Politecnico di Torino

IP Networks Operation

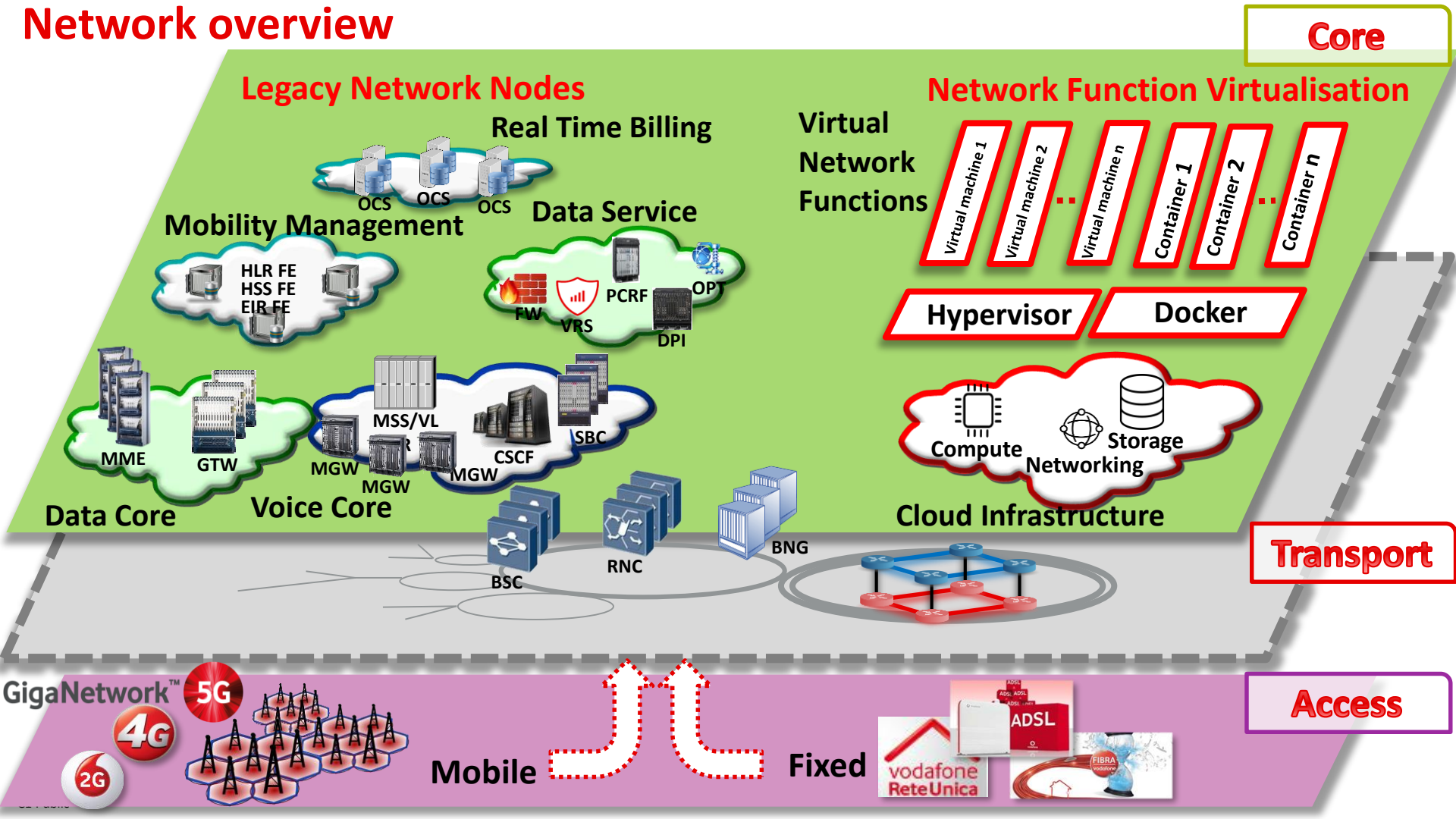
stefano.gollinucci@vodafone.com

Torino, January 10th, 2024

Agenda

1. Network overview: access, transport, core
2. IP backhauling, IP Core and underlying TX
3. IP MPLS and Segment Routing
4. SDN & NFV
5. IP Network Operation Challenges & Evolution
6. Wrap-Up and Q&A

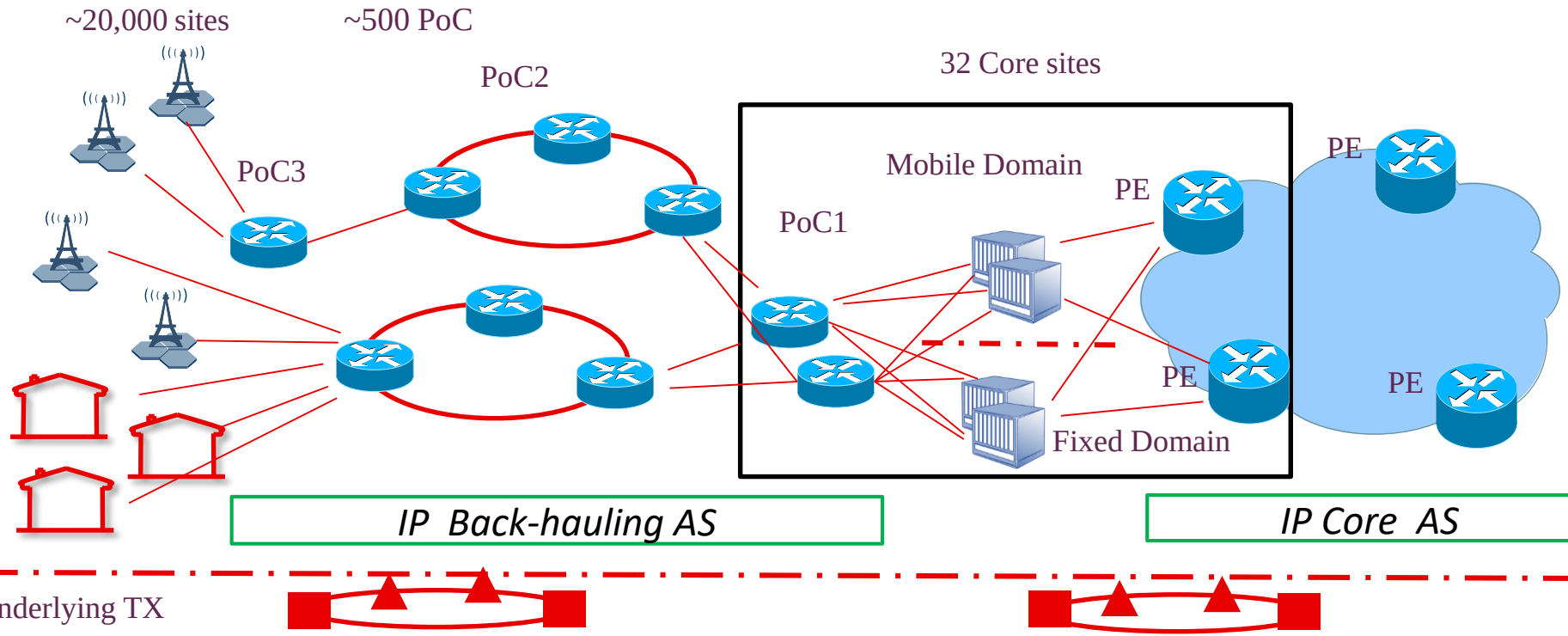
Network overview



Agenda

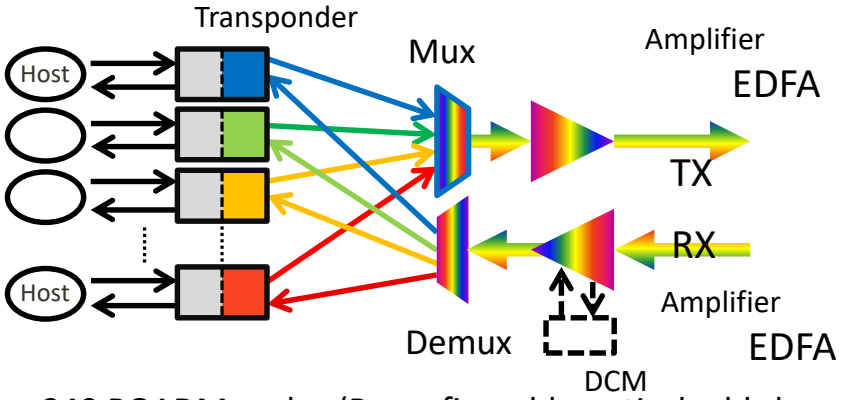
1. Network overview: access, transport, core
2. IP backhauling, IP Core and underlying TX
3. IP MPLS and Segment Routing
4. SDN & NFV
5. IP Network Operation Challenges & Evolution
6. Wrap-Up and Q&A

