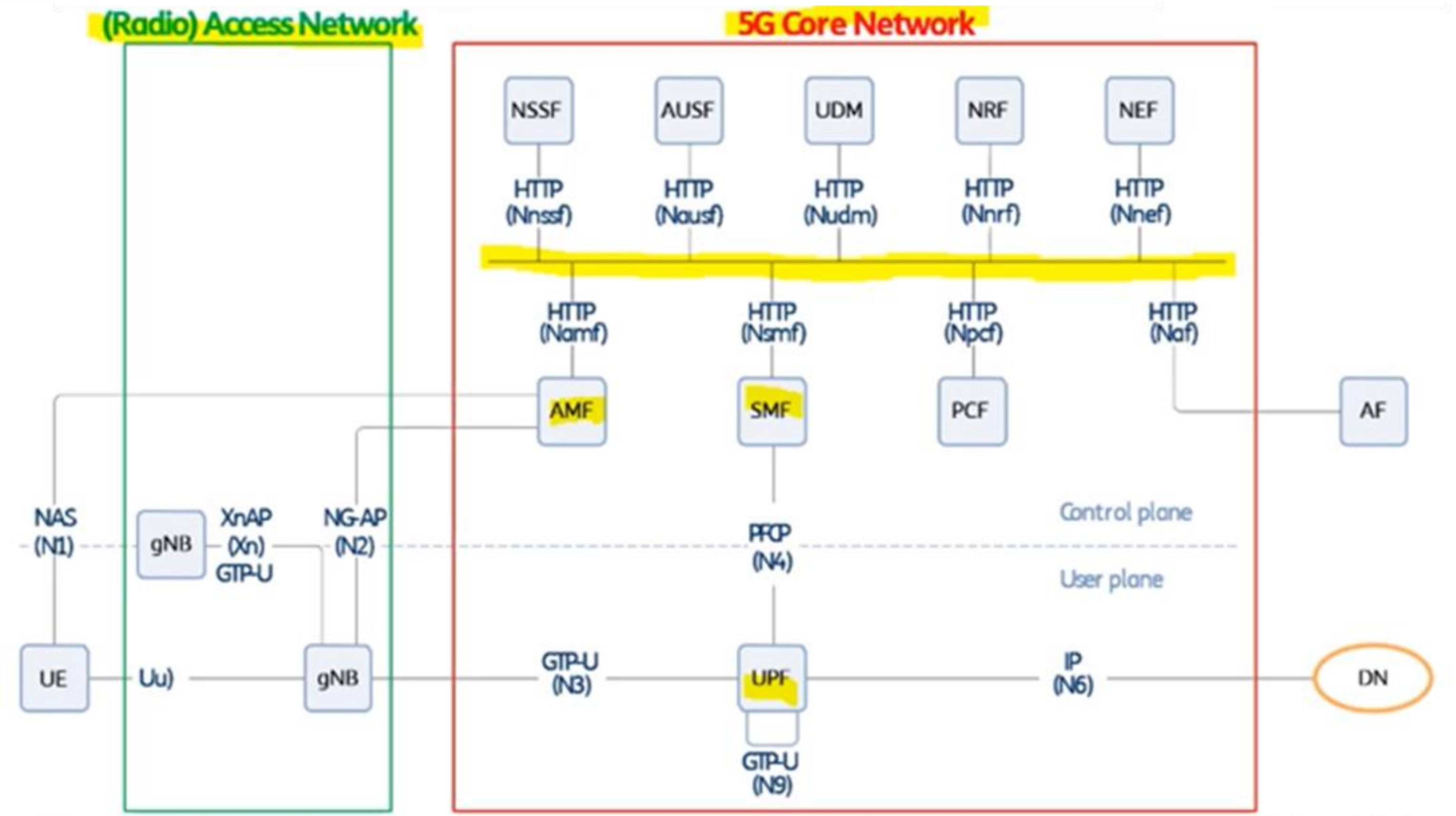
- Modern CPUs and chipsets can handle new types of workloads efficiently
- Control plane and data plane (currently with some limitations) network functions can be implemented on general purpose CPU and can take advantage of virtualization technologies (virtual machines ore containers)



