



TELECOM INFRA PROJECT

Distributed Disaggregated Backbone Router (DDBR)

Technical Requirements Document



Authors:

- **Eva Rossi**
 - Head of Transport, Vodafone.
 - Eva.Rossi@vodafone.com
- **Jose Angel Perez**
 - Principal Engineer, Vodafone.
 - jose-angel.perez@vodafone.com
- **Kenji Kumaki**
 - General Manager/Chief Architect, IP Network Department, KDDI.
 - ke-kumaki@kddi.com
- **Ryuji Matsunaga**
 - Head of IP & MPLS Core Networks, KDDI.
 - ry-matsunaga@kddi.com
- **Yuji Sonoki**
 - Assistant Manager of IP & MPLS Core Networks, KDDI.
 - yu-sonoki@kddi.com
- **Ahmed Hatem**
 - Technical Program Manager, Facebook.
 - ahatem@fb.com
- **Diego Marí Moretón**
 - Connectivity Technologies & Ecosystems Manager, Facebook.
 - dmmorten@fb.com



Change Tracking

Date	Revision	Author(s)	Comments
17/11/2020	V1.0	Ahmed Hatem	Draft version
9/12/2020	V1.1	Kenji Kumaki	Additional edits & contents
11/12/2020	V1.2	José Ángel Pérez	Additional edits & contents
21/1/2021	V2.0	Kenji Kumaki	Additional edits & contents
21/01/2021	V2.1	José Ángel Pérez	Additional edits & contents



Table of Contents

1. Introduction	7
1.1 Scope of the document	7
1.2 Document Structure	8
1.3 Why DDBR?	9
1.3.1 DDBR Solution Description	9
1.3.2 Overview of IP backbone network challenges	10
1.3.2.1 Lack of Supply Chain Diversity	10
1.3.2.2 Monolithic nature	11
1.3.2.3 Chassis based	12
1.3.2.4 Time to upgrade the installed base	13
2. DDBR System Architecture & Scaling Path	14
2.1 Scale-up in Traditional IP backbone systems	14
2.2 Transformation to Disaggregated Spine & Leaf Architecture	15
2.3 Achieving Disaggregated Backbone Router	16
3. Data Plan Requirements	18
3.1 Whiteboxes requirements	19
3.2 ASIC firmware requirements	21
4. Control Plan Requirements	21
4.1 NOS SW architecture	21
4.2 DDS SW features	22
4.2.1 Interface support	22
4.2.2 Routing support	22
4.2.3 Quality of Service (QoS) support	22
4.2.4 Hierarchical Quality of Service (H-QoS) support	24
4.2.5 Security support	24
4.2.6 Services Support	25
4.2.7 Management Support	25
4.2.8 SDN & Telemetry	25
4.2.9 Scalability Figures	26
4.2.10 Hardware Scalability:	26
4.2.11 IGW SW Scalability:	28
4.2.12 P-router SW Scalability:	28



5. Management Plan Requirements	29
5.1 Telemetry & SDN readiness.....	29
5.2 Standards support	30
6. General Requirements	31
6.1 Regulatory requirements	31
6.2 Access security and anti-theft requirements	31
7. Glossary	32



Table of Figures

<i>Figure 1. Disaggregated Open Router Scope</i>	<i>8</i>
<i>Figure 2. Monolithic IP Backbone Routers.....</i>	<i>11</i>
<i>Figure 3. Traditional scale-up path</i>	<i>14</i>
<i>Figure 4. Disaggregated Clos Architecture</i>	<i>15</i>
<i>Figure 5. Virtualized Control Plane.....</i>	<i>17</i>
<i>Figure 6. DDBR Cluster Sizes.....</i>	<i>18</i>
<i>Figure 7. Hardware scalability figures.....</i>	<i>26</i>
<i>Figure 8. IGW Software scalability figures</i>	<i>28</i>
<i>Figure 9. P-router Software scalability figures</i>	<i>29</i>
<i>Figure 10. Open Transport SDN Architecture Vision.....</i>	<i>30</i>



1. Introduction

As part of Telecom Infra Project (TIP) Open Optical & Packet Transport (OOPT) Project Group, a new subgroup DOR (Disaggregated Open Router) has been formed with a mission to accelerate innovation in IP backbone networks and ultimately help service providers provide better connectivity for their mobile & broadband customers.

The DOR subgroup members have together analysed the current challenges they face when building and scaling their IP backbone networks and have envisaged an evolution path to their backbone network which introduces innovation, efficiency and primarily openness where they can disaggregate the IP backbone devices and have the flexibility of selecting the best of breed IP products in the market.

This IP backbone evolution will also enable having the full suite of open transport building blocks which can be used across the different segments of their transport networks (access , aggregation & backbone) and attain the benefits that have been achieved with the introduction of different open transport products (ex. DCSG , Cassini , ...) into their transport networks.

A high-level description of a Disaggregated Open Router was developed by the DOR subgroup members and will be shared in this document.

1.1 Scope of the document

This document defines a proposal for the shift in the IP backbone architecture from monolithic chassis-based to a disaggregated Spine & Leaf architecture. The document also describes the technical aspects of a Disaggregated Open Router (DOR) which is a versatile device that can be deployed in IP core/backbone networks as depicted in **Figure-1** below and act as an IP/MPLS core/edge routers (P/PE routers) or an Internet Gateway router (IGW)