Transport network: mobile-fixed convergence on IP networks

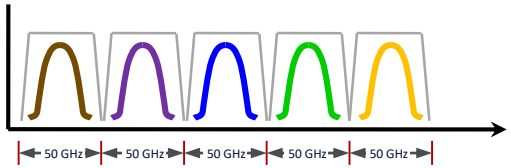


The underlying TX layer: DWDM

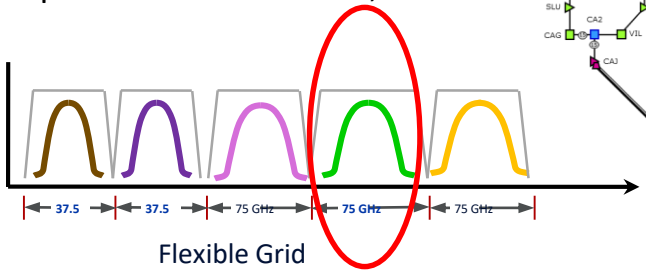
DWDM (Dense Wavelength Division Mux)
3rd window (1,550 nm)



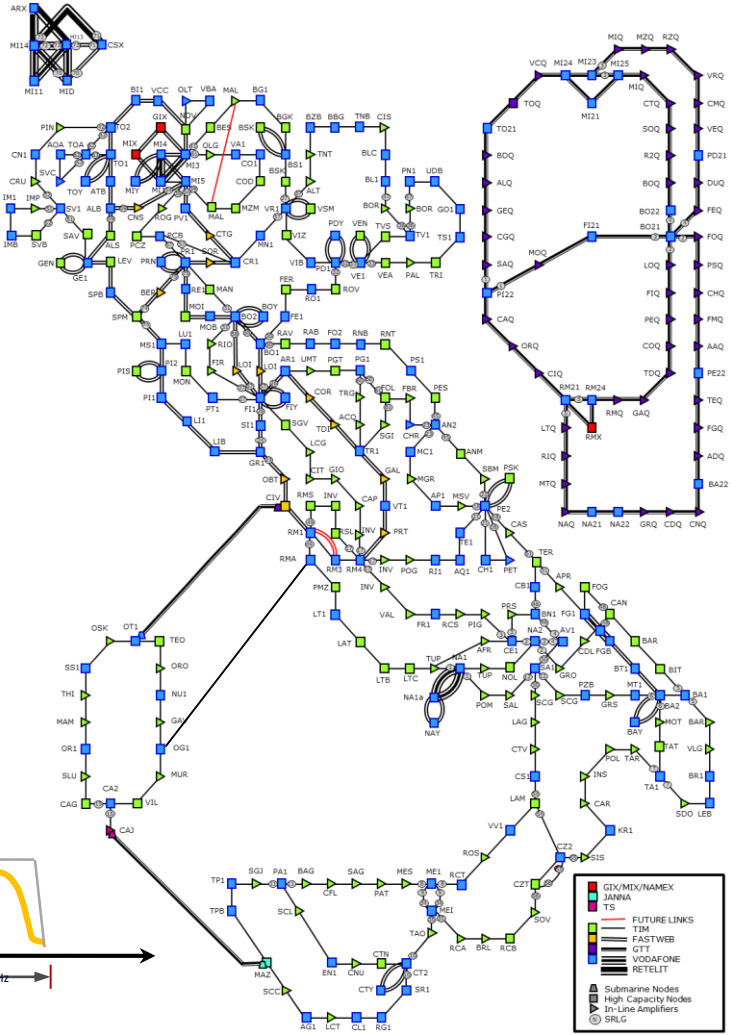
~240 ROADM nodes (Reconfigurable optical add-drop mux)
~140 regeneration nodes
FlexGrid technology with flexible channel size and frequency.
Standard 50Ghz and probabilistic shape modulation 75GHz,
Without fixed filter constraints