CNF: Containerized Network Function

5G Core as a set of cloud native functions

5G Core Network has been standardized assuming a cloud native approach

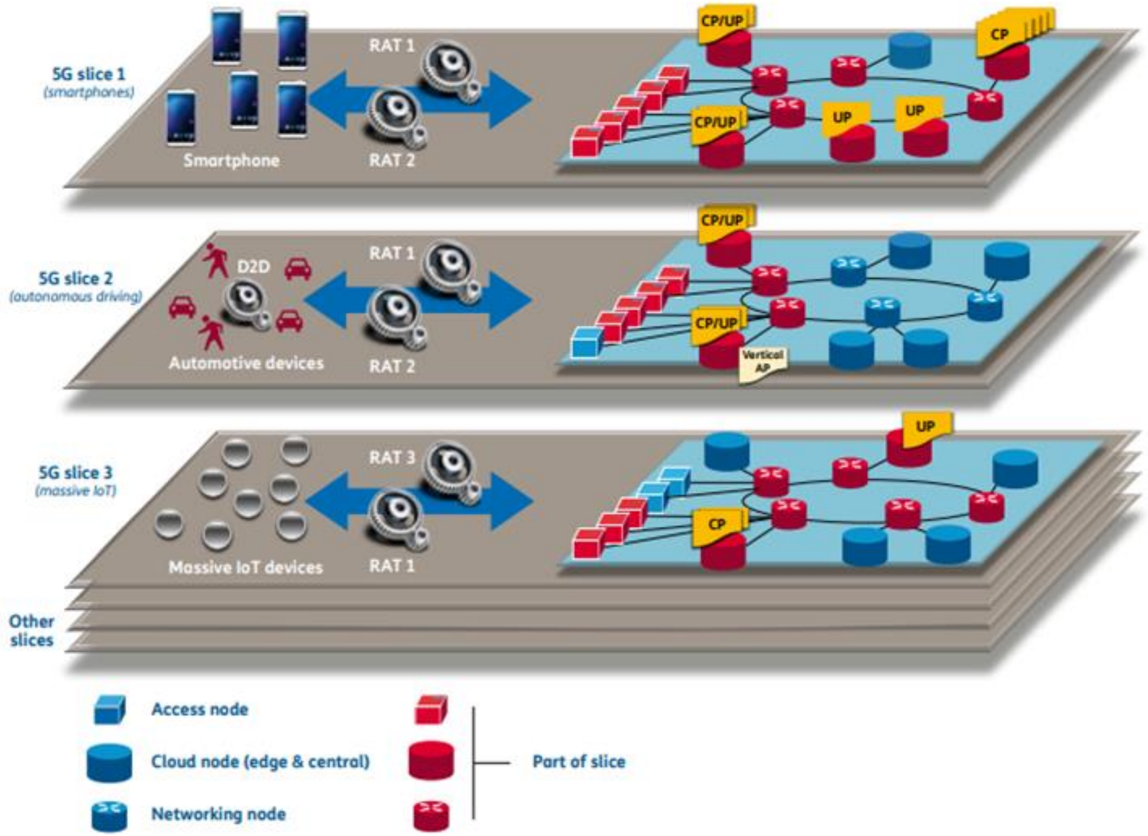


AF: Application Function
AMF: Access and Mobility Management Function
AUSF: AUthentication Server Function
DN: Data Network
gNB: Next generation NodeB
NEF: Network Exposure Function
NRF: Network Repository Function

NSSF: Network Slice Selection Function
PCF: Policy Control Function
SMF: Session Management Function
UDM: Unified Data Management
UE: User Equipment
UPF: User Plane Function

GTP-U: GPRS Tunneling Protocol User plane
NAS: Non-Access Stratum
NG-AP: Next Generation Application Protocol
PFCP: Packet Forwarding Control Protocol
SBI: Service Based Interfaces
XnAP: Xn Application Protocol

Advantages of NFV



An example: 5G network slicing

HW resources can be dynamically allocated on the basis of real needs: better efficiency and scalability

HW resources can be easily (i.e. automatically) re-assigned to different network applications: faster deployment of new network applications

Possibility to leverage features of the virtualization infrastructure

Issues with NFV

Functional issues

Cloud technologies are not originally developed to fulfill the requirements of Telco applications.

They're being integrated with additional features required by CNFs, especially for networking.

Performance issues

While CPU performances are increasing fast, the packet throughput they offer is still much lower than what specialized ASIC are able to do.

