

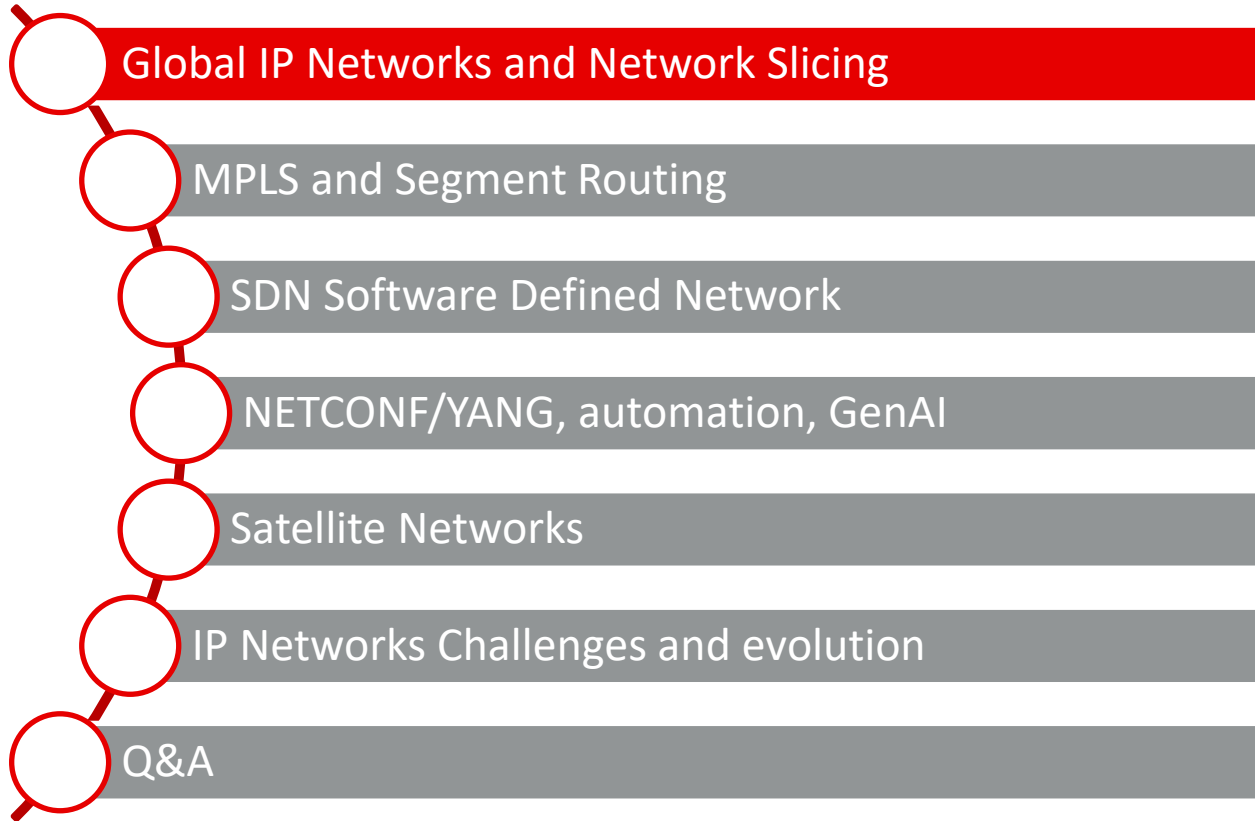


Politecnico
di Torino

IP NETWORKS OPERATION



Agenda

- 
- Global IP Networks and Network Slicing
 - MPLS and Segment Routing
 - SDN Software Defined Network
 - NETCONF/YANG, automation, GenAI
 - Satellite Networks
 - IP Networks Challenges and evolution
 - Q&A



Global IP network

International IP backbone

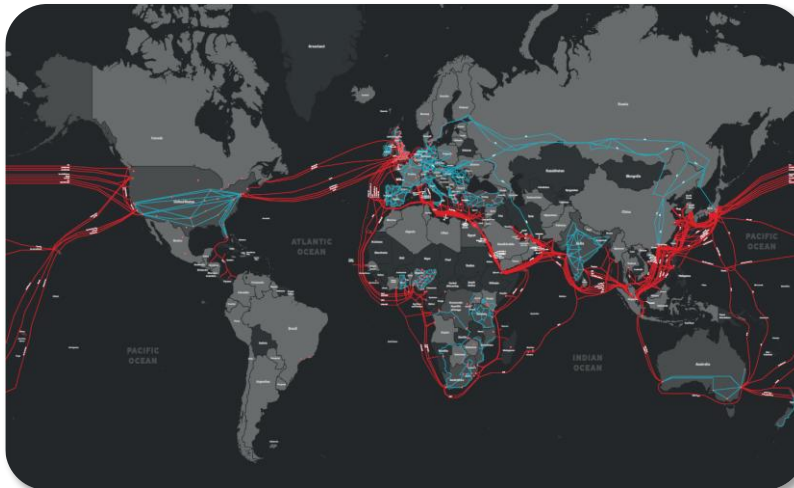
International core connectivity to Vodafone Operating Companies, Datacenters, and Partner Networks

Managed Service Provider

International MPLS VPN services to Enterprise customers

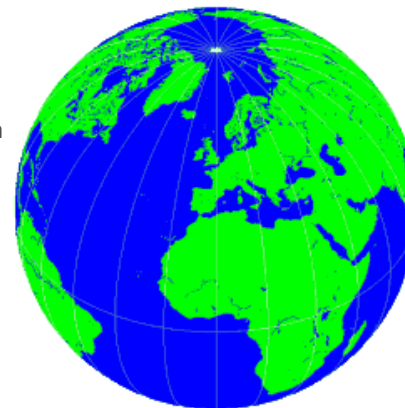
Internet Transit

Internet services to Vodafone Operating Companies, Partner Networks, connection to peering partners and Content Providers

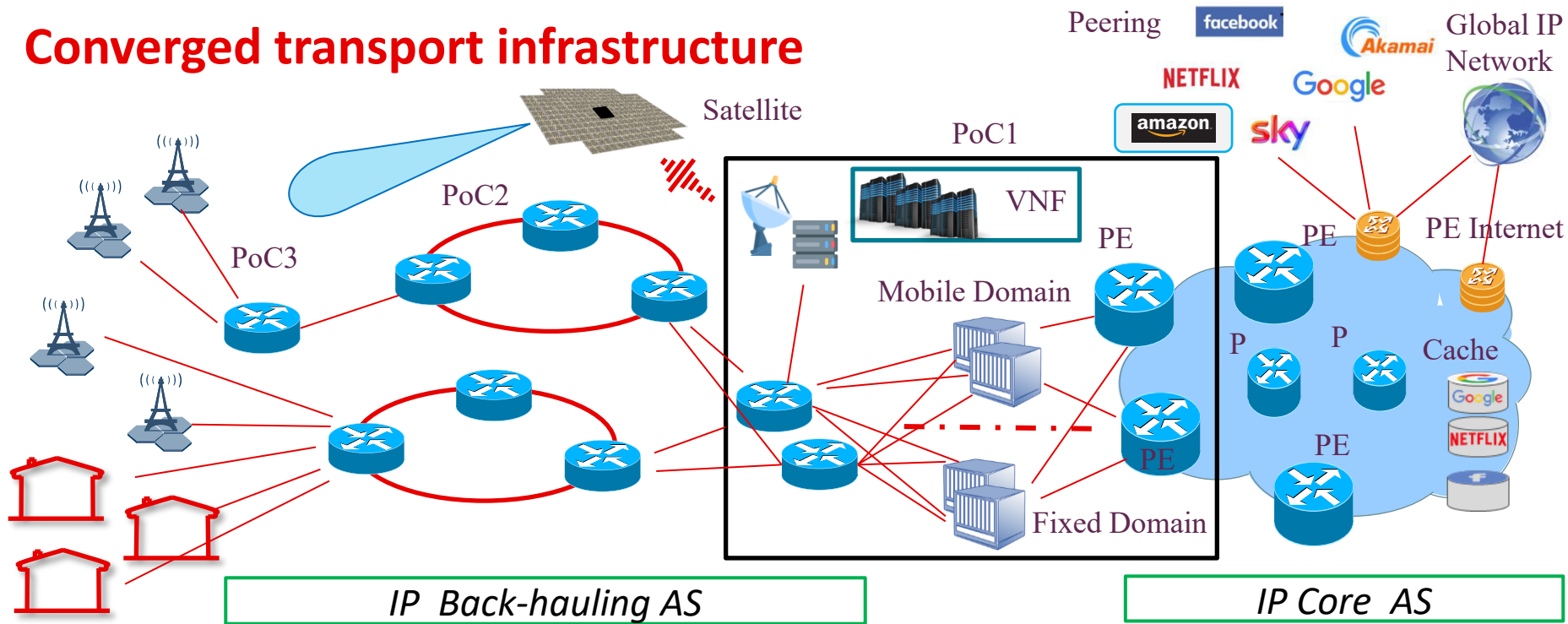


- ❖ 5 Continents, **200+ POPs** in 45 countries
- ❖ **220 +** International carriers
- ❖ **190** Submarine cable landing stations
- ❖ **14000+** Enterprise Customer Globally