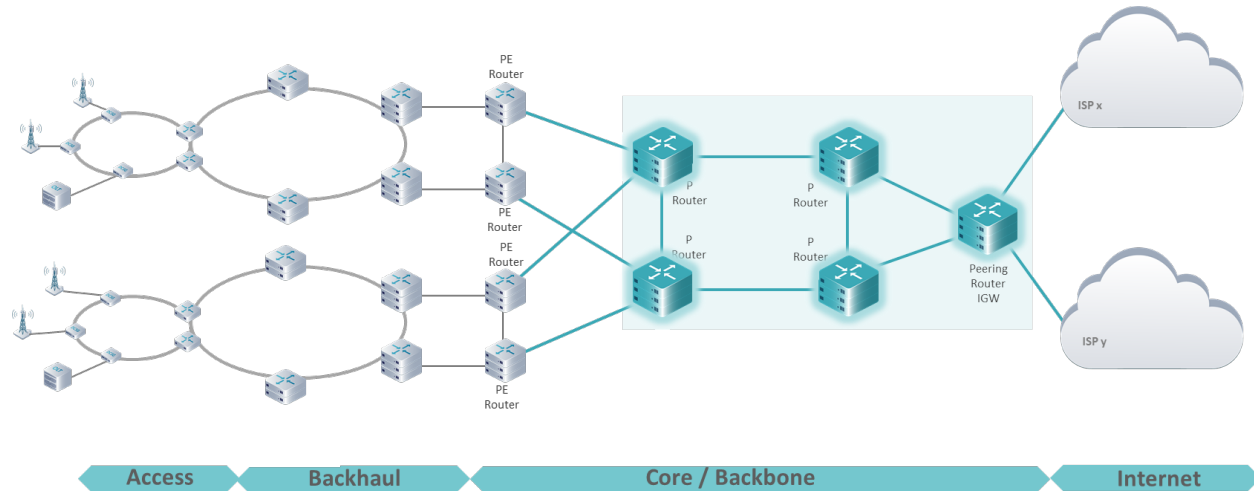


Figure 1. Disaggregated Open Router Scope

The document describes the necessary hardware, software, management and general requirements that need to be fulfilled by a DOR compliant platform taking into consideration not only the current service providers needs when deploying core/backbone transport networks but also staying ahead of the evolving needs in terms of resiliency, capacity scaling & E2E network automation.

The Disaggregated Distributed Backbone Router (**DDBR**) will be the name used in this document to refer to a DOR compliant platform according to the technical requirements detailed in this document.

The definition of a detailed low-level TRS (Technical Requirement Specification) will be done immediately after the publishing of this document, as a basis for further technical discussions with candidate platform HW & SW providers.

1.2 Document Structure

This document is structured as follows:

- Chapter 1: Introduction
- Chapter 2: DDS System Architecture & Scaling Path



- Chapter 3: Data Plane Requirements
- Chapter 4: Control Plane Requirements
- Chapter 5: Management Plane Requirements
- Chapter 6: General Requirements
- Chapter 7: Glossary

1.3 Why DDBR?

The objective of this project is to develop a solution that overcomes the most relevant challenges (examples will be stated in the upcoming sections) the service providers are facing nowadays when deploying or expanding their IP backbone networks.

1.3.1 DDBR Solution Description

Before diving deep into the current challenges, means to overcome the challenges and the technical requirements details, a high-level description of the key aspects to be considered in the DDBR solution is given below:

- **Disaggregation driving competition:** opening-up the market with new suppliers improving the cost savings
- **No backplane Limitations:** Transport networks need to become smarter and more flexible to meet specific customers' and service's needs and demands.
- **Pay as you grow:** reducing initial investment and optimizing the power efficiency without any growth limitation
- **Innovation:** open SW and HW to improve flexibility and innovation on SW development and reduce time to market.
- **Operational Efficiency:** Taking advantage of Software Defining Network to make the network operation simpler, give tools for automation, enhance the capabilities of our network, and introduce a set of capabilities that today are not present.
- **Reliability:** Always targeting higher availability & multi-level redundancy



1.3.2 Overview of IP backbone network challenges

The role of IP backbone networks is to route the mobile & broadband traffic between different access networks at a national or regional level within the service provider network in addition to providing connectivity with external networks ex. Other service providers, public cloud providers, content data networks, Internet exchange peers and IP transit providers exchange traffic and access the internet.

New services (ex. IaaS, PaaS, SaaS, immersive AR/VR, cloud gaming, eMBB, mMTC and URLLC etc..) are driving the increased bandwidth, connectivity, uptime and latency demands and are dictating substantial transformations on the E2E network architecture and economics to cope with these new services requirements.

The IP backbone network in turn has to continuously scale to support the internet traffic growth, to improve resiliency in order to meet the mission-critical type of communications and to create an evolution path for agility and automation to lower the network cost and enhance the overall customer experience.

In the following section, we will list the key challenges that currently exist in the IP backbone networking space and different proposals to address these challenges in the DOR.

1.3.2.1 Lack of Supply Chain Diversity

Similar to all segments of the telecom network (Radio Access, Transport & Core), the ongoing consolidations & acquisitions in the core routers supply market have led to:

- High dependency on a reduced number of suppliers.
- Less competitive market which is at greater risk from increasing costs
- Limited Innovation and time-to-market speed.
- Limited 3rd party interoperability across different hardware components

1.3.2.2 Monolithic nature

Traditionally the service providers are deploying monolithic IP Backbone routers which are based on vertically integrated proprietary components as modelled in **Figure-2** below which are a bottom-up tightly coupled.

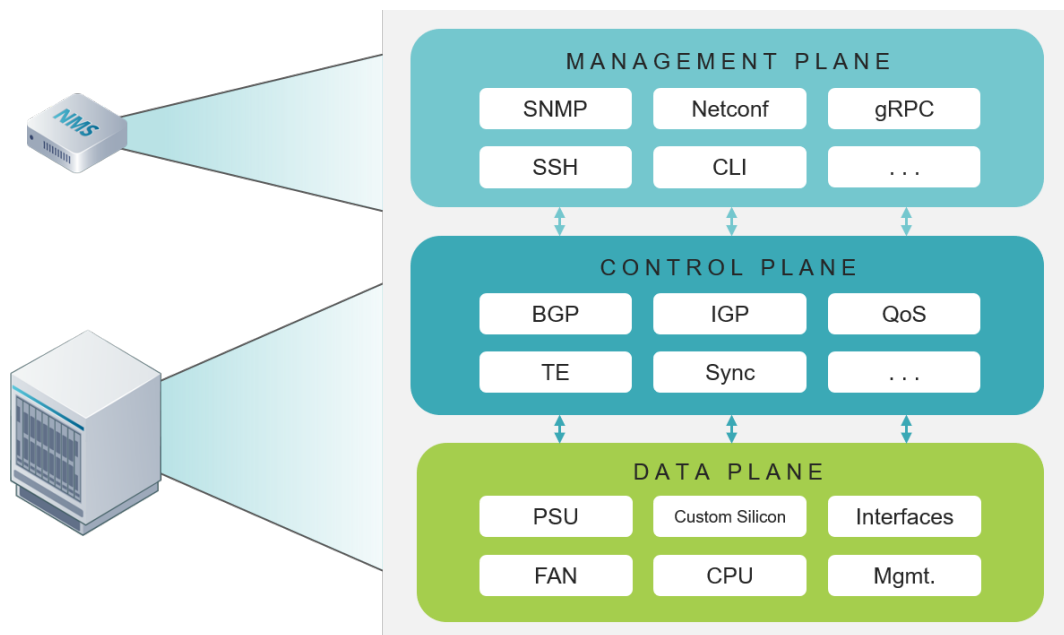


Figure 2. Monolithic IP Backbone Routers

Starting from the **data plane** hardware where custom purpose silicon chipsets are used to handle the packet processing, traffic management, forwarding and expose the fabric interfaces.

