OGN RFI

Overview and Requirements

IP Core Router Disaggregation

July 12th, 2023
Version 1.3

Disclaimer

This notice constitutes a Request for Information (RFI) for the purpose of determining market capability of sources or obtaining information. It does not constitute a Request for Proposals (RFP), a Request for Quote (RFQ) or an indication that Orange will contract for any of the items and/or services discussed in this notice. Any formal solicitation that may subsequently be issued will be announced separately. Information on the specific topics of interest is provided in the following sections of this announcement. Orange will not be responsible for any cost incurred by responders in furnishing this information.

Table of contents

1 Scope of document

This document provides the bidder with a global view of our key requirements on OGN. OGN (Open Global Network) is the OINIS IP international network hosting enterprise and wholesale services, as described later in this document. This RFI does not cover the French perimeter (RAEI).

We need to assess if a disaggregated router could replace an integrated core router on OGN.

Beyond the technical evaluation of the bidder's proposal, that is the key objective of this RFI, we also need to anticipate the potential impacts of router disaggregation on OGN (operational support model, software & hardware lifecycle, security, network management, SLA, etc.).

We need to have an extensive visibility of the vendor capabilities with regards to those requirements. The vendor will provide a roadmap in case the requirement is not supported.

All the requirements must be supported on all the hardware (e.g. all the features should be supported from 1GE to 800GE interfaces). If it is not the case, the vendor should list and explain the associated constraints.

The vendor is asked to provide (in the boxes included in this document) detailed answers to each requirement listed or described in this document.

Note 1:

It is important to distinguish between the RFI and the RFP process:

1. In this RFI, we are not asking for prices, only technical information. We will evaluate the technical answers based on the written answers, i.e. we are not asking for a PoC (Proof of Concept).

2. In 2024, we plan to launch an RFP with similar requirements (but with much larger technical questionnaire) while pricing quotation and PoC will be asked. At the end of the RFP, we will select a candidate (see 3.1)

2 Objective of the RFI

2.1 Disaggregated core router

The present RFI is dedicated to the core router disaggregation solutions. As far the OGN core routers are also offering the wholesale *IP transit* service to connect the ISPs, the P/PE terminology can be used indifferently to designate those 'core' routers.

A disaggregated router solution allows a third-party router software running on various third-parties hardware platforms. In this model, the software is generally provided by NOS providers (Network Operating System) while the hardware – generally called "white box" - is provided by another provider.

In addition to the NOS providers and "white boxes" providers, traditional vendors are invited to answer this RFI, but only if they propose a disaggregation solution.

In this document we will describe our functional needs in addition to the capacity and control plane scalability needs. The capacity need refers to our regular needs for ever more powerful routers. For this purpose, three generic core router profiles are provided in chapter 10 with SMALL, MEDIUM and LARGE profiles **ranging from 1GE to 800GE interfaces.**

A total of 31 routers are concerned, as far as we assume a 1:1 router swap is possible; if not, the bidder could propose more white boxes, especially for the LARGE profile, using DDC or IP CLOS models.

The SMALL, MEDIUM and LARGE profiles are provided in this RFI to determine the power consumption and the carbon emission of the solution that will be provided by the bidder. Please note these profiles are not provided to calculate any price.

The proposed platform or solution should be scalable while offering an attractive licensing model and on 'pay as you grow' pricing model. So, even if we are not asking for the actual prices here, we are willing to know more about the licensing and pricing model, as well as any other elements that could impact the pricing structure.

2.2 Evaluating the technical feasibility and the support model

The aim of this RFI is mainly to assess the technical maturity of the router disaggregation market with regards to our needs. Another important point we need to evaluate is related to the support model, as discussed just below.

Traditional routers vendors offer turnkey and proprietary solution by integrating their own software with their own hardware. In a disaggregated model, this software-to-hardware integration is generally performed by the NOS provider, in close cooperation with the hardware providers. How much flexible and open is this model? Our first perception is that this integration remains proprietary- the NOS provider playing the same role as a traditional vendor - but the hardware choice looks more open.

Vendor answer:

Network Disaggregation, brings with it a significant increase in flexibility and openness compared to traditional, proprietary networking solutions

Open Standards

The use of open standards like those from the Telecom Infra Project (TIP), which encourages a more open, disaggregated approach to networking, is a fundamental principle of this model. These standards help to ensure interoperability between different

hardware and software components from different vendors, breaking down the walled gardens that proprietary systems often create. This fosters competition, drives innovation, and allows network operators to pick and choose the best solutions for their needs.

Hardware and Software Agility and Independence

In a disaggregated model, you gain hardware independence, meaning you can choose hardware and a Network Operating System (NOS) that fit your needs, without being tied to a single vendor's ecosystem. This flexibility allows for independent evolution of hardware and software, promoting innovation and enabling you to easily adopt improvements without waiting for vendor-specific updates.

Customisable scalability.

The decoupled model enables better network customisability and scalability. Businesses can mix and match different hardware and software to better meet their specific networking requirements. It also allows for scaling out (adding more devices) rather than just scaling up (upgrading to more powerful devices), which can be a more cost-effective approach for network expansion.

Reduced Power Consumption

Koomey's Law proves that the number of computations per joule of energy has been doubling approximately every 1.57 years, the disaggregated model can leverage this efficiency evolution to be more energy-efficient. This is due to the ability to use the most energy-efficient available hardware at each capacity upgrade without being constrained by the need to use a particular vendor's equipment. With power consumption being a significant operating expense for large-scale networks, this can lead to considerable cost savings over time.

Migration Flexibility

In a disaggregated model, the separation of hardware and software allows the operators to upgrade, replace or change each independently as per their requirements. This means that a network operator could, for example, decide to migrate to a more advanced hardware platform to gain additional capabilities, or switch to a different NOS that better suits their needs, without needing to replace their entire networking infrastructure.

DriveNets Advantage - Commercial Support and Integration

Despite the decoupling of hardware and software, DriveNets and ecosystem partners in a disaggregated model typically work in close cooperation. This ensures that the NOS will function correctly with the chosen hardware. DriveNets offers commercial end-to-end support that provide the same level of support as a traditional integrated vendor, including assistance with troubleshooting, updates, and integration with other systems. DriveNets works closely with all the ecosystem partners to provide support for both the hardware and software components, further reducing the complexity of managing a disaggregated

network.

Overall, the DriveNets disaggregated model can offer a high degree of flexibility and openness, although it does require a different approach to network management and support. The benefits in terms of customisation, cost reduction, power efficiency, and the ability to mix and match hardware and software, are leading many network operators to work with DriveNets and the DDC ecosystems to move to the DDC model over traditional, monolithic, and proprietary solutions.

2.3 Relying on an independent NOS provider or on the SONIC community?

As far as we are using the SONIC community software for the disaggregated switch currently under deployment in France, should we or could we apply the same strategy for the disaggregated router? Is that technically possible? Could Orange get internal resources to inhouse a SONIC model while making our needs supported by the community on the long term?

A router being much more complex than a switch, not only the feature set but also the performance and scalability aspects need to be assessed.

So, the vendor should be aware that SONIC is considered as a possible alternative to NOS commercial solutions. Oppositely, NOS providers are invited to explain why this model would not be the best appropriate for us. This RFI is to be seen as an opportunity for all of us to learn the pros & cons of a SONIC versus NOS solution and the bidder is invited to share its view and proposal.

3 RFI planning

3.1 Disaggregation – Orange general context

Figure 1 below provides the global Network Disaggregation roadmap of Orange.

As you can see, we have launched in France the deployment of disaggregated switches – based on Edgecore Networks switches running SONIC NOS. These switches will complement and/or replace the Cisco catalyst 4500. This project is recent and requires Orange INNOVATION to support SONIC. This is a brand-new operational support model. At the time of writing, we have little operational experience on this operational model. Over time, this project will help us to know if a SONIC solution support can realistically apply to the use case of a disaggregated OGN core router.

Main idea of Orange approach is to progressively deploy disaggregation form the less to the most complex features set, starting with disaggregated switch, then with disaggregated core router, then disaggregated PE.

Figure 1 OINIS Disaggregated Network roadmap

The focus of this RFI is summarized in the figure above (mid-term part). As you will see, we are raising many different questions because we are still maturing ourselves. Especially, we do not know yet if a SONIC solution is applicable to our use case, or if a disaggregated commercial solution is the only way to go.

Long term approach would be to deploy disaggregated PEs. No Orange study has yet been performed on OGN PE (IGN+IMN PEs). The DISRUPT RFP is probably a good source of information for OINIS, however it was too early to engage this RFP, being focused on the edge.

3.2 RFI Timeline

The OGN Disaggregation RFI is planned to be launched by end of June 2023 early July. Even if it is a formal exercise, we wish this RFI to be very open to discussion, given the objective is to comprehensively understand the bidder's technical proposal.

We propose to present this document to the bidder, from July 6th to July 12th, to ensure that our needs are clearly understood, while answering to any questions.

From July 13th, the bidder should be able to answer to this document as well as to the technical questionnaire. We propose a two-months period during which the bidder can prepare his answer and possibly continue to ask additional questions. The submission should be done on September 8th.

OINIS and Orange INNOV will analyze the bidders' answers during the following five weeks, until October 6th, with possible Q&A during the analysis time.

We are asking the bidder to present its proposal in detail during the defense meetings, that will be organized later-on during the mid-to-end October period.

In early November, we would like to determine if some disaggregation solutions proposed in this RFI could be considered for the RFP that will follow on early 2024. We emphasize this step will be crucial because it could lead to a new network paradigm for the ONIS infrastructure itself, the considered use case (OGN core) being highly critical for OINIS.

On behalf of ONIS and Orange INNOV, we would like to thank in advance the strong involvement of the bidder to that RFI.

Figure 2 Disaggregated Core router RFI timeline

3.3 No PoC required for the RFI

As explained in Chapter 1, the technical evaluation will be exclusively based on the bidder's written answers. We do not ask any PoC to test the bidder solution. A POC will be asked later-on, in 2025, at the RFP time. Please note at that time, power consumption measurement will be asked (for the profiles defined in chapter 10) because we admit theoretical figures have their own limits: they are theoretical!

3.4 An RFP will follow the RFI

As explained earlier, this RFI will help us to know about the technical feasibility of building a disaggregated OGN core router (including support model). A short list of disaggregated NOS candidates could then be defined for the RFP, that is mandatory to introduce new entrants in the Orange catalog, especially to define the contractual agreements.

Note that, in the RFP, not only NOS providers or white box providers can be invited but also the traditional vendors offering disaggregated and/or integrated router solutions. This is because the focus of the RFP will be to optimize our TCO, i.e. to reduce our costs without impacting the services offered to our customers, whatever the proposed solution if it answers all our needs.

From a timing standpoint, we plan to launch the RFP in Q1 2024 to deploy first disaggregated routers (or *integrated* routers) in 2025, given our deployment plan should elapse over the 2025-2029 period.

4 Introduction

4.1 OGN overview

By the end of 2022, OINIS has merged its two international IP networks - the enterprise IGN network and the Internet tier 1 OTI network -, in one single IP infrastructure called OGN, Open Global Network (see Figure 3 describing the objective and Figure 4 describing the existing architecture). It is important to emphasize that we performed an IGP merger (ISIS merger), not a BGP merger.

Before end 2022, we had two separate IGN and OTI IP infrastructures:

⇨ IGN – IP Global Network – was an IP infrastructure dedicated to the enterprise services, fully separated from Internet. IGN was built with dedicated P routers (MPLS LSRs) and dedicated Edge PEs running the enterprise services. During the IGN-OTI merger, only the IGN Ps were merged with OTI, i.e. the IGN PEs remain untouched and are still dedicated to the enterprise services. In this document we use the term 'IGN PEs' to refer to the dedicated belt of PEs offering services to our Multinational enterprise Customers (MNCs).

⇨ OTI – Open Transit Internet – designated the Tier 1 Orange Internet backbone, offering Internet wholesales services to ISPs and other key Internet players (CDN, ASP, etc.). OTI was a flat network, i.e. any transit router could be used to connect ISPs (wholesale service context). The flagship *IP Transit* service allows to interconnect ISPs and is complemented with a powerful anti-ddos solution. OTI was also used to connect IMN PEs, a dedicated set of PEs running L2/L3 VPN wholesale services for the mobile operators. Like IGN PEs, IMN PEs remain untouched and are still dedicated to wholesale customers.

OGN is the result of the interconnection of the IGN Ps with the OTI transit routers, forming a single SR/MPLS domain with a single L2 ISIS level, as shown Figure 3 and Figure 4.

1. OGN appears the new core for the IGN PEs. Still, OGN remains a flat network for the wholesale service.
2. OGN remains the Orange tier 1 Internet network but with an extended footprint thanks to the ex-IGN Ps. Therefore, ALL the OGN core routers host the Internet full routing table.
3. OGN core routers are dual stack IPv4/IPv6, even if backbone links are working in IPv4 exclusively, due to Flexalgo implementation choices. Full routing IPV6 is offered at the access, and we use 6PE to connect ISPs.
4. IGN PE and IMN PEs connect to OGN but are out of scope of this RFI. They are mentioned here to highlight their potential impact on the OGN control plane scalability because they share the same IGP.

The main functional difference between OGN and OTI relates to the support of Flexalgo. In short, Flexalgo is used on OGN to preserve the routing policies that were in place before the IGN/OTI merger. Flexalgo runs within the green area of Figure 4:

1. FA-128 is used to carry wholesale traffic (ex-OTI) based on bandwidth-driven routing policy.
2. Default algo 0 is used to carry the enterprise traffic, based on latency-driven routing policy.

OGN is a very new ecosystem, built around ~70 ex-IGN Ps and ~100 ex-OTI transit routers:

1. Cisco NCS5504, 5508 and 5516, deployed since 2017.
   These are targeting very high-capacity requirements, candidates for swap with LARGE profile defined in chapter 9.
2. Juniper Mx480 and Mx960, deployed since mid-2019, and now Cisco ASR9K
   These are covering smaller capacity requirements. They can be "compared" with the MEDIUM and SMALL profiles defined in chapter 10.

Other important features (but not really new) will be described later-on in this document (chapter 65.6) but globally, we need to cover the ex-IGN P + ex-OTI features requirements.

Figure 3 IGN/OTI merger objective

Figure 4 OGN (Open Global Network)

4.2 Commercial models

As shown in Table 1, 4 commercial models are generally considered:

1. The vendor offers an integrated NOS (Network Operating System) + hardware
   This monolithic model is NOT considered in this RFI, because the RFI is purely devoted to the disaggregation solutions. However, at the RFP time, it will be possible to answer with this model.

2. The vendor can provide a white box + a commercial NOS. In such a case the vendor shall be responsible for the whole solution (i.e. hardware + NOS) support/maintenance. If not, then the bidder will describe its support model.

3. The vendor can provide a white box + an open-source NOS (i.e. SONIC) with a commercial distribution. In such a case the vendor shall be responsible for the whole solution (i.e. hardware + NOS) support/maintenance. If not, then the bidder will describe its support model.

4. The vendor can provide only a white box and Orange will rely on Open-Source NOS (i.e. SONIC). In such a case, Orange will develop the missing features in SONIC and will be responsible for the SONIC life cycle and support. The vendor will be responsible for the hardware support. The bidder will describe its support model.

Table 1 Disaggregation model - cost structures

In this RFI, the vendor will be invited to answer with the possible models #2, #3 or #4. Model #1 is excluded. Please describe the proposed model. It is allowed to answer with several models, but each model should support the entire solution: we prefer to NOT mix the above models, because we privilege homogeneous solution. Mixing models seems too complex to us in a context where we already change our network paradigm.

Note that in model 4, Orange is the integrator, like we do for the ODOS project (disaggregated Edgecore switch running SONIC). Possible support is welcome from the provider, but Orange remains the only one integrator.

Vendor answer:

Our approach is based on model #2, and we will complete the model for this RFI using data and information for UfiSpace hardware. *However, it is important to note that we support hardware appliances from various hardware vendors which comply with the DDC/DDBR platform specifications.*

This includes merchant silicon vendors like Broadcom, Silicon One and Nvidia, and from many ODM's such as UfiSpace, EdgeCore, Acton and many others.

DriveNets is committed to certifying any open DDBR/DDC ODM vendor, ensuring that our software is optimized and fully compatible with their hardware appliances. We believe in providing our customers with the flexibility to choose from a diverse range of hardware options while enjoying the benefits of our powerful and feature-rich NOS.

DriveNets is responding to this RFI based on a DDC/DDBR approach for clarity, however it should be noted that the DriveNets Network Cloud and software stack fully supports IP CLOS architectures and has been deployed into Tier 1 operators using IP CLOS approaches.

5 Architecture aspects

5.1 DDC, IP CLOS, chassis, may be other options

To deal with very high-capacity router needs, the bidder could propose a disaggregated router based on DDC (OPC Distributed Disaggregated Chassis) or IP CLOS architecture or on a single chassis.

- In the case of DDC, the disaggregated router can be made of several white boxes interconnected to each other using dedicated links to form the fabric. As shown in Figure 5, DDC is based on spine/leaf architecture where the spine is made of multiple white boxes, the Network Cloud Fabric (NCF) that are exclusively used to switch traffic between the leaves called Network Cloud Packet Forwarders (NCP). These later can be compared to the Line cards of an integrated router based on chassis architecture. DDC also includes additional devices such as the NCC.

- In the case of an IP CLOS architecture, as shown Figure 6, similar spine/leaf architecture is generally proposed. The difference with the DDC model relates to the fact this is an IP solution where each node forming the cluster is an ISIS node.

- In the chassis model, the fabric is internal (traditional model, no figure).

The vendor shall describe the solution proposed amongst the three listed above. A full explanation is expected, describing the internal mechanics of the DDC, IP CLOS or chassis architectures.

A mix of DDC and IP models remains theoretically possible, but we are not in favor of such approach, because it will add operational complexity. So we are asking the bidder to privilege a unique model, either DDC or IP fabric, while possibly explaining the pros & cons that make the difference.