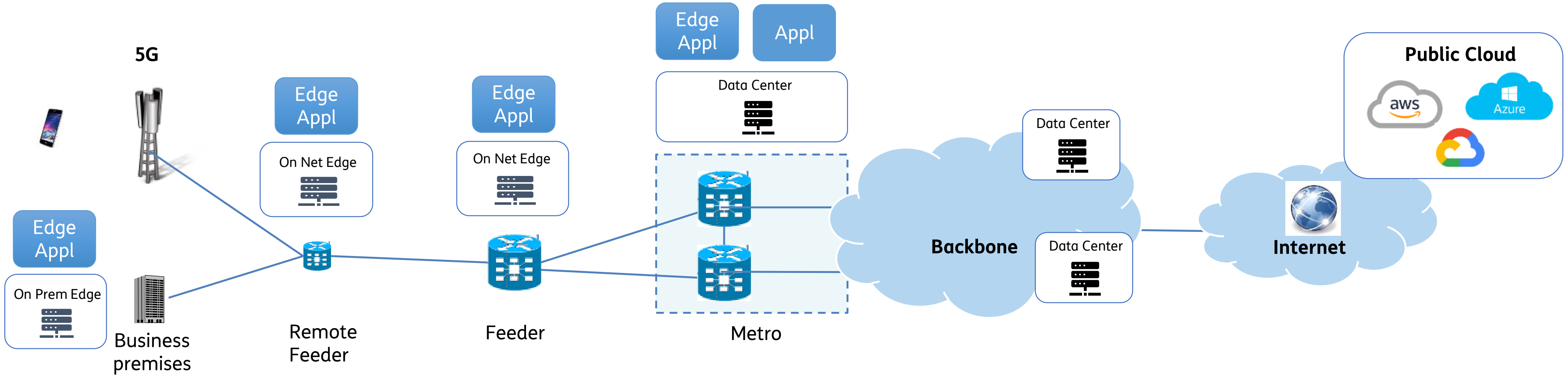
In many cases, general purpose CPUs need to be assisted by SmartNICs, hardware accelerators, etc.

Opportunities enabled by NFV: Edge Computing

Edge Computing is a style of cloud computing realized moving data and processing power closer to the source of data generation, where things and people produce or consume that information; it offers the "capability" to solve specific use cases

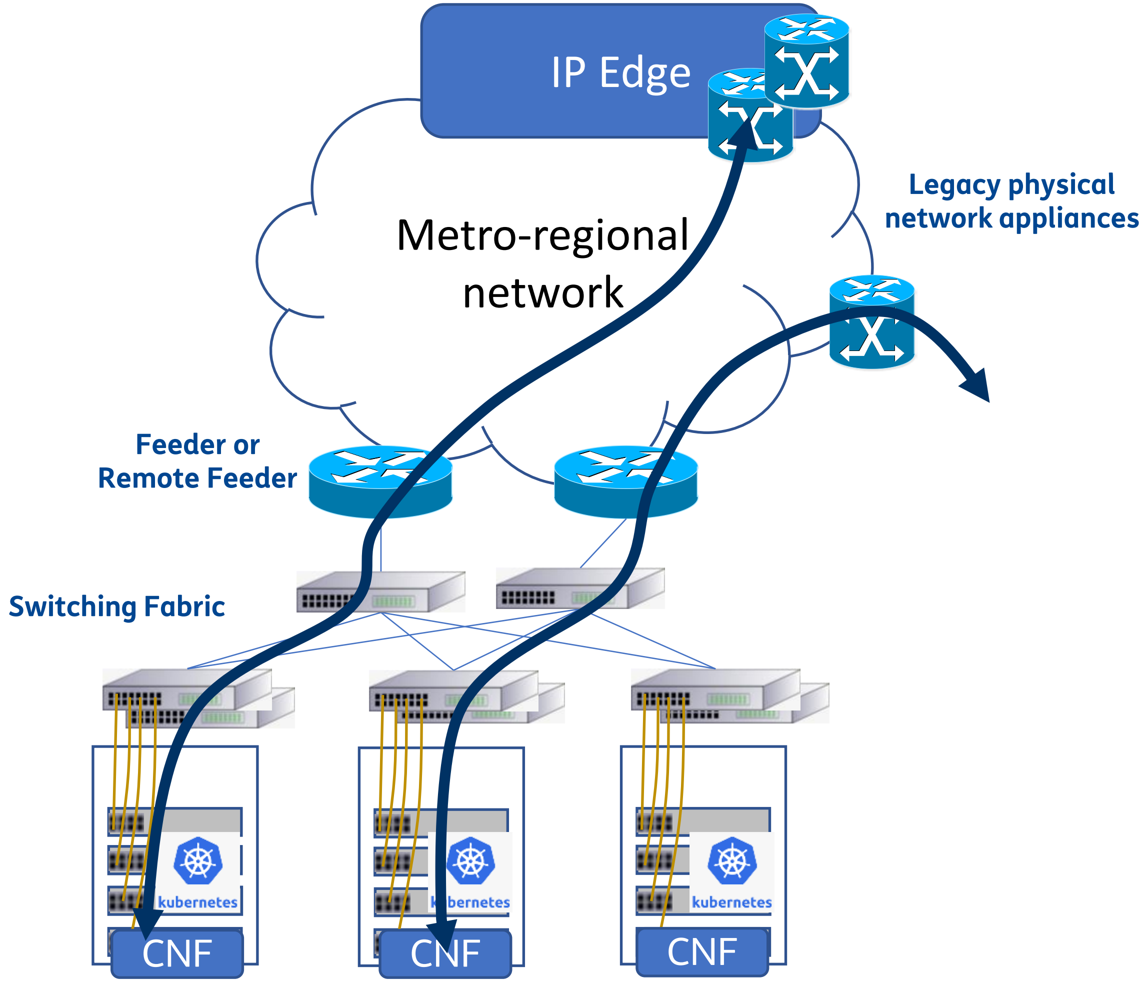
Edge Solution Capability	Example of use case
Low Latency Ultra-low latency (≈ ms) is critical for real-time type of application	**Robotic (Industry 4.0)** **AR/VR (cloud) network centric** **Mobile gaming**
Local Processing Elaboration of data produced locally to extract information and/or take decision avoiding large data transfer toward central D.C.	**Video surveillance** **IoT** **Content Caching** **Sport Event Experience**
Privacy / Security	**Data localization**
Limited Autonomy Ability to continue to run also when disconnected from central Data Center	**Private network services** **Enterprise / Campus Network**