In the **control plane**, a custom networking operating system (NOS) which is purposely built to optimally run only on the custom hardware and consists proprietary code and mandatory licensing. That spans the drivers which control all the hardware components power, cooling, routing circuits, etc. The firmware is responsible for loading the networking operating system image when the router boots and the networking software stack which executes the routing protocols & different policies.

The third component is the **management plane**, which is responsible for the overall platform management for instance the interfaces configuration, services provisioning, inventory management, alarm reporting, faults handling, performance monitoring.



It worth noting that some suppliers have started to build platforms based on merchant silicon chips and port on this hardware on their proprietary NOS software, however the fact of having the hardware tied only to this proprietary NOS software still imposes on the service providers the same challenges of the monolithic nature.

These monolithic IP backbone routers have served the key performance needs (capacity, availability, etc..) and proven to be fit for purpose for a long time. However, having the platform vertically integrated impeded the service providers from unleashing the potential of open networking, limited the supply choices and generally slowed down the innovation in the IP backbone networks.

For instance, having the data plane tightly coupled with the control plane lead to a high dependency on the existing supplier's roadmap and dictated the need to completely replace the hardware plus the NOS software in order to benefit from a feature available in a 3rd party NOS supplier.

Additionally, for the management plane while several suppliers have offered robust Network Management Systems (NMS) and SDN (Software Defined Network) controllers to efficiently manage their monolithic products and provided support for third party products still the services providers are experiencing challenges when it comes to the complex & high integration cost to manage third party products via the existing NMS. Also, while several suppliers have implemented the promising Netconf (RFC 6241) protocol there is very limited progress in standard network data model definition and there is lot of efforts needed to create a vendor-neutral data model to describe the network or device configuration.

1.3.2.3 Chassis based

The existing IP backbone routers are predominantly built based on a chassis structure with front access where the Interfaces (NNI/UNI) cards and the control boards are plugged into a common backplane.

Given the critical role of the IP backbone routers in the network and the high volume of traffic it is carrying, this chassis had to offer:

- Extreme resiliency and robustness in order to maintain nonstop connectivity to the dependent mobile and broadband customers
- Powerful computing capability and routing table storage for Ipv4/Ipv6 prefixes at the size of internet
- High capacity to support the customers and services growth.



Consequently, the chassis had to be equipped with:

- Units' redundancy at all levels: control processing, switching fabric, cooling and power
- Powerful computing capability, deeper buffers and large TCAM (Ternary Content Addressable Memory) chips
- Wide range of advanced control plane features including NSR (Non-Stop-Routing) & ISSU (In-Service Software Upgrade)
- High port density, number of slots and backplane switching capacity

That resulted a high cost, power hungry & bulky size platforms which require upfront investments, reserve larger footprint in datacenters and consume high power and does not provide a model to optimally grow based on the needs.

Moreover, in case of running out of slots a completely new chassis will be needed to add a single extra interface which leads to a complicated network topology, suboptimal traffic flow a non-linear cost per port model. Also, this upgrade model is not flexible enough to allow the service providers to promptly react to unplanned upgrade requests which leads to missing the opportunity to connect new customers due to the lengthy upgrade process.

Additionally, having all the NNI & UNI interfaces centralized into the same chassis is imposing an operational risks of losing the entire node in the case of a software glitch, undesirable state propagation due to misconfiguration , power issue, executing the wrong Method of Procedure (MoP) when rebooting the device or activating new link.

1.3.2.4 Time to upgrade the installed base

With the industry shift happening in the optical pluggable transceivers and the dawn of 400G QSFP56-DD optics, the services providers need to replace the current installed base to higher capacity, more compact dimensions, flexible thermal management ports which enable supporting higher capacity links with optimum port density per RU.

In particular, the 10/25G/40G UNI interfaces need to be upgraded to 100G and the 100G NNI interfaces to 400G which means boards or complete chassis replacement to support the new interfaces QSFP56-DD and get the outmost of the interfaces capacity through the backplane bus.

Accordingly, the service providers would look for a new approach when replacing the installed base to protect their investment in IP backbone networks.

2. DDBR System Architecture & Scaling Path

In this section, we will describe the high-level architecture of the proposed changes to the IP backbone router and the envisioned path to efficiently scale-out the capacity and the number of interfaces based on the need for the upgrade

2.1 Scale-up in Traditional IP backbone systems

As stated earlier, currently the IP backbone routers are predominantly based on integrated modular chassis designs. Accordingly, the upgrade path for a traditional IP backbone system is achieved as shown in **Figure-3** via adding extra line cards which is a scale-up model and that go till all the available slots are consumed. However, with this scale-up model provides extra interfaces while the switching capacity and the routing engine processing & memory doesn't scale with it as its limited with the chassis fabric chips capabilities which develops to become a bottleneck for the control plane performance and the overall supported system capacity and the upgrade path for a traditional IP backbone system is to completely replace the chassis as illustrated in Figure-3 with a more powerful switching , processing and memory chips to support the anticipated growth.



Figure 3. Traditional scale-up path

2.2 Transformation to Disaggregated Spine & Leaf Architecture

One step towards the scale-out path is to move to Spine & Leaf based architecture and disaggregate the control plane from the data plane as illustrated in **Figure-4** which instantly solves the dependency on the router switching capacity and the number of interfaces.