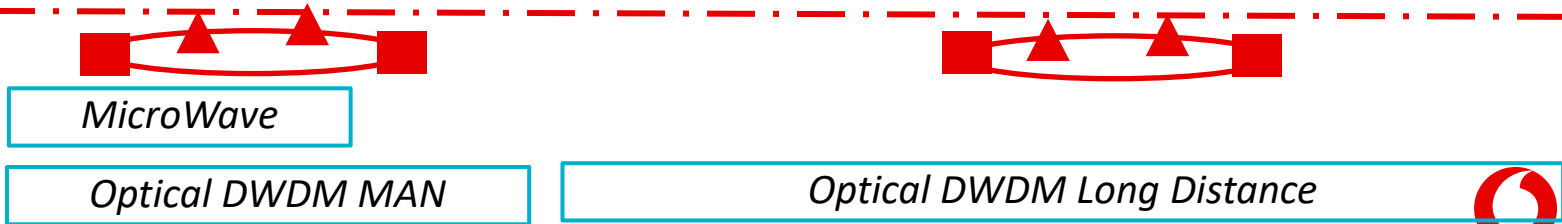
- ❖ **15 VF Operating Companies:** Europe, Asia, Africa
- ❖ **45+ Partner markets** globally



Converged transport infrastructure

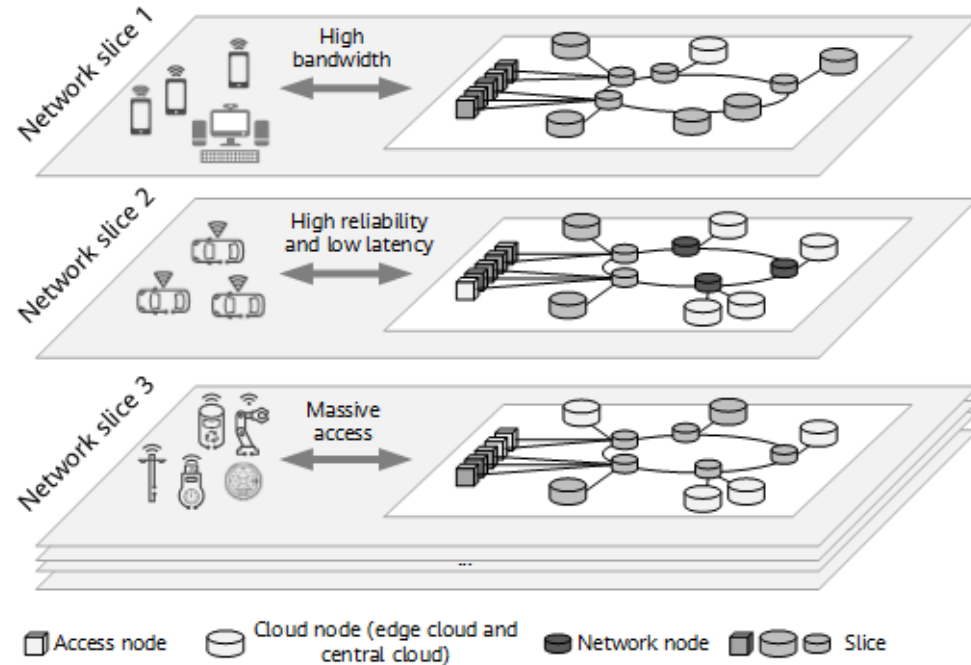


Underlying TX



Network Slicing and Network As A Service

- IP networks deliver a variety of connectivity services at a global scale.
- The «Network Slicing» architecture allocates resources on a per service base, creating customized virtual networks fitting the specific service requirements
- As cloud computing spreads in the industry, as Network Function Virtualization spreads in datacenters, «Network Slicing» meets the concept of «Network As A Service», that is exposing network resources to set up an integrated end to end service architecture.
- Flexibility, simplification and programmability of IP networks become essential ingredients in network operation



Agenda

- Global IP Networks and Network Slicing
- **MPLS and Segment Routing**
- SDN Software Defined Network
- NETCONF/YANG, automation, GenAI
- Satellite Networks
- IP Networks Challenges and evolution
- Q&A



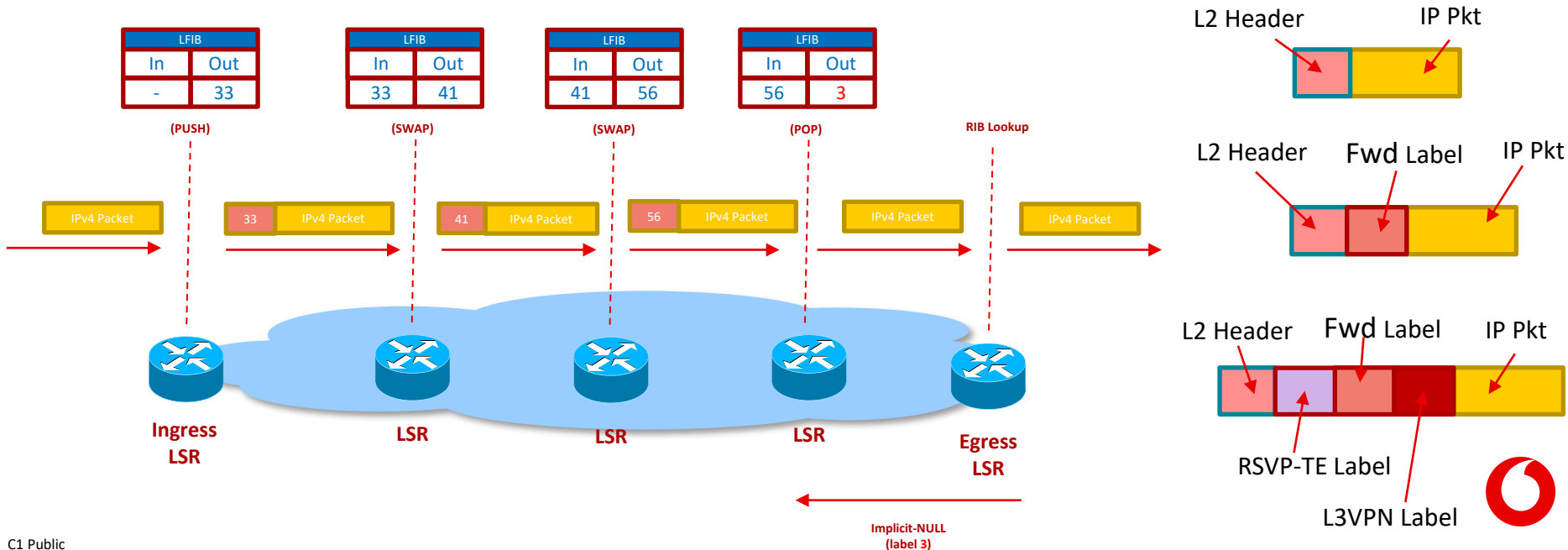
MPLS (Multi Protocol Label Switching)

- 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)



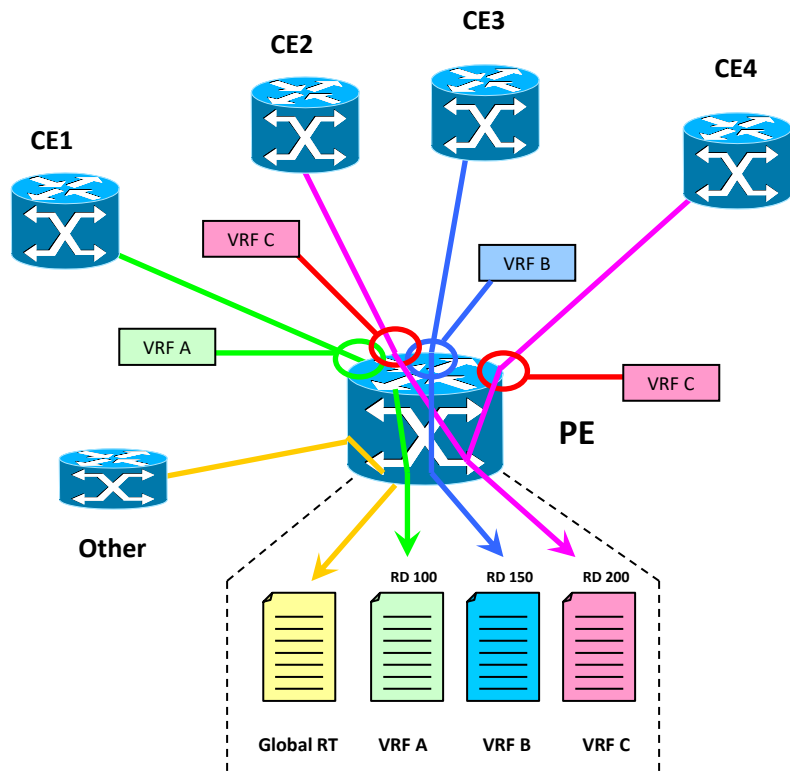
Label Switching

- 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 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.