Network architecture to support Edge Computing



On Net Edge Cloud sites are (very) small datacenters deployed in a subset of peripheral central offices of the metro-regional network.
Edge Cloud sites must host CNFs for 5G Core and/or IP Edge functions to provide the break-out of access traffic towards edge applications.

New challenges for the network architecture



Need to provide the interworking between CNFs and legacy network functions.
Different network solutions for traditional IP WAN (MPLS) and DC network (VxLAN).
The problem is being tackled from both sides, but many aspects are not properly handled yet

Evolution of network management

Configuration Automation

Services can be described using standard description languages (e.g. YANG, YAML, etc.)
Service descriptions can be passed to network controllers through programming interfaces (API)
The network controllers transform the service description into device configurations and automatically apply changes

Telemetry

Streaming telemetry provides a continuous flow of statistics from the devices to the NMS using a push model:

- Source-timestamped
- Event-driven: push as soon as the data changes (low latency), push only when the data changes (low throughput)
- Subscription-based

Closed Loop

The control loop can be closed with code that is able to correlate statistics to service behavior and automatically apply changes in case of problems

Closed loop fault management

Analytics

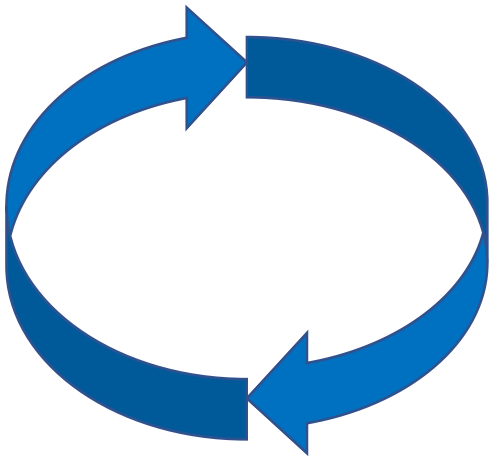
Provide insights based on collected data (e.g. machine learning)

Intelligence

Provide specific decisions and recommendations
AI models, policies and intents

Analysis

Decision



Collection

Execution

Data collection

Monitor the manages entities and provide live fault and performance data

Orchestration & Control

Automate workflows to handle lifecycle management entities
Individually steer the state of managed entties

GRAZIE