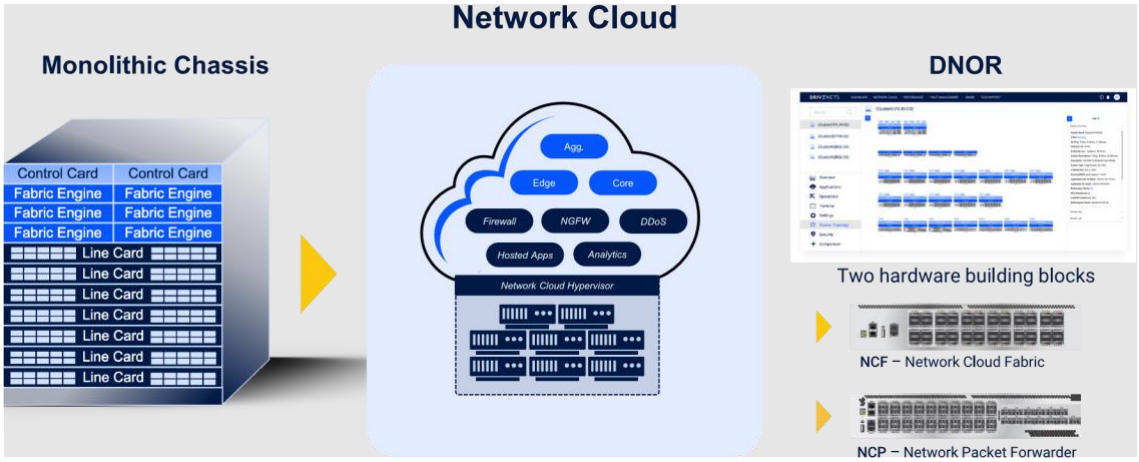
There might be other solutions different from the DDC cluster, IP CLOS cluster or single chassis, and the vendor is free to propose any alternate cluster solutions to meet our needs. Still, we are targeting non-blocking fabric solution, with the same level of features set, redundancy, control plane scalability etc., as discussed later in the document. Also, the solution must still be based on software / hardware disaggregation principle, as defined in 2.1.

The bidder is invited to detail his architecture model below and why he thinks this best suit our needs. Especially, how is the NOS software integrated on a given hardware? Also, please describe the process and time to perform this software / hardware integration.

Vendor answer:

The DriveNets Network Cloud architecture offers a high degree of flexibility and modularity, enabling multiple deployment models to suit different network requirements and needs. It can be deployed in standalone mode within a single white box or in a cluster mode where multiple white boxes are interconnected using a Clos topology, effectively functioning as a single very scalable and highly reliable router.

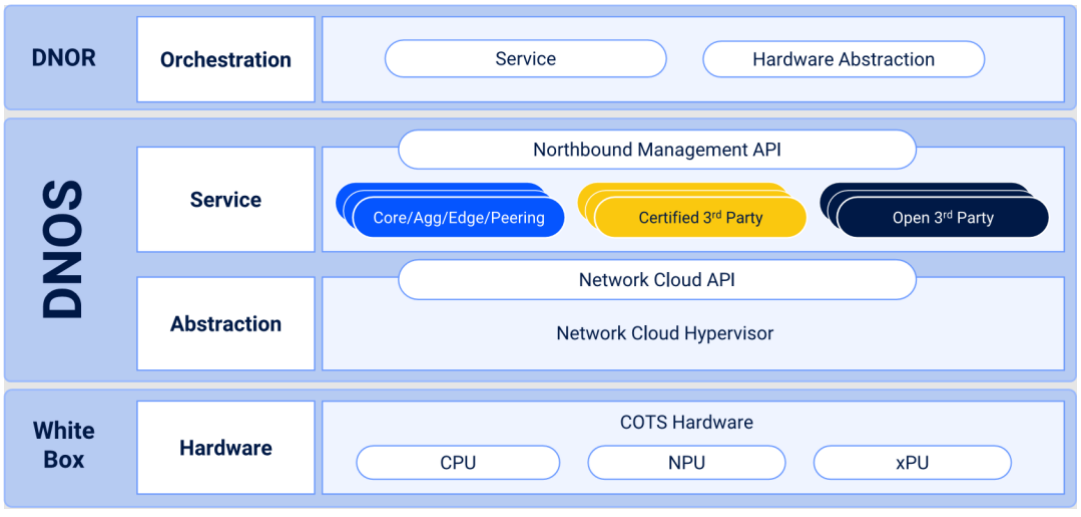
By breaking down the big router into white box building blocks and running cloud-based software on top, DriveNets Network Cloud provides a disaggregated approach. This architecture separates the control plane and data plane, allowing each to scale independently. The control plane runs on x86 servers, while the data plane is implemented using a cluster of white boxes.



The data plane consists of two main building blocks: the Network Cloud Packet Forwarder (NCP) and the Network Cloud Fabric (NCF). It can scale from a standalone solution with a capacity ranging from 2.4 to 12.8Tbps to a large cluster comprising dozens of white boxes, operating as a single routing entity with a massive capacity of 691.2Tbps.

DriveNets Network Cloud introduces a new way of building networks. It replaces the large, monolithic routers with multiple similar, simplified and vendor-neutral white boxes. It then applies hyperscale cloud operational principles over them to simplify the entire operational model. This enables extreme growth, rapid service innovation and greater service profitability.

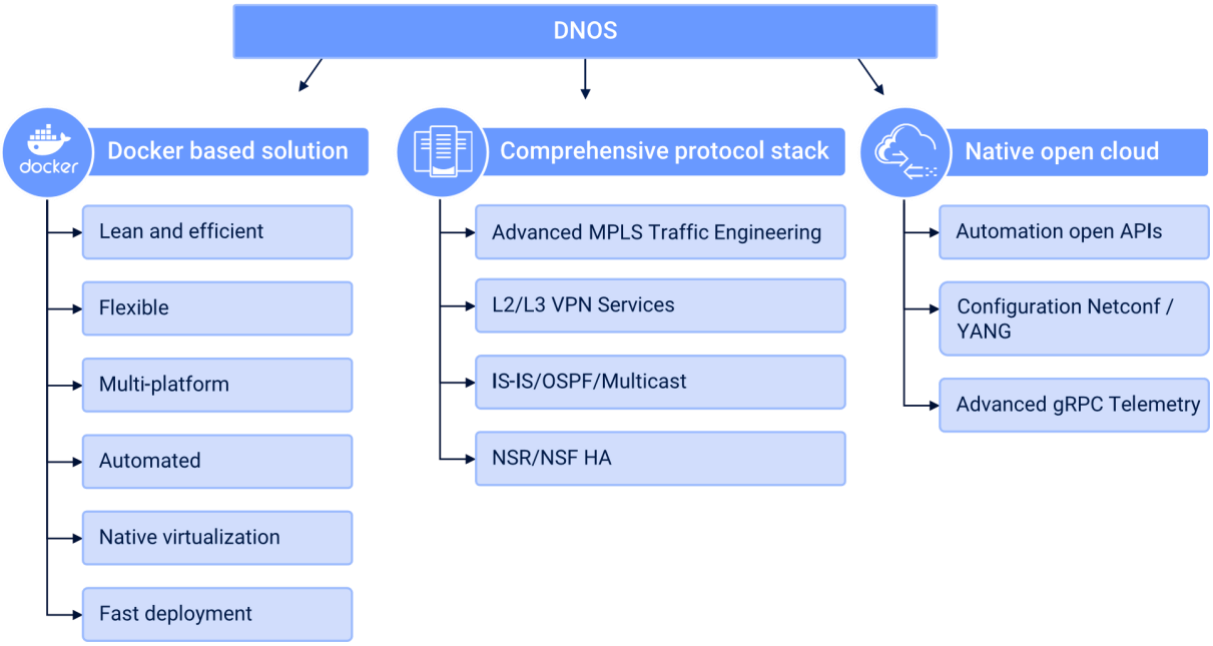
DNOS was designed from the ground up to run on multiple ASICs in different setups and to easily adapt to different types of hardware with relatively low effort. The logical separation between the control and data planes ensures a high level of flexibility and quick adaptation.



Network Cloud highlights include:

- Web scale software architecture: The NOS design is based on a microservice architecture, allowing maximal independence between functions so they can scale and be maintained easily using simple standard automation tools.
- High availability: DNOS architecture inherently enables high availability, where each microservice is backed by another. Using health-check mechanisms for monitoring containers, processes and system resources means a microservice can recover quickly and seamlessly. DNOS' layered and distributed high availability combines classic router high-availability features, such as non-stop routing (NSR)/non-stop forwarding (NSF), with microservice internal orchestration and other high-availability mechanisms.
- Natively disaggregated control and data planes: The data plane is wrapped by a hardware abstraction layer (HAL), resulting in low chipset dependency, thus expanding the range of deployable chipsets/chip manufacturers. The flexible interfaces between them ensure easy adaptation.
- Same software suite for all deployments: DriveNets disaggregated router supports small to very large routers using the same white box building blocks and can scale from a single box-based router to the largest router available– all with the same NOS software. Once provisioned, the router cluster formation, no matter how large, acts as a single network entity, like the familiar chassis-based router.
- Underlying standard Linux distribution: DNOS provides a scalable, reliable, and programmable infrastructure to run any data and control plane functions (routing and others). Built on a Linux-based OS, containerized microservices and open APIs
- Zero-touch provisioning: Supported from the ground-up, zero-touch provisioning allows for fast and automated deployment. Using an orchestration system, which has an API to the NOS, DNOS automatically detects a scale-up procedure of a white box in a cluster.

DNOS patent-based technologies – such as distributed logic, two-phase configuration sync, and a high-scale ultra-fast messaging bus – enable the implementation of network services over a distributed architecture at telco-grade timing and scale.



Network Cloud Software Design

DriveNets has designed and built Network Cloud with modern cloud centric architectures and this agile development approaches. This has allowed us to develop DNOS as much more than a traditional network operating system; it is a virtualization layer running over white boxes and servers. To ensure this, the following DNOS design guidelines were put forward:

- Natively distributed NOS: Contrary to monolithic software, DriveNets DNOS does not assume any specific location for any management or networking function; every element is encapsulated as a container, which provides the flexibility to orchestrate it.
- Extensive use of containers: To ease development, deployment and upgrading, DNOS containers function as services that are built, tested and deployed as units. Eventually development is done the same way as testing and deployment in the field.
- Optimized resource utilization: Servers are not the only source of compute resources. The compute for services like LACP, BFD, flow monitoring, etc., can be handled locally on the white box (the NCP – Network Cloud Packet Forwarder) without overloading the controller (the NCC – Network Cloud Controller). This allows for linear growth whenever a new NCP is added.

Abstraction and Orchestration of the Router Elements

DriveNets DNOS is a full-featured networking stack, ready to run on any Network Cloud-certified hardware platform. It creates a unified, shared network infrastructure that spans multiple servers and white boxes and is managed as a single network entity. Combining cloud and virtualization technologies, DNOS enables running any service on the unified shared infrastructure and attaching any service to any port.

With DriveNets Network Cloud, every element is a repository of resources. Control card, fabric or line cards all become logical functions that need to be orchestrated and allocated by DNOS to the right place, creating a unified network element.
Every element in the cluster is abstracted in the same way so it is easy to stack them. The server and white box contain an x86 chip as both a compute resource and as a networking resource; they also have a switching ASIC (e.g., Broadcom, S1, etc.) or software-based data plane (e.g., DPDK).

To enhance flexibility and compatibility, the data plane is wrapped by a hardware abstraction layer (HAL). This abstraction layer reduces chipset dependency, enabling a wider range of deployable chipsets and chip manufacturers. The flexible interfaces between the hardware components ensure seamless adaptation and integration within the DriveNets Network Cloud architecture.

The advantages of DriveNets Network Clouds distributed cloud-native NOS includes:

- Optimal scaling: This DriveNets approach addresses any scale with telco-grade high availability. Like in any distributed and non-distributed system, when scale comes into play it amplifies the probability of error, exposing any design weakness.
- Consistent features across platforms: From the smallest router to the largest, the hierarchy and syntax of the commands are the same.
- No performance degradation: Using a virtualization layer, the data plane scales by adding more white boxes to the same logical network element with no performance degradation or downtime. The control plane scales by simply adding more resources to the server.
- Seamless integration and automation: These are achieved via open standard northbound interfaces, enabling rapid integration into traditional network operations environments and modern DevOp's and automated operational environments.

Summary

The DNOS best-in-class enabling architecture was built for scale, service growth and orchestration. It completely reinvents router architecture by basing it on the web scale architecture of the cloud. DNOS is a distributed software that enables resource optimization and simplification while still behaving like the familiar monolithic router OS.

DNOS is easily portable and can be deployed to various NPU and ODM platforms. It can be deployed either as a standalone self-contained software package or as very large clusters, supporting 10s to 100s of white boxes as a single orchestrated routing entity.

Figure 5 DDC router integration to OGN (spine/leaf cluster)

Figure 6 IP CLOS router integration into OGN (spine/leaf cluster)

5.2 Impact analysis of DDC and IP CLOS models

DDC and IP CLOS are based on spine/leaf architecture, where multiple white boxes are part of the node. This is a new approach to OINIS and we need to fully understand the challenges of such approaches.

Intuitively, we would tend to limit the number of white boxes because:

1. The number of white boxes could impact the ISIS scalability (IP CLOS model): number of ISIS nodes/prefixes/MPLS labels will increase (given today we are still using both LDP and SR)
2. It could make the cabling management harder than today (on a router, we have no external cabling to build a fabric, “leaves”/Line cards being meshed to each other by the fabric itself)
3. We are very concerned with the power consumption: the more white boxes the more power consumption, unless specific mechanism exist to optimize the power consumption.

We also need to better characterise the impacts of DDC and IP CLOS models, to determine how each model is open and evolutive. What kind of lock-in are exposed to?

1. In the DDC model, we think of the following possible impacts:
   - chipset diversity (see next section)
   - software procedure: how much is it disruptive, how is the degradation controlled during the s/w or upgrade, how much time does it take to upgrade a large profile node?
   - scale out procedure
     If we want to add a leaf, this will require to add cables with extra s/w configuration for the new and existing leaves and spines devices. We need a procedure that is ideally non-disruptive and provide fast insertion of the new leaf or spine in the DDC node
   - ISIS scalability seems less than the IP CLOS, but we don’t really know if this model requires each device of the DDC node to run IP addresses and
   - power consumption
   - cabling management
   - overhead

2. In the IP CLOS model
   - how a large profile router is built and managed when several IP white boxes are required
   - scalability impact on ISIS seems noticeable here, unless some particular mechanism allows to rationalize the spine/leaf IP fabric from an ISIS and IP address usage viewpoint.

We invite the bidder to share their impact analysis, i.e. the pros & cons of DDC/IP CLOS/chassis solution.

Vendor answer:

Q: Software procedure: how much is it disruptive, how is the degradation controlled during the s/w or upgrade, how much time does it take to upgrade a large profile node?

A:
To put it simply, the DDC and chassis architectures are not vastly different, as they share similar components:

- Leaf (NCP) aligns with LC
- Fabric (NCF) corresponds with Fabric cards
- Route Engine (NCC) matches with RE
- They both include an internal switch

While the primary components remain the same, the differences between the two architectures on the software side are more significant when it comes to DDC:

1. The software components are constructed independent of specific hardware, made possible through the creation of a Hardware Abstraction Layer.
2. The scalability of the solution is far more robust and can accommodate greater growth.
3. DNOS is a modern NOS built using the latest development approaches and techniques, such as Secure By Design development, CI/CD integrated QA, Cloud Native Container based service environment and modern API driven integration.

These approaches allow DNOS to deliver robust outcomes for network lifecycle management, service agility and network availability.

Q: scale out procedure
If we want to add a leaf, this will require to add cables with extra s/w configuration for the new and existing leaves and spines devices. We need a procedure that is ideally non-disruptive and provide fast insertion of the new leaf or spine in the DDC node

A: Adding a new leaf system is hitless and not traffic disruptive the same as adding a new line card to a Chassis system. The DriveNets Network Cloud will automatically adopt the new leaf, assign it as an NCP within the cluster and make the additional ports and services available – without intervention and with modification or reconfiguration to the other nodes or running configuration and services.

Q: ISIS scalability seems less than the IP CLOS, but we don't really know if this model requires each device of the DDC node to run IP addresses and

A: From a network standpoint, the DDC behaves as a singular node in the topology, irrespective of the number of Leaf/Spine boxes (NCP/NCF) involved. This means that there is only one loopback/router ID address utilized by network protocols like ISIS, BGP, SR, etc., and as perceived by NMS/OSS systems. The System is managed as a single entity through standard interfaces. (NetConf / RESTCONF / gNMI / gRPC / EMS / CLI, etc.)

Q: power consumption

A:
Distributed Disaggregated Core Routers leverage modern hardware and software technologies to optimize for power efficiency. The principles of selective just-in-time scaling and Koomey's Law both contribute to these systems' ability to deliver high performance with lower energy consumption.:

Scalability: In a traditional setup, you might have to overprovision your routers to handle peak traffic, meaning you'd have excess capacity that's wasted during off-peak times. With

a disaggregated router, you can add hardware as needed, reducing idle capacity and therefore energy usage.

Dynamic Resource Allocation: The disaggregated setup allows for selective just-in-time scaling. This means you can turn on/off specific modules based on the actual demand, rather than running everything at full tilt all the time. This is more energy-efficient because you're only using the power you need.

Hardware Optimization: Their modular setup allows for specialized, energy-efficient hardware, in line with Koomey's Law, which states that energy efficiency in computing improves over time.

Improved Airflow and Cooling: The distributed nature of DDC architecture often results in improved airflow and cooling mechanisms, allowing the components to distributed in the environment, allowing efficient cooling design - avoiding hot spots, under and over cooling, etc - allowing for significant reductions in environmental power usage.

Selective just-in-time scaling ensures resources are used only when needed, minimizing waste. Koomey's Law suggests that as hardware gets more energy-efficient, these routers will continue to use less power for the same performance, making them increasingly efficient over time.

These features make Distributed Disaggregated Core Routers efficient in terms of power consumption, which is beneficial not just for operational costs but also for the environmental impact.

We have provided full power consumption details in the XLS as requested, it should be noted as the builds are point in time, Like for like forklift swaps they do not benefit from any of the scalability power savings or optimisations and as such are significantly sub-optimal in terms of power usage.

Q: cabling management

A:
The DDC offers significantly enhanced flexibility and scalability when it comes to commissioning network elements. The distributed nature of DDC systems allows for the easier setup and integration of new components or systems within the network. This scalability means that as the network grows or changes, additional elements can be commissioned efficiently without major disruption or reconfiguration of the existing infrastructure. Each component, such as NCP/NCF/NCC (Spine / Leaf / Route Engine), can be installed separately throughout the co-location. This brings several notable benefits:

- If power or space per rack is limited, installation can be distributed across multiple racks.
- In cases of power or cooling issues, it provides improved heat dissipation options.