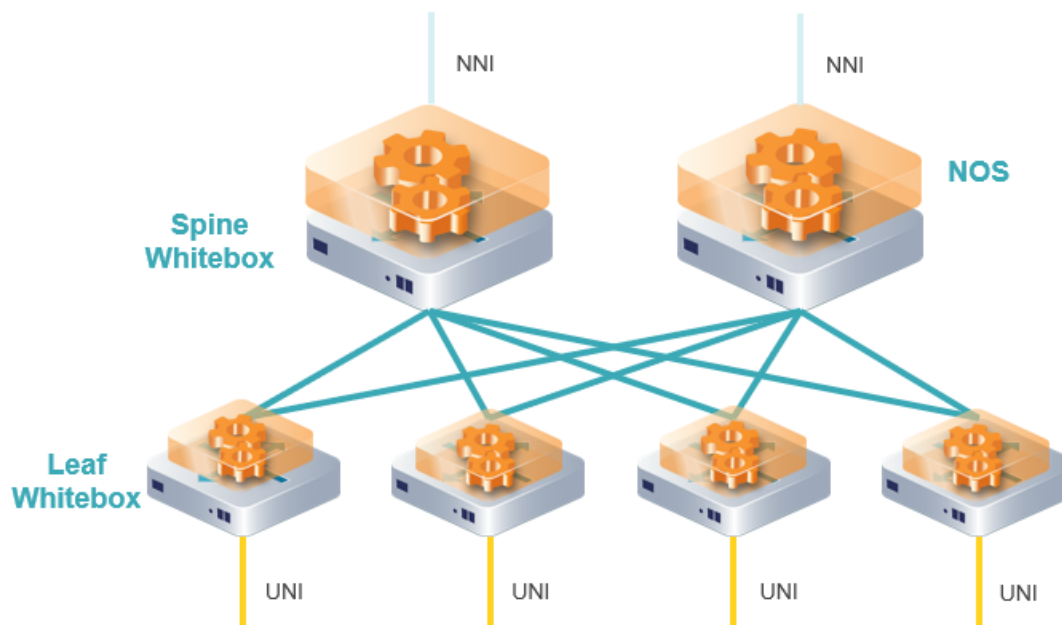


Figure 4. Disaggregated Spine & Leaf Architecture

The Spine & Leaf based architecture has been adopted in the datacenter space for a while and have helped the web-scale companies to efficiently grow their infrastructure to a massive scale that can deal with big data sets like for instance replicating copies of the internet across geographically distributed datacenters.

The combination of Spine & Leaf based architecture and disaggregation can lead to tremendous gains, including but not limited to:

- **Disjointed innovation paths:** between the data plane and control plane and allow replacing the NOS software while re-using same hardware and even mixing hardware among spine and leaf layers from multiple suppliers
- **Moving away from costly platforms:** benefiting from the low-cost merchant silicon



- **Scaling Efficiently** in a Pay-As-You-Grow model: start small and increment 1-2U at a time based on the growth needs while capitalizing on the investment made on the initial white boxes
- **Increased agility in physical deployment:** with less risks compared to entirely migrating the service to a new chassis in the scale-up model, upgrades in Spine & Leaf-based architecture is imposing less operational risk for instance you just need to connect a new spine router to increase the overall system capacity and connect a Leaf router to increase the number of interfaces
- **Deterministic latency:** with a fixed number of hops between spine and leaf routers, the overall system latency (from ingress to egress) is deterministic and homogenous across all ports
- **High performance:** High capacity can be achieved with variable over-subscription 1:1 to N:1 where the total bandwidth connected to the leaf routers can surpass the overall capacity offered by the spine routers
- **High Availability:** Path redundancy with multipath thanks to ECMP (Equal Cost Multi Path)
Relatively smaller failure domain in the network (e.g. In case of SW issue in CP, SW reboot of one node in a Clos Topology instead of turning a full chassis down)
- **Foster competition:** disaggregation will lead to more HW & SW companies competing to build more innovative & agile solutions.

2.3 Achieving Disaggregated Distributed Backbone Router

A second step to get the outmost benefits of the scaling-out is to move onto a centralized control plane as shown in **Figure-5** running on an on-prem x86 server or as a container in a cloud-native fashion which does all the heavy lifting of the route computation algorithms while keeping a lighter software version on the white boxes CPUs for running the initial booting configuration, sending keep alive messages or responding to the control messages received from the x86 server or VM hosting the control plane.

As a consequence of the control plane virtualization, below additional benefits will be achieved:

1. A high scale routing solution made of a cluster of white boxes managed by a centralized control plane
2. Ability of leveraging the value of Private/Public cloud computing to provide better compute scalability through virtualization or cloud bursting and benefiting from open-source solutions like OpenStack..
3. The cluster is acting as a single network entity, which accordingly save the:
 - 2.1 IP addresses needs to assign IP addresses on both Spine and Leaf in CLOS based architecture
 - 2.2 Cost as no need to use a special optics between Spine and Leaf because of a cell-based packet
4. Advanced QoS handling, deep buffers, large TCAM