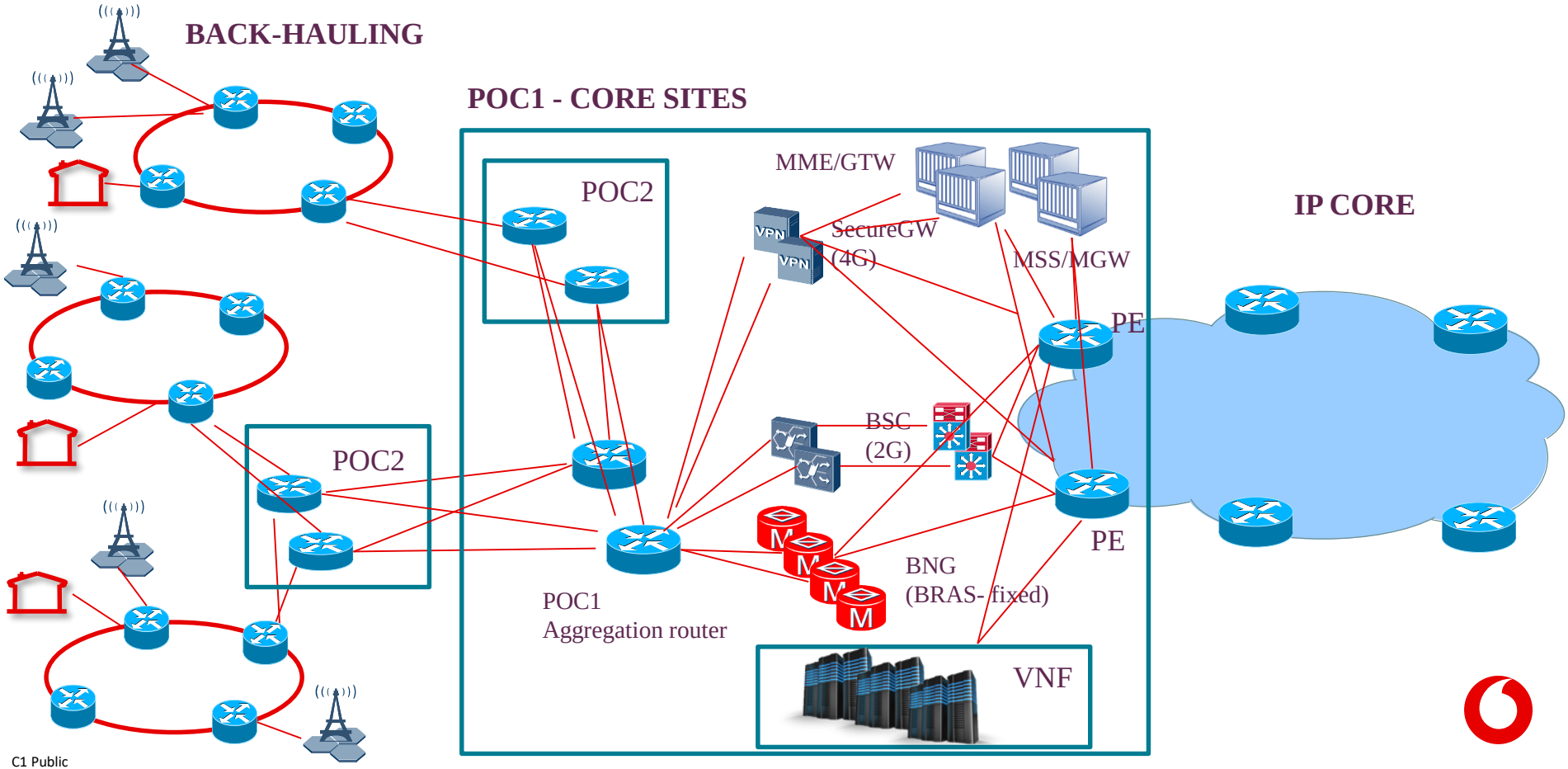
Fixed 50 GHz Grid



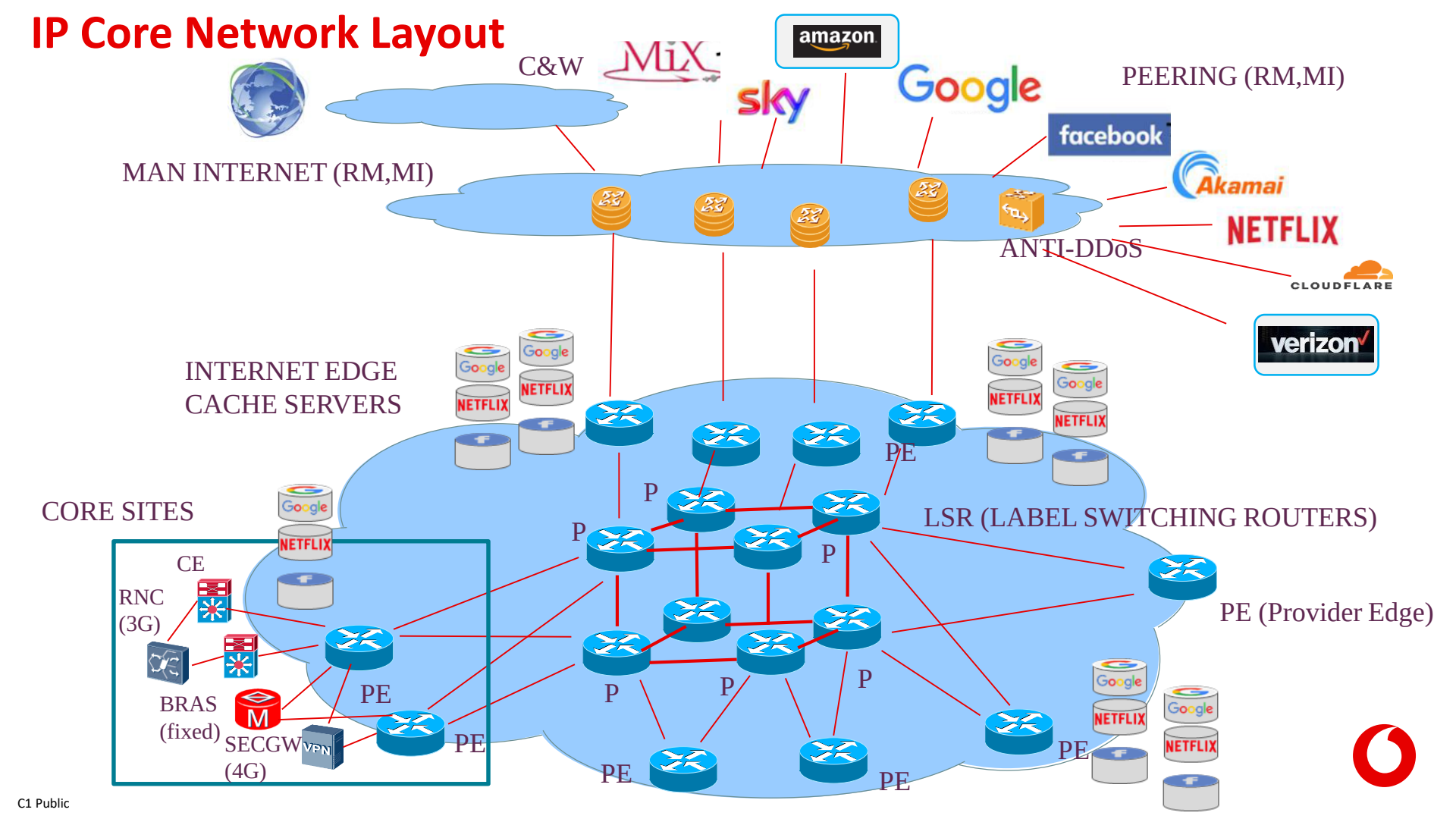
Flexible Grid



IP Core – Core sites overview



IP Core Network Layout



IP Core Network

The IP Core consists of:

- PE routers (Label Switching Edge) as ingress/egress modes of the IP MPLS Core
- P routers (Label Switching Router) in a two-layers fully redundant architecture
- Route Reflectors to manage iBGP sessions scalability issue
- Dedicated PEs towards Internet, with cache servers to increase efficiency with OTTs traffic and to announce eBGP routes
- Cache Servers to locally store internet contents and deliver them mitigating bandwidth consumption and improving latency
- Internet Peering points as well as interconnections with internatonal carrier in Roma, Milano
- Anti-DDOS systems

Agenda

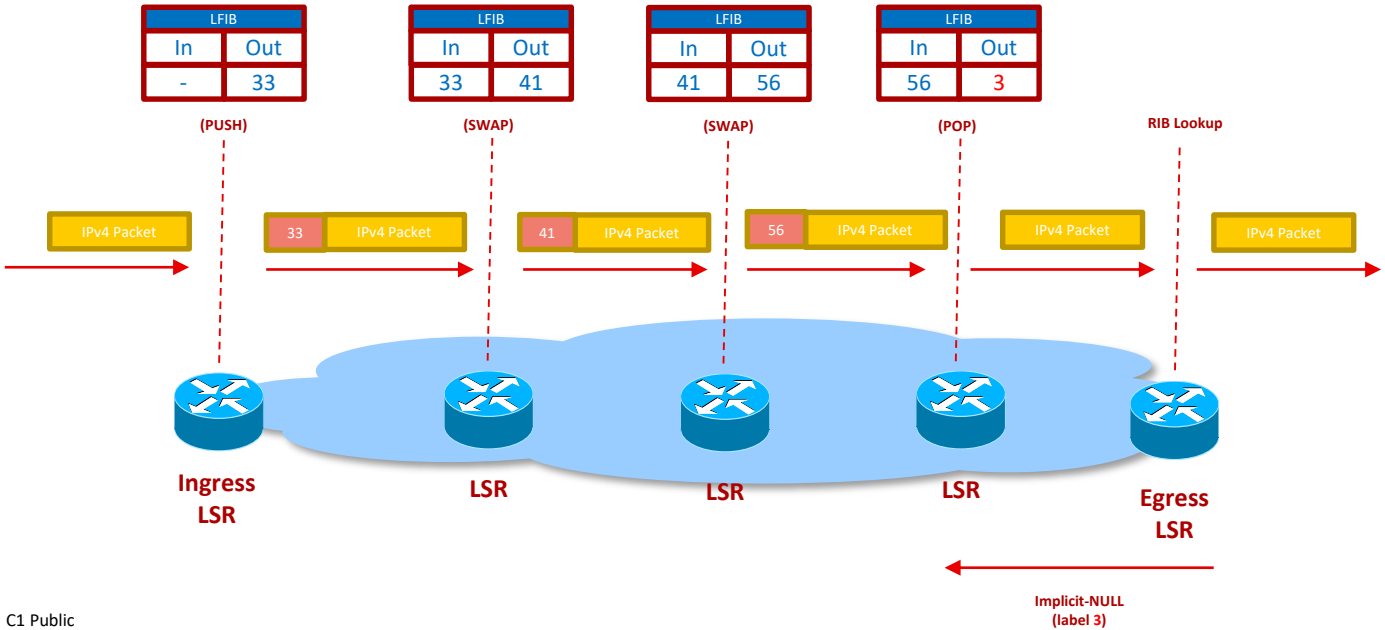
1. Network overview: access, transport, core
2. IP backhauling, IP Core and underlying TX
3. IP MPLS and Segment Routing
4. SDN & NFV
5. IP Network Operation Challenges & Evolution
6. Wrap-Up and Q&A

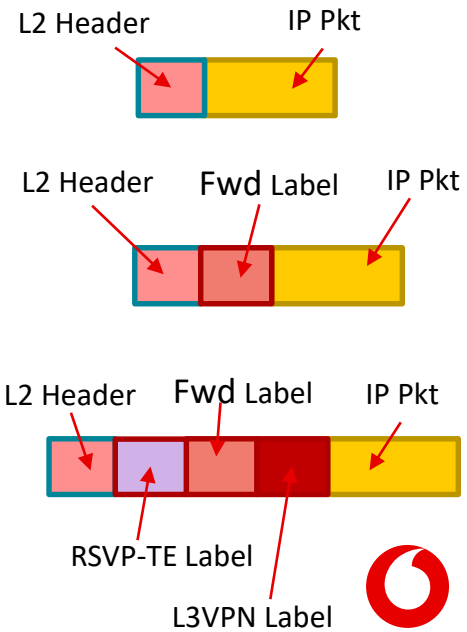
MPLS (Multi Protocol Label Switching)

- Different services with different service requirements (latency, bandwidth, reliability, etc.)
- MPLS makes it possible to segregate traffic flows through the creation of VPNs (Virtual Private Networks)
- MPLS implements FEC (Forwarding Equivalence Class), that is a group of IP packets which are forwarded in the same manner, over the same path, and with the same forwarding treatment. While in a plain IP network the FEC is determined at each hop, on an MPLS network the FEC is determined once, at the ingress of the network.
- Routing is based on distribution and swap of labels between routers rather than less efficient IP routing table lookup
- Traffic engineering is supported through the creation of MPLS tunnels or LSPs (Label Switched Paths)