- Cable management becomes more efficient as, instead of connecting to a single point (chassis), NCPs can be installed closer to the network connections.
- DDC components can be distributed within the switch room or data-centre to optimise cooling and power availability.

Q: the pros & cons of DDC/IP CLOS/chassis solution.

A:
Following are the major points for comparing DDC to IP Clos solution:

- *Reduces complexity*
  Logical single instance for all network services – independent of DDC cluster size
  Single control-plane management (One CLI for the full cluster vs multiple systems OS)
  Single RIB & FIB update
  No IP addressing is required on fabric links.

-*Improves reliability*
  No shared fate across components for chassis services
  Predictable distributed power utilisation
  Reliable orchestrated containerised network services
  Ingress allocation for End-to-end Quality of Service (QoS)
  Predictable Fabric Bandwidth Allocation

- *Facilitates automation*
  By moving the network services to the software layer enables the network to be orchestrated and automated for operations in the same way as cloud software services.
  Built from the ground up for API first automation approaches.
  Support for standard automation toolchains
  Single upgrades across all network devices with traffic protection to minimize disruption and improve service availability.

- *Improved scalability*
  Not limited by IGP scalability on the nodes
  Spine / Leaf numbers not Limited by ECMP scale
  Network topology it is a single node in the network versus number of nodes and complexity
  Cell-based fabric offers significant performance and scalability capabilities versus less efficient ethernet based fabric techniques.

5.3 Platforms support

The bidder is expected to provide the exhaustive list of platforms (white boxes, servers, switches, optics, etc.) and ensure that the features required in this document are equally supported on the various white boxes or chassis hardware models.

Vendor answer:

DriveNets support the following off the Shelf NPU's Broadcom Jericho family: (J2, J2c, J2c+, Ramon, currently evaluating J3, Ramon3) and is proven to operate on other merchant silicon NPU families.

At DriveNets we are committed to enabling the vision of DDC by disconnecting the hardware and software we enable operators like Orange to take advantage of the best most appropriate hardware and to change the software as needed. To enable this flexibility and allow Orange the most network agility and efficiency, DriveNets are committed to ensuring our DNOS and Network Cloud is able to run on any DDC/DDBR Whitebox hardware platforms our customers want. We will certify additional ecosystem partners as needed by our customers and will NOT restrict any of our customers from changing to new hardware platforms or removing our software and running other NOS solutions on the hardware platforms. We believe that DDC should be an open ecosystem.

To ensure this we name our cluster components based on the function and the number and type of ports offered – Any ecosystem hardware provider platforms can be utilised.

NCP HW platforms supported today (Chipset):

NCF-48CD:	48x400GE (Ramon)
NCP-10CD:	10x400GE Fabric 13x400GE (J2)
NCP-40C:	40x100GE Fabric 13x400GE (J2)
NCP-36CD:	32x400GE Fabric 40x400GE (J2c+)
NCP-64X12C:	64x1/10/25/GE + 12x100GE Fabric 6x400GE (J2c)
NCP-64X8C2CD:	64x1/10/25/GE + 12x100GE Fabric 6x400GE (J2c)

Planned roadmap for H2 2024:

NCF-64DCCC :	64x800GE (Ramon3)
NCP-18DCCC :	18x800GE / 36x400GE Fabric 20x800GE (J3)

NCM:

NCM-16I32D:	16*10GE + 32*1GE (Broadcom QMX based)

NCC (Compute Route Engine):

HPE DL360 / DL380 - 32 Core/40 Core
Dell R640 / Dell R740 - 30 Core/40 Core
Any standard COTS server platform.

Fabric / Spine = NCF
Leaf = NCP
(D=1GE, X=10GE, C=100GE, CD=400GE, DCCC=800GE)

5.4 Chipset diversity

Chipset diversity refers to the way of mixing multiple chipsets from multiple silicon merchants or from different models or generation if the solution is based on a single merchant silicon. This is of particular interest when we need to upgrade only part of the DDC leaves or when we want to introduce new generation line cards in a chassis, for instance:

- In the case of DDC can we mix different white boxes using different chipset families or different generations?
- In the case of chassis, can we mix different line cards with different chipset families or with different chipsets generations?
- The IP CLOS model is not exposed to this type of potential limitation because the model is IP based.

Taking the example of Broadcom, can we mix Jericho, Jericho+ and Jericho2 chipset in an DDC or chassis model?

Please describe the chipsets proposed in your solution and the diversity of chipsets supported in your solution (e.g. in a DDC or chassis cluster)

Vendor answer:

Currently, within the same cluster, we support different generations of the Broadcom Jericho family: J2, J2c, J2c+, along with their respective leaf NCP types: NCP-10CD/NCP-40C, NCP-64x12C, NCP36CD.

The DriveNets NOS strategy is to ensure that the Jericho3 and Ramon3 based platforms are backwards compatible with all existing NCP and NCF platforms and that the DNOS software provides common and superset functionality across all present Jericho/2/2c NCP so that our operator customers can effectively evolve their networks as new power efficient platforms become available without impact to the core networking functionality.

As it pertains to the support of silicon other than Broadcom, as of today 2023, DNOS (DriveNets Network Operating System) is commercially available only on Broadcom-based Jericho family silicon. DNOS is deployed working and operational on other common merchant silicon based NPU families and whitebox ODM platforms.

DriveNets has no limitation in terms of supporting other silicon vendors and platforms. Indeed, we are currently in the process of expanding DNOS to support silicon from other vendors.

5.5 Redundancy

Redundancy is a key subject. Especially, we need control plane redundancy, as far as this is already supported on our network by the Cisco NCS/ASR9K routers and Juniper MX routers.

- how is the power, control plane and data plane redundancy provided by the bidder?
- Do you provide the same level of redundancy whatever the profiles depicted in chapter 10?
- Do you provide N:1 fabric redundancy for all profiles?
- Is power supply redundant for all profiles?
- …

Vendor answer:

DriveNets solutions are operational in some of the largest Tier-1 networks worldwide. The system availability and redundancy have undergone rigorous testing in the most stringent labs and have proven their reliability on extensive networks. Here are our primary areas of focus concerning redundancy:

- Every element (NCP / NCF / NCC / NCM) is equipped with a N+1 Power supply and N+1 Fans for redundancy.
- The cluster configuration can be designed with various degrees of redundancy as required.
  - The NCF (Fabric) can support N+2 or even higher levels of redundancy.
  - The NCC (Route Engine) is deployed with N+1 redundancy.
  - The NCM (Internal Switch) has N+1 redundancy.

Unlike traditional chassis approaches the level of cluster redundancy can be increased and changed by the addition of new hardware, changing the Fabric (NCF) and Port appliance (NCP) mix and changing the software configuration and distribution across the platforms.

All our software components ensure at least N+1 redundancy, at the level of Docker containers and processes. DNOS supports NSR/NSF for all proposed protocols, offering a seamless switchover between Route Engines and local restarts.

5.6 About the fabric Overbooking

Today, the Cisco NCS, ASR9K and Juniper Mx routers deployed on OGN have non-blocking fabric. This means the fabric does not perform overbooking: each packet is carried internally within the router without any chance to be dropped by the fabric itself. So, the fabric cannot be a bottleneck.

In a disaggregated solution, we therefore want to have similar solution: we don't want to overbook the fabric. Not only this would impact our existing planning rules, making more difficult the operational management and planning exercise, but also, we need to compare apples and apples. How can we compare our deployed solution - without fabric overbooking - with another one that would be based on a specific fabric overbooking? Moreover, a complete study would be required to know which overbooking factor could apply in the future: we are not at that stage in this RFI.

For these two reasons, we ask vendors to provide their disaggregation solution without fabric overbooking. In a disaggregated solution using DDC or IP CLOS models, this translates into providing as much capacity on fabric (links between spine and leaf devices) as the one required to absorb the ports capacity specified of the largest routers (see Table 6).

6 OGN Functional Requirements

In this chapter, we will describe the key OGN functional requirements that we want to focus on with the vendor, to complement the technical questionnaire associated to this RFI.

Important Note: the bidders answering with commercial model #4 do not need to answer the questions below unless some hardware optimisation is done for some specific features (MACSEC, convergence – e.g. TI LFA, etc.). We still ask the bidder to answer to the questions if hardware optimization is implemented for a given feature. ALL bidders must answer the questions related to the scalability (number of routes, etc.).

6.1 Segment Routing

6.1.1 SR MPLS IPv4

OGN is a Segment Routing MPLS IPv4 network. We do not plan to use SR MPLS IPv6.

As far as OGN is dual stack IPv4/IPv6, it offers IPv6 connectivity to the customers using 6PE.

Topology Independent LFA is deployed on top of the OGN SR domain.

Please confirm that SR MPLS IPv4 is supported and explain if the implementation has any limitations.

Vendor answer:

DNOS fully supports SR MPLS, and its key features such as SR-TE, Flex-Algo, Dynamic ODN, PCEP, BGP-LS, BGP Prefix SID, SRMS, IPv6 over SR-MPLS, etc. DriveNets constantly continues to develop and enhance our DNOS SR capabilities in the domains of SR-TE, PCEP, Flex-Aglo and many others.

- SRGB Default: Base 16000, Range 8000
- MIN BASE: Any available MAX BASE: 700K
- MAX SRGB range is 256K, MIN SRGB Size 4000.

Following might be considered as implementation limitations.

- SRGB must be contiguous
- SRGB Changes may require a reboot.
- Protocol SRGB takes precedence over global SRGB.
- A node-SID must be /32 address attached to a local loopback interface (1 per system)
- Regardless of the configuration style the advertisement will be always done as base and index and not as absolute value.
- Prefix-SID outside of the local SRGB should not be used and a log message is generated.

6.1.2 SRv6 (for information only)

At the time of writing, OINIS does not plan to deploy SRv6 on the mid-term, may be on the longer term, in case of technology evolutions requiring specific features that would be available only in SRv6. For this reason, we need to follow-up the SRv6 activity, to anticipate the future.

The vendor is invited to share his strategy with regards to SRv6, including feature support and roadmap.

Vendor answer:

We are closely observing the market's evolution and adoption of SRv6, while gathering requirements from our customers.

Currently, DNOS fully supports IPv6 over SR-MPLS topology, including all key SR related features, such as – Flex-Algo, SR-TE, ODN, TI-LFA, uLoop avoidance, BGP prefix-sid – All supported in IPv6 over SR-MPLS as well. This provides a solid solution for migrating an IPv4 MPLS SR based network (Such as Orange's), to a multi-topology network with IPv6 as well, while slowly migrating to IPv6. SR-MPLS IPv6 provides a more gradual transitory solution to migrate to IPv6. Once that is achieved, SRv6 can be considered as well, and MPLS will be phased out from the network.

Our verifications have confirmed that DNOS, in conjunction with the underlying Broadcom HW Jericho chipset, is fully capable of supporting SRv6 features, providing a complete solution for switching to SRv6, as the next migration phase, after SR-MPLS over IPv6. As of this writing, DriveNets does not yet have a committed roadmap for SRv6 support.

6.2 Traffic engineering strategy

6.2.1 Flexalgo

As mentioned earlier in this document, Flexalgo is used to preserve on OGN the routing policies that were running on IGN and OTI separately from each other (in 2022).

Before the IGN/OTI merger:

1. Enterprise traffic was running on IGN (PE+P) to optimize the customer traffic latency: default IGP metric was reflecting link latency.
2. Wholesale traffic was running on OTI to optimize the customer traffic bandwidth usage: default IGP metric was reflecting link bandwidth.

After the IGN/OTI merger, so on OGN:

1. Enterprise traffic is running on OGN to optimize the customer traffic latency: default IGP metric is reflecting latency. No change.
2. Wholesale traffic is running on OGN Flexalgo FA-128 to optimize the customer traffic bandwidth usage: the ASLA TE metric is reflecting bandwidth (with same values as before the merger). ASLA refers to the Application Specific Link Attribute RFC (draft-ginsberg-lsr-rfc8919bis-02 (ietf.org).

Therefore, we need to know if the vendor supports Flexalgo and if it fully interoperates with Cisco and Juniper Flexalgo implementations.

Please describe the FA implementation, its potential limitations, and your roadmap. It should cover L3 and L2 VPWS/EVPN cases. Amongst others, here below are some questions related to Flexalgo support:

- Does the bidder support IPv4/IPv6 traffic steering to Flexalgo?

- Does the bidder support L3vPN steering to Flexalgo?
- Please describe the vendors' interop you have tested
- Are the ASLA TE (priority 1) and DELAY (priority 2) metrics supported? Is the legacy bit (L-flag) available?
- The vendor will describe the dynamic steering principles and implementation details (static, dynamic steering). Today we use BGP routes coloring to steer traffic to FA-128.
- We are also willing to steer L2VPN traffic: do we have to use EVPN (BGP based) to steer colored routes to FA128 or do you also offer the option of dynamically steering point-to-point PW (VPWS) to FA128?
- Please provide the max number of FA instances supported by the implementation and if there are any limitations associated to the maximum number of instances.

Please fully detail your Flexalgo implementation and roadmap.

Vendor answer:

DNOS fully supports the following with respect to Flex-Algo:

- ISIS SR-MPLS IPv4 & IPv6 Multi-topology Flex-Algo
- BGP automated steering over Flex-Algo IPv4/6 - VPNv4, VPNv6, IPv4 Unicast, IPv6 Unicast, 6PE, IPV4/6-LU, EVPN, according to BGP color extended communities.
- Support "static steering" as well, of L2VPN-VPWS over specific Flex-Algo and/or SR-TE policies.
- Support both legacy TE TLVs and ASLA in Flex-Algo
- IGP metric, TE-Metric, Static / Dynamic Delay, SRLG, Admin-Groups (standard and extended)
  - Dynamic Delay will be based on Simple-TWAMP (TWAMP-Light) calculations.
- IPv4 & IPv6 TI-LFA (link, node, SRLG protection) per Flex-Algo
- IPv4 & IPv6 uLoop avoidance per Flex-Algo
- Supporting 10 Algorithms per ISIS-Instance (spf, strict-spf, and 8 more user-defined Flex-Algo)
- Configurable 'No-fallback' ("drop-upon-invalid") option on SR-TE policy and on Flex-Algo
- Multi ISIS-SR instance (With no redistribution between instances)
- Flex-Algo SIDs OAM (Ping and Traceroute)
- Support ECMP of up to 64 paths over a given Flex-Algo.
- Supported on all platforms supported by Drivenets, including standalone and clusters.
- Support optional color configuration for Flex-Algo participation, for direct steering over Flex-Algo, with no need to create SR-TE policies or auto-policies (ODN) templates.
- Support SR-TE policy creation over ISIS-SR Flex-Algo, auto-policy (dynamic ODN) over ISIS-SR Flex-Algo, and Dynamic SR-TE policies, with CSPF computation over algo0, algo1 and Flex-Algo topologies. DNOS also provides a unique value proposition of computing dynamic SR-TE policies, over Flex-Algo topology, and adds additional constraints on top of the existing ones of the Flex-Algo topology, to be taken into consideration in the SR-TE policy dynamic computation.

DriveNets is actively developing our SR-TE and Flex-Algo, capabilities. Some highlights of our 2024 roadmap includes:
:

- Flex-Algo Prefix-metric for multi-level ISIS environments.

- ISIS Algorithm Related IGP-Adjacency SID Advertisement
- BGP Color Aware Routing (CAR) - Inter-domain color MPLS
- Per-Flow traffic steering to SR-TE policies, and Flex-Algo (CBTS solution for SR-TE and Flex-Algo)
- OSPFv2-SR Flex-Algo, including multi-area and prefix-metric support.
- OSPFv2-SR auto-policies (dynamic ODN) over SR-TE and Flex-Algo

Q: Does the bidder support IPv4/IPv6 traffic steering to Flexalgo?
A:Yes

Q: Does the bidder support L3vPN steering to Flexalgo?
A: Yes
BGP-based routes (L3VPN, EVPN, INET, INET6) – Traffic will be steered to an Algo via BGP Colour extended community.

If a received BGP route has a colour extended community with a value equal to a colour associated with a specific Flex-Algo, it will be resolved through that Algo's topology (The same goes for SR policies).

The order of colour matching is:

1. If colour matches an existing SR Policy colour OR Flex-Algo colour, resolve via that SR policy or Flex-Algo.

2. If no match is found, and If colour matches an SR Policy ODN template, create an automatic policy towards the received NH in the route. ODN template indicates whether the policy needs to be calculated locally (default behaviour) or by a PCE (user configurable).

3. If no match is found, resolve on MPLS-NH algo0 (equivalent to inet.3). There is a knob ('no-fallback') for disabling behaviour #3 (Last resort resolving on Algo 0) – I.e., if no match was found for an SR policy nor for a Flex-Algo, the router shouldn't resolve the route on algo 0, and traffic will be blackholed.

Q: Please describe the vendors' interop you have tested
A:
DNOS is tested to have compliance with the following vendors, Cisco, Juniper, Nokia and others include testing platforms such as IXIA and Spirent.

Q: Are the ASLA TE (priority 1) and DELAY (priority 2) metrics supported? Is the legacy bit (L-flag) available?
A: Yes, to all

Q: The vendor will describe the dynamic steering principles and implementation details (static, dynamic steering). Today we use BGP routes colouring to steer traffic to FA-128.

A: DNOS fully supports automated (dynamic steering) of BGP routes (INET, INET6, VPNv4, VPNv6, EVPN, BGP-LU) over Flex-Algo, SR-TE policies and dynamic ODN policies (auto-policies), based on received BGP colour extended communities. Automated/dynamic steering process is described above, at the L3VPN steering part. On top of that, DNOS also fully supports L2VPN (VPWS) static steering, by associating a colour, or SR-TE policy name, or Flex-Algo colour, to a PW. This allows to stitch L2VPN traffic over a specific-coloured solution. The static steering feature is called "Steer-path". And it's located under the VPWS PW configuration.

Q: We are also willing to steer L2VPN traffic: do we have to use EVPN (BGP based) to steer coloured routes to FA128 or do you also offer the option of dynamically steering point-to-point PW (VPWS) to FA128?
A: Both options are fully supported today.