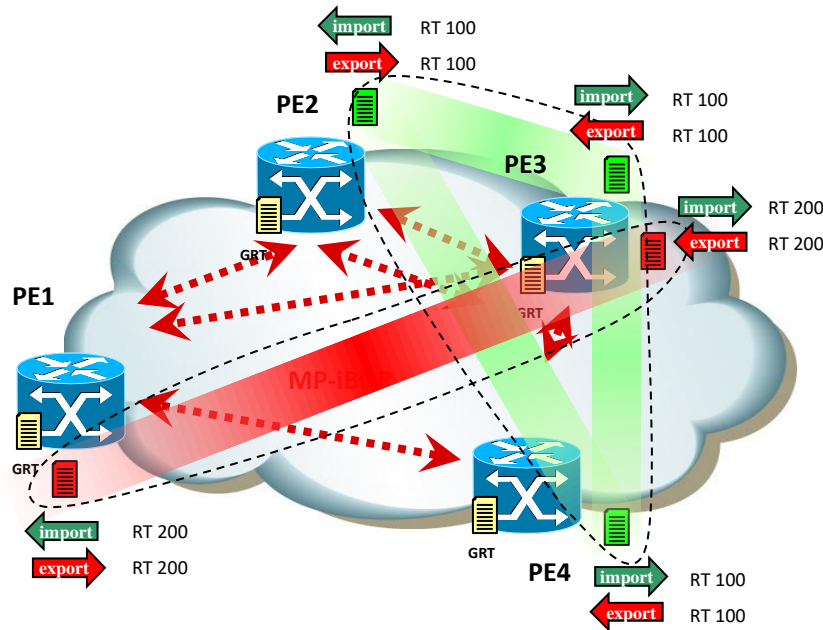
Each physical/logical router interface can be associated (at most) to one VRF. By doing so that interface will be bound to the corresponding VRF. If a VRF is not specified, the interface will be bound to the Global RT.

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.

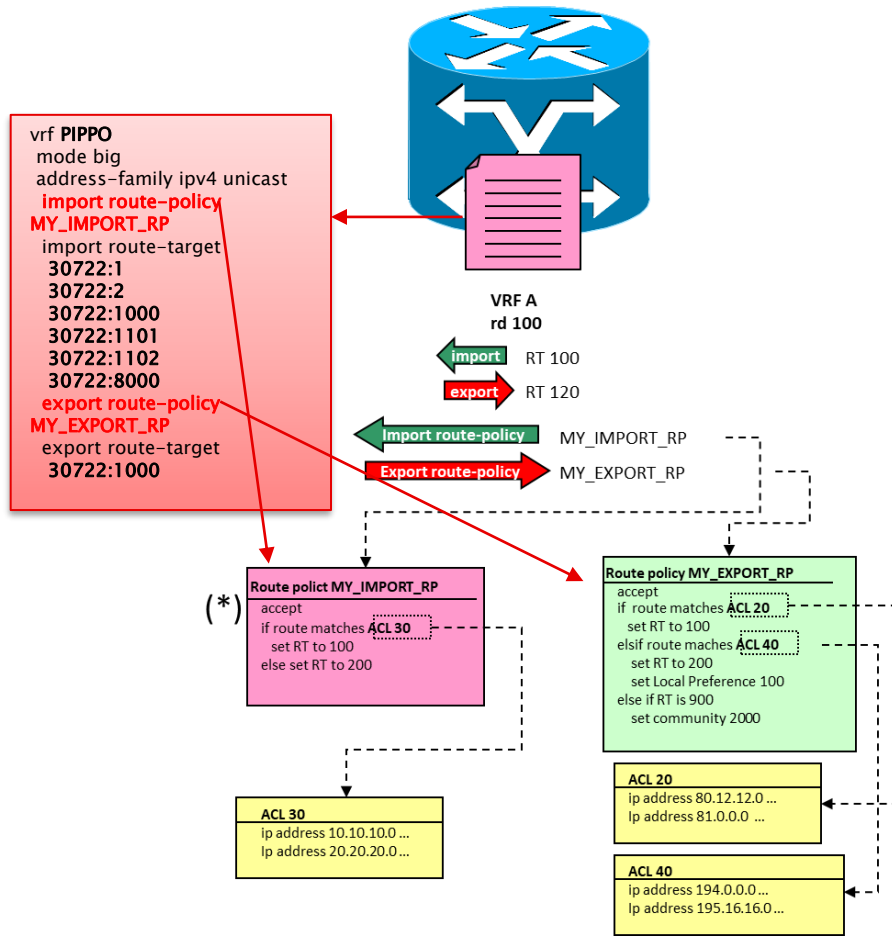


VRF and Routing Policies

Besides specifying the list of import and export, the VRF associates an **Import Routing Policy** and an **Export Routing Policy** to a Route Map

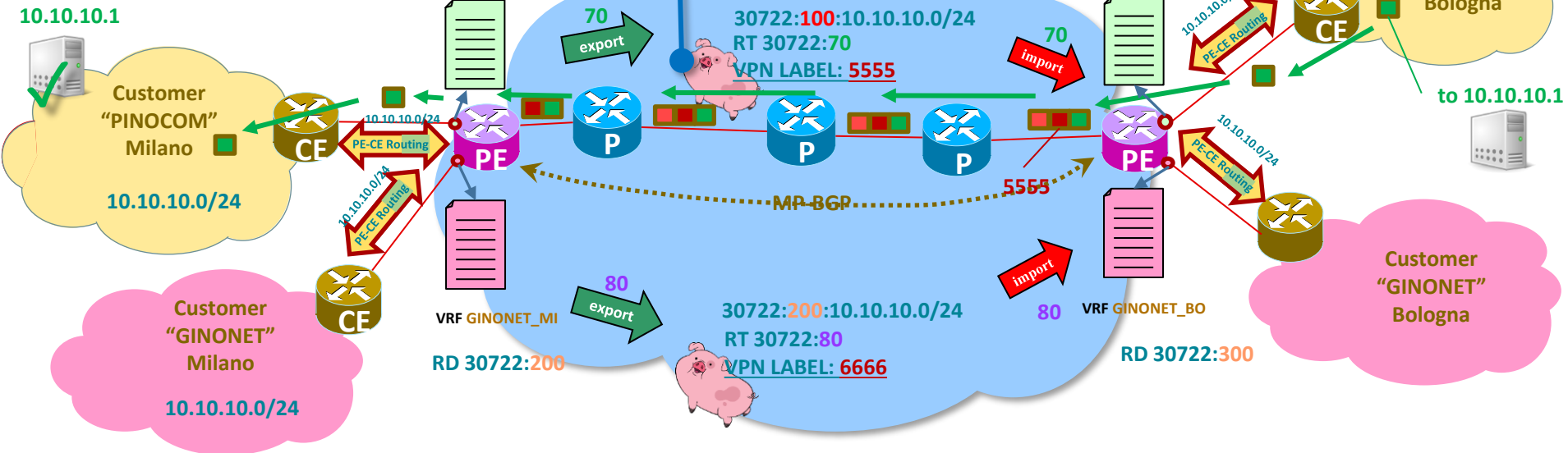
A **Route Map** is an algorithm which scans BGP routes and applies pre-defined criteria to accept or route traffic, like ACL, local preference mechanisms, etc.

The Route Policy syntax is similar to a programming language and allows to manage criteria to accept or propagate BGP routes, define criteria to associate a FEC to traffic flows, routing criteria, re-routing mechanisms in case of fault, etc.



VPN Labels are *piggybacked* on MP-BGP Announcements

* PE-CE Protocol
(OSPF, BGP, Static routes, ...)