Label Switching

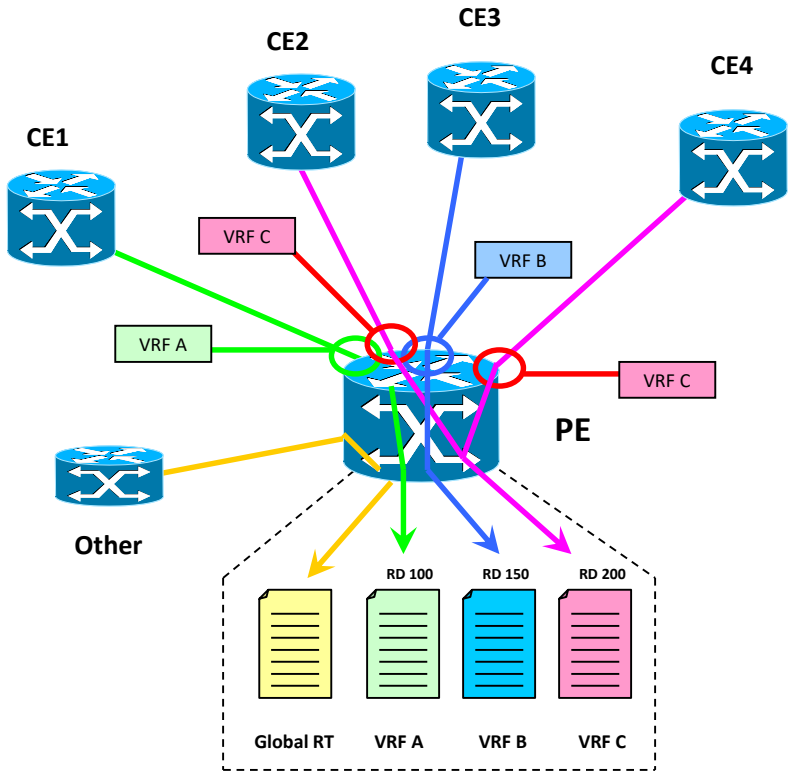
- At the ingress point Provider Edge (PE) routers ‘‘push’’ labels to IP packets of the specific traffic flow
- Intermediate Label Switch Routers (LSR or P routers), ‘‘swap’’ labels to select the path
- At the egress point PE routers ‘‘pop’’ the labels and and perform local Routing Information Base (RIB) lookup (Penultimate Hop Popping may be used to off-load PEs)
- Creation of VPN and traffic engineering are supported through L3VPN and RSVP-TE protocols respectively





VRF – VIRTUAL ROUTING AND FORWARDING

Provider Edge (PE) routers segregate traffic of different VPNs creating VRFs



MPLS PEs support the creation VRFs. Each **VRF** constitutes a separate routing and forwarding table, isolated from the others.

The "regular" routing table is called **Global Routing Table**, and by default routes/packets refer to this table when a VRF is not specified

VRF names have only local significance. Having the same VRF name among different routers does not mean the two VRFs are part of the same VPN.

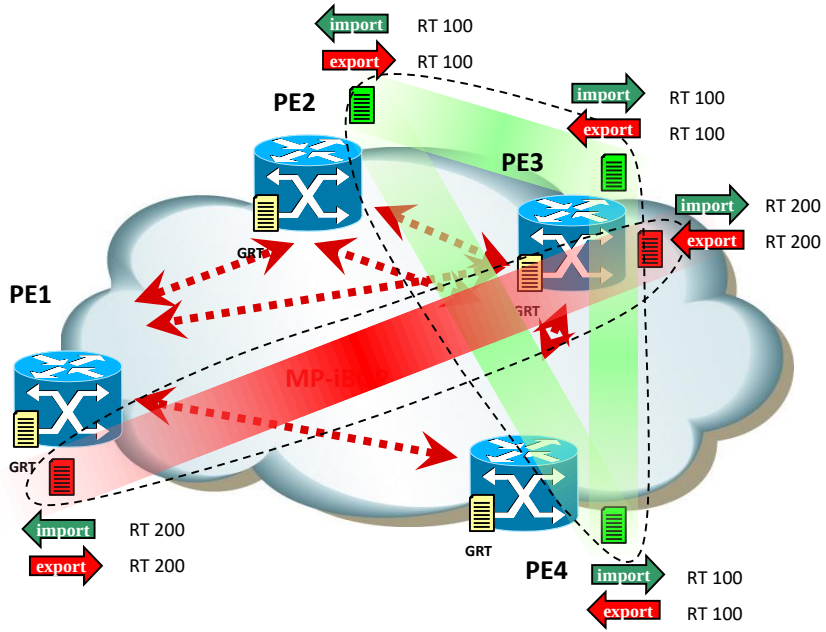
Each VRF has an associated (unique to the router) **Route Distinguisher (RD)**. The RD is used by MP-BGP to avoid confusing routes with overlapping IP addresses from different VPNs. It's not used to decide which route will be part of which VPN (the Route Target is used instead for this).
Even if it's common to use the same RD for "similar" VRFs on different PEs, this is not always the case.

Each physical/logical router interface can be associated (at most) to one VRF. By doing so that interface will be bound to the corresponding VRF. If a VRF is not specified, the interface will be bound to the Global RT.

One common situation is to have many CEs, each connected with a physical interface to the PE, with each interface associated to one of the PE's VRFs.

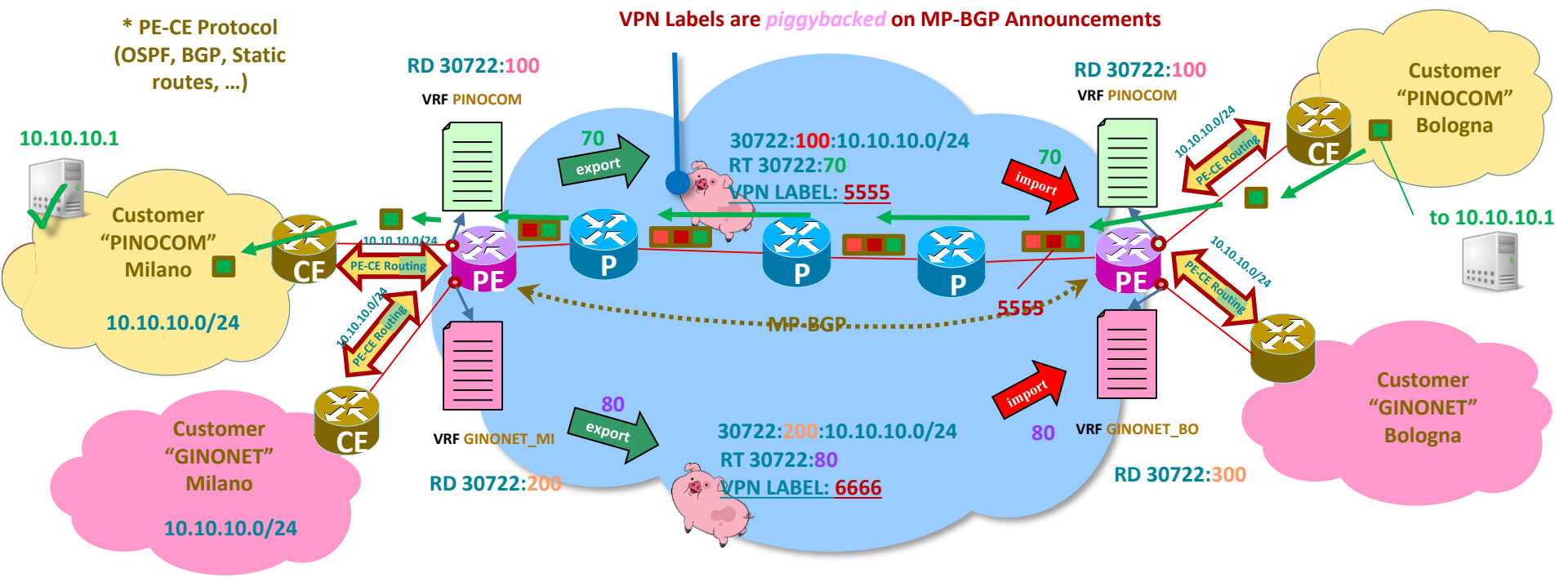
VPN – VIRTUAL PRIVATE NETWORK

MPLS supports the creation of L3VPNs using Multi Protocol – BGP (MP-BGP) extension in a very flexible way



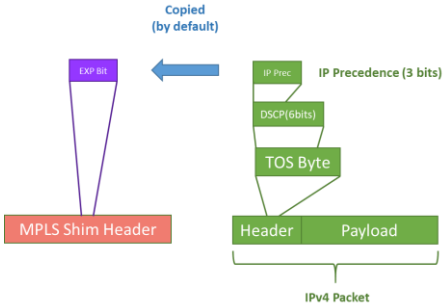
For example, using a RT value to denote a specific VPN, we can build full-mesh VPNs, completely isolated one from each other.