Q: Please provide the max number of FA instances supported by the implementation and if there are any limitations associated to the maximum number of instances.
A: DNOS supports 8 user-defined Flexible-Algorithms per ISIS instance. On top of that, DNOS also support Algo 0 and Algo 1 (strict-spf). Overall, 10 algorithms are supported in each ISIS instance, out of which 8 are Flexible-Algorithms.

6.2.2 Segment Routing Traffic Engineering (SR TE)

OGN deployed two types of traffic engineering for specific needs:

- RSVP
  1. to set up backup path and to fall over in case the primary path fails
  2. to avoid certain node/link per customer's request.

- Policy based routing
  OGN currently uses policy-based routing to re-direct some of the traffic in the core when congestion happens due to link failure or event-driven traffic burst. Not all the traffic needs to be re-routed so the target selection is done carefully with traffic monitoring tools.

In 2023, we plan to replace these two RSVP TE and PBR techniques by SR TE and the possibility to define a Flexalgo policy as a static route's next-hop. Is that later option available?

The vendor will provide all the details related to its SR TE solution, especially when it comes to the dynamic and automatic steering implementation that is considered as a MUST HAVE on our side. This dynamic steering – based on route coloring policy - is required to facilitate and optimise the day-to-day Operational activity.

The vendor will specify the potential SR TE implementation limitations, especially if the extended ISIS TE (priority 1) and DELAY (priority 2) metrics for SR TE are supported.

Please specify the label stack depth, i.e. how any labels can the vendor stack.

Vendor answer:

The following describes the supported capabilities in DNOS ISIS SR-TE solution:

- ISIS NSR and GR

- ISIS-SR IPv4 & IPv6
- Node, ADJ, Anycast SIDs
- ISIS-SR IPv4 & IPv6 ECMP
- SR-MPLS OAM (Ping, Trace – Nil-fec, node-sids, Flex-Algo sids)
- SR-TE Explicit Policy
- Prefix-SID, ADJ-SID, absolute labels
- Up to 16 paths
- Up to 8 segment lists per path
- SR-TE dynamic policy
- Maximum segment lists - Maximum dynamic path segment-lists to be used on a given dynamic SR-TE path. DNOS provides a unique value proposition of dynamically computing up to 8 different dynamic segment-lists, for ECMP purposes.
- No stack compression – By default, DNOS optimizes the path as much as possible, towards using node-sids and leverage ECMP, while honouring the desired constraints. This knob allows the user to state that only adj-sids are to be used.
- Constraints
  Include admin-group
  Exclude admin-group
  Exclude SRLG
  algorithms – 0,1,128-255
  adj-sid-protection – desired/mandatory/unprotected-desired/unprotected-mandatory

- Metrics:
  IGP, TE-metric, min-delay
  Metric limit – limit accepted path metric to a specific value.
  Margin – Allows to set a metric margin for path to still be considered equal cost.
- Up to 16 paths
- Up to 8 dynamic segment lists per path
- SR-TE auto-policy (dynamic ODN) templates. Allows to leverage the dynamic SR-TE policy capabilities described above, but without pre-configuring SR-TE policies. When BGP routes are received with color extended communities, these templates can automatically create SR-TE policies, with the template's configuration.
- ISIS-SR TI-LFA IPv4 & IPv6
- Link, node, SRLG disjoint, ADJ-SID protection.
- SR-TE IGP shortcut
- ISIS-SR Flex-Algo (IPv4+IPv6 MT)
- ISIS-SR uLoop avoidance IPv4 and IPv6
- LDP Interworking
- SRMC, SRMS, LDP stitching to SR/SR-TE, LDP tunnelling over SR-TE
- PCC Initiated (PCEP Delegation)
- PCE initiated Q1'24 roadmap.
- ISIS Static & Dynamic delay – Advertising delay related TLVs
- ISIS-SR BGP-LS

- Automated Steering over colored SR-TE – According to the received BGP color extended communities
- Automated Steering over colored Flex-Ago (IPv4&6) – According to the received BGP color extended communities
- L2VPN Steer-path over SR-TE and Flex-Algo – Static steering of VPWS PWs over specific color/SR-TE/Flex-Algo solution.
- ISIS-SR Multi-instance (No redistribution between instances)
- ISIS-SR multi-level

6.2.3 PCEP

To better support SR and Flexalgo, OGN plans to deploy PCE to assist with the traffic engineering needs like in the case of path diversity or Egress Peer Engineering (EPE). Vendor shall describe PECP support and successful deployment examples of different kinds of PCE.

In the particular case of policy-based routing (static route) aforementioned in section 6.2.2, manual policy injection is needed.

Today, the target traffic and associated IP destination is identified at the core router's interface and static routes are implemented at the core router. We need to find new solution after IP traffic is migrated on SR/FA. A possible solution could be using PCE/PCEP to inject the SRTE policy at the ingress edge router.

The vendor shall describe PCEP support of the device and suggest if a particular PCE solution was tested to work well with this device.

Vendor answer:

DNOS supports PCC initiated (delegated) SR-TE policies.

DNOS is tested and certified against standard PCEs, such as ODL, IXIA, Spirent.

The implementation is standard, according to the latest RFCs and drafts.

Current supported RFCs/Drafts:
- RFC 5440,
- RFC 8231 (except initiation),
- RFC 8664,
= RFC 9256.

DriveNets are in the work of adding the support of the following capabilities by Q1'24:

PCE initiated SR-TE policies (RFC 8231 continuation), with the ability to signal SR-TE policy colour via PCEP, per SR-TE path PCE delegation, supporting PCE delegated and controlled SR-TE paths in parallel to dynamic/static paths, under the same policy, path-protected (E2E protected, 1:1/1:1+R protection) SR-TE policies, with association and delegation to PCE, enforce IGP shortcuts for "tactical" PCE initiated SR-TE policies, catering exactly to the use-case Orange described above, and more.

The described additions will add support of the following standards:
- RFC 8697,
- RFC 8745,
- draft-ietf-pce-segment-routing-policy-cp,
- draft-ietf-pce-binding-label-sid.

6.3 BGP

BGP protocol is the corner stone of OGN and is therefore a must have. We have no doubt that the vendor supports it, however we would like to focus on few use case requiring specific BGP support.

6.3.1 Local-as

Local-as is already deployed at the Edge of OGN (so out of scope) and on the Internet gateways that could be merged into OGN.

Please describe the local-as implementation details (e.g. configuration template, behavior, etc.).

Vendor answer:

By specifying an alternate AS for this BGP process when interacting with the specified peer, you allow the peer to appear to simultaneously belong to both the former AS and the new AS, without changing the peering arrangements.
To configure a local AS number for the neighbour:

Command syntax: local-as [local-as-number] type [as-path-prepend-type]
Hierarchies
- protocols bgp neighbor
- protocols bgp neighbor-group
- network-services vrf instance protocols bgp neighbor
- network-services vrf instance protocols bgp neighbor-group

6.3.2 BGP Flowspec

BGP Flowspec is running on OGN today, as part of the anti-ddos solution.

OGN is considering using BGP Flowspec to achieve the following goals:

- Dynamically implement ACL on a specific interconnection point when DDoS attack is detected
- Dynamically redirect some traffic on a given interco into a VRF in case of DDoS attack

The vendor is welcome to describe its BGP Flowspec implementation.

Vendor answer:

DNOS BGP Flowspec implementation supports the following:

- Match: IPv4/IPv6

- match:
  - src/dst addr,
  - DSCP,
  - Traffic-class,
  - src/dst-ports,
  - protocols (ie. ICMP),
  - packet-length,
  - TCP-flags,
  - fragmented;

Actions: rate-limit, redirect to VRF and NH

All typical scenarios for RTBH or DDoS architectures redirecting the affected traffic via the GRT or a VRF are supported.

6.3.3 BGP TCP AO

As far as BGP TCP AO is expected to be backward compatible with MD5 authentication, we could deploy it in the future. The vendor is more than welcome to provide BGP TCP AO support to help OGN's security feature evolution.

Possible deployment could be on RR MP-iBGP sessions, as a start. Do you have examples of implementations? What are the limitations to be considered in the context of a massive TCP AO deployment?

Vendor answer:

On roadmap for 2H 2024.

6.3.4 BGP add-path

Selective BGP add-path is required on OGN core so that a subset of prefixes can be managed.

Vendor answer:

DNOS doesn't support add-path filtering with route-policy currently.

6.3.5 6PE

OGN offers dual stack IPv4/IPv6 connectivity to the ISPs. Internally, the traffic is SR MPLS switched. IPv6 traffic is carried using 6PE so that the transport is based on IPv4 MPLS.

Note that 6PE is expected to be compatible with the Flexalgo vendor solution: it should be possible to steer IPv6 traffic a FA-128.

The vendor will detail if 6PE is supported and the potential limitations.

Vendor answer:

DNOS fully supports 6PE, also in combination with Flexalgo.

6.3.6 L3 IPVN functionality

L3VPN functionality is required, even if we do not plan to use it for our customers: L3VPN services are running today on dedicated IGN or IMN PEs.

Still, we need that functionality for internal purposes. For instance, in the case of the anti-DDOS service, we use BGP Flowspec to redirect the traffic under attack into a vrf.

Vendor answer:

DNOS supports L3VPN and also supports the anti-DDoS service architectures via VRFs.

6.3.7 BGP LU

The BGP Labeled Unicast (BGP-LU, RFC 3107) Multiprotocol extension is used to distribute an MPLS label that is mapped to a particular route. Even it is not used today on OGN, we might require this functionality it for the mid-term.

The bidder will describe the BGP-LU solution, in particular the possibility of BGP LU redistribution in to ISIS, and the way the BGP-LU labels can be mapped to LDP ones. This can happen when a BGP-LU domain need to exchange with a non-BGP-LU domain (ISIS/LDP)

Vendor answer:

DNOS supports standard BGP-LU according to RFC 3107.

Redistribution of BGP-LU into IGP/LDP is a roadmap item.

6.3.8 BGP LS

BGP Link-sate (BGP-LS, RFC 9085) will be necessary on OGN to collect TE topology for PCE (see 6.2.3). BGP-LS should include the extensions required for Segment Routing.

Vendor answer:

DNOS supports BGP-LS according to RFC 9085 and the extensions for Segment Routing.

6.3.9 BGP PIC

PIC (Prefix Independent Convergence) is a Cisco feature (at least) to decrease the data plane convergence time. There are two flavors:

- BGP PIC Edge: (noticeably) reduces convergence time when a PE router fails and BGP has to switch to a different PE router.
- BGP PIC Core: (noticeably) reduces convergence time when a core router fails and IGP has to find a new best path to the PE router.

<u>BGP PIC Edge</u>

BGP PIC Edge is deployed for the IGN PEs. PIC feature makes the BGP convergence time independent from the number of customers BGP prefixes. Instead, the BGP convergence depends on their BGP next hops (our IGN PEs loopbacks), not on the BGP customer prefixes anymore. So instead of updating potentially tens of thousands of routes, only few tens or very few hundreds of next-hops need to be updated. That makes the overall convergence time really much faster. Please refer to the following link for a complete description of this feature.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/asr903/17-1-1/b-irg-xe-17-1-asr903/b-irg-xe-17-1-asr903_chapter_01.pdf

BGP PIC is used today for our L3VPN services but could be considered for the OGN IP transit service as well, one day or another.

Juniper has similar feature called Indirect Next Hop.

As far as this feature seems to be implementation specific feature, it is mandatory for us to have it available, at least for the mid-term. Please detail your answer regarding the support of Prefix Independent Convergence solution, where the BGP convergence is reduced to the IGP convergence.

Vendor answer:

DNOS supports BGP PIC Edge.

BGP PIC CORE

BGP PIC CORE provides the same convergence mechanism, based on BGP next hops convergence rather than the BGP prefix itself.

Vendor answer:

DNOS supports BGP PIC Core.

6.4 L2 Ethernet services

OGN supports today L2 Ethernet services (Point-to-Point) and plans to evolve to EVPN. Please describe if you support VPWS, VPLS and EVPN.

Vendor answer:

DNOS supports port x-connects for transparent local switching, VPWS (Point-to-Point) incl. port and VLAN mode as well as EVPN.

6.5 Multicast

OGN support multicast for specific purposes.

The OGN core routers support IP multicast in Global Routing Table using PIM sparse-mode (ASM and SSM modes).

The vendor will describe any other multicast forwarding technics the core router supports or will support (mLDP or others) and will give his view on the preferable technic.

The vendor will indicate the compatibility (coexistence) of his multicast implementation with any Traffic Engineering features he may support for unicast.

We do not expect that multicast should be compatible with Flexalgo, but the vendor is invited to share if their multicast implementation is compatible with Flexalgo, or if there are plans to do so.

Vendor answer:

The DriveNets network cloud has Mulitcast support including support for mLDP, mBGP, mLSP (P2P and P2MP). The solution supports mLDP NSR and MoFRR capabilities within the data plane. Multicast entries are lodged into dedicated RIB and FIB entries on the NCP's allowing full platform TE, ACL and CPRL controls to be applied to Multicast traffic. All Network cloud Interfaces and forwarding endpoints are multicast enabled by default.

We currently support the following Multicast RFC and standards:

- RFC7761 Protocol Independent Multicast - Sparse Mode (PIM-SM)
- RFC4607 Source-Specific Multicast for IP
- RFC3569 An Overview of Source-Specific Multicast (SSM)
- RFC2365 Administratively Scoped IP Multicast
- RFC5059 Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)
- RFC4602 Protocol Independent Multicast - Sparse Mode (PIM-SM) IETF Proposed Standard Requirements Analysis
- RFC5771 IANA Guidelines for IPv4 Multicast Address Assignments
- RFC5132 IP Multicast MIB
- RFC2934 Protocol Independent Multicast MIB for IPv4
- RFC5060 Protocol Independent Multicast MIB
- RFC7431 MoFRR

We currently have not deployed Multicast within a FlexAlgo environment – however as the current implementation and selection process for Multicast egress is integrated into our standard RIB / FIB architecture it should be practical to include FlexAlgo into the egress interface and endpoint selection process.

6.6 Core Class of Service

OGN CoS model uses the EXP field (EXP0 to 7) to define 5 core classes (CRT to carry RT voice, C1 to carry RT video and high priority data, C2 to carry medium/low priority data, C3 to carry Internet traffic as Best Effort traffic, NC class reserved for the Core network control traffic).

Therefore, the vendor must support the OGN CoS model for the platforms proposed, whatever the solution is based on chassis or cluster (DDC, IP CLOS).

Vendor answer:

The DriveNets Network Cloud / DNOS supports advanced CoS / QoS Marking, Remarking, and reading. These features are supported on ingress, egress, and in-flight flows.

We support utilising the DSCP, MPLS-EXP PCP_DEI bits for flagging CoS to the solution. All bits can be marked, remarked, or swapped in ingress or egress.

Note that the SR-TE label stack > 4 is bottom most labels and are NOT remarked on egress when SR is utilised.

6.7 LAG

LAG is an important feature, that is systematically deployed because we use lots of parallel links to reach very link capacities.

Vendor answer:

DNOS fully supports LAG including support for Multispeed bundles (interfaces of different rates in the same LAG), LAG's with members in multiple NCP (Leaf Nodes) or within a single NCP. We fully support LACP for the control and monitoring of LAG groups.

DNOS supports up to 300 LAG's each containing up to 64 members (max: 32 physical interfaces) within a single DDC cluster.

6.8 ECMP

ECMP remains used for the end-to-end connectivity, i.e. there might be several paths between two OGN end-points and ECMP is required in that case. We are referring to the IGP ECMP paths, that should be possible in Flexalgo context.

The ECMP FEC table has some limitation with the Jericho chipset (on OGN implementation at least), and we had to optimize its use.

Today we are using ECMP in Flexlago 128 but not in the default algo 0: we can deactivate ECMP in the default IGP.

Can you provide similar option of using IGP ECMP on per Flexalgo instance?

Can you please provide the ECMP FEC table limitations in the proposed solution, based on Jericho in the chipset family proposed by the vendor?

Vendor answer:

The proposed solution from DriveNets is not based on platforms with Jericho NPU and therefor also not impacted by the described limitations.

The described limitations seem to impact edge devices at ingress. It is not expected to have any negative impact using Jericho based edge devices connecting to the new OGN network.

6.9 BFD, micro-BFD

BFD is required to detect failures between routers that are not directly connected to each other, generally because they connect across a third-party carrier. Micro-BFD is also used for the LAG bundles.

Please describe your BFD implementation (e.g. can it be running on data plane), and the key scalability figures (number of BFD sessions versus BFD timers, if any dependency between both values).

Vendor answer:

DNOS Fully supports BFD, uBFD, BFDoMPLS, SH-BFD and MH-BFD supporting the following standards:

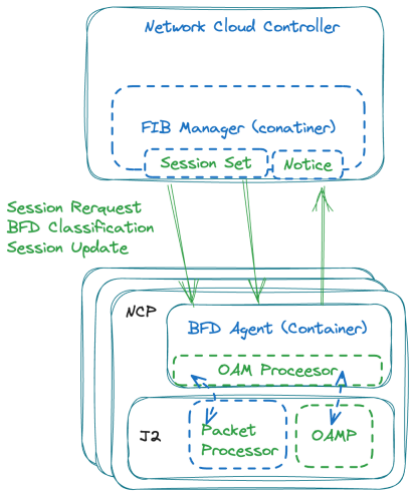
- rfc5880 Bidirectional Forwarding Detection
- rfc5881 Single-hop BFD
- rfc5882 Generic application of BFD. Usage of BFD failure detection by different applications (BGP, OSPF, …)
- rfc5883 Multi-hop BFD
- BFD standard YANG BFD IETF data-module. Covers BFD configuration data, operational data and notifications.
- rfc7331 IETF BFD MIB. Covers BFD SNMP Traps

Our BFD architecture is based upon a modern distributed approach:

BFD sessions are established, Monitored, and classified from the FIB manager container set on the Network Cloud Controller COTS platform. This allows highly flexible BFD session resource management and control.

Within the NCP (Leaf Nodes) a BFD agent container set is hosted on the NCP's embedded compute platform - This agent is responsible for deploying the BFD session into the underlying Packet processing NPU's and monitoring for the Operational Status of each BFD session. This includes Correlating updates to uBFD sets and VoQ's classifiers. The BFD sessions are installed directly by the BFD agent onto the underlying NPU which is responsible for generating the BFD sessions and raising events via the OAM Processor for successful and unsuccessful BFD sessions.