Multi-Protocol BGP

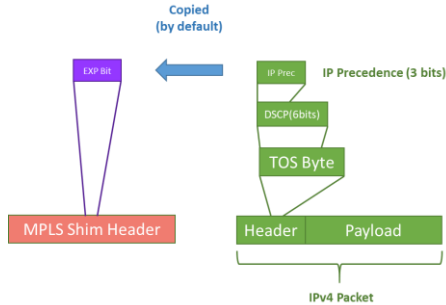
Route Distinguisher
4 byte – To manage IP
address overlapping
VPNv4 Address Family

Route Target – BGP Extended
Community (4 byte) – To
import/export routes in VRFs



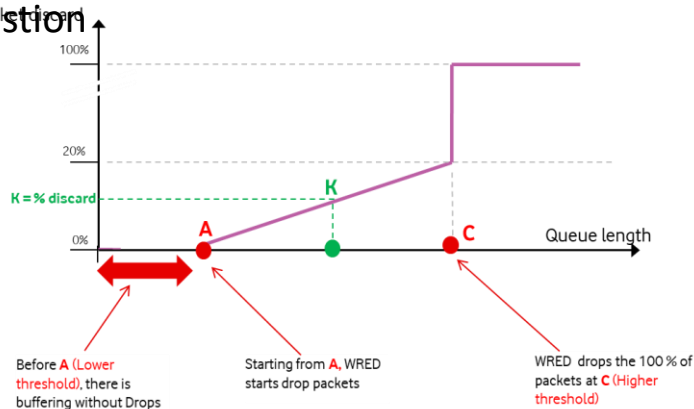
QOS

- 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 traffic, with WRED (Weighted Random Early Detection) algorithm to handle congestion



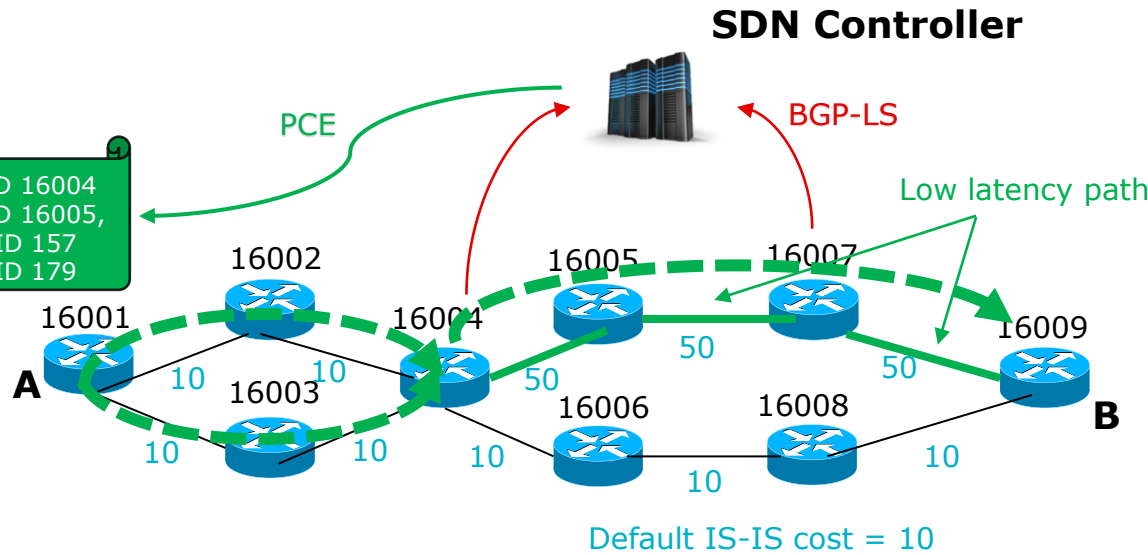
SEGMENT ROUTING

- 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)
 - Adjacency 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)

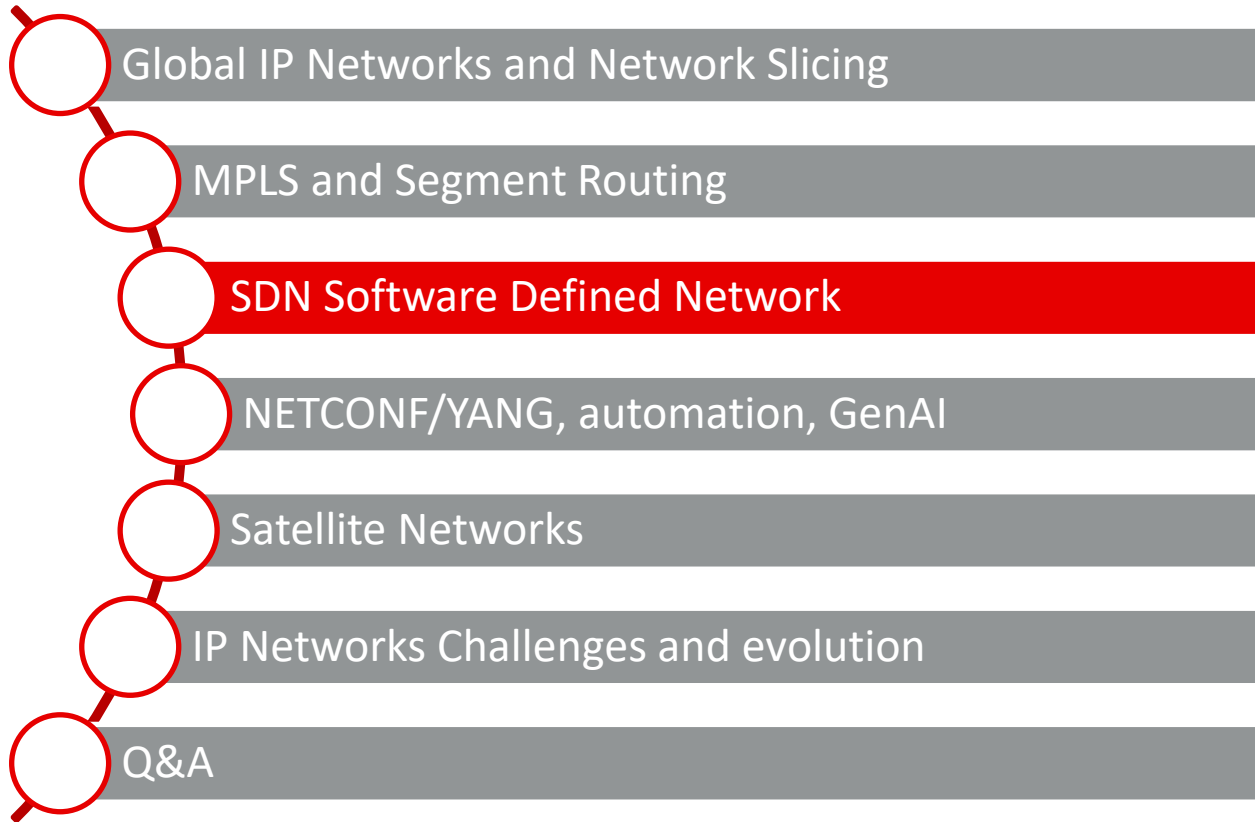
Segment Routing enables centralised traffic engineering, agile programming source nodes only via Southbound Interface PCEP (Path Computational Element Protocol). No per flow state and signaling needed at midpoints and tail end routers



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

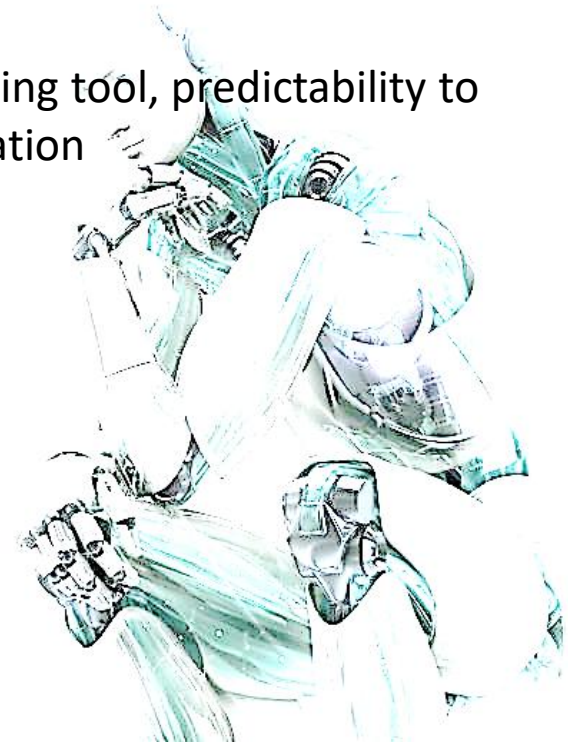
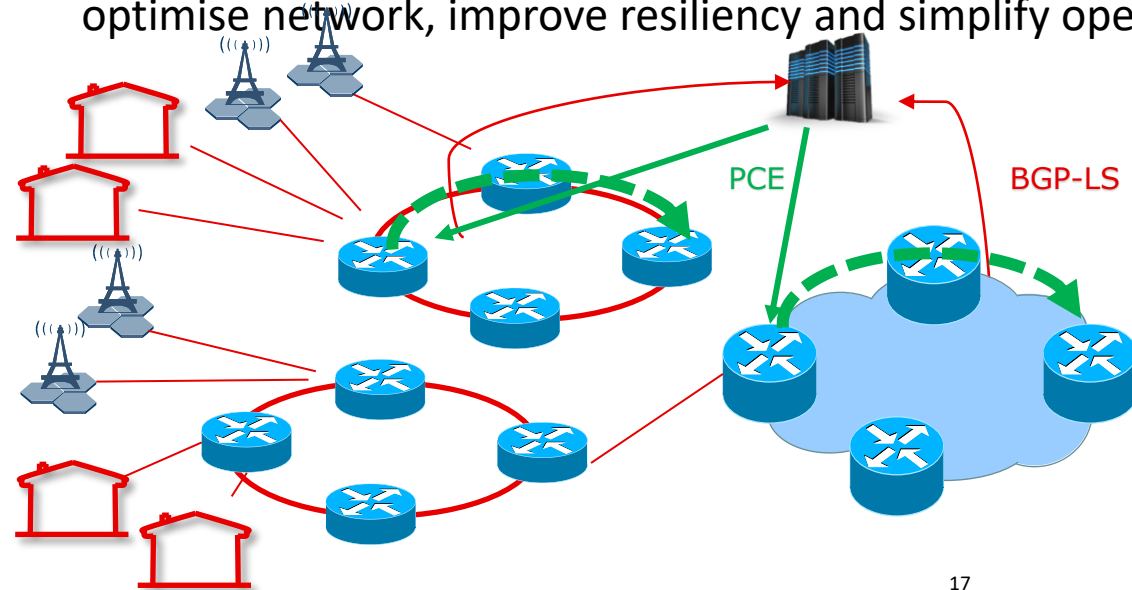
- 
- Global IP Networks and Network Slicing
 - MPLS and Segment Routing
 - SDN Software Defined Network**
 - NETCONF/YANG, automation, GenAI
 - Satellite Networks
 - IP Networks Challenges and evolution
 - Q&A