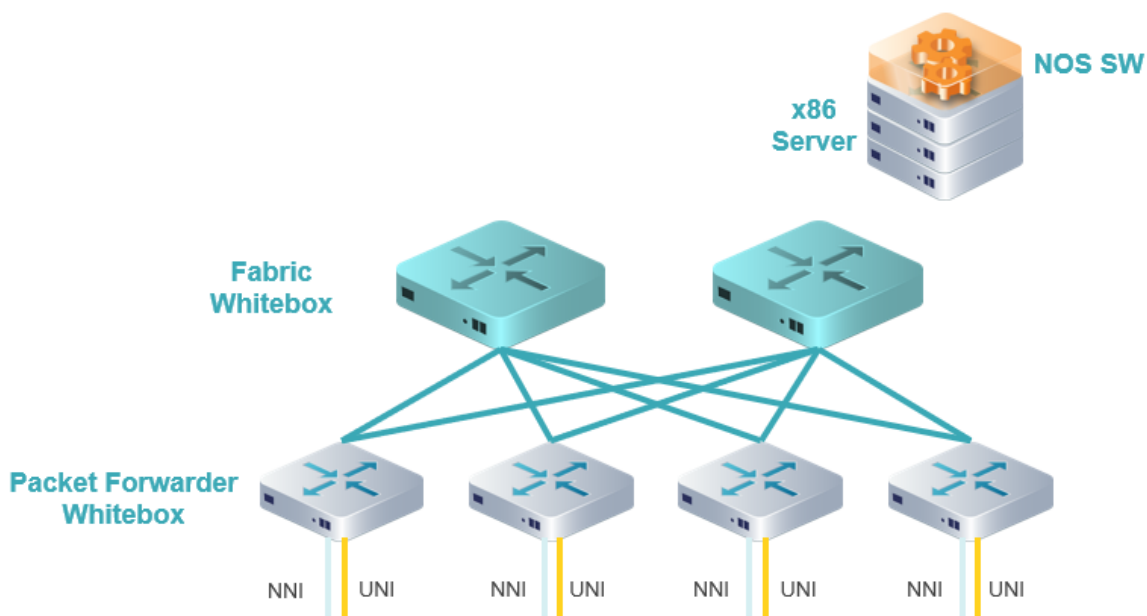


Figure 5. Distributed Disaggregated Backbone Router

Also, this virtualization step removes the bottleneck in the chassis-based model which was the limitation of the chassis built in CPU. Now processing can scale with servers or VM addition in a fully modular approach. It will also open the door for service chaining by adding multiple functions on the same hardware accordingly the router is not anymore, a specialized appliance but it can run multiple VNF instances to do the functions of load-balancer, Firewall, NAT, EPC ...

3. Data Plane Requirements

As shown in section-2 the platform architecture is modular and is basically a cluster of routers which consists of the following two building blocks:

- **Fabric Whitebox:** which represents the spine of the cluster and acts as the backplane
- **Packet Forwarder Whitebox:** which represents the leaf of the cluster and acts as the line cards

The white boxes shall be based on a 64-bit x86 architecture. At the time of this writing, this is the CPU architecture that has the most robust developer ecosystem and the most appealing roadmap to ensure platform longevity.

The forwarding capacity of the ASIC used in the white boxes shall support line-rate forwarding across all ports without any limitation and provide at least 4Tb/s full duplex capacity which will form the basic building block or smallest cluster size to start with,

The overall cluster capacity is the result of staging Fabric & Packet Forwarder white boxes in Clos-based interconnection, below are reference examples of different cluster sizes which are initially thought by the operators to be fulfilled by a DDS platform which should fit for their current needs, however a DDS platform shall offer seamless intra & inter cluster scaling and shall not prevent achieving higher cluster sizes with further staged whiteboxes.

	Standalone	Small Cluster	Medium Cluster	Large Cluster	Extra Large Cluster
Max Capacity	4Tb	16Tb	96Tb	192Tb	768Tb
Port Density	40x100G	160x100G	960x100G	1920x100G	7680x100G
	10x400G	40x400G	240x400G	480x400G	1920x400G
	80x10G/25G	320x10G/25G	1920x10G/25G	3840x10G/25G	15360x10G/25G
Packet Forwarder Whitebox	1	4	24	48	192
Fabric Whitebox	-	2	7	13	13

Figure 6. DDS Cluster Sizes



There are common aspects between both the Fabric & Packer Forwarder whiteboxes, for instance the architecture, form factor, power supply, mechanical and environmental requirements while the key differences will be the merchant silicon chip which defines the type and number of interfaces that the platform will support in addition to the CPU, deep buffer, TCAM, buffer size..

3.1 Whiteboxes requirements

The Fabric & Packet Forwarder whiteboxes need to support Ethernet switching, extensible deep buffering with carrier-grade traffic management and subscriber-level virtual output queueing should be provided and support below different port types:

- 400GbE
- 100GbE
- 10GbE via breakout cabling solutions

Concerning the Transceiver Optics types, below types shall be considered:

- **For 400G interfaces:**
 - Support all relevant IEEE standards (IEEE 802.3bs)
 - Support all requirements concurrently while forwarding at line rate, in all conditions (independently from number/types of services/flows) on multiple port line cards each port is expected to run at line rate concurrently.
 - Support all physical interface connectors must be IETF compliant and not Vendor specific.
 - Support for 400GBASE-FR8
 - Support for 400GBASE-FR4
 - Support for 400GBASE-LR8
 - Support for 400GBASE-LR4
 - Support for 400GBASE-FR8 and FR4 with QSFP56-DD
 - Support for 400GBASE-LR8 and LR4 with QSFP56-DD
 - Support for 400GBASE-FR8 and FR-4 with 3rd party QSFP56-DD
 - Support for 400GBASE-LR8 and LR-4 with 3rd party QSFP56-DD
 - Support for long reach / high power CFP2/4/8
 - Support for long reach / high power 3rd party CFP2/4/8
 - Synchronous Ethernet according to G.8261 G.8262, G8264 for all types of interfaces
 - Multi rate slot, please specify details (QSFP DD/56/28)

- **For 100G interfaces:**
 - Support all relevant IEEE standards (IEEE 802.3ba)
 - Support all requirements concurrently while forwarding at line rate.
 - On multiple port line cards each port is expected to run at line rate concurrently
 - Support all physical interface connectors must be IETF compliant
 - Support for 100GBASE-SR10
 - Support for 100GBASE-LR4
 - Support for 100GBASE-ER4
 - Support for 100GBASE-SR10 with QSFP28.
 - Support for 100GBASE-LR4 with QSFP28.
 - Support for 100GBASE-ER4 with QSFP28.
 - Support for 100GBASE-SR10 with 3rd party QSFP28
 - Support for 100GBASE-LR4 with 3rd party QSFP28
 - Support for 100GBASE-ER4 with 3rd party QSFP28
 - Support for long reach / high power CFP2/4/8
 - Support for long reach / high power 3rd party CFP2/4/8
 - Support for 100G coherent DCO CFP2
 - Support for 100G coherent DCO with third party CFP2
 - Support for 100G-Base-CWDM4
 - Support for 100G-Base-CWDM4
 - Synchronous Ethernet according to G.8261 G.8262, G8264 for all type of interfaces

The platform shall be fully interoperable with any 3rd-party pluggable optics, with no impact on customer/content traffic and equipment capabilities (payload, header, QoS, synchronization, etc.), able to report SFP data [via Digital Diagnostic Monitoring, and support SFP dynamic data logging](#).