This hierarchical approach allows the resources available for BFD sessions to scale with each additional Whitebox / LEAF node added to the cluster. This approach removes the traditional limitations on Session number vs. Session Timing seen in more traditional Data plane / control plane.



This architecture allows:

2^{32} Max BFD sessions per DDC cluster
4K Max BFD Sessions per NCP with counters (8K counter sets Total)
16K MAX BFD Sessions (J2 Limitation)
8 Timing poll intervals per NCP (ie. 50ms, 100ms, 150ms, etc)

6.10 RPKI

We believe we must do our best to participate in the improvement of the Internet's stability and security: that's why Orange is deploying RPKI in its Wholesale internet backbone, OGN (AS 5511).

However, this must be done carefully and with efficient means to monitor & troubleshoot. A pilot is planned before end of this year, and a progressive deployment can be anticipated for the next year.

The vendor will describe its RPKI implementation that Orange could further assess compared to its on-going implementation plan.

At the time of writing, we are looking for an efficient way to track prefixes that are denied by a route policy. The use case is the following: in a given RPKI implementation, if a provider decides to drop RPKI-invalids, these prefixes are no longer visible once dropped, preventing efficient troubleshooting, monitoring, customer/peer reporting. To do that, one approach is to store in some dedicated memory those invalid routes, but we do not want to rely on memory intensive solutions. So, the vendor should propose 'memory free' solution or another way to signal these invalid routes.

Another approach would be to implement Telemetry to report various RPKI events, including the assignment of an RPKI "invalid" state on any prefix. Use case: monitoring/troubleshooting/customer or peer reporting upon receiving an invalid advertisement.

Vendor answer:

The DriveNets DNOS fully supports BGP RPKI and it is used in production by a number of our largest customers.

Our implementation supports

- RFC 6810,
- RFC 8210
- RFC 6811
- RFC 8097

We support exporting RPKI validation information as part of BGP Extended communities' attributes.

To enable trouble shooting and tracking of RPKI activities we support extensive event generation on RPKI events validation status, prefix – these events can be logged to Syslog or exported via telemetry streaming.

6.11 Security aspects

The bidder is asked to describe any feature, configuration or implementation specifics that are used to enforce the security of the solution. We generally think of ISIS authentication, control plane protection, data plane protection (e.g. MACSEC), ACLs, filters, limiting the number of routes when redistributed from a protocol to another, user access management using specific authentication methods, etc.

Vendor answer:

The DriveNets Network Cloud is built from the ground up to meet the demands of modern telecommunication environments. A key part of these requirements is ensuring that the Network Cloud environment meets modern security standards and telecom regulations. To achieve this we follow a modern secure by design development that embeds are security principles into everything we create.

Our guiding security principles are:

- All software will be digitally signed using secure asymmetrical cryptography – to ensure trust and prevent supply chain attacks.

- Secure Secrets storage – All stored secret information must be secured using a high security hashing algorithm or cryptographic technique. Any secret information entered in plain must be protected automatically.

- A least privilege model will be used for all containers, services, and functions – Limit access to the minimum required.

- Operate a disabled / denied by default model – All services and ports will be disabled by default.

- Encrypted Access – All access to the platforms (CLI, API, etc) and between components must be encrypted and secured by default.

As Part of our secure by design model we have adopted and developed security to match the latest secure networking and general security best practices, including:

Management Plane:
- Digitally signed Software
- Software and Image verification
- HostOS Integrity Verification
- Hardened and Secured containers
- Salted encryption and authentication on all management traffic
- Secure Password and secret storage
- Prohibit direct root access
- ACL's for all management protocols
- Control Plane Rate Limiting – support full cPRL for all management protocols.

Control Plane
- Control Plane Rate Limiting – Full cPRL support for all Control plane traffic
- Control Plane ACL – Full ACL's for all control plane traffic – Default ACL rule is deny.
- Martian Address blocking.
- Closed TCP/USP ports – Ignore packets received on closed TCP and USP ports
- Ignore Invalid Packets – IPv4, IPv6, TCP, UDP, ICMPv4/v6 and Raw.
- Support all routing protocol authentication (RPKI, ISIS Auth, etc)
- Support limiting of route redistribution and leaking.

Data Plane
- All ports disabled by default
- Data Plane ACL with full packet match capabilities.
- Disable by default IP source routing and Record router.
- Disable IP directed Broadcasts by default.
- Disable Proxy ARP by default
- Support uRPF
- Disable insecure ICMP by default – Source Quench, Timestamp, Redirect
- IP Fragmentation protection – Forwarding of fragments, reassemble for forwarding and CPRL, MTU policing
- Block all unconfigured control plane ports by default

6.12 MACSEC

There is no MACSEC today deployed on OGN. However, our security team could consider either tactical or general deployment of MACSEC depending on the needs.

The vendor is invited to share his capabilities with regards to MACSEC, especially when it comes to 100GE/400G/800GE Ethernet speeds.

Vendor answer:

MACsec is natively supported by Broadcom J2c+ & J3 NPU's. However, to utilise MACSec requires specific PHY's be included in the Whitebox platform. SKU's are not commonly available for MACsec enabled platforms. When the capability for MACsec is commonly available DriveNets will plan to add the capability to our roadmap.

It should be noted that enabling MACSec increases power consumption per port by 19-23% on all hardware platforms.

6.13 Software/hardware cluster/chassis upgrade policy

Does the vendor provide any procedure such as ISSU (In Service Software Upgrade) to make the software upgrade process non-disruptive, i.e. a procedure allowing the services to continue during the software upgrade?

How is possible to upgrade a cluster or a chassis without any service disruption? Please describe the procedure required to add a new white box in the cluster.

Vendor answer:

The DriveNets Network Cloud is based upon a modern software design model and hardware principles this allows us to utilise more modern approaches to ensure "hitless" upgrades and software changes.

Traditional ISSU

The upgrading of network equipment using ISSU has been a common practice withing service provider networks for a number of years – this process generally involves disconnecting the routing and control plane from the forwarding ports of the router – allowing the RE/Control plane to be updated while the forwarding ports continue to pass traffic, usually the router continues in a forwarding only state until the new software image becomes active at which point the configuration is re-imported and the RE/Control plane will attempt to reapply configuration and normal operation can continue. This process is most effective in the control plane, with data plane / forwarding updates requiring service interruptions.

The Cloud and DriveNets approach

The DriveNets Network Cloud is based upon a modern containerised software stack, each software component runs a separate service pod, each pod containing multiple containers required to run service. Individual containers within a pod have their own lifecycles and can be upgraded / changed as needed. This software stack approach allows us to utilise modern hitless upgrade approaches.

Modern software infrastructures offer different update strategies:

- A 'rolling update' updates the services incrementally. It is simple and less risky than updating all at the same time.
- Blue-green deployment utilizes two identical environments running different versions while gradually shifting users to the new environment. It is simple and easy to implement.

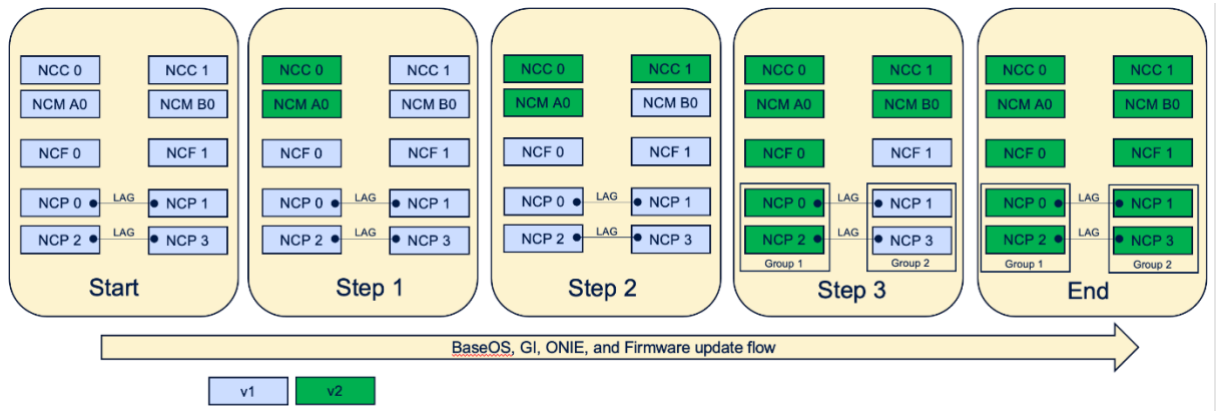
- Canary update releases new services in small phases to a subset of users.

Hitless updates guarantee zero service disruption or minimize outage to seconds, thus, eliminating the need for maintenance windows and reducing the risk during the update process itself. To enable this process, we use the standard rolling update approach.

To update the software stack, we divide the cluster into two or more groups and serially update group by group while leveraging the separation of the control and data plane.

First, we update the control plane without touching the data plane. The update individual stacks and services gradually on the redundant nodes, checking that the upgrade passes automated tests to ensure the green services are stable and functional. Once the services are confirmed operational the matching nodes are updated using the same process (e.g., NCC-0, NCM A0 then NCC-1, NCM B0).

To guarantee traffic continuity, we divide the NCP nodes into logical groups based on the bundle/LAG/redundancy configuration (e.g., if port NCP-3/port-1 is bundled to port NCP-2/port-7, then NCP-3 and NCP-2 are in two different groups). We then upgrade the groups serially. During the process, the cluster is in a transient state in which different NCP nodes run different software versions. When the upgraded nodes become active and are ready to handle traffic, we move to the next set of groups until the entire cluster moves to the target version.



This update process ensures that the network service continues without impact to traffic flows and control plane operations. The process is designed to be automated and orchestrated but can be utilised directly via DNOR and the DNOS cli.

A similar process can be applied for “hot-patching” or container updates in which a blue-green rolling update process is followed.

6.14 Automation

We would like to draw the vendor's attention relatively to the OGN automation strategy and the vendor is invited to give his global feedback with regards to it. We also would like to know if any caveat should be considered in case the vendor would be selected but would require specific adaptation on our side.

Today, Cisco NSO product is used on IGN for multiple cases and should remain the fundamental brick to enable the development of automated solutions such as L2VPN today or even L3VPN in the future. We need to anticipate that the new OGN (disaggregated) core router is compatible with NSO for all the enterprise and wholesales services that are running on OGN. NSO is also used to build specific tools for the operations as a complement to what is already achieved with Ansible.

Here below are some questions the bidders is invited to answer:

- Does the bider support Netconf and Restconf ?
- Do you support the ietf and openconfig YANG model or is the vendor YANG model a vendor specific implementation?
- Does the NOS support Ansible collections?
- Do you support gRPC/gNMI protocols ?

For information, the following NSO use cases are listed below:

- Production of L2VPN services (based on VPWS/VPLS) is planned in the context of the Network On Demand project
- Customer migration (Ethernet customers attached to Cisco ESR10K or 7600 migrated to ASR1K)
- Backbone configuration production
- PE CoS configuration sometimes contains error, NSO is used by the Operations to correct them (for the specific case of low bandwidth connection, also known as LBW)

Vendor answer:

The solution provides advanced telemetry and configuration tools and seamlessly integrates with various network management and orchestration systems in live T1 operator deployments. It fully supports Netconf (both natively and via SSH) and RESTconf protocols for configuration, operational status, and remote RPC operations.

The Netconf/RESTconf interfaces strictly adhere to industry standards and employ standard YANG models. Our compliance extends to the following Netconf standards:

YANG:

- RFC 6020,
- RFC 6087,
- RFC 6095,
- RFC 6991,
- RFC 7224,
- RFC 7950: YANG - Data Modelling Language, abstractions, and types

Netconf:

- RFC 6241: Network Configuration Protocol (NETCONF)
- RFC 6242: Netconf over SSH

- RFC 6243: With-defaults Capability for Netconf
- RFC 6470: Netconf base notifications
- RFC 6536: Netconf Access Control Modelling
- RFC 5277: NETCONF Event Notifications
- RFC 5717: Partial Lock Remote Procedure Call (RPC) for Netconf
- RFC 6022: YANG module for NETCONF Monitoring

Our solution offers a standard RFC-compliant YANG model, an OpenConfig YANG model (accessible at https://github.com/openconfig/public - Configuration and Telemetry), and a publicly available platform YANG model.

The Network Cloud fully supports gRPC/gNMI for configuration, management, and telemetry streaming. We provide support for read operations (GET), as well as sample-based and on-change-based subscription methods (SUBSCRIBE).

While we currently don't have an official Ansible collection, we do support all standard Ansible connection options for NETCONF, gNMI, and CLI. Additionally, we provide standard YANG models that can be utilized within Ansible.

6.15 Telemetry

The vendor shall describe what telemetry solution is supported, especially for Segment Routing MPLS iPV4 and if it can be supported for Flexalgo. Globally, the list of supported counters could be provided here below (not limited to SR).

Vendor answer:

The solution offers robust support for both gRPC and RPC-based telemetry streaming, enabling the export of performance metrics in a highly flexible and scalable manner. By incorporating gRPC interfaces, the system utilizes a subscribe push model that empowers multiple external management platforms to subscribe to various metrics, dimensions, and measurements in a controlled and efficient manner.

The gRPC/gNMI (gRPC Network Management Interface) telemetry model goes beyond basic data transmission by providing advanced features. These features include timed (scheduled) subscriptions, which allow for the retrieval statistics with updates occurring at regular intervals, such as every X millisecond. This capability ensures that real-time information is readily available to Monitoring and management systems.

Additionally, the gRPC/gNMI telemetry model supports on-change subscriptions, which trigger updates whenever a value within the monitored parameters changes. For example, this can be useful for tracking the state of network neighbours, ensuring that updates are promptly delivered whenever a neighbour's status changes. By capturing these changes in a timely manner, administrators, and network operators can promptly respond to dynamic network conditions.

The incorporation of gRPC and RPC-based telemetry streaming in the solution provides a powerful and adaptable framework for exporting performance metrics. The use of gRPC interfaces enables controlled subscription to specific metrics, while the gRPC/gNMI telemetry model offers both timed and on-change subscriptions, enhancing the granularity and responsiveness of performance monitoring and management processes.

The We can make the full gNMI/gRPC YANG model and documentation available, below are a few examples of commonly monitored gRPC/gNMI statistics:

```
Path: /drivenets-top/protocols/rsvp/lsps/lsp[tunnel-id='*' lsp-id='*' tunnel-source='*'
tunnel-destination='*']/oper-items
Mode: SAMPLE
Interval: 60,000,000,000 ns

Path: /drivenets-top/protocols/rsvp/lsps/lsp[tunnel-id='*' lsp-id='*' tunnel-source='*'
tunnel-destination='*']/oper-items
Mode: SAMPLE
Interval: 60,000,000,000 ns

Path: /drivenets-top/interfaces/interface[name='*']/qos-target/qos-target-entry[direction='*'
policy-name='*']
Mode: SAMPLE
Interval: 300,000,000,000 ns


Path: /drivenets-top/interfaces/interface[name='bundle*']/oper-items/counters/total-
forwarding-drop-counters
Mode: SAMPLE
Interval: 60,000,000,000 ns

Path: /drivenets-top/interfaces/interface[name='bundle*']/oper-items/counters/forwarding-
counters
Mode: SAMPLE
Interval: 60,000,000,000 ns

Path: /drivenets-top/interfaces/interface[name='bundle*']/oper-items/interface-speed
Mode: ON-CHANGE

Path: /drivenets-top/protocols/rsvp/lsps/lsp[tunnel-id='*' lsp-id='*' tunnel-source='*'
tunnel-destination='*']/oper-items
Mode: SAMPLE
Interval: 300,000,000,000 ns

Path: /drivenets-top/interfaces/interface[name='fab-ncf*']/oper-items
Mode: SAMPLE
Interval: 1,800,000,000,000 ns

Path: /drivenets-top/interfaces/interface[name='fab-ncp*']/oper-items
Mode: SAMPLE
Interval: 1,800,000,000,000 ns

Path: /drivenets-top/interfaces/interface[name='ge100*']/oper-items
Mode: SAMPLE
Interval: 300,000,000,000 ns

Path: /drivenets-top/interfaces/interface[name='ge400*']/oper-items
Mode: SAMPLE
Interval: 300,000,000,000 ns

Path: /drivenets-top/interfaces/interface[name='bundle*']/oper-items
Mode: SAMPLE
Interval: 300,000,000,000 ns

Path: /drivenets-top/system/ncps/ncp[ncp-id='*']/oper-items/backplane-statistics
Mode: SAMPLE
Interval: 300,000,000,000 ns

Path: /drivenets-top/system/ncps/ncp[ncp-id='*']/oper-items/backplane-reachability-statistics
Mode: SAMPLE
Interval: 300,000,000,000 ns
```

```
Path: /drivenets-top/interfaces/interface[name='fab-ncf*']/oper-items/counters/fabric-counters
Mode: SAMPLE
Interval: 300,000,000,000 ns

Path: /drivenets-top/interfaces/interface[name='bundle*']/oper-items/counters/total-
forwarding-drop-counters
Mode: SAMPLE
Interval: 60,000,000,000 ns

Path: /drivenets-top/interfaces/interface[name='bundle*']/oper-items/counters/forwarding-
counters
Mode: SAMPLE
Interval: 60,000,000,000 ns

Path: /drivenets-top/interfaces/interface[name='bundle*']/oper-items/interface-speed
Mode: SAMPLE
Interval: 60,000,000,000 ns
```

6.16 Other features and services

The following features should be supported by the supplier.

6.16.1 Multi-instance ISIS

ISIS multi-instance is required on few OGN routers to interconnect with the RAEI, and potentially other OINIS networks.

The vendor will describe its multi-instance ISIS implementation and any potential limitations.

Vendor answer:

DNOS supports up to 32 independent ISIS instances at the same time. Each instance must be configured with a different administrative distance. ISIS works with metric style wide by default.

6.16.2 FlexEthernet

We could use in the future Flexible Ethernet bonding (nx100GE) to load balance some elephant flows (that is not possible with LAG or ECMP). What is the vendor strategy and roadmap with regards to Flexible Ethernet support?

Vendor answer:

FlexE adoption in the industry is low considering that the technology is already available for some years. There are some reasons why it is not broadly adopted in core and edge networks. One is that the FlexE/G.mnt require additional hardware support in form of FPGAs or directly from the NPU. This additional hardware support comes at the expense of higher power consumption – comparable to MacSec.