In this example we have **two full-meshed VPNs**, one associated with RT 100 and the other with RT 200.


* PE-CE Protocol (OSPF, BGP, Static routes, …)
VPN Labels are piggybacked on MP-BGP Announcements
RD 30722:100
VRF PINOCOM
10.10.10.1
Customer "PINOCOM" Milano
10.10.10.0/24
CE
PE-CE Routing
10.10.10.0/24
PE
P
P
P
PE
70
export
30722:100:10.10.10.0/24
RT 30722:70
VPN LABEL: 5555
MP-BGP
5555
70
import
RD 30722:100
VRF PINOCOM
10.10.10.0/24
PE-CE Routing
CE
Customer "PINOCOM" Bologna
to 10.10.10.1
10.10.10.0/24
PE-CE Routing
10.10.10.0/24
PE-CE Routing
CE
Customer "GINONET" Milano
10.10.10.0/24
80
export
VRF GINONET_MI
RD 30722:200
30722:200:10.10.10.0/24
RT 30722:80
VPN LABEL: 6666
import
80
VRF GINONET_BO
RD 30722:300
Customer "GINONET" Bologna
Multi-Protocol BGP
Route Distinguisher 4 byte – To manage IP address overlapping VPNv4 Address Family
Route Target – BGP Extended Community (4 byte) – To import/export routes in VRFs

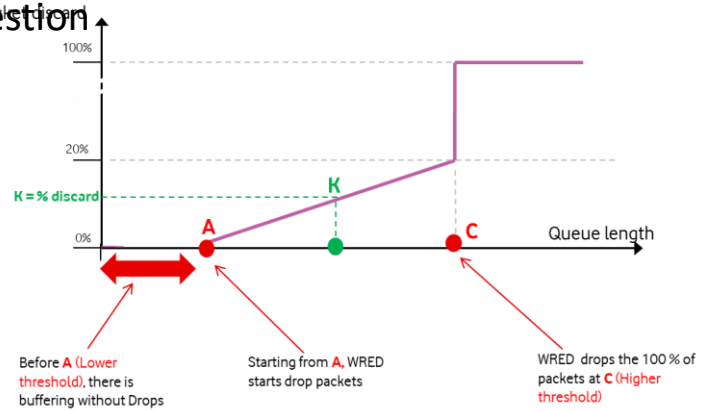
QOS

- QOS class mapping in MPLS networks done using EXP bits.



Class	DSCP	EXP bits	Queuing Algorithm	Scheduler
Control Plane	CS6, CS7	6,7	-	PQ
Voice	EF	5	-	PQ
Enhanced/Standard	AF31, AF32, AF41, AF42	1,2,3,4	WRED	PQ, CBWF, MDRR
Default	default	0	WRED	PQ, CBWF, MDRR

- Strict priority classes assigned to voice services and signaling, Default, Standard or Enhanced classes assigned to data draffic, with WRED (Weighted Random Early Detection) algorithm to handle congestion

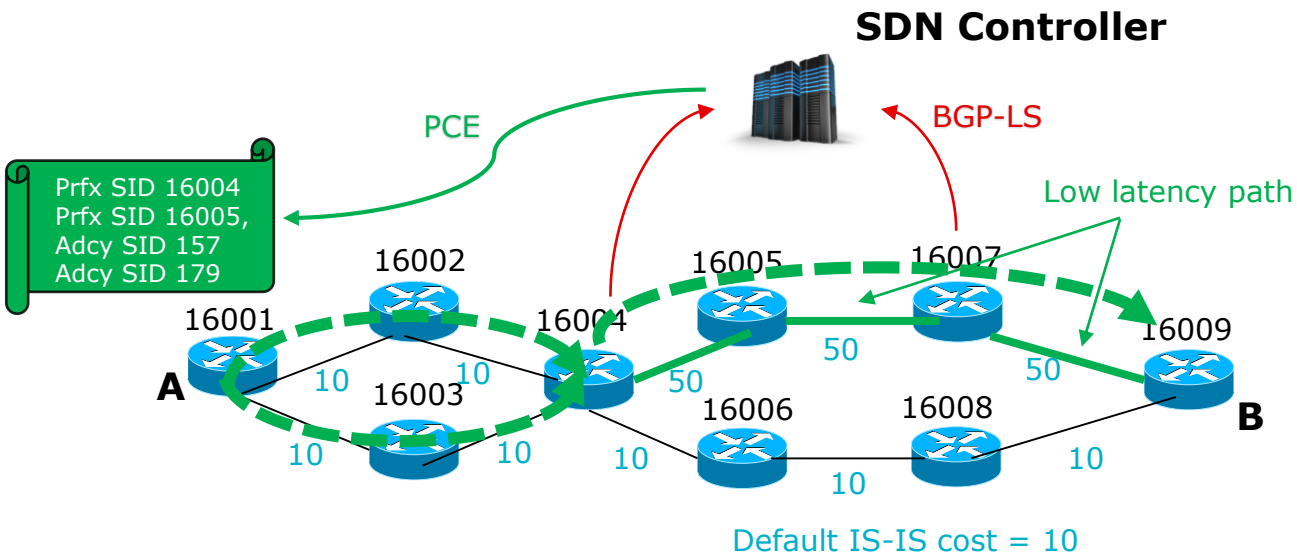


SEGMENT ROUTING

- MPLS networks face a growing complexity in terms of variety of service requirements and scalability of LDP databases and number of tunnels.
- Segment Routing (SR) is a source-based routing: the source injects into the network the set of instructions to follow the routing path and encodes it in the packet header as an ordered list of segments
- SR can be directly applied to the MPLS architecture and integrates with multi-service capabilities including Layer 3 VPNs (L3VPN). A list of segments is encoded as a stack of MPLS labels.
- Segment IDs are distributed using IGP (IS-IS, OSPF) extensions only:
  - Prefix Ids, which uniquely identify a node (default SRGB 16000-23999)
  - Adjancency IDs which locally identify a link towards a neighbouring router
- No need of LDP or RSVP-TE to allocate Segment IDs or program forwarding information
- Traffic protection against link and node failures is faster (<50 msec convergence)
- Egress peering traffic engineering using BGP Segment IDs
- Dual plane networks natively supported using Segment IDs anycast
- Plug&Play deployment thanks to interoperability with existing MPLS LDP dataplane

SEGMENT ROUTING and SDN (Software Defined Network)

Segment Routing enables centralised traffic engineering, agile programming source nodes only via Southbound Interface PCEP (Path Computational Element Protocol). No per flow state and signaling needed at midpoints and tail end routers



Application Engineered Routing

- Segment IDs and topology info fed into SDN controller via BGP-LS
- Low latency service request from A to B
- Controller computes path and programs A with list of segments
- Equal Cost Multi Path using node prefix SegmentID
- Low latency path selected using Adjacency SegmentID