Additionally, the merchant silicon chip shall support the typical Telco routing protocols including but not limited to:

- IEEE 1588v2 & SyncE
- L2
- OSPF & ISIS
- MPLS
- SR
- VPLS



- L2VPNs
- L3VPNs
- QoS & HQoS
- OAM

3.2 ASIC firmware requirements

When possible, network operating systems for this platform should be provided in the form of binary installers compatible with the Open Network Install Environment (ONIE) specification, as defined by the Open Compute Project (OCP).

4. Control Plane Requirements

4.1 NOS SW architecture

The DOR is being thought as a modular box, that can run any SW on top of the selected HW versions. In order to ensure the maximum flexibility in terms of the SW that can be loaded in the DOR, it will be equipped with ONIE. ONIE will enable any operating system to run on top of the DOR.

ONIE defines an open source “install environment” that runs on routers and switches subsystem. This environment allows end SW suppliers to install the target NOS as part of the initial system setup.

In order to enable different software packages, the DDS solution shall rely on “trusted based” systems so there is no need to have a licensing server or internet connectivity. In most of the cases it’s expected that the SDN controller or the management systems will be able to activate the different software packages based on the operator request.

The control plane flavors for the DOR shall initially support the P-router & Internet Gateway functionalities. In below section we will be listing the minimum set of software features that need to be supported for both targeted functionalities. There should not be any limitation to support a customized NOS which introduces further functionalities ex. Load balancer, Firewall.



4.2 DDBR SW features

4.2.1 Interface support

- LACP & HW based BFD
- Flapping protection (carrier delay/interface dampening)

4.2.2 Routing support

- IPv4/IPv6 static route
- OSPF/ISIS w/ BFD (graceful restart, ldp igp sync)
- MP-BGP
- LDP (LDP over RSVP)
- RSVP-TE
- SR MPLS
- PIM-SM

4.2.3 Quality of Service (QoS) support

The DDS platform shall generally handle all QoS functions like traffic classification, marking, metering, shaping & scheduling and particularly be able to:

- Classify incoming customer packets or frames into QoS classes based on 802.1p, DSCP or by static value that will follow the packet/frame through the platform
- Police customer packets/frames within classes using a dual rate policer to drop packets or to set a QoS class profile that will follow the packet/frame through the platform
- Police all incoming customer traffic within individual services or the total traffic in a group of services, which can be configured on a per-service basis
- Where a service uses only a single QoS class, police both the service and service group simultaneously. The service policer shall also be able to set the QoS class profile.
- Set egress MPLS EXP markings based on a configurable mapping from customer QoS class & QoS class profile.
- Schedule MPLS packets using at least 6 queues with at least 2 being capable of expedited behavior and all being capable of having an assured bandwidth or ratio.
- Operate at least two WRED profiles with MPLS queues based on a packet/frame's QoS class profile.
- Classify incoming MPLS packet's class & class profile either from the MPLS EXP markings or, where



the packet is destined for a connected customer access circuit, by the IP packet's DSCP markings. Both operations shall be possible simultaneously on the platform with the behavior specified on a per-service or service-group basis.

- Deploy up to 8 egress queues for QoS classes on each service with up to 2 being expedited queues and all queues being capable of assured bandwidth.
- Deploy up to 8 egress queues for QoS classes, each one of them should be independently configured as priority queue, weighted fair queueing or best effort.
- Police traffic on egress class queues and have at least 2 WRED levels (preferred 3) within service egress assured classes
- Shape service egress traffic on a per-service or total of a service group, where there is no policing within the classes, the platform should be able to egress shape on both service & service-group basis simultaneously and the egress shape service egress traffic on a per-service and per-service group basis simultaneously.
- Shape all traffic leaving a customer service ports.
- Set 802.1p COS based on QoS class
- Where the platform has multiple control plane elements, the platform shall ensure traffic forwarding continues uninterrupted throughout any failover between them. Where the platform's makes requirements of other platforms to achieve this, they should be clearly stated.
- Where the platform has multiple control plane elements, the platform should reestablish control plane signaling with other devices in a manner that results in no impact to traffic forwarding.
- The Platform shall support Avoidance of Head of Line Blocking (HOLB), as follows:
 - Once off the ingress line and into the buffer, no HOLB shall occur. The switch fabric must give the same consideration to QoS as the line cards.
 - Packets of a higher priority must be given access to the fabric without being blocked by larger packets of a lower priority.
- For the QoS marking function:
 - Marking of Platform self-generated control traffic: The Platform shall allow the IP Precedence of the following IP packets to be configured independently of each other by the operator : LDP, RSVP-TE, BGP, OSPF (all versions), ISIS, VRRP, PCEP, NETCONF, TLS & TELEMETRY
 - QoS marking function - self-generated OAM traffic
 - The Platform shall allow the IP Precedence of the following IP packets to be independently configured by the operator : SSH including SCP, SNMP read (all SNMP versions), SNMP traps (all SNMP versions), SYSLOG, NTP, Flow-record transport (e.g. IPFIX WG), FTP, TFTP, PCEP, NETCONF, TLS & TELEMETRY



- MPLS-Diffserv tunneling modes:
 - Long Pipe Model of MPLS-DiffServ tunneling (in accordance with RFC3270)
 - Uniform Model of MPLS-DiffServ tunneling (in accordance with RFC3270)
 - Short Pipe Model of MPLS-DiffServ tunneling (in accordance with RFC3270)
 - The Platform shall be configurable to set each of the three modes on a per egress sub-interface basis. i.e. it may be required to set Uniform Model on one sub-interface and Short Pipe Model on another sub-interface of the same common physical interface.
 - Pipe Model, Uniform Model and Short Pipe Model shall be supported on all interface types.

4.2.4 Hierarchical Quality of Service (H-QoS) support

The DDS platform shall support the following, in addition to the essential QOS functions mentioned in previous section:

- The platform shall support multiple hierarchical levels and the preferably 5 queues within each of the levels
- Each hierarchical level shall support as a minimum, a Low Latency Queue (LLQ)
- Each hierarchical level shall support 4 weighted round robin queues as a minimum
- Each hierarchical level shall support policing (shaping)
- Simultaneous traffic shaping at VLAN, VLAN group and Port Level (access ports)
- Traffic shaping at Port Level (NNI)
- Traffic shaping at VLAN Level (NNI)
- Traffic shaping at VLAN Group Level (NNI). Please provide number of VLANs per group are supported.
- It must be possible to apply H-QoS in a pseudowire termination architecture (where a pseudowire is terminated into a VRF)
- It must be possible to apply a single H-QoS policy to both L2 and L3 services simultaneously.