FlexE supports sub and super-rating use cases. Super-rating requires the FlexE shim layer over all physical interfaces contributing to the bundle. This adds some limitations when hardware redundancy is also required. Sub-rating might become available if the FlexE shim layer comes as part of the optical plug. In this case it can be easily supported by the NOS.

6.16.3 Netflow carrying Flexalgo information

Netflow packets will be used in the context of SR Flexalgo to generate the OGN traffic matrix. In that context, we need to understand the vendor Netflow implementation for the 4 below cases:

1. IPv4 edge node
2. IPv4 core node
3. IPv6 (6PE) edge node
4. IPv6 (6PE) core node

In particular, the vendor will describe how the following Netflow fields are populated:

1. bgpNextHopIPv4Address (ID 18) or bgpNextHopIPv6Address (ID 63)
2. mplsTopLabelIPv4Address (ID 47) or any other egress PE identifier

Globally, the vendor will describe if the Netflow packet is built in conformance with the Flexalgo path computation. In other words, the information related to the egress router as per Flexalgo computation should be recovered within the Netflow packet.

Vendor answer:

DNOS supports NetFlow templates for all traffic types described above.

DNOS NetFlow implementation supports the specific fields requested above.

DNOS supports Flow monitoring, with two export types: IPFIX and NetFlow v9.
DNOS supports 4 types of flow monitoring templates: IPv4, IPv6, IPv4-over-MPLS and IPv6-over-MPLS.

All current supported HW by DriveNets, support a very large scale of 8M cached entries, for every NCP (Line card) within the cluster.

Flow monitoring sample rate is configurable, in the range of 1-out-of <1-65535>.

BgpNextHopIPv4Address – Will hold the BGP IPv4 next hop value, for IPv4 flow templates. For IPv4oMPLS templates, this field will be set to 0.
BgpNextHopIPv6Address - Will hold the BGP IPv6 next hop value, for IPv6 flow templates. For IPv6oMPLS templates, this field will be set to 0.
MplsTopLabelIPv4Address – Will refer to the prefix represented by the MPLS label as appears in the MPLS-NH (inet.3 equivalent) table. Specifically for SR, and Flex-Algo, it will be set with the prefix represented by the SR/Flex-Algo label installed in the MPLS-NH table.
MplsTopLabelIPv6Address - Will refer to the prefix represented by the MPLS label as appears in the MPLS-NH (inet.3 equivalent) table. Specifically for SR, and Flex-Algo, it will be set with the prefix represented by the SR/Flex-Algo label installed in the MPLS-NH table.

6.16.4 TWAMP

TWAMP is used to measure link/path quality between the OGN PoPs and is also performed between some IGN PE routers. TWAMP client and TWAMP server features can be used.

Vendor answer:

The DriveNets Network Cloud fully supports IPv4 & IPv6 TWAMP server and Simple-TWAMP (TWAMP-Light) as sender and reflector, both for endpoint delay and link delay measurements.

Fully complying with:
- RFC 5357,
- RFC 4656,
- RFC 5618,
- RFC 5938,
- RFC 6038,
- RFC 8762 (In unauthenticated and stateless mode)

7 Control plane scalability

In 2023, the OGN ISIS infrastructure supports near 7.5K IP prefixes, covering both enterprise (~5.5K) and wholesale (~2K) perimeters. Amongst those 7.5k prefixes, OGN supports near 4K /32 loopbacks that are SR and LDP labeled. The other prefixes are /29, /30, /31 prefixes. On the mid-term, LDP is planned to be phased-out.

ALL bidders are expected to answer the questions below, whatever the commercial model proposed.

	2025	2026	2027	2028	2029	Comments
RIB - IPv4 Paths	12,62	13,26	13,92	14,47	15,05	linear extrapolation of IPv4 paths for the IPv4 routes (Million)
RIB - IPv4 entries	1,05	1,10	1,16	1,21	1,25	linear extrapolation of best path IPv4 routes (Million)
RIB - IPv6 Paths	3,02	4,26	6,01	8,47	11,94	exponential extrapolation of IPv6 paths for the IPv6 routes (Million)
RIB - IPv6 entries	0,30	0,43	0,60	0,85	1,19	exponential extrapolation of best path IPv6 routes (Million)
FIB - IPv4 routes entries	1,58	1,66	1,74	1,81	1,88	linear IPv4 extrapolation (Million)
FIB - IPv6 routes entries	0,45	0,64	0,90	1,27	1,79	exponential IPv6 extrapolation (Million)
Number of VRFs	< 100					Short term need for infrastructure VRFs, e.g. for management or internal services purposes Max #IPv4 VRF, Max #IPv6 VRF supported by the vendor?
VPNv4 entries	One or two thousands					
VPNv6 entries	one or two thousands					
Number of PWEs - VPWS	700	750	800	850	900	Today, we run point-to-point VPWS Ethernet service (LDE)
VPLS instances	50	100	150	200	250	VPLS is not yet ilmplemented but we might require it
MAC@						VPLS specific : Max MAC@ per VPLS instance by the vendor?
Number of queues per VLAN	8					
Number of eBGP ipv4 peers	150					Figures based on OINIS best practice meshing rules These are not related to the actual service growth Please also refer to the technical questionnaire
Number of eBGP ipv6 peers	100					
Number of BFD sessions	500					
Number of PIM sessions	150					
Number of multicast routes	2000					
Number of Unique Policy Maps	100					

Table 2 Control plane scalability - OGN requirements

Please refer to the technical questionnaire to get the entire set of control plane scalability questions.

Vendor answer:

Complaint – full details provided in the XLS

8 Additional Requirements (for information only)

These questions are more related to the RFP than to this RFI. Please do not consider them as mandatory at all, this section if for our information only.

8.1 Labs support

OINIS Engineering and Orange Innovation will need to test in-house the bidder platform that will be selected at the end of the RFP process (in 2025). So, even if it is out this RFI scope, but we would appreciate to get first vendor proposals, e.g. would the bidder accept to offer for free the material required for the Engineering and Orange Innovation testing lab. The number of routers could be specified at the RFP stage.

Vendor answer:

DriveNets understands the need and the importance of OINIS and Orange Innovation having a Lab each. DriveNets can offer non-commercial DNOS and DNOR licenses for the Lab and testing environments. The SW which will be made available will have full parity and performance as the Commercially licensed SW. Any Software (DNOS / DNOR) for lab and testing use will benefit best effort Maintenance and Support including software updates and version upgrades as needed.

In addition to the above, DriveNets has staged a CL-32 for Orange to enable a PoC. This equipment can be offered to Orange in case of DriveNets' selection after RFP.

8.2 Resident Engineer

Similarly, would you provide dedicated on-site resident engineer for free until the platform is ready for deployment (includes whole qualification phase of the platform as well as Pilot)?

Vendor answer:

To ensure the best results for everyone involved, DriveNets strongly recommends utilizing Resident Engineers. These professionals will assist with effective knowledge sharing, help integrate operations, and contribute to the overall success of the project. The specific details—such as the number of engineers, how long they'll be involved, and any related costs—should be discussed and finalized during the Request for Proposal (RFP) phase. The scale and complexity of the project will determine the level of effort needed for knowledge transfer and successful completion.

To support Orange in its Disaggregation journey, DriveNets is pleased to offer a Resident Engineer at no cost for a one-year period.

8.3 Training

At RFP time, the vendor will be asked to make a training to the OINIS Engineering, including Orange Innovation, as well the OINIS Operations. This could represent 30 to 40 persons, that could be done in three different regions (Europe, USA, Asia).

Vendor answer:

The DriveNets Network Academy provides a comprehensive array of courses, both introductory and advanced, focusing on various aspects of the DriveNets suite—specifically, the Network Cloud solution, DriveNets Network Operating System (DNOS), and DriveNets Network Orchestrator (DNOR).

These courses are designed primarily for network engineers who are either already working with the DriveNets Network Cloud or who intend to implement DriveNets technologies in various environments, whether for proof of concept, certification, or production use. Additionally, we offer overview presentations and trainings tailored for a non-technical audience who require an understanding of the products and technologies in use.

Here's a snapshot of our certification paths:

DriveNets Network Cloud Overview (DNO, T0): This is a 4-hour session that provides an introduction to the DriveNets Network Cloud, its system architecture, and orchestration features.

DriveNets Network Cloud Administrators (DNCA – T4): This is a 3-day, instructor-led course that can be attended either on-site or online. The course covers the installation and lifecycle management of a DriveNets Network Cloud cluster using DNOR.

DriveNets Network Cloud Operators (DNCO – T3): This 5-day, on-site, instructor-led course offers an in-depth look into operating a Network Cloud cluster. It starts with the basics of software and hardware architecture and progresses to command-line operations, management, and routing features, including hands-on exercises for configuration and troubleshooting.

DriveNets Network Cloud Expert (DNCE – T6): This 3-day, on-site, instructor-led course delves into all facets of deploying, managing, and troubleshooting the DriveNets Network Cloud solution.

DriveNets NCE Workshop (DNWorkshop – T8): This intensive 2-day course covers architecture, deployment, administration, and the basic configuration processes for the DriveNets Network Cloud cluster.

Training options are flexible: courses are available both on-site and online, and can be tailored to meet individual customer needs. This could include combining elements from different courses.

On-the-Job Training sessions are also customizable and are designed to meet the specific requirements of the customer.

All training materials and assessments are accessible via the DriveNets Training Academy website.

DriveNets has successfully conducted on-site training for Orange team members in various locations including Europe, the USA, and Asia, and anticipates no obstacles in continuing to do so.

8.4 Maintenance and support

This RFI is not only considering the technical aspects but is also considering the support model. Note this later depends on the commercial models amongst the ones presented in section 4.2.

The support model should be detailed by the bidder to help us better understand all the interdependencies, responsibilities perimeters and operational impacts. This will be very useful to measure the distortion compared to our existing support model.

Amongst others, the questions should be discussed with the bidder:

- What's the integration process and how can Orange potentially participate or influence it?
- What if a new need is expressed by Orange: what is the NOS provider policy concerning the new features adoption and the time to deliver it?
- What contractual agreement exist between NOS provider and the h/w one?
- Can we rapidly apply a s/w patch of given release in case of critical bug (security)?
- What type of guarantees can Orange benefit from it?
- As mentioned in 6.12, the new OGN disaggregated router is expected to be compatible with our IT ecosystem, and the tools impact should be considered by Orange
    - service automation strategy that is currently based on Cisco NSO. How compatible is the NOS provider solution compatible with it?
- Other items such supervision, configuration, reporting, etc. will have to be considered, even if the key objective of the RFI is the technical maturity assessment. We could anyway further dig all those questions during the next step that is the RFP (planned next year)
- …

Coverage
OGN having worldwide coverage, it is important that the vendor be able to provide a support model that is reactive enough in case of problem. This can concern hardware maintenance and software support policy, amongst other possible points.

Lifecycle
The white box or chassis lifecycle should be supported as many years as possible, more than 5 years if possible. Ideally 10 years h/w & s/w support should be provided after the corresponding End of Sales announcement (EoS)

Here below, the vendor should describe its maintenance and support model, as per the items considered above.

Vendor answer:

DriveNets has collaborated with top Original Design Manufacturer (ODM) vendors in the networking industry. We've successfully adapted our DriveNets Network Operating System

(DNOS) to multiple platforms, demonstrating its flexibility and hardware-agnostic capabilities. This accomplishment required substantial research, software development, and testing. As the hardware market evolves, especially with Whitebox ODMs, DriveNets is committed to ensuring DNOS compatibility with the most efficient hardware platforms. In choosing these platforms, customer needs, as well as those of leading global service providers, play a key role. If Orange chooses DriveNets as its Network Operating System (NOS) vendor, Orange's preferences will influence our selection of ODM platforms.

Furthermore, Orange can contribute to the integration of new hardware platforms by reviewing and improving the test plans for DNOS compatibility. Orange may also become a 'First Field Customer' for new solutions, granting Orange influence in the decision to move a product to General Availability based on its operational criteria.

Regarding any new needs expressed by Orange, DriveNets has a process for New Feature Requirements (NFRs). The priority of these NFRs is based on business justification, operational need, and customer importance. For Orange, a key customer, this priority will be accelerated for specific needs like Flex-Algo features. Periodic updates and meetings with Product Management will be established.

Maintenance & Support:

The DriveNets Technical Support Center (DTSC) is staffed around the clock and offers comprehensive maintenance and support. Orange will have a designated Program Manager for issue resolution. DTSC services include, but are not limited to, troubleshooting, incident management, and root cause analysis, backed by an experienced management team.

Through the DTSC offering we deliver the following advantages to ensure day-to-day services function efficiently and effectively in support of both in warranty and post warranty activities:

- Experienced and proven management team – successfully demonstrating compliance. Our management plan focuses on performance-based customer satisfaction in operations and management readiness.

- Ability to implement cutting-edge technology – regularly delivering to customers the very latest innovations and cost savings.

- The DTSC model engages with an expanded team that currently supports Service Providers. Our services include maintenance, field services, help desk services, staffing, infrastructure support (hardware and software), maintenance services, network operations and training support.

DriveNets is qualified to provide this support to assist in your mission to perform and deliver results in the highest level of customer experience.

Services Overview: T2 and T3 Technical Support

- Troubleshooting and Root Cause Analysis
- Analyze DriveNets Products Platform / Infrastructure Alerts
- Incident Management
- Troubleshooting and Debugging
- Root Cause Analysis of issues identified in the DriveNets Products application
- Interaction with DriveNets Tier 4 Engineering Support

Service Models:

Our support model includes DriveNets, the hardware provider, and a local Value-Added Reseller (VAR). DriveNets will handle all tickets and ensure timely responses in line with Service Level Agreements (SLAs). Orange can directly report any issue to DriveNets Customer Support, who will manage the issue's resolution, engaging with ODM or partners as needed.

Software Upgrades:

DriveNets Orchestrator (DNOR) centralizes inventory management and software upgrades. For quick issue resolution, we offer both hot and cold patches relevant to bug fixes.

Additional Services:

DriveNets' network of global System Integrators and local VARs can provide localized services such as hardware sourcing, technical support, and warehousing.

By offering these comprehensive services, DriveNets is fully equipped to support Orange in delivering a high-quality customer experience.

8.5 Delivery

We would like to have light and generic information regarding the delivery policy of the bidder, and the list of partnerships used for the delivery.

Here below are some criteria the vendor is invited to consider:

- Time to deliver per country basis (6 to 8 weeks? several months? …)
- Deployment (where do you deliver? do you have a list of countries where you can deliver? …)
- Do you provide Next Business Day delivery service for the RMA (Return Merchandise Authorization)?
- Do you have DOA (Dead On Arrival) process?

Here below is the list of countries to be considered by the bidder: do you deliver directly to those countries?

EMEA

1. EUROPE (18 countries)

AUSTRIA, BELGIUM, BULGARIA, CZECH REPUBLIC, DENMARK, FRANCE, GERMANY, HUNGARY, ITALY, NETHERLANDS, NORWAY, POLAND, PORTUGAL, ROMANIA, SLOVAKIA, SPAIN, SWEDEN, SWITZERLAND, UNITED KINGDOM

2. AFRICA (12 countries)
   BURKINA FASO, COTE D'IVOIRE, DJIBOUTI, GHANA, JORDAN, KENYA, LIBERIA, MALI, NIGERIA, REUNION, SENEGAL, SOUTH AFRICA,

3. UNITED ARAB EMIRATES

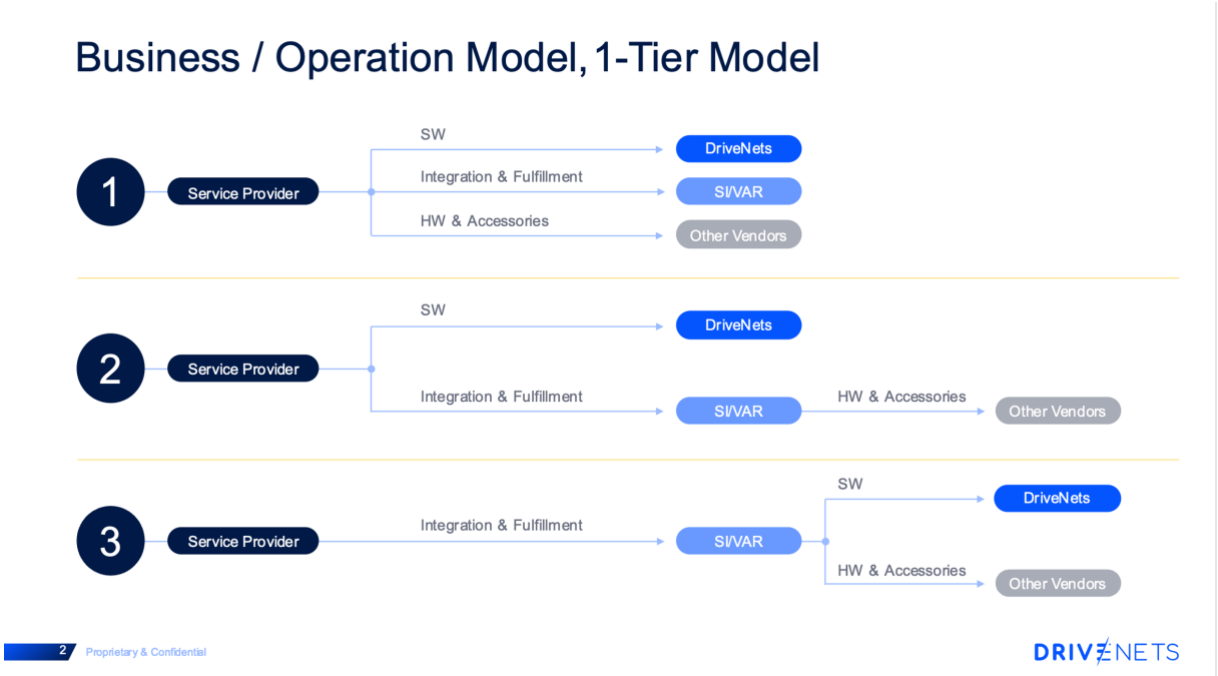
AMERICA (3 countries)
1. UNITED STATES
2. BRAZIL
3. CARIBBEAN
   MARTINIQUE, GUADELOUPE

ASIA (3 countries)
HONG KONG, JAPAN, SINGAPORE

The bidder is invited to detail his answer below, based on the questions (including countries coverage) mentioned above.