Software Defined Network

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

- Programmability, policy control, SLA fulfilment 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

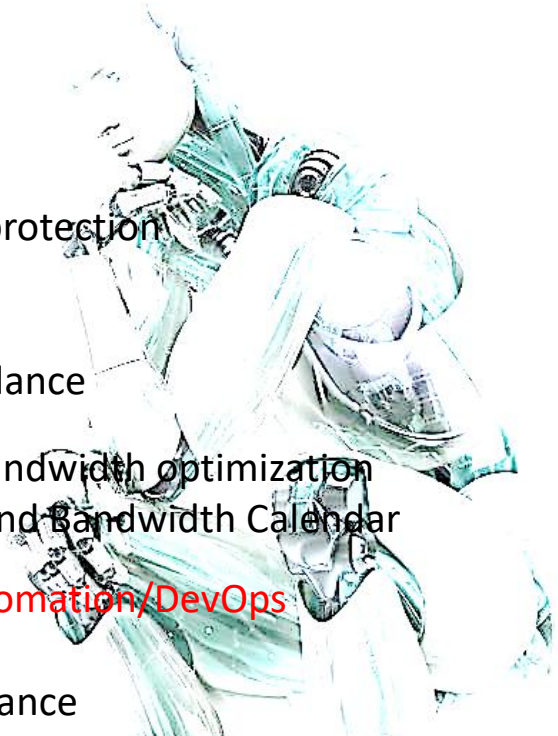
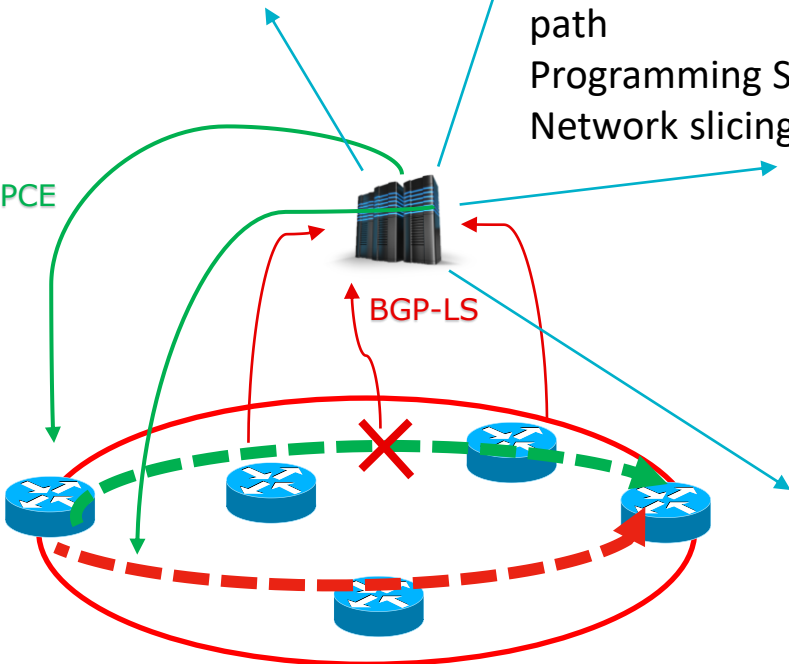
- Service modeling using NETCONF/YANG
- Computation of SLA adhering path and protection path
- Programming Source nodes via PCEP
- Network slicing/Disjoint Path/Path Avoidance

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

FROM

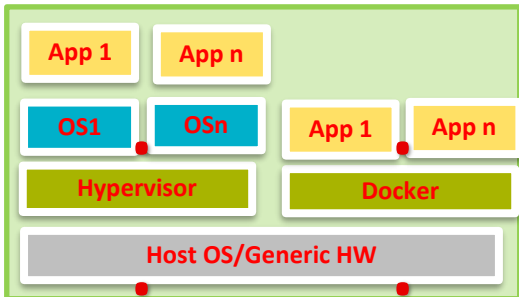
BARE METAL
MSS, MGW, CSDB, IN,
OCS, SGW, etc.



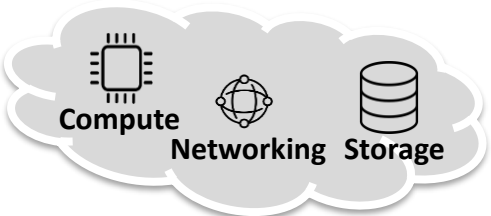
TO

VNF/CNF
vGTW , vMME , vDNS, vMSP
vDRA, vIMS, etc.,

**Virtualization
Layer
HW**



IaaS/PaaS/SaaS



- **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**

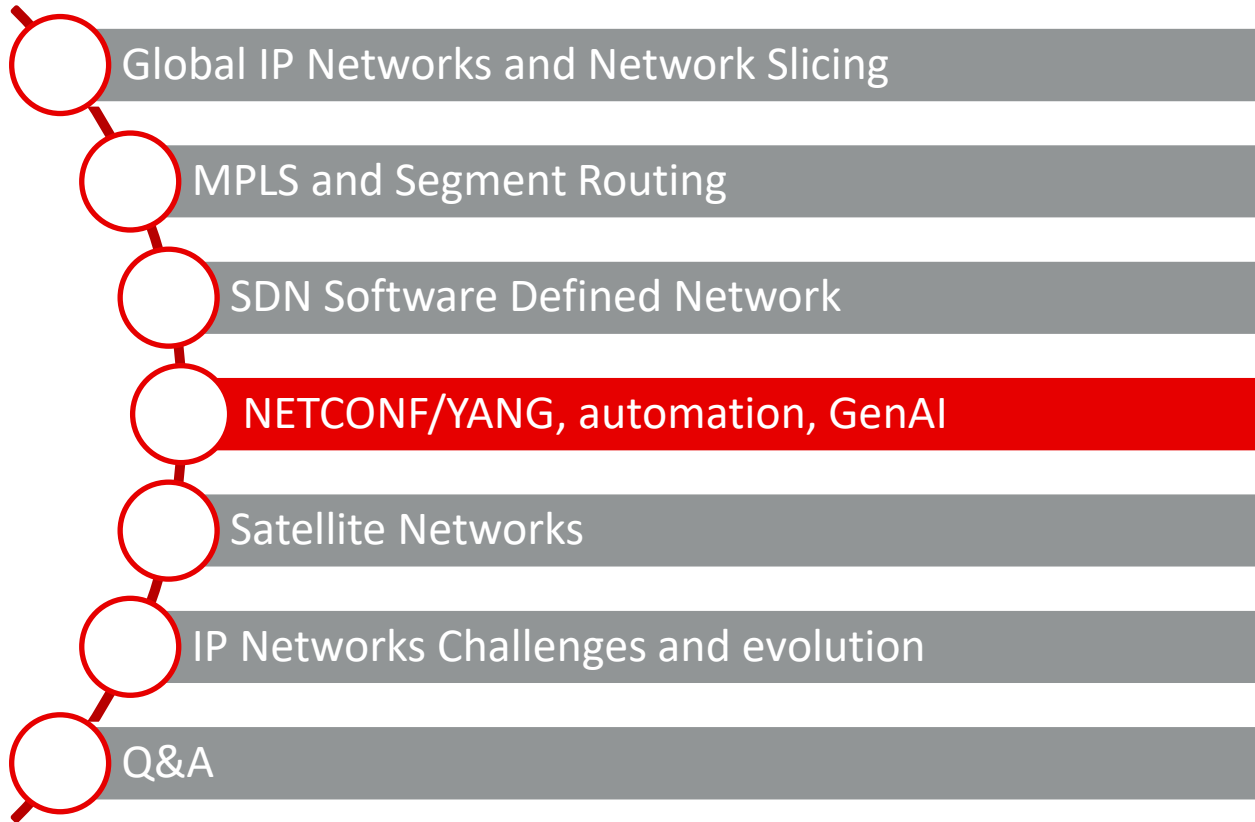


SDN and NFV

- 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, elastically 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