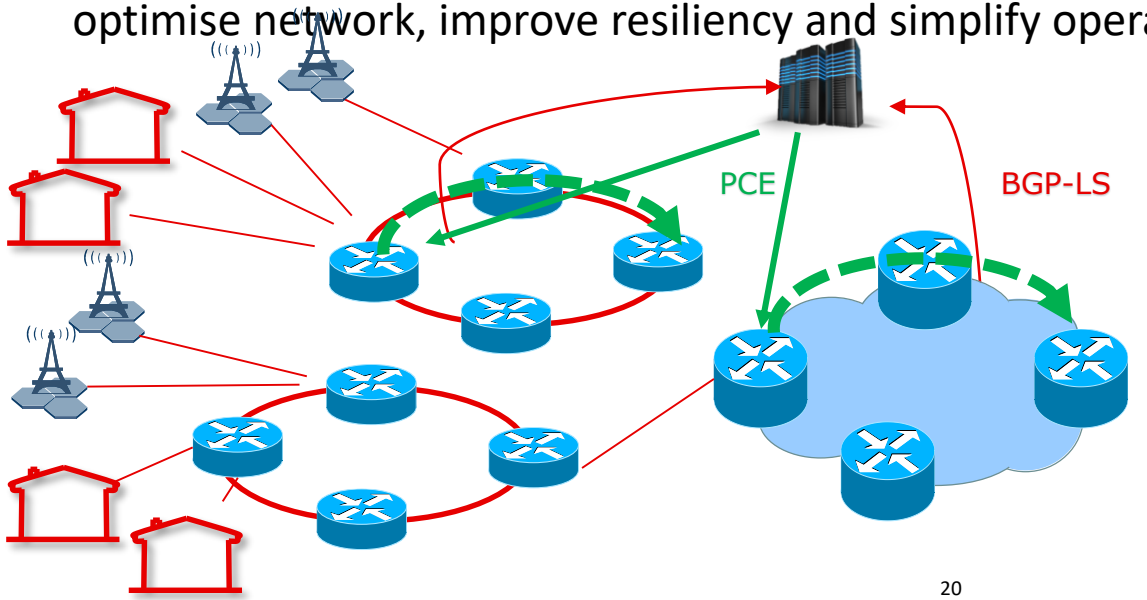
Agenda

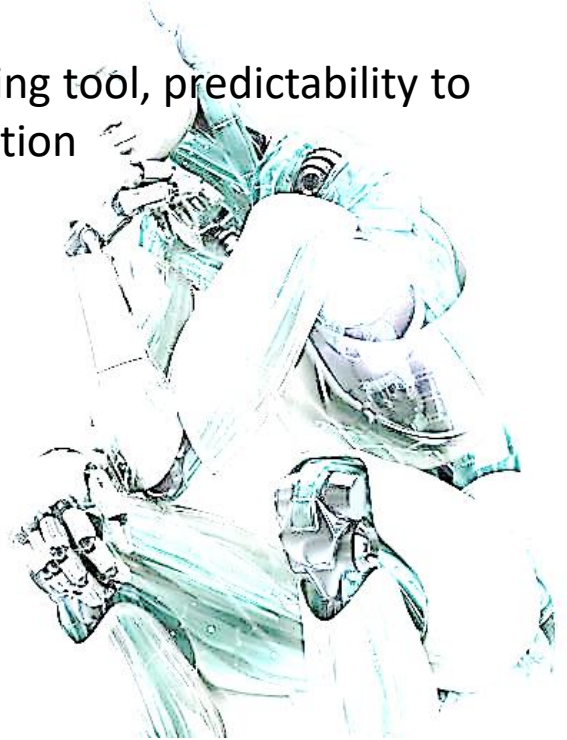
1. Network overview: access, transport , core
2. IP backhauling, IP Core and underlying TX
3. IP MPLS and Segment Routing
4. SDN & NFV
5. IP Network Operation Challenges & Evolution
6. Wrap-Up and Q&A

Software Defined Network

SDN exposes transport network resources, supporting Network As A Platform architecture:

- Programmability, policy control, SLA fullfilment to support network slicing and service differentiation demand (capacity, latency, jitter, etc.)
- Automation, on line performance monitoring and planning tool, predictability to optimise network, improve resiliency and simplify operation





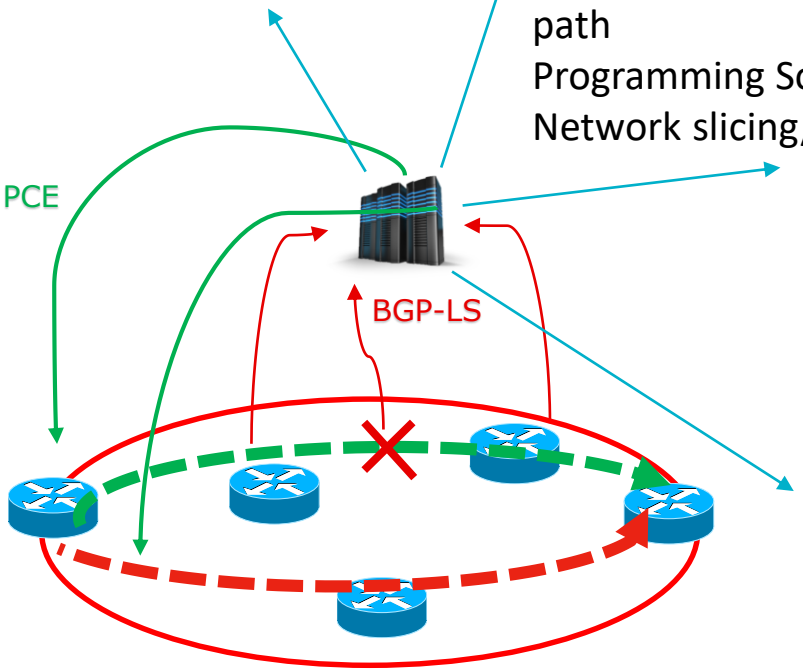
Software Defined Network: use cases

Network and services autodiscovery:

Topology Discovery using BGP-LS

Dynamic network inventory

3° Party nodes control



Service instantiation and provisioning

Service modeling using NETCONF/YOUNG

Computation of SLA adhering path and protection path

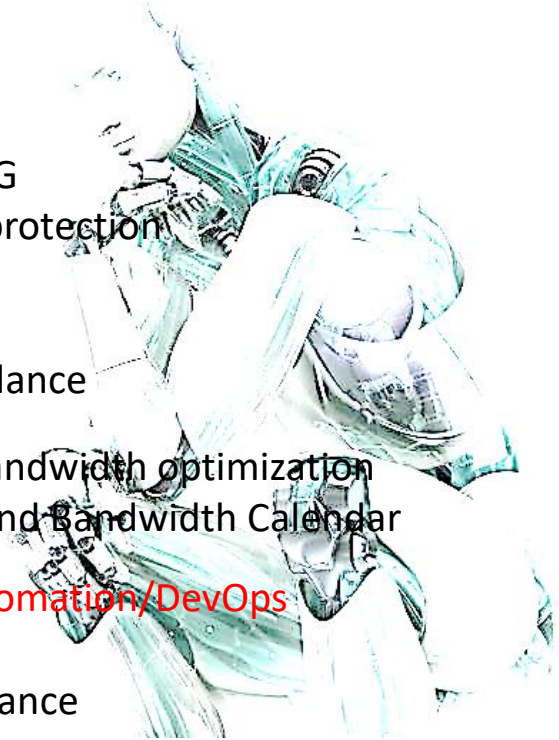
Programming Source nodes via PCEP

Network slicing/Disjoint Path/Path Avoidance

Network Optimisation

Capacity planning and bandwidth optimization

Bandwidth on demand and Bandwidth Calendar



Programmable automation/DevOps

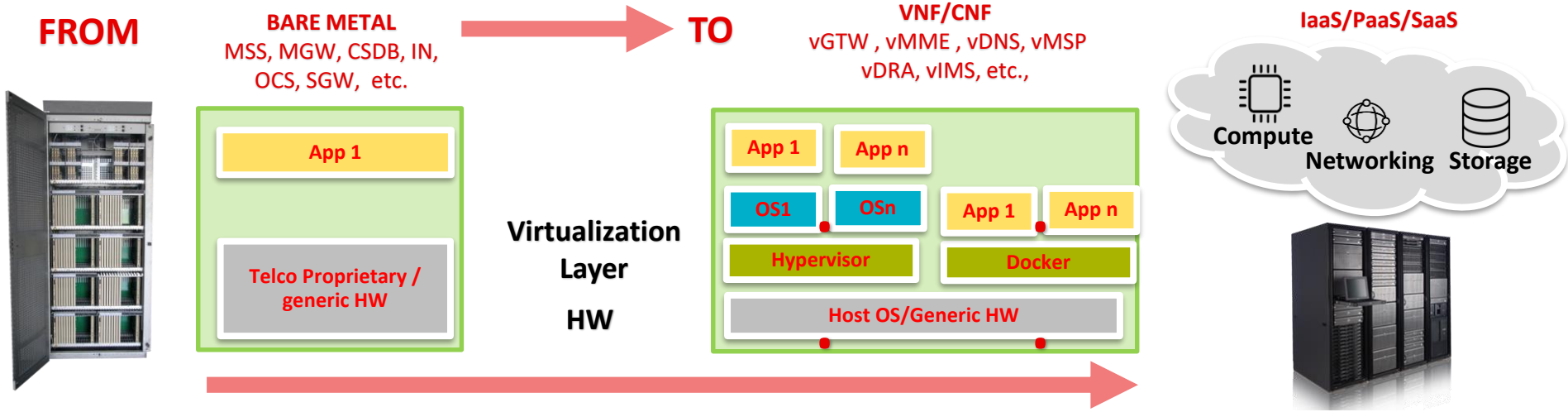
Anomaly detection

Predictive maintenance

What-if analysis

Dynamic congestion detection and alternative path creation

Network Function Virtualization



- **Bare metal** solutions have been progressively replaced by **Virtual Machines**, software instances complete of their own operating system, memory and other resources, co-located on a physical machine through an **hypervisor**
- **Containerized** network functions are executable images with software applications and their dependencies, sharing the same operating system using an orchestration platform, like **Kubernetes.** Containers are more lightweight and portable than VMs and support microservices
- **Faster delivery**, **scalability**, **self-healing** mechanisms, better **asset utilization** and **pay per use** are among cloud benefits
- Resiliency: **Infra and Geo Redundancy**, **High Availability**, **vMotion**