4.2.5 Security support

In general, its essential that the NOS SW performs all remote operation and maintenance tasks via encrypted protocols (e.g. SSH, SSL, TLS/DTLS).

Additionally, below features need to be supported:

- ISIS MD5, BGP MD5
- BGP FlowSpec



- Compliance with IETF RFC5575 & RFC7674
- IEEE802.1x/EAP-TLS
- ISIS MD5
- BGP MD5

4.2.6 Services Support

- IPv6 L3VPN
- CE-PE IPv6 L3VPN eBGP

4.2.7 Management Support

- Netconf/Telnet/SSH
- Ping/Traceroute
- IP-SLA
- SNMP/Telemetry
- TWAMP
- TACACS+

4.2.8 SDN & Telemetry

- PCEP
- NETCONF
- BGP LS
- SNMP/Telemetry



4.2.9 Scalability Figures


As a reference, the following scalability figures shall be supported by the DSS platform

4.2.10 Hardware Scalability:

Given that the hardware parameters and scalability figures will depend mainly on the number of whiteboxes used and consequently the cluster size. We are presenting the scalability requirements for the commonly used cluster sizes (in particular 4 scaling sizes) for the P-router in Figure-7 & for the Internet Gateway in Figure-8

Item	Small Cluster	Medium Cluster	Large Cluster	Extra Large Cluster
Size (RU)/Depth (mm)	16RU	68RU	130RU	430RU
Bidirectional throughput (Tbps), value for FULL DUPLEX	min. 16TB	min. 96TB	min. 192TB	min. 768TB
Maximum Number of 10GE ports per Packet Forwarder Whitebox	min. 40	min 240	min 480	min. 1920
Maximum Number of native 100GE ports per Packet Forwarder Whitebox without breakout solutions	min. 160	min. 960	min. 1920	min. 7680
Maximum Number of native 400GE ports per Packet Forwarder Whitebox without breakout solutions	min. 40	min 240	min 480	min. 1920

Figure 7. Hardware scalability figures for P-router



Item	Small Cluster	Medium Cluster	Large Cluster	Extra Large Cluster
Size (RU)	≈2RU	≈16RU	≈32RU	≈48
Bidirectional throughput (Tbps), value for FULL DUPLEX	min. 4TB	min. 16TB	min. 32TB	min. 92TB
Maximum Number of native 100GE ports per Packet Forwarder Whitebox without breakout solutions	min. 40	min. 160	min. 320	min. 920
Maximum Number of native 400GE ports per Packet Forwarder Whitebox without breakout solutions	min. 10	min 36	min 72	min. 252

Figure 8. Hardware scalability figures for Internet IGW



4.2.11 P-router SW Scalability:

Item	Small Cluster	Medium Cluster	Large Cluster	Extra Large Cluster
Maximum number of OSPF adjacencies	500	500	500	500
Maximum number of OSPF LSAs (Intra/Inter/Ext)	6000/1500/1500	6000/1500/1500	6000/1500/1500	6000/1500/1500
Maximum number of prefixes per Global Routing Table	2M	2M	2M	2M
Maximum number of BGP peers	210	210	210	210
Maximum number of BGP prefixes	2M	2M	2M	2M
Maximum number of PIM neighbors	500	500	500	500
Maximum number of entries for PIM(*,G)/(S,G)	500/100	500/100	500/100	500/100
Maximum number of LSP (LER/LSR) per system	1000/6000	1000/6000	1000/6000	1000/6000
Maximum number LDP FECs	500	500	500	500
Maximum number of T-LDP Sessions	150	150	150	150
Maximum number of T-LDP Routes	9000	9000	9000	9000
Max. SR IPv4 label stack depth without recirculation	8	8	8	8
Max. SR IPv4 label stack depth	8	8	8	8
Max. number of OSPFv3 adjacencies	500	500	500	500
Max. number of OSPFv3 LSAs(Intra/Ext)	500/10	500/10	500/10	500/10
Max. no. of IPv6 prefixes per Global Routing Table	1M	1M	1M	1M
Max. number of BGP peers for IPv6	260	260	260	260
Max. number of BGP IPv6 prefixes	1M	1M	1M	1M

Figure 9.P-router Software scalability figures



4.2.12 IGW SW Scalability:

Item IPv4/IPv6	Scale
Maximum number of IS-IS adjacencies	10
Maximum number IS-IS instances	1
Maximum number of NEs per IS-IS area	10000
Maximum number of prefixes per Global Routing Table	1M
Maximum number of VRF per system	max 4
Maximum number of IPv4 prefixes per VRF	max 500
Maximum number of IS-IS adjacencies	
Maximum number of BGP peers	2000
Maximum number of BGP prefixes	1M
Maximum number of LSP (LER/LSR) per system	Only VPN
Maximum number LDP FECs	max 4 VRF

Figure 10. Internet GW Software scalability figures

5. Management Plan Requirements

5.1 Telemetry & SDN readiness

As Network operators are moving away from the CLI and towards network programmability, DDS device being a key part of the Transport network shall conform with the Open Transport Architecture represented in **Figure-6**. That network programmability can be achieved by employing a hybrid SDN hierarchical architecture, in which the management and control functionalities are split between the devices and the controller.

The main goals of such SDN solutions are:

- Agile Network Programmability, enabling full network automation and reduced time-to-market service creation.
- Network Abstraction, simplifying Operation Support Systems (OSS) and orchestrators, and their interactions, by performing the adequate level of abstraction at each layer.

- Network Intelligence, enabling Traffic Engineering (TE) and automated service provisioning mechanisms between different layers and different vendor technologies.