Vendor answer:

Disaggregated model allows higher flexibility on the delivery model. Orange may choose between different below models:



Model 1: Orange takes full direct relationship with all suppliers (DN, HW vendors, SI/VAR).
Model 2: DN handles SW directly with Orange and HW is handled by SI/VAR or HW vendors.
Model 3: VAR is the prime, B2B agreements with the rest of ecosystem.

For additional delivery services, DN global System Integrators and local VARs network may cover localized services in different counties. Such services may include HW sourcing and logistics, warehousing, staging, hardware technical support & maintenance, spare parts, RMA service, etc.

8.6 Pricing model

We are not asking for pricing here but pricing model. We know that 800GE access deployment will happen at some point in time (see chapter 10). In that context, the 'pay as you grow' model seems particularly suited because this model allows us to invest only where the 800GE will be effectively deployed.

Can you please describe your pricing model?

Vendor answer:

DriveNets offers a variety of pricing models designed to align with the unique economic conditions and business goals of each service provider. By providing flexible pricing options, we aim to accommodate different financial constraints and operational requirements. Below are the pricing models you can choose from:

- Perpetual Licenses Based on Physical Port Capacity: This model allows service providers to pay a one-time fee for licenses based on the speed of physical ports. The port speeds available for this option range from 1G to 800G, with intermediary options including 10G, 25G, 100G, and 400G. Once purchased, the license will not expire and is yours to use indefinitely.

- Subscription Licenses Based on Physical Port Capacity: This model follows a subscription-based approach, offering licenses for various physical port speeds from 1G to 800G, similar to the perpetual license model. Instead of a one-time purchase, this option involves regular payments, typically on an annual basis, for the duration of the subscription period.

- Enterprise Agreement: This is a more comprehensive and customized option tailored to your specific needs. An Enterprise Agreement often includes various combinations of perpetual and subscription licenses, along with additional support and services, in a single, bundled offering. This agreement is usually designed for long-term partnerships and can be customized to align with strategic business objectives.

These pricing models are created to offer service providers the flexibility to select the approach that best suits their financial outlook and business strategies. Whether you're looking for a long-term investment, operational agility, or a customized package, DriveNets has a pricing model to meet your needs.

8.7 Licensing model

Orange is willing to have an efficient license tracking mode.

The vendor is invited to describe his solution to manage our licenses in a centralized manner, the server hosting our licences having to be located within the Orange premises.

These licences should not be enforced, not to impact our services, but should allow to alert us when a licence has not been paid. The licence enforcement should be prohibited.

Vendor answer:

DriveNets currently does not implement a License Server to count/control/police the licenses in a Service Provider Network. As it stands today and in the near future, the Licensing model is managed on trust basis and DriveNets relies on the Service Provider to purchase extra licenses when purchased capacity is exceeded.

Following Market demand, DriveNets will build a Licensing Monitoring capability which may reside as part of DNOR or as a standalone entity, whatever is the final solution and design, the Licensing Monitoring capability will be in the SP's Network without remote access and will not have any policing or enforcing capabilities. As DriveNets believes that between partners where trust relationships are established, there is no need and no plan to enforce / limit / control the network elements by the license servers.

9 Green strategy

In this RFI, we are asking the bidder to provide the carbon emission and power consumption required for the proposed solution during the 5 years long deployment. The bidder shall provide the total amount of carbon required to manufacture, deliver, and recycle the clusters or chassis.

In the case of DDC or IP CLOS solutions, not only the individual white boxes should be considered but also the switches, servers, and optics used for the fabric. We let the bidder propose the most appropriate servers and switches for the proposed solution, and then rely on the technical power consumption specifications of the product. The bidder could share any measurement done for the proposed hardware even if the configurations would differ from the profiles specified in chapter 10.

More globally, the vendor will describe its green strategy to reduce its carbon footprint, in particular are your product EE measure process compliant to the following specification:
ES 203 136 - V1.2.0 - Environmental Engineering (EE); Measurement methods for energy efficiency of router and switch equipment (etsi.org)

Vendor answer:

DriveNets is revolutionizing the network industry by shifting its core focus from hardware to software, introducing game-changing efficiencies and flexibility for service providers. More than a technological pivot, this move also aligns with pressing environmental objectives, contributing to a sustainable, energy-efficient future in line with Koomey's Law, which posits that the energy efficiency of computing doubles approximately every 1.5 years.

Hardware-Agnostic Approach for Peak Efficiency: Our DriveNets Operating System (DNOS) allows service providers to choose and seamlessly transition to hardware platforms that are at the cutting edge of performance and energy efficiency. The power to switch to more efficient hardware without system-wide upheaval means that as advances are made in hardware energy efficiency—consistent with Koomey's Law—service providers can readily adopt these advances. This hardware-agnostic strategy offers a direct pathway for reducing greenhouse gas emissions and achieving a more sustainable operational model.

Sustainable Network Design: DNOS's innovative design capability places an emphasis on reducing redundant hardware components like power units and fabric modules. This minimalistic, optimized design approach not only lowers capital expenditures but also significantly reduces energy consumption. In line with the scientific understanding that energy usage is a major contributor to climate change, this strategy can substantially lower a service provider's carbon footprint.

Resource Lifecycle Extension: With DNOS serving as a unifying software platform, the service provider's infrastructure footprint is minimized. This optimization extends the useful life of both hardware and software, effectively reducing electronic waste, another significant environmental issue. The net result is a more efficient use of materials and lower energy requirements for manufacturing and disposal, in compliance with circular economy principles.

Harnessing AI for Sustainable Operation: We are heavily invested in integrating artificial intelligence technologies into our platform. By using AI algorithms for network monitoring and predictive maintenance, service providers can achieve a level of operational excellence that significantly reduces the need for energy-intensive manual oversight. This computational efficiency is another nod to Koomey's Law, highlighting how improved algorithms can result in energy savings.

Green Innovation Through Software: As DriveNets continues to invest in software-driven solutions, we are directly contributing to the tenets of Koomey's Law by improving the energy efficiency of computational tasks. This leads to a lower energy cost per transaction, making our network solutions not just economically advantageous, but also environmentally responsible.

In sum, DriveNets is not just innovating for the sake of technological progress; we are conscientiously developing solutions that have a lower environmental impact. By adhering to principles supported by Koomey's Law and other scientific facts, we are actively contributing to a more sustainable and energy-efficient future for the networking industry.

9.1 Carbon footprint reduction

9.1.1 What is the bidder's green strategy?

Orange is very concerned with the support of solutions requiring minimal carbon emission.

We are considering the following two items, but only the first item must be provided by the vendor:

1. The **embedded emissions** are due to the manufacturing, delivery and recycling of the chassis, or clusters (white boxes, switches, servers, optics & cables required for the cluster's fabric**). This information shall be provided by the vendor and fulfilled to the line titled " "embedded emissions" (CO2e tonnes)" of the tables Table 8 to Table 13.**
   We are also asking the vendor is some measured values or abacus have been performed by the vendor for some configuration looking be like ours, or if any measurement have been performed.

2. The **emissions in use** are due to the actual power consumption.
   This corresponds to the carbon emission that is tight to the power consumption and depends on the route profile (disaggregated or not) and on each country where the electricity is produced. This type of emission is NOT asked to the vendor, Orange will compute that figure based on the power consumption figures provided by the vendor.

Can the vendor highlight the key elements impacting the carbon emission with regards to the proposed solution (white box or chassis manufacturing and support, transport for storage and delivery at Orange premises, ….)?

More globally, the vendor should describe his strategy to reduce the CO2 consumption, and possibly the associated procedures or methodology.

Vendor answer:

DriveNets License Servers are designed solely to track and monitor licenses within a Service Provider Network. Positioned within Orange's internal network, these servers operate on a foundation of trust between partners. DriveNets has no intention to enforce, limit, or control network elements via the license server, adhering to established trust relationships.

9.1.2 Target countries of the RFI

As explained in the previous section, the *embedded carbon emissions* relate to the manufacturing, delivery and recycling of the hardware platforms used for the solution. In this section, we focus on the delivery distances, because they directly influence the level of carbon emissions: the longer distances the more carbon emissions.

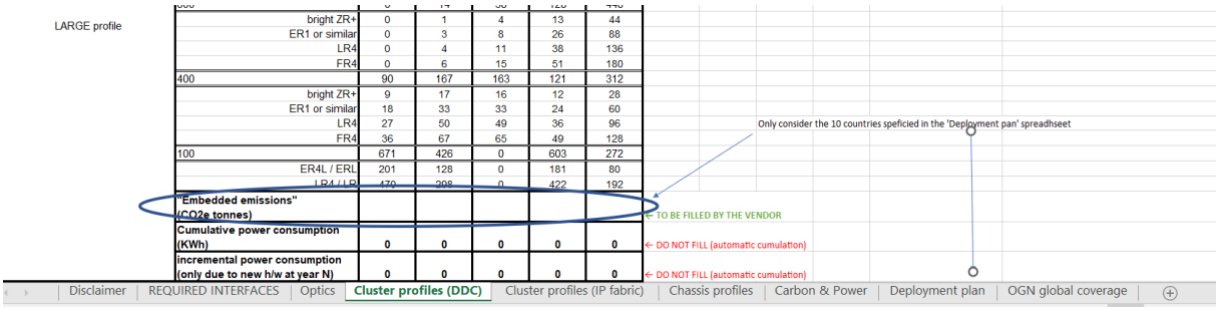
Table 3 below provides the list of target countries where the 31 (disaggregated) routers are planned to be deployed. This is useful to compute the *embedded carbon emissions* related to the transport, because it allows the bidder to determine the actual distances between those Orange locations and the bidder's storage centers.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1		2025			2026			2027			2028			2029		
2		S	M	L	S	M	L	S	M	L	S	M	L	S	M	L
3	Belgium														BRUx1	
4	France	PARx1		PARx1	PARx1 QYRx1		PARx1	PARx1			MRSx1	PARx1	PARx1	PARx1 QYRx1	PARx1	PARx2
5	Germany									FRAx1						FRAx1
6	Hungary	BUDx1														
7	Netherland														AMSx1	
8	Spain								MADx1			BCNx1				MADx1
9	Dubai										DXBx1			DXBx1		
10	Ghana				ACCx2											
11	Honk-Hong	HKGx3														
12	Nigeria				LOSx1						LOSx1					
13	TOTAL S/M/L	5	0	1	5	0	1	1	1	1	3	2	1	3	3	4
14	Embedded Emission carbon related to delivery (CO2 tonnes) - per year															
15																
16																
17	IATA codes	ACC: Accra; AMS: Amsterdam; BUD: Budapest; BRU: Brussels; DXB: Dubai; FRA: Frankfurt; HKG: Honk-Hong; LOS: Lagos; MAD: Madrid; MRS: Marseille; PAR: Paris; QYR: Troyes For exemple, HKGx3 column 'S' in 2025 means that 3 SMALL profile routers are planned to be deployed in Honk-Hong in 2025														

Table 3 Target countries

The computation of the embedded emission carbon should be limited to the target 10 countries mentioned in the table above (Belgium, France, Germany, etc.). The values in lines 13-16 related to the delivery must be fulfilled in the *Orange OGN RFI - router profiles 2025-2029* excel file ('Deployment plan' sheet).

As an example, the values specified in cells D14, G14, J14, M14 and P14 of Table 3 should be added to the values of carbon emission for the manufacturing and recycling of the hardware platform for the LARGE profile (2025-2029 period), as shown below. As a reminder, the sum of carbon emissions for delivery, manufacturing and recycling represent the embedded emissions.



9.2 Power consumption

Power consumption has an impact not only on the carbon footprint but also on the energy costs.

The bidder should provide the references and the explanations to help us understanding where the figures are coming from and how they are computed.

Especially, the bidder shall provide the power consumed by the proposed solution, on yearly basis, as required in chapter 10.

Please refer to the Excel to fulfil the expected figures.

Here below, feel free to describe the effort put on your power consumption optimisation strategy.

Vendor answer:

DriveNets is committed to pioneering software innovations that substantially elevate power efficiency and shrink our carbon footprint. By transitioning from a hardware-centric to a software-driven network design, we revolutionize the approach to network architecture. Our strategy aligns closely with Koomey's Law, which states that the energy efficiency of computing doubles approximately every 1.5 years. Below are key strategies that not only exemplify efficient design but also integrate green approaches:

Energy-Efficient Network Architecture

In our response, 23 out of 31 smaller sites, mainly handling north-south traffic, achieved a 50% improvement in efficiency compared to traditional chassis systems. Specifically:

- The energy efficiency ratio (Watt/Gbps) in our discrete Whitebox nodes is three times better than that in chassis/fabric-based nodes.
- By eliminating or minimizing large, fabric-based nodes in favour of smaller, discrete Whitebox nodes, we reduce power consumption.
- Our network topology itself ensures required redundancy and scalability, negating the need for power-hungry components.
- A simple discrete whitebox approach simplifies sparing, warehousing and inventory management

Extended Strategies for Power-Efficiency and Sustainability:

1. Optimized Network Design for Energy Efficiency

Smaller, Modular Elements: Our approach decentralizes the network through smaller routing elements, effectively dispersing energy requirements. This decentralization better aligns with Koomey's law, as smaller, more energy-efficient technologies can be deployed faster than large, centralized systems.

Inventory & Environmental Impact: By minimizing the number of components required for each unit, we reduce inventory costs and the overall environmental footprint. This approach adheres to the principles of green computing, where reducing material consumption goes together with reducing energy consumption.

2. Disaggregation of Hardware and Software

Vendor Flexibility: The ability to interchange hardware and software vendors not only provides operational flexibility but also enables easier adoption of the latest, more energy-efficient technologies. This adaptability allows networks to consistently align with the improvements predicted by Koomey's law.

Unified Monitoring: Centralized monitoring under this architecture is more energy-efficient due to reduced computational overhead. Fewer machines need to be kept running for diagnostics and monitoring, and software-based operations can be far more energy-efficient than hardware operations, especially as software optimization technologies advance.

3. Multi-Service Resource Pooling

Dynamic Resource Allocation: Our Network Cloud architecture abstracts hardware resources into a pool that can dynamically serve multiple network functions. This approach dramatically improves resource utilization rates, reducing idle time and thereby lowering overall energy consumption in line with Koomey's law.

Cost & Energy Efficient Non-Routing Functions: Incorporating non-routing functions like firewalls and DPI within the existing architecture removes the need for additional energy-consuming hardware. This elimination of extra hardware contributes to lower energy costs and a reduced carbon footprint.

4. Circular Economy and Lifecycle Management

Hardware Repurposing: This strategy extends the useful life of hardware, mitigating the environmental impacts of manufacturing and disposal. Extending hardware lifespan is a significant energy saver, given that a large percentage of a device's total energy consumption is often embedded in its manufacturing.

Software Longevity: Prolonged software EoL policies mean that hardware can remain in use longer, reducing the frequency of hardware turnover and thereby further minimizing environmental impact. This is another manifestation of green computing, which is becoming increasingly vital as part of global sustainability strategies.

By embedding these strategies into our operations, DriveNets is pushing the envelope on what it means to be an energy-efficient, sustainable organization in the tech industry. These practices not only optimize performance but also set a precedent for environmental responsibility, directly in line with Koomey's law and broader global sustainability goals.

10 OGN core router profiles & deployment roadmap

OINIS plan to replace 31 legacy routers with 31 'new generation routers' on OGN during the 2025-2029 period.

The term 'router' refers to our usual 1:1 router swap policy that applied for decades (for technology refresh or capacity upgrade purposes): one legacy router was systematically replaced with one 'new generation' router. In this RFI, a single 'new generation router' can be in the form-factor of a single white box, or a single cluster of multiple white boxes, or a single chassis.

We therefore anticipate that more than 31 "white boxes" will be required to replace the 31 'legacy' routers on OGN. This is because a single white box might not answer our capacity needs, depending on the profiles (described just after in section 10.1).

Hence, the fact a single legacy router can be swapped with one white box or cluster of white boxes, or chassis impacts our standard swap policy, leading the following swap policy options:

1. "1 router:1 white box" swap policy
2. "1 router:1 cluster" swap policy
3. "1 router:1chassis" swap policy (our usual policy)

The first two swap policies are specific to NOS providers solutions where a single white box would be enough to meet the SMALL profile, and either a single white box or a cluster of white boxes (DDC or IP CLOS model) could be required for the MEDIUM and LARGE profile.

The last swap policy is suited to providers offering chassis.

We also need to know the number of additional devices – other than the white boxes themselves - required to build the solution. For instance, this can be the total number of servers or switches required to implement and manage the solution in case of a DDC or IP CLOS proposal.

To make it short, the vendor shall explain how many “white boxes”, switches, servers and optics used for the chassis (Table 8, Table 9, Table 10) or DDC/IP CLOS models (Table 11,

		Increment (yearly orders) 6 routers - average profiles				
		2025	2026	2027	2028	20
MEDIUM profile	**#clusters →**	0	0	1	2	3
	white box (spine role) - type #1					
	white box (spine role) - type #2					
	white box (leaf role) - type #1					
	white box (leaf role) - type #2					
	white box (leaf role) - type #3					
	white box (leaf role) - type #4					
	#switches (management)					
	#servers (control plane)					
	#optics for the fabric					
	#rack units					
	#fabric cables					
	GE Interfaces ↓					
	400	0	0	34	92	20
	bright ZR+	0	0	5	14	3
	ER1	0	0	5	14	3
	LR4	0	0	12	32	7
	FR4	0	0	12	32	7
	100	0	0	163	276	7
	ER4L / ERL	0	0	16	28	6
	LR4 / LR	0	0	147	248	6
	10	0	0	123	68	57
	ER	0	0	12	8	5
	LR	0	0	111	60	51
	"Embedded emissions" (CO2e tonnes)	0	0			
	Cumulative power consumption (KWh)	**0**	**0**	**0**	**0**	**0**
	incremental power consumption (only due to new h/w at year N)	**0**	**0**	**0**	**0**	**0**

Table 12, **Error! Reference source not found.**) OINIS should deploy until 2029. This information is required to know the carbon footprint and total power consumption of the proposed solutions.

10.1 Router Profiles

To facilitate the overall analysis, the 31 legacy OGN routers have been classified in three generic profiles – LARGE, MEDIUM and SMALL-, depending on the connectivity needs (Table 4). Yearly increments of new routers or interfaces are provided per profile from 2025 until 2029 (see section 10.3).