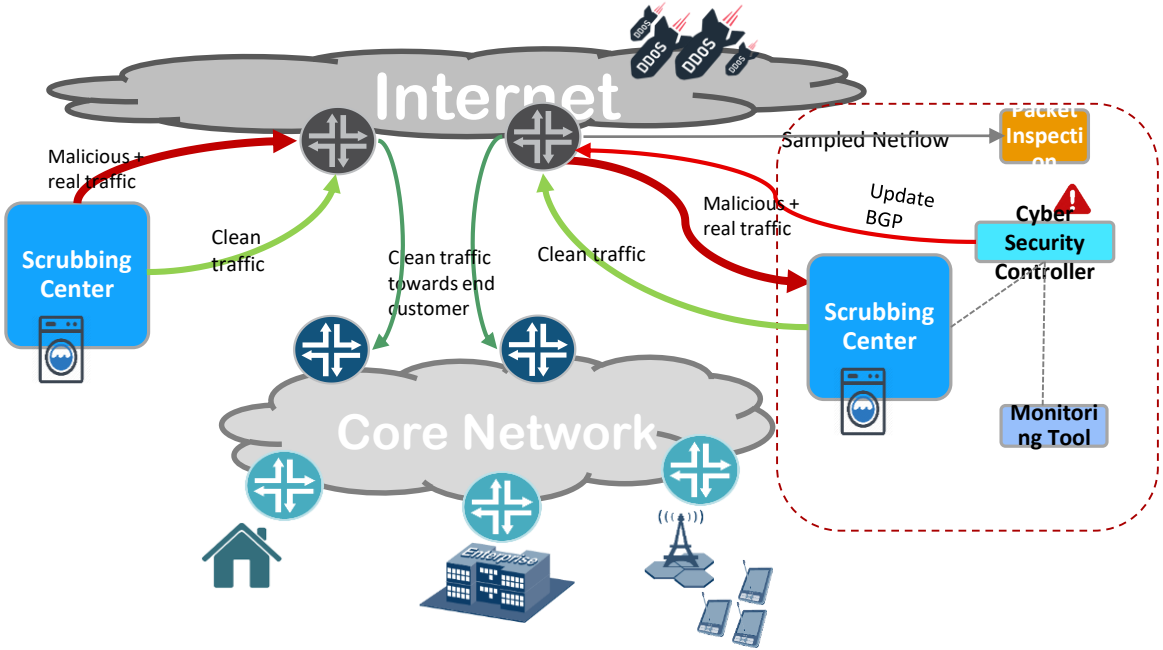
SDN and NFV

- SDN and NFV do not require each other, but:
- Besides the advantages in terms of efficiency and flexibility to cope with a rapidly changing demand, NFV adds complexity to IP transport in managing the multiple traffic flows.
- SDN (combined with SR) provides a natural way to route packets between VNFs/CNFs associated to manifold services
- Virtualization of routing functions, elastical deployment of VNFs/CNFs, geo-redundancy or high availability mechanisms to re-route traffic from a data center to another, can be simplified through SDN and automation
- Moreover, 5G is designed to be a multi-service network, where ideally the physical network is «sliced» in multiple isolated logical networks on a per service basis, each network slice including the network functions and the transmission resources needed to meet the service requirements
- As a future step, Cloud-RAN will enable virtualization of radio base band processing, and locally deployed MECs (Multiaccess Edge Computing) will enable low latency, location aware new services. Network slicing through SDN and NFV will ensure per service performance levels and isolation.

Agenda

1. Network overview: access, transport, core
2. IP backhauling, IP Core and underlying TX
3. IP MPLS and Segment Routing
4. SDN & NFV
5. IP Network Operation Challenges & Evolution
6. Wrap-Up and Q&A

IP security challenge: DDoS attacks



- DDoS (Distributed Denial of Service) malicious attempt to disrupt service using “Botnets”, networks of compromised “zombie” computers
- Common DDoS attack strategies exploit different techniques to overload target servers with flooding UDP, ICMP (ping) traffic, or causing disruption attacking NTP servers or DNS servers.
- *Anti DDoS systems aim is to detect the attack, to scrub the malicious traffic*

IP security challenge: piracy and vulnerabilities

- **BGP Hijacking** – whenever an operator announces a more specific route (i.e. /24) by mistake or aiming at illegal scope the traffic is deviated. *Operators detect prefix announcements on routers which are visible on public platforms and can react by announcing a more specific network*.
- **Internet Piracy**: illegal broadcasting of TV or sport events or other illegal contents from IP addresses have to be blocked in a timely manner according to local regulations. *Operators can implement automatic scripts to receive via BGP the suspect addresses and deviate their traffic to null route.*
- **Zero-day vulnerabilities**: attackers exploit software bugs which make routers or firewalls vulnerable while patches are not yet available. *Patching process has to be implemented to implement patches or work-around in a timely manner*
- **Malicious logical access** to the network, aimed to cause damage or to steal information, dealt with *2FA (Two Factor Authentication) for remote access , PAM (Privileged Access Management) systems to store and manage privileged user passwords, and mitigated by hardening and patching policies.*

IP security challenge: operational complexity

- **Automation**: whilst automation is a key factor to minimize the probability of execution errors, however applying massive changes via automatic script from a single controller without careful testing is in itself a risk of critical outage.
- **Deadlock scenarios**: the combination of loss of IP connectivity and the restrictions implied by PAM systems could weaken or be an impediment to the ability of operation teams to apply a remedy, which has to be guaranteed in all circumstances.

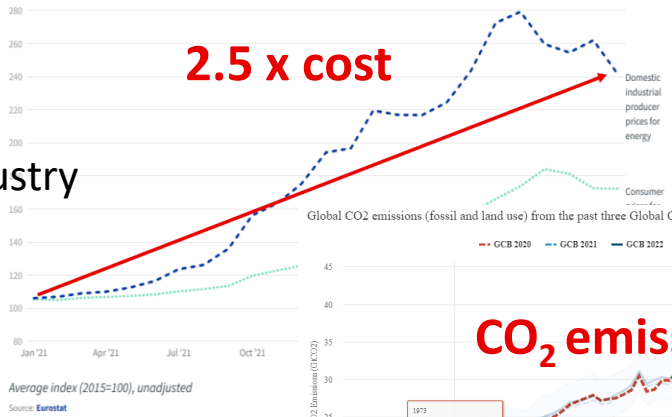
Traffic trend, capacity management and low latency applications

- Data traffic growth is both technology and market driven
- Non linear effects play an increasing role in traffic profiles: streaming of special events such as football matches, simultaneous software upgrade downloads, gaming platforms updates, etc.
- IoT and 5G applications in general imply very low latency reqs

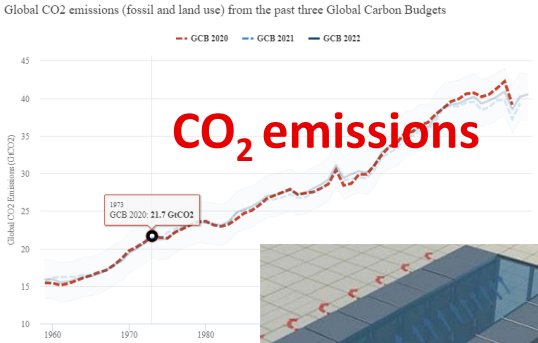
- Cache servers , direct peering points
- QOS!
- SDN capabilities to support and enhance capacity planning processes

Energy Puzzle

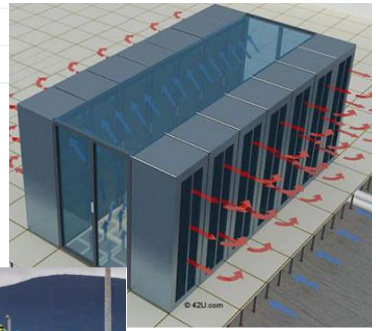
- Energy costs unsustainable in the medium term
- Zero-impact energy policy a priority for the industry



- Energy from renewable sources
- Energy efficiency :
  - Shut down of unused hardware
  - Adoption of energy efficient hardware
- Advanced automation use cases
  - Automatic shut down/switch hardware resources according to traffic or capacity
  - Efficient software!
- Cooling efficiency
  - Free cooling, cold mass reduction in rack cooling, liquid cooling, etc.
  - futuristic solutions: boiling pools, submarine data centers!