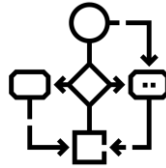
- 
- Global IP Networks and Network Slicing
 - MPLS and Segment Routing
 - SDN Software Defined Network
 - NETCONF/YANG, automation, GenAI**
 - Satellite Networks
 - IP Networks Challenges and evolution
 - Q&A



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

YANG-based and NETCONF/RESTCONF/gNMI automation

- It is possible to gather automatically config data from network elements and to modify the same preparing scripts (ie. in Python) executing CLI commands (Command Line Interface).
- CLI syntax, as well as the data structure of network elements are vendor-dependent.
- YANG (Yet Another Next Generation), see IETF [RFC6020](#) e [RFC7950](#), is a standard created to model config data and it is adopted by the major manufacturers such as Cisco, Juniper, Nokia, Huawei, Ciena, etc.
- Protocols like NETCONF, RESTCONF or gNMI allow to gather or modify config data in YANG format independently from the vendor, providing optimal means to manage a multivendor network environment
- NETCONF (IETF RFC6241), coded XML, implements SSH as a transport layer, and adopts a Remote Procedure Call mechanism to execute data collection or to apply changes to data config, using instructions like GET, GET-CONFIG, EDIT-CONFIG, etc.
- RESTCONF uses HTTPs, and is less fitting to massive operation, while gNMI, although with similar limitations, does fit to real-time applications.



YANG-NETCONF automation examples

- YANG models: hierarchical and modular
- NETCONF session based read/write/edit, transactional with confirmation/test/rollback
- Network Modeling (netmod)
- Network Configuration (netconf)

```

$ yang -f tree Cisco-IOS-XR-ipv6-ospfv3-oper@2015-11-09.yang
module: Cisco-IOS-XR-ipv6-ospfv3-oper
  +--ro ospfv3
    +--ro processes
      +--ro process* [process-name]
        +--ro vrfs
          +--ro vrf* [vrf-name]
            +--ro vrf-name
              XR:Cisco-ios-xr-string
            +--ro summary-prefixes
              +--ro summary-prefix*
                +--ro prefix?
                +--ro prefix-length?
                +--ro prefix-metric?
                +--ro prefix-metric-type?
                +--ro tag?
  ...
  ...
  
```

Downloaded from server (router)

Module name

Container

List entry (note "**")

Leaf

Type defined in another module

inet:ipv6-address-no-zone

xr:Ipv6-prefix-length

uint32

ospfv3-default-metric

uint32

Read-only (operational) data

```

$ yang -f tree ietf-netconf@2011-06-01.yang
module: ietf-netconf
  rpcs:
    +---x get-config
      +---w input
        +---w source
          +---w (config-source)
            +---:(candidate)
              | +---w candidate? empty {candidate}?
              +---:(running)
                | +---w running? empty
                +---:(startup)
                  +---w startup? empty {startup}?
          +---w filter?
        +---ro output
        +---ro data?
    +---x edit-config
  ...
  
```

Module name

RPC definition

Config data store types

Choice (select one of the following cases:)

Only valid if device supports "candidate datastore" feature

Link utili:

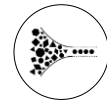
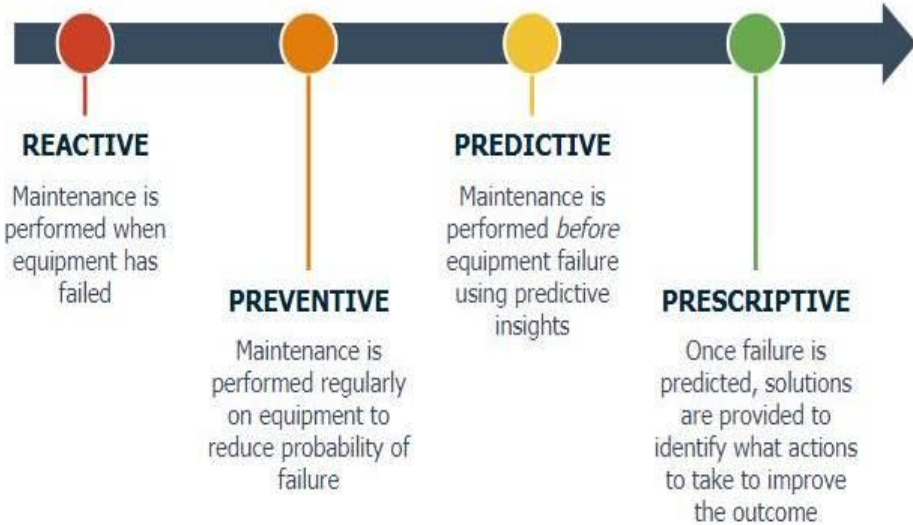
<https://cisco-tailf.gitbook.io/nso-docs/guides/development/get-started>

[GitHub - YangModels/yang: YANG modules from standards organizations such as the IETF, The IEEE, The Metro Ethernet Forum, open source such as Open Daylight or vendor specific modules](#)

[public/release/models at master · openconfig/public · GitHub](#)



From Preventive To Prescriptive



Big Data



Machine Learning

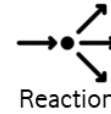
Traditional



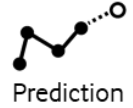
Vs.



Machine Learning



Reaction



Prediction



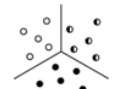
Pre-defined criteria



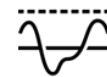
Classification



Human similarity observation



Clustering



Threshold Approach



Anomaly detection



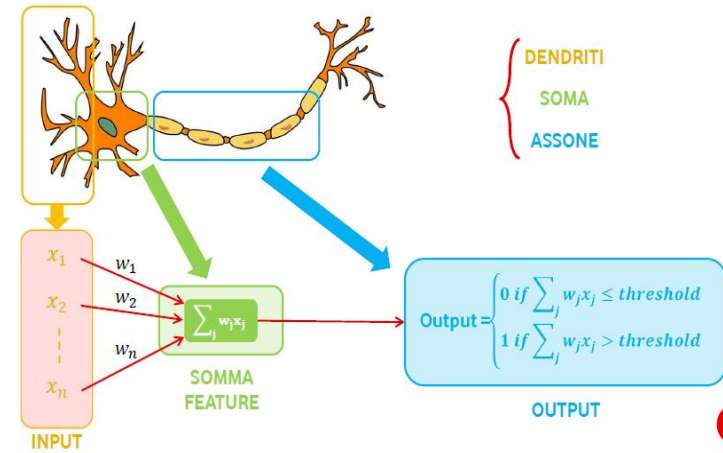
Predictive Models

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

		Prediction	
		False	True
Reality	False	80	10
	True	5	5

Reality and model coincide (Green) Reality and model diverge (Red)



GenAI Applications

Large Language Models are based on statistical prediction of sequential tokens: given a sequence of tokens, the model predicts the probability of the next token weighing the relevance of the components of the sequence, using advanced techniques of representation (self-attention) and unsupervised pre-training and following fine-tuning leveraging billions of parameters.

In the telco industry LLMs are being used to:

Python coding

Man-Machine Interface for advanced operating management systems

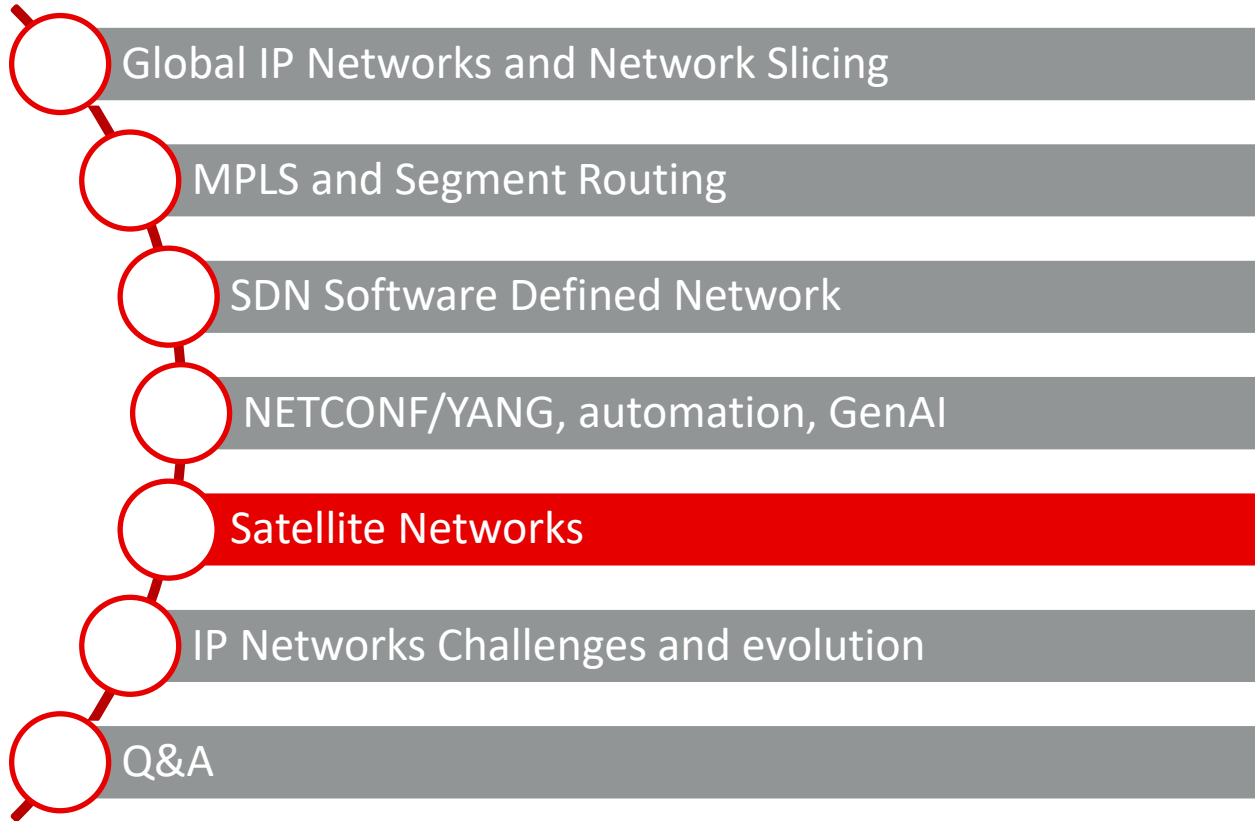
Free text fields analysis in large volumes of customer tickets