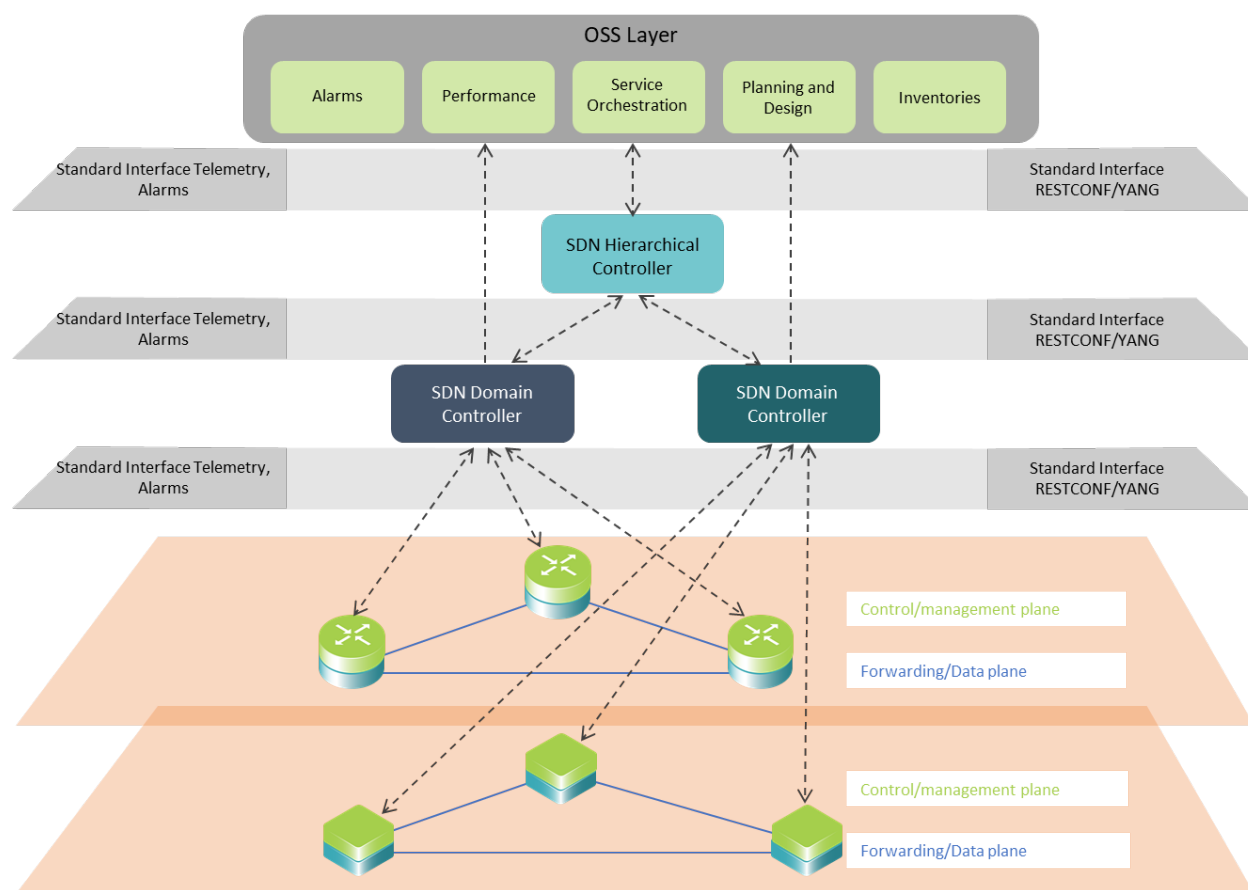


Figure 11. Open Transport SDN Architecture Vision

5.2 Standards support



The SDN & Network programmability concepts have been promising objectives for many operators and crucial for achieving agility in network provisioning and operation. In the past few years, standardization bodies and industry fora have spent lot of effort to standardize the SDN implementation and they have developed OpenConfig & Netconf RFC 6241

However, the network operators found a challenge to achieve network programmability and automation when it comes to a multi-vendor network. They soon realized that the programmatic interfaces available from networking vendors vary quite widely in form and function. The commands and data models used on vendor-A devices are completely different on vendor-B devices.

Recently, a group of network operators have joined efforts to tackle this challenge and collaborate in a new Telecom Infra Project (TIP) subgroup named MUST (Mandatory Use Case Requirements for SDN Transport) with the aim of accelerating and driving the adoption of SDN standards for IP/MPLS, Optical and Microwave transport technologies.

As illustrated in Figure-6 , The operators have shared their vision for the Transport SDN architecture with standardized North Bound and South Bound interfaces between different layers (Hierarchical controller, domain controllers & the devices).

We expect the partners developing DDS devices will follow the architecture standards and guidelines coming as a result TIP MUST subgroup collaboration

6. General Requirements

6.1 Regulatory requirements

The solution shall be compliant with EU GDPR regulation: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

6.2 Access security and anti-theft requirements

In general, the solution must support the necessary security mechanisms to authenticate and encrypt communications between the network element and its management system or controller.



The network element should offer the possibility of only enabling local traffic after the device has been authenticated by the management platform/controller.

The system should also offer the possibility to enable anti-theft mechanisms that prevent the use of the equipment in any other environment than the one it was conceived in.

7. Glossary

NSR Non-Stop-Routing



ISSU	In-Service Software Upgrade
ECMP	Equal Cost Multi Path
DOR	Disaggregated Open Router
P-router	IP/MPLS core router
IGW	Internet Gateway Router
TRS	Technical Requirement Specification
NOS	Networking Operating System
NMS	Network Management System
SDN	Software Defined Network
NNI	Network-Network Interface
UNI	User-Network Interface
DCSG	Disaggregated Cell Site Gateway
BGP	Border Gateway Protocol
OAM	Operations, Administrations, Management
TCAM	Ternary Content Addressable Memory
MOP	Method of Procedure
QSFP	Quad Small Form-factor Pluggable
IaaS	Infrastructure As A Service
PaaS	Platform As A Service
SaaS	Software As A Service
AR	Augmented Reality
VR	Virtual Reality



eMBB extreme Mobile Broadband

mMTC Massive Scale Communications

URLLC Ultra Reliable Low Latency Communications

MOP Method of Procedure

Copyright © 2021 Telecom Infra Project, Inc. A TIP Participant, as that term is defined in TIP's Bylaws, may make copies, distribute, display or publish this Specification solely as needed for the Participant to produce conformant implementations of the Specification, alone or in combination with its authorized partners. All other rights reserved.

The Telecom Infra Project logo is a trademark of Telecom Infra Project, Inc. (the "Project") in the United States or other countries and is registered in one or more countries. Removal of any of the notices or disclaimers contained in this document is strictly prohibited.