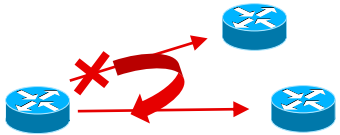


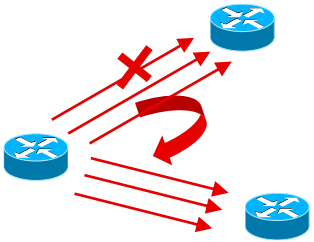
DCs absorb up to 2MW each



Resiliency

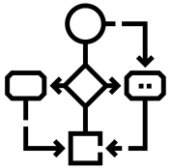
- **Redundancy mechanisms** supported by MPLS, enhanced by SR, automated via SDN, taking care of operational aspects: active sharing vs primary/secondary, minimum link
- **Risk analysis** on likelihood of double failures, critical components failure rate, expected time to recovery.
- **Disaster recovery** Extraordinary events like heartquakes, flood, accidental fire may seriously impact service continuity. Specific recovery plans have to be designed and periodically tested to ensure Business Continuity





Automation in Operation

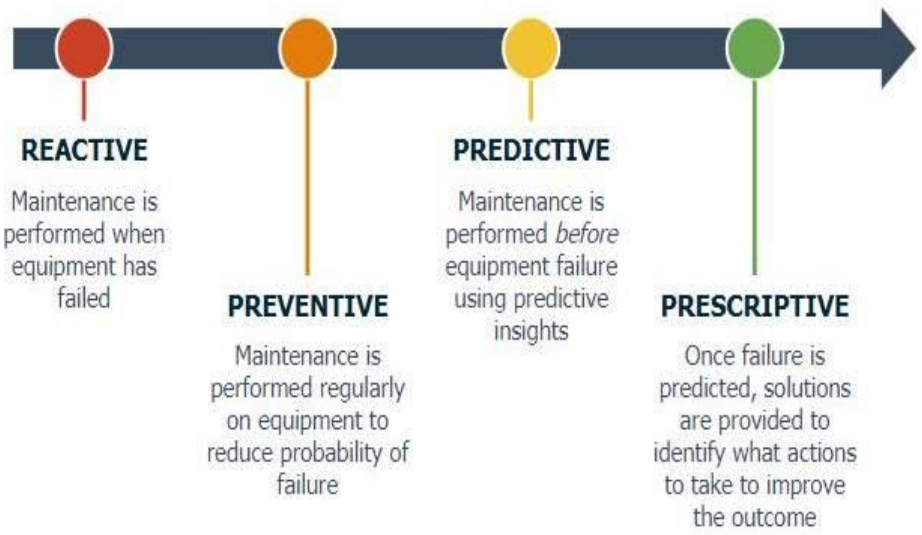
RPA



WORKFLOW AUTOMATION

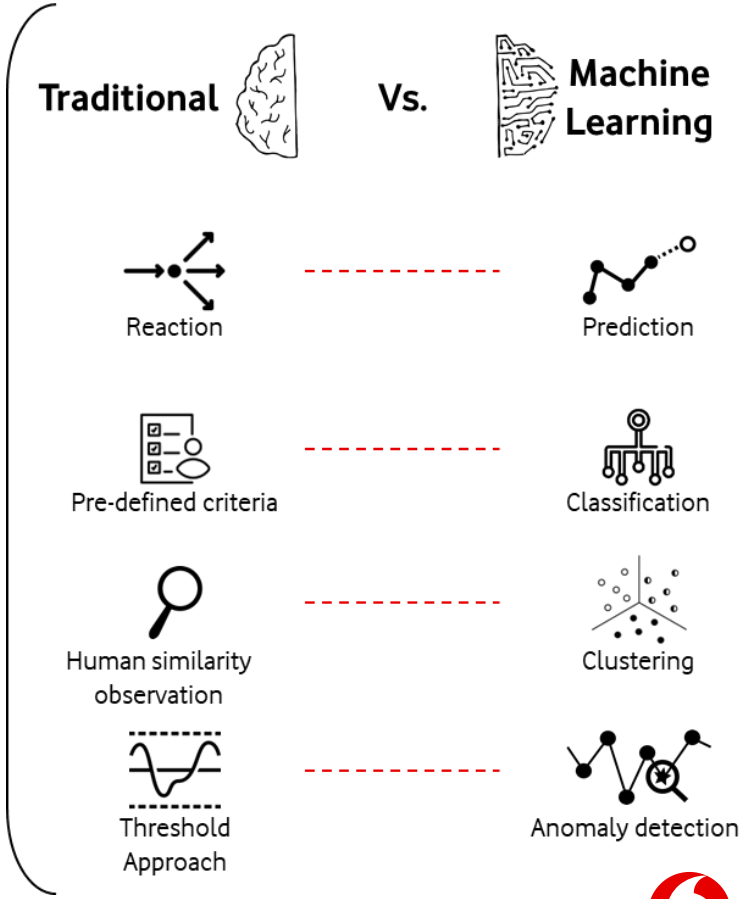
- Monitor alarms and trigger incident management
- Self-healing and automatic trouble-shooting
- Preventive maintenance and healthchecks
- Automatic inventory
- Automatic massive configuration and provisioning tasks
- Support or execute repetitive tasks

From Preventive To Prescriptive



Big Data

Machine Learning



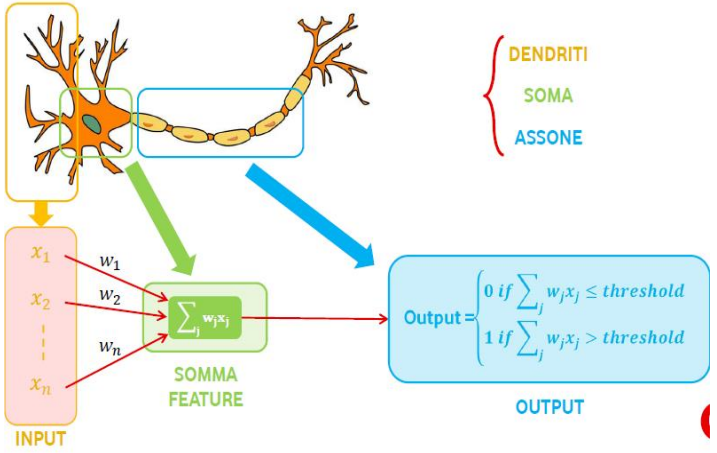
Predictive Models

Deep learning/machine learning algorithms (Neural Networks, Random Forest, Vector Machine, Logistic Regression, etc.) are able to correlate events, identify patterns and make predictions

Precision, Recall, AUC KPIs used to estimate suitability to provide reliable predictions

Algorithms need training and fine-tuning.

Training could take advantage on expert hints rather than relying on a black box approach



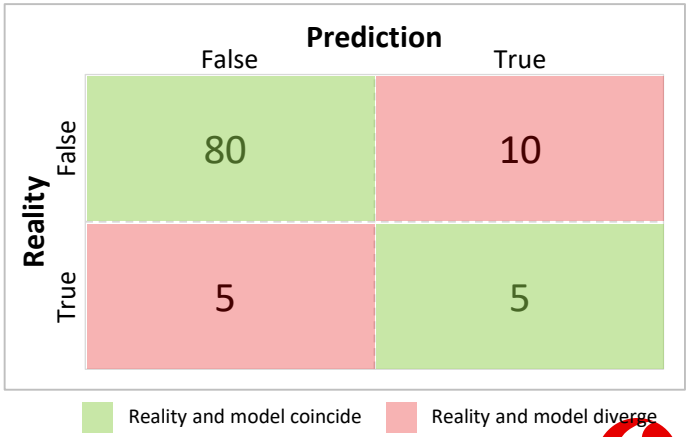
PRECISION

$$\frac{\text{Nr. of events correctly predicted TRUE}}{\text{Nr. Of events predicted TRUE}} = \frac{5}{15} = 33\%$$

RECALL

$$\frac{\text{Nr. of events correctly predicted TRUE}}{\text{Nr. of events actually occurred TRUE}} = \frac{5}{10} = 50\%$$

Confusion Matrix



Agenda

1. Network overview: access, transport, core
2. IP backhauling, IP Core and underlying TX
3. IP MPLS and Segment Routing
4. SDN & NFV
5. IP Network Operation Challenges & Evolution
6. Wrap-Up and Q&A

In summary:

- IP networks are a key component of telco networks, they are growing in size and complexity, a growth that is going to pose considerable challenges in manageability, let alone security aspects.
- The flexibility of MPLS based networks, simplification with Segment Routing and programmability through SDN become an indispensable aid for both design and operation.
- IP technologies do require from engineers high profile, very specialized skills. Nevertheless understanding the needs and the inclination to cooperate with experts from other areas, as well as the unrelenting thirst to learn new things will be the ultimate key for success
- And.. despite appearances, operating a network offers you a lot of pride, adrenaline, and fun!!


Thank you!