The main limitations of the current LLMs are a lack of dependencies on “local” context and lack of abstract and global view. These limits make LLMs unsuitable or sub-optimal for the resolution of complex mathematical problems, long term predictions, or in general for solving complex problems requiring logical coherence at an abstract level. These limits caused “hallucinations” phenomena to raise.

Recently, the adoption of reinforcement algorithms helped to mitigate the effects of a lack of global context view.

Finally, the upcoming “World Model” approach should overcome the current limitations in terms of global coherence as the generative neural networks are being designed to create an abstract representation of the environment.

Agenda

- 
- Global IP Networks and Network Slicing
 - MPLS and Segment Routing
 - SDN Software Defined Network
 - NETCONF/YANG, automation, GenAI
 - Satellite Networks**
 - IP Networks Challenges and evolution
 - Q&A



What Satellite technology is there?

Latest Generation Satellites

Low Earth Satellites (LEO)

600 to 1500km



Smaller Satellites
Large constellation
Lots of Earth Gateways

- Global footprint > 200 satellites
- Highest system capacity
- Lower Latency (50ms *)

AST
SpaceMobile

Medium Earth Satellites (MEO)

8000 to 20000km



Larger Satellites
Small constellation
Regional Earth Gateways

- Global footprint < 10 satellites
- Higher capacity vs GEO
- Moderate Latency (150ms *)



Geosynchronous Satellites (GEO)

~ 35000km



Very Large Satellites
Very small constellation
Few Earth Gateways

Most common legacy system

- Global footprint < 5 satellites
- Lowest system capacity
- Very High Latency (500ms *)



LEO impact 4 areas

Progress

Direct to Mobile (DTM)



- 4G/5G services from satellite to Smart Phone

Explore

Fixed Broadband



- Satellite Broadband for users outside terrestrial coverage areas

Explore

Enterprise/IoT



- Connectivity to remote private networks, VPN, SDWAN, IOT services

Very Limited (Europe)

Explore (Africa)