As a complementary information, the maximum hardware configuration of each profile is provided in Table 6: **the vendor must provide these maximum configurations**, whatever the proposed disaggregation solution.

10.1.1 Generic profiles: LARGE, MEDIUM and SMALL

As mentioned just above, we propose to classify our needs based on the following three profiles:

- LARGE profile introduces the need for 800GE. No 1/10GE ports in this profile

- 8 routers concerned
- MEDIUM profile requires 400GE/100GE ports density and introduces 10GE support compared to LARGE profile. No 1GE.
  - 6 routers concerned
- SMALL profile shall mainly support 1GE-to-100GE connectivity, while offering 400GE capability
  - 17 routers concerned

This is illustrated in the table below.

	GE Interfaces				
router profiles ↓	800	400	100	10	1
large	√	√	√		
medium		√	√	√	
small		few	√	√	√

Table 4 Routers profiles definition

Table 5 provides the total number of interfaces per each profile. It also gives the total number of 1GE/10/100GE/400GE/800GE ports required for this RFI (total is ~6000 ports)

	Required GE interfaces per profile (all 31 routers)				
router profiles ↓	800	400	100	10	1
LARGE (8)	628	853	1972		
MEDIUM (6)		330	514	761	
SMALL (17)		19	189	412	288
Total	628	1202	2675	1173	288

Table 5 Global number of interfaces per router profile

We remain at the disposal of the bidder to present these profiles during the RFI.

10.1.2 Maximum configurations

A maximum h/w configuration is also provided for each of the three profiles. This is because the generic profiles correspond to an average whereas we also need to cover the maximum size for each profile, that corresponds to the configuration in 2029.

The vendor must support the following MAXIMUM configurations.

We can see from Table 6 that, approximately:

1. The **MAXIMUM LARGE** profile is requiring ~**250Tbps** switching capacity
2. the **MAXIMUM MEDIUM** profile is requiting ~**50Tbps** switching capacity
3. the **MAXIMUM SMALL** profile is requiring ~**3.5Tbps** switching capacity

As explained in next section, the fabric should be non-blocking, i.e. there must be NO fabric overbooking in this RFI exercise, including the maximum configurations shown above.

Concerning the LARGE and potentially the MEDIUM profiles, the vendor could propose a cluster solution (so multi-chassis or multi-white boxes) that might be different from the DDC and IP CLOS fabric solutions. In such case, the bidder will describe the solution (see chapter 5).

For the SMALL profile, we assume a single white box or chassis (possibly with smaller form factor) should answer our needs. Still the bidder is able to propose cluster or multi-chassis solution even for the SMALL profile.

		Maximum number of GE interfaces						
	Biggest router configuration per profile (2029) ↓	800	400	100	10	1	TOTAL capacity (Tbps)	APPROXIMATIVE TARGET capacity (Tbps)
		153	204	479			252	250
MAX LARGE	bright ZR+	15	20					
	ER1 or similar	31	41	143				
	LR4	46	61	336				
	FR4	61	82					
			83	130	193		48	50
MAX MEDIUM	bright ZR+		8					
	ER1 or similar		17	39	58			
	LR4		25	91	135			
	FR4		33					
			2	23	39	36	3,5	3,5
MAX SMALL	ER4L / ERL		1	16	27			
	LR4 /LR		1	7	12	36		

Table 6 Largest router configuration of each profile (reached in 2029)

Note: ER optics for the SMALL is indeed rare, we use it mainly in Paris.

Please describe your solution to support the MAX configuration of each profile. Please use the "*OINIS Disaggregation RFI – router profiles 2025-2029 (June 26th)*" Excel file for that purpose.

Vendor answer:

Please see details in XLS

10.1.3 Optics

Please note that optics for 10GE, 100GE, 400GE and 800GE ports shall be integrated in the vendor proposal. The vendor shall also specify if the following optics are supported:

- 10G: ER (40km), LR (10km)
- 100G: ER4L/ERL (40km), LR4/LR (10km)
- 400G: ZR+ bright, ER1 (40km), LR4 (10km), FR4 (2km)
- 800G: ZR+ bright, ER1 (40km), LR4 (10km), FR4 (2km)

Please provide the corresponding quantities for the entire solution for the 2025-2029 period, so that the power consumption includes ALL those optics. Power consumption for each type of optics should be provided as well (please use the "*OINIS Disaggregation RFI – router profiles 2025-2029 (June 26th)*" Excel file for that purpose).

Please describe your optics support solution.

Do you support third party providers ?

Vendor answer:

As a Software NOS provider, we support all Optics' and transceivers which present as standard form factor to the underlying ODM.

We qualify and test specific Optics and transceivers requested by our customers, but do not limit our customers to any specific manufacturer. We operate a Similarity Policy: for Optical transceivers you may use any transceivers (supported by the ODM) with identical speeds and types to those listed in our documentation from ANY vendor and the solution will be fully supported by DriveNets.

We currently have certified optical and coherent transceivers from:

Acacia
Cisco
Juniper
Finisar
Innolight
Intel
Colorchip
Precision
Mellanox
Mollex

10.1.4 Breakout cables

Note that breakout cables can be proposed and in such a case it should be clearly described. For instance, it might be of interest for the bidder having many 800GE ports to sue some of them to offer 2x400GE ports. Any breakout options is possible (including 10GE breakout to offer 1GE connectivity).

Breakout cables can be used for the network ports (the ones used to connect our customer or our backbone links) and fabric ports (even if this latter case does not sound a common practice to our knowledge). Please feel free to adapt the 'Optics' sheet of the excel file named '*Orange OGN RFI – router profiles 2025-2029*'

Please describe your break-out solution.

Vendor answer:

To Optimise the power consumption, we propose to utilize breakout cables within the solution. We will include the power consumption required by the breakouts within the power figures provided for the relevant optics in the router profile spreadsheets. We will utilize the most power and port optimal breakouts within the relevant DDC builds.

We propose the following breakouts as needed to address the Orange port requirements:

800G DR8 (MPO16 / Dual MPO12) to QSFP28 8x100D-DR1 (500m)
800G DR8+ (MPO16 / Dual MPO12) to QSFP28 8x100D-FR1 (2km)
800G 2xLR4 (Dual Duplex LC) to QSFP-DD 400G-LR4 x 2 (10km)
800G 8x100G-LR (Dual MPO12) to QSFP28 100G-LR1 x 8 (10km)
400G DR4 (Breakout 4x100G)
400G LR (Breakout 4x100G)
400G-DR4+ (Breakout 4x100G)
400G-DR4 (Breakout 4x100G)

10.2 How to fulfil carbon emission and power consumption?

We are asking the bidder to provide the carbon emission and power consumption information for each router profile or cluster profile (SMALL, MEDIUM, LARGE).

Table 8 to Table 13 provide the expected GE ports distribution per each profile definition. The carbon emissions and power consumption figures should be fulfilled by the vendor in each of those tables at the dedicated line titled 'embedded emissions' and 'cumulative power consumption' respectively.

Table 8 to Table 13 contains carbon footprint and power consumption entries to be fulfilled by the vendor based on the following rules:

⇨ Concerning the power consumption calculation, we ask vendor to fulfil the dedicated line titled 'embedded emissions' based on the following rule:

- Year 2025: power consumption is computed end of the year (this is true for all the years)
- Year 2026: Year 2026 + 2x2025
- Year 2027: Year 2027 + 2x Year 2026 + 3x Year 2025
- Year 2028: Year 2028 + 2x Year 2027 + 3x Year 2026 + 4x Year 2025
- Year 2029: Year 2029 + 2xYears 2028 + 3x2027 + 4x2026 + 5x2025

Year 2029 provides the total power consumed by the solution, per profile.

⇨ Concerning the carbon emission calculation, the vendor should provide the figure required for a given year. There is no cumulative effect, it's a one-shot figure, provided year per year, and correspond to the carbon emitted for the manufacturing of the interfaces & chassis/cluster to be deployed at a given year.

- Year 2025 : embedded emission carbon required for the material to be deployed in 2025
- Year 2026 : embedded emission carbon required for the material to be deployed in 2026
- Year 2027 : embedded emission carbon required for the material to be deployed in 2027
- Year 2028 : embedded emission carbon required for the material to be deployed in 2028
- Year 2029 : embedded emission carbon required for the material to be deployed in 2029

To know the total, we must sum the carbon emission during the five years (for each profile class).

Total carbon emission = year 2025+… + year 2029.

We need a summary table to see briefly how much carbon emissions and power will be "required" for the proposed solution during the 2025-2029 period. For this purpose, the bidder must report in Table 7 below**:**

- **Power consumption values**

Those should be extracted from the last line (titled “cumulated power consumption”) of Table 8 to Table 13 in Year 2029 (cell of last row last column). As detailed just above, **Year 2029 corresponds to the cumulative power consumption during the 2025-2029 period**.

- **Carbon emission values**
  Those should be extracted from the last line of Table 8 to Table 13: for each line titled ‘Embedded emissions’ sum the carbon emission values (year 2025+… + year 2029. The three sums corresponding to the carbon emission of the three profiles must be reported in the table below.

	LARGE	MEDIUM	SMALL	TOTAL
CARBON EMISSION "embedded emissions" (CO2e tonnes)	**sum 'Y25-'Y29**	**sum 'Y25-'Y29**	**sum 'Y25-'Y29**	
CUMULATIVE POWER CONSUMPTION (KWH)	**'Y29**	**'Y29**	**'Y29**	

Table 7 Carbon emission & power consumption (2025-2029 period)

10.3 Deployment plan

The table below provides the number of routers to be swapped with disaggregated routers (single white boxes, clusters, or chassis). It is always difficult to provide forecast because things can change noticeably in 5 years, so the planning is based on steady growth + margin exercise and 1:1 swap policy as explained earlier. Those figures are not committed and might change over time but represent the most precise view we can share at the time of the RFI. We do not plan to adapt them at the RFP/RFQ time, even if could happen.

In the case of chassis-based solution, we propose an incremental approach. For instance, in 2025 we plan to order one LARGE router and the year after another one with additional cards.

The new cards ordered in 2026 should be shared amongst the two routers ordered in 2025 and 2026, so they have similar configurations. Same logic should apply until 2029 so that the 8 LARGE routers have equivalent h/w Line Cards distribution.

We propose at least two table formats:

1. One table format that should be used by the bidders offering chassis-based solutions (Table 8, Table 9, Table 10).
   Here, we assume the bidder has one chassis with possibly several form factors (depending on the number of line cards): by default, we assume we can perform a 1:1 router swap. However, for the LARGE profile, that is ~250Tbps capable, a second chassis could be required. In such case, the additional ports and optics required to interconnect the two chassis (if not more) should be mentioned.

2. One table format that should be used by the NOS provider bidders offering cluster-based solutions (Table 11, Table 12, Table 13)
   Here, we ask the bidder to fill the number of devices required depending on the proposed model (DDC, IP CLOS, potentially other architectures). Each disaggregated router is formed by a cluster of devices (spine devices, leaf devices, switches, servers). We consider we will have to deploy the same number of clusters in Table 11, Table 12, Table 13 as the number of chassis mentioned in Table 8, Table 9 Table 10 respectively. So, the total of #clusters should not exceed 31, even if there will more than 31 devices (white boxes, servers, management switches). Table 11, Table 12, Table 13 can also be used for other clusters definition than the DDC and the IP CLOS, if required, because the hardware elements of the cluster should be the same à priori, as far we consider only the software solution forming the cluster could differ. This later point could be discussed during the RFI, if needed.

		Increment (yearly orders) 8 routers - average profiles				
		2025	2026	2027	2028	2029
LARGE profile	**#chassis →**	1	1	1	1	4
	#Line card type#1					
	#Line card type#2					
	#Line card type#3					
	#Line card type#4					
	#rack units					
	GE Interfaces ↓					
	800	0	14	38	128	448
	bright ZR+	0	1	4	13	44
	ER1 or similar	0	3	8	26	88
	LR4	0	4	11	38	136
	FR4	0	6	15	51	180
	400	90	167	163	121	312
	bright ZR+	9	17	16	12	28
	ER1 or similar	18	33	33	24	60
	LR4	27	50	49	36	96
	FR4	36	67	65	49	128
	100	671	426	0	603	272
	ER4L / ERL	201	128	0	181	80
	LR4 / LR	470	298	0	422	192
	"Embedded emissions" (CO2e tonnes)					
	Cumulative power consumption (KWh)	**0**	**0**	**0**	**0**	**0**
	Incremental power consumption (only due to new h/w at year N)	**0**	**0**	**0**	**0**	**0**

Table 8 LARGE profile (chassis architecture)

		Increment (yearly orders) 6 routers - average profiles				
		2025	2026	2027	2028	2029
MEDIUM profile	**#chassis →**	0	0	1	2	3
	#Line card type#1	0	0			
	#Line card type#2	0	0			
	#Line card type#3	0	0			
	#Line card type#4	0	0			
	#rack units					
	GE Interfaces ↓					
	400	0	0	34	92	204
	bright ZR+	0	0	5	14	30
	ER1	0	0	5	14	30
	LR4	0	0	12	32	72
	FR4	0	0	12	32	72
	100	0	0	163	276	75
	ER4L / ERL	0	0	16	28	6
	LR4 / LR	0	0	147	248	69
	10	0	0	123	68	570
	ER	0	0	12	8	57
	LR	0	0	111	60	513
	"Embedded emissions" (CO2e tonnes)	**0**	**0**			
	Cumulative power consumption (KWh)	**0**	**0**	**0**	**0**	**0**
	incremental power consumption (only due to new h/w at year N)	**0**	**0**	**0**	**0**	**0**

Table 9 MEDIUM profile (chassis architecture)

		Increment (yearly orders) 17 routers - average profiles				
		2025	2026	2027	2028	2029
SMALL profile	**#chassis →**	8	6	1	1	1
	#Line card type#1					
	#Line card type#2					
	#Line card type#3					
	#Line card type#4					
	#rack units					
	GE Interfaces ↓					
	400	0	0	1	9	9
	LR4	0	0	1	6	6
	FR4	0	0	0	3	3
	100	50	35	17	45	42
	ER4L / ERL	5	5	1	3	3
	LR4 / LR	45	30	16	42	39
	10	210	0	34	78	90
	ER	10	0	2	3	6
	LR	200	0	32	75	84
	1	70	40	22	72	84
	"embedded emissions" (CO2e tonnes)					
	Cumulative power consumption (KWh)	**0**	**0**	**0**	**0**	**0**
	incremental power consumption (only due to new h/w at year N)	**0**	**0**	**0**	**0**	**0**

Table 10 SMALL profile (chassis architecture)

		Increment (yearly orders) 8 routers - average profiles				
		2025	2026	2027	2028	2029
LARGE profile	**#clusters →**	1	1	1	1	4
	white box (spine role) - type #1					
	white box (spine role) - type #2					
	white box (leaf role) - type #1					
	white box (leaf role) - type #2					
	white box (leaf role) - type #3					
	white box (leaf role) - type #4					
	#switches (management)					
	#servers (control plane)					
	#optics for the fabric					
	#rack units					
	#fabric cables					
	GE Interfaces ↓					
	800	0	14	38	128	448
	bright ZR+	0	1	4	13	44
	ER1 or similar	0	3	8	26	88
	LR4	0	4	11	38	136
	FR4	0	6	15	51	180
	400	90	167	163	121	312
	bright ZR+	9	17	16	12	28
	ER1 or similar	18	33	33	24	60
	LR4	27	50	49	36	96
	FR4	36	67	65	49	128
	100	671	426	0	603	272
	ER4L / ERL	201	128	0	181	80
	LR4 / LR	470	298	0	422	192
	Cumulative power consumption (KWh)	**0**	**0**	**0**	**0**	**0**
	incremental power consumption (only due to new h/w at year N)	**0**	**0**	**0**	**0**	**0**

Table 11 LARGE profile (DDC, IP CLOS, or other type of architecture)

		Increment (yearly orders) 6 routers - average profiles				
		2025	2026	2027	2028	2029
MEDIUM profile	**#clusters →**	0	0	1	2	3
	white box (spine role) - type #1					
	white box (spine role) - type #2					
	white box (leaf role) - type #1					
	white box (leaf role) - type #2					
	white box (leaf role) - type #3					
	white box (leaf role) - type #4					
	#switches (management)					
	#servers (control plane)					
	#optics for the fabric					
	#rack units					
	#fabric cables					
	GE Interfaces ↓					
	400	0	0	34	92	204
	bright ZR+	0	0	5	14	30
	ER1	0	0	5	14	30
	LR4	0	0	12	32	72
	FR4	0	0	12	32	72
	100	0	0	163	276	75
	ER4L / ERL	0	0	16	28	6
	LR4 / LR	0	0	147	248	69
	10	0	0	123	68	570
	ER	0	0	12	8	57
	LR	0	0	111	60	513
	"Embedded emissions" (CO2e tonnes)	**0**	**0**			
	Cumulative power consumption (KWh)	**0**	**0**	**0**	**0**	**0**
	incremental power consumption (only due to new h/w at year N)	**0**	**0**	**0**	**0**	**0**

Table 12 MEDIUM profile (DDC, IP CLOS, or other type of architecture)

		Increment (yearly orders) 17 routers - average profiles				
		2025	2026	2027	2028	2029
SMALL profile	**#White boxes →**	5	5	1	3	3
	white box (spine role) - type #1					
	white box (spine role) - type #2					
	white box (leaf role) - type #1					
	white box (leaf role) - type #2					
	white box (leaf role) - type #3					
	white box (leaf role) - type #4					
	#switches (management)					
	#servers (control plane)					
	#optics for the fabric					
	#rack units					
	#fabric cables					
	GE Interfaces ↓	(optical power consumption)				
	400	0	0	1	9	9
	LR4	0	0	1	6	6
	FR4	0	0	0	3	3
	100	50	35	17	45	42
	ER4L / ERL	5	5	1	3	3
	LR4 / LR	45	30	16	42	39
	10	210	0	34	78	90
	ER	10	0	2	3	6
	LR	200	0	32	75	84
	1	70	40	22	72	84
	"Embedded emissions" (CO2e tonnes)					
	Cumulative power consumption (KWh)	**0**	**0**	**0**	**0**	**0**
	incremental power consumption (only due to new h/w at year N)	**0**	**0**	**0**	**0**	**0**

Table 13 SMALL profile (DDC, IP CLOS, or other type of architecture)