Mobile Backhaul

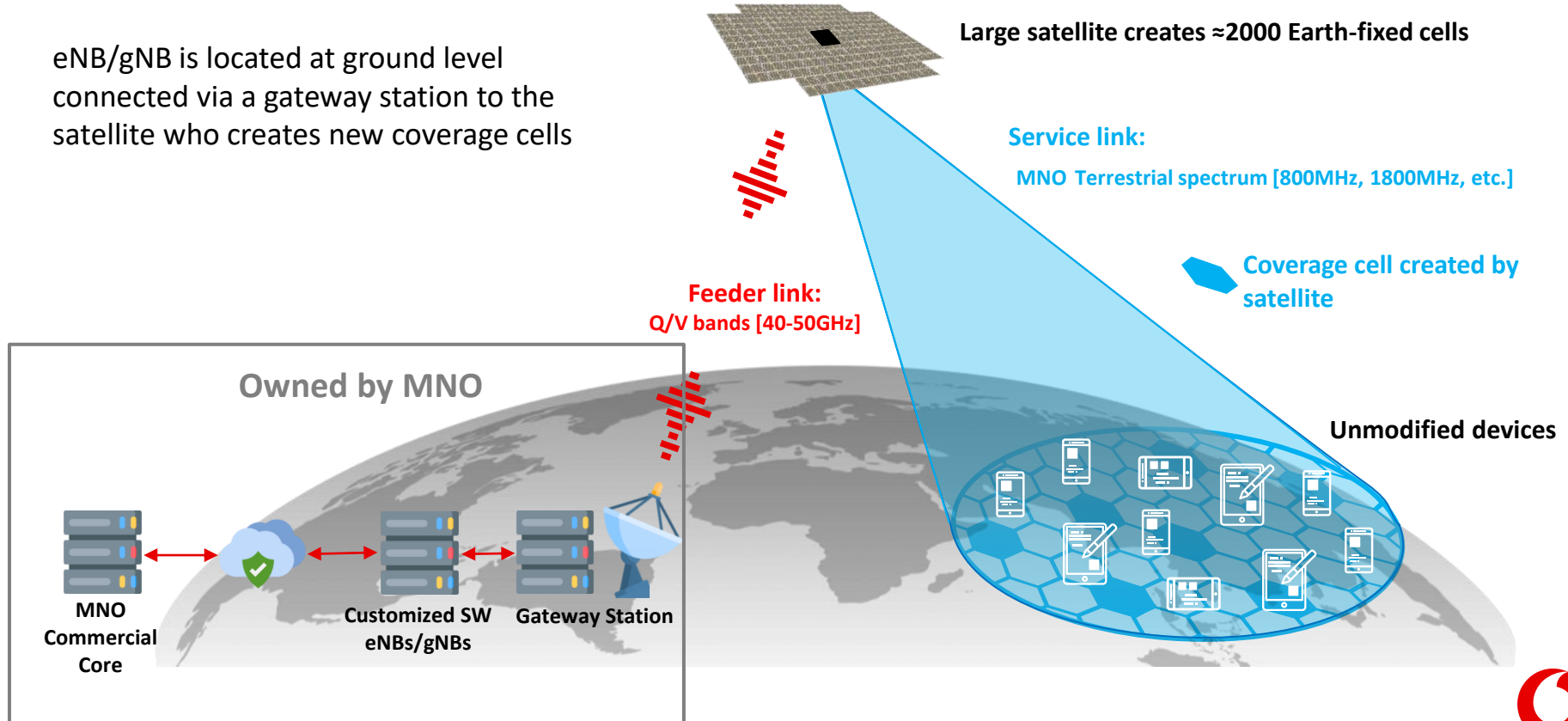


- Satellite backhaul for low-capacity 4G/5G sites

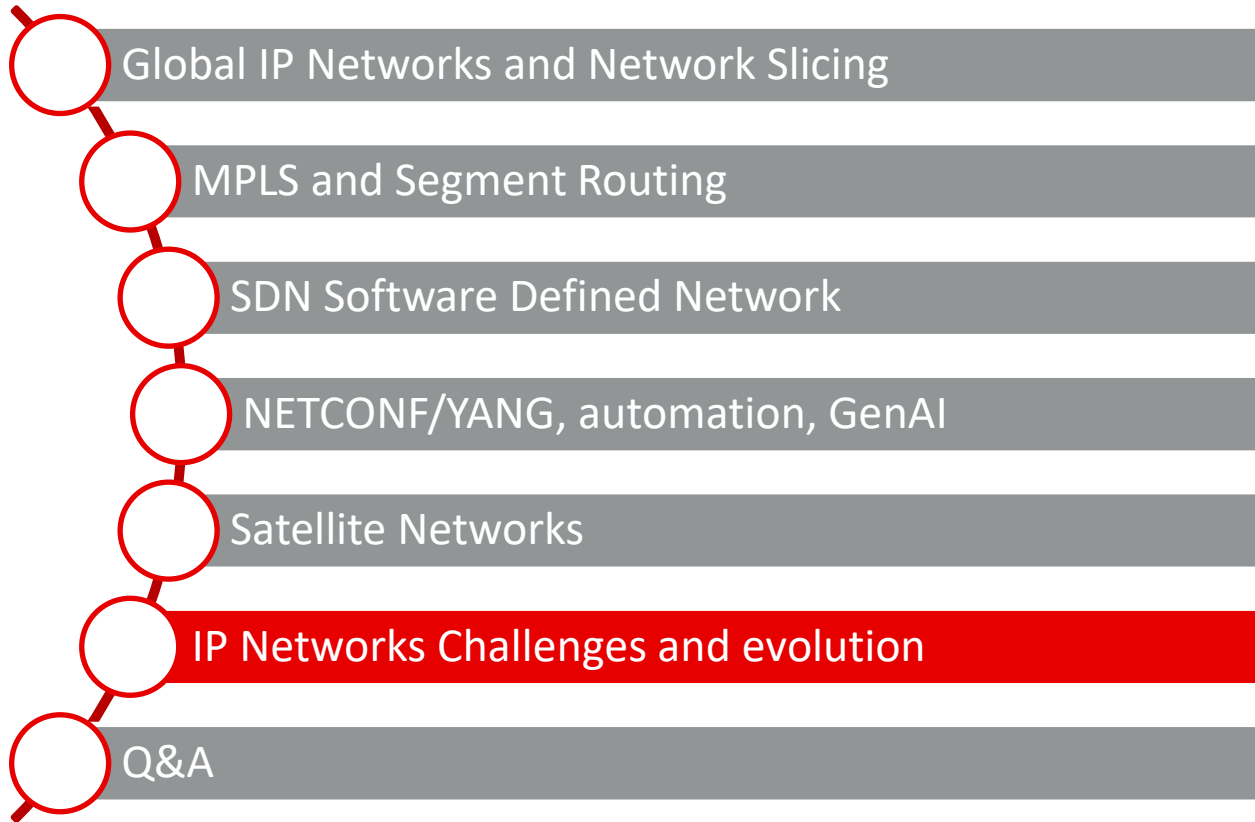


Direct to Mobile Architecture

eNB/gNB is located at ground level connected via a gateway station to the satellite who creates new coverage cells



Agenda

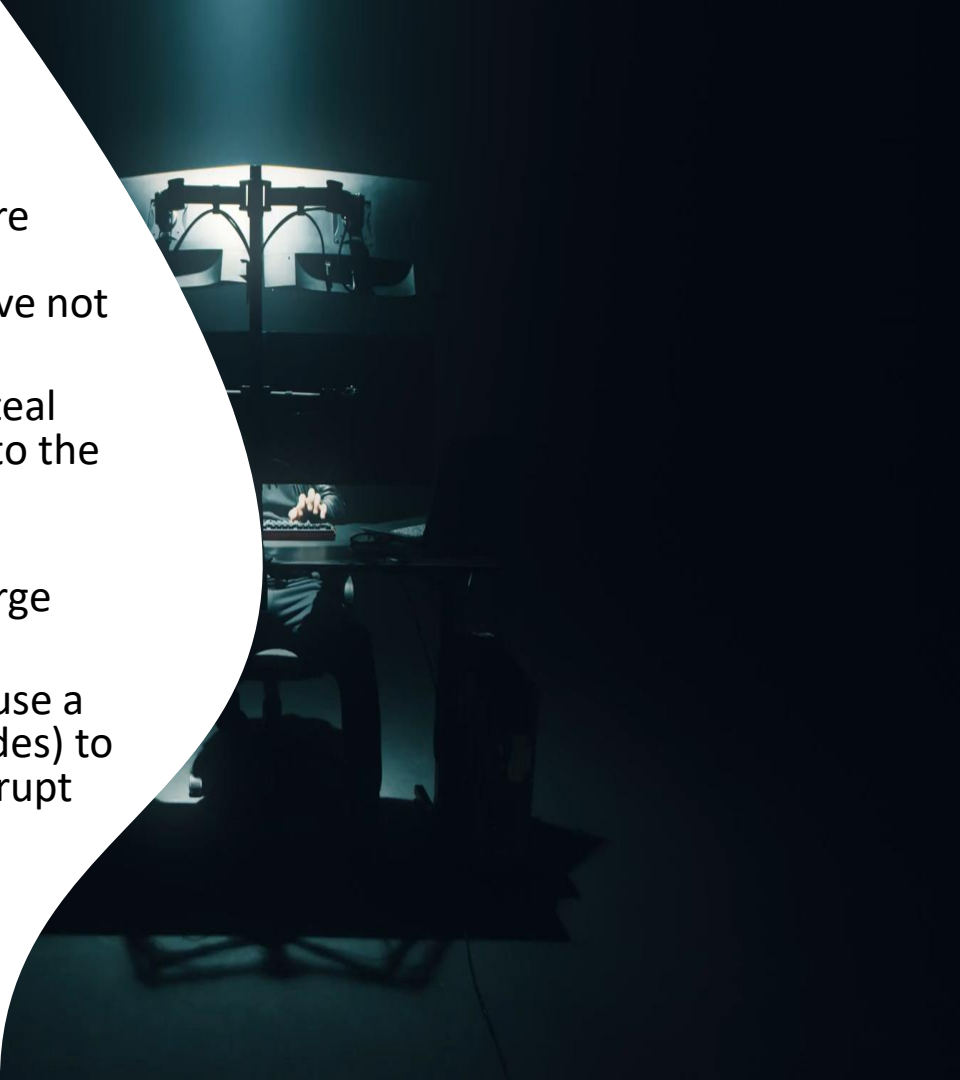
- 
- Global IP Networks and Network Slicing
 - MPLS and Segment Routing
 - SDN Software Defined Network
 - NETCONF/YANG, automation, GenAI
 - Satellite Networks
 - IP Networks Challenges and evolution**
 - Q&A



Security aspects

Some of the most common security threats:

- **Zero Day vulnerabilities:** hackers exploit software vulnerabilities in those elements which security patches have not yet been made available or have not yet been implemented for.
- **Security Breach of Privileged Access:** hackers steal privilege access credentials to get illegal access to the elements
- **Human mistake:** misconfiguration on network elements which cause service disruption on a large scale.
- **DDOS (Distributed Denial Of Service) :** hackers use a network of compromised resources (zombie nodes) to orchestrate an attack aimed to overload and disrupt critical resources.



Risks related to automation

Centralizing critical network control increases the impact in case of malicious access or human mistake.

National or international regulations may apply to centralized automation systems: GDPR, Anti Sabotage, Golden Power, PNSC, etc.

Mitigation recommended actions:

- **Hardening**
- **Testing and automation virtual lab**
- **2FA, authorization processes for PA accounts, leavers and zombie users management.**
- **Personal, functional and group users process management.**
- **Segregation of duties per domain and profile**
- **Password safes and Privileged Access management**
- **Advanced log collection and analysis**
- **Backup systems protection and segregation of duties in access to backup systems**
- **Study and risk mitigation in worst case, corner case and deadlock scenarios**

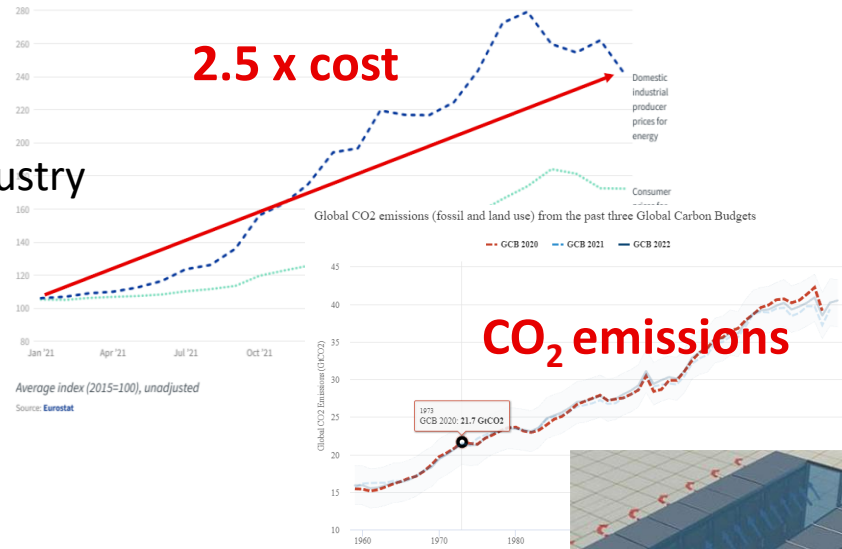


Energy Puzzle

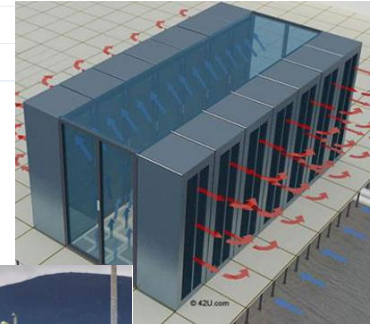
- Energy costs highly unstable
- Zero-impact energy policy a priority for the industry




- 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



Agenda

- 
- Global IP Networks and Network Slicing
 - MPLS and Segment Routing
 - SDN Software Defined Network
 - NETCONF/YANG, automation, GenAI
 - Satellite Networks
 - IP Networks Challenges and evolution
 - 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!

