RfP for acquiring Network Services Orchestration Platform Solution

Level Access	Authorized Person	Storage Place	Electronic copy sending	Paper Copy Access
Internal Access: Group **Internal-Group**	*This document and the information in it is intended for use only by authorized group employees or an employee, designated by the creator of the document.*	*In electronic form the document can be stored in all folders, workstations, laptops and portable media in the company where only authorized employees have access. Outside Neterra the document can be stored on laptops and portable media with encrypted shares with access only by the authorized employees.*	*The current document can be sent only to the official e-mails (neterra.net, neterra.tv) of the authorized employees.*	*Access to this document on paper, within the offices of the Neterra, have authorized employees who are required to exercise full control over the document throughout its use.* *A copy of the document can be transmitted only to another employee with access referred to in the document.* *Every copy shall be destroyed upon completion of work with it.*
Authorized persons:	***Network planning***			
External Access: Authorized Persons **External-Authorized Persons**	*Outside Neterra information in the document is intended for use only by authorized persons explicitly specified in the document.*	*In electronic form, the document may only be stored on servers and personal folders of authorized persons, who must keep the confidential nature of information and have an obligation for its nondisclosure.*	*The document can be sent by email outside the company only to the persons, specified in it.*	*Access to the paper copy of the document have only authorized persons and they must exercise full control over the document throughout the use and storage.* *The copy of the document can be transmitted only to authorized person, referred to in the document.* *The copy of the document must be destroyed upon completion of work with it.*
Authorized persons:	***Solution vendors***			

Table of Contents

1. Document History

Created 20 May 2019 by Yordan Kritski;

2. Introduction

The current document represents a Request for Proposal (RFP) for a software platform capable of delivering automation of the processes of provisioning of services over telecommunication network infrastructure.

Neterra is looking to purchase a solution, which provides the means for rapid and automated deployment of predefined telco service with the minimum participation of human operators.

This is a preliminary RfP, providing the scope of the activity and trying to evaluate the resources, costs and time needed.

The response to this request must result in a commercial offer for products and services.

3. Information Concerning the Proposal Process

3.1. Purchaser’s Name and Contact Information

Purchaser’s name and contact information is:

Neterra Ltd,

3 Grigorii Gorbatenko Str.,

Sofia 1784, Bulgaria

Tel.: +359 2 975 1616

Fax: +359 2 975 3436

Technical contact person:	Mr. Yordan Kritski	E-mail: ykritski@neterra.net
Commercial contact person:	Mr. Yordan Kritski	E-mail: ykritski@neterra.net

3.2. Delivery of the Proposal

The Proposal shall be sent to:

Neterra Ltd,

Commercial contact person: Mr. Yordan Kritski E-mail: ykritski@neterra.net / pg@neterra.net

The Proposal is expected to be received no later than **15.01.2020 15.00 PM UTC.**

3.3. Proposal Format

The Proposal must include:

- detailed price offer (bill of materials and services).
- a compliance statement to the requirements in a table form included in the different parts of the RFP. If there is non-compliance with some of the requirements those should be explained in detail. The compliance statement will form the basis of the Contract.

The Proposal shall be submitted as an electronic document(s). Adobe PDF, OpenOffice/LibreOffice or Microsoft Word/Excel file formats are acceptable where OpenOffice/LibreOffice is the preferred one.

3.4. Procedure for Questions

The Supplier prepares its Proposal based on the requirements and the information included in this RFP. If any question related to the RFP contents arises, the Supplier shall forward it by e-mail , as follows:

a) questions regarding technical issues to ykritski@neterra.net

b) questions regarding commercial issues to ykritski@neterra.net

The questions will be answered as fast and precise as possible.

3.5. Expenses

All expenses related to the submission, preparation and presentation of the proposal by the Supplier including transport, daily allowance and hotel accommodations shall be borne by the Supplier.

3.6. Confidentiality

All information in this document and other documents or subjects related to this RFP shall be regarded as strictly confidential.

Suppliers replying to this RFP must sign a formal Agreement of Confidentiality and return it before receiving the detailed RFP.

Any material or information received from Neterra is Neterra’s property and must not be shared with or distributed to any third party without Neterra’s consent.

4. Scope

The successful Supplier is required to provide the following Services related to the supply of the product which must be part of the Bid and will be included in the Contract:

a) Delivery of the product design and operations documentation

b) Delivery of the product

Supplier should deliver the product under DDP Sofia delivery terms.

c) Delivery of general documentation, detailed descriptions, O&M manuals, drawing and other necessary documentation for each appropriate unit of the supplied equipment.

d) Provision of after-sales services, hardware and software maintenance, back-up service, supervision and the repair of all supplied equipment during the warranty period.

e) Supply of spares for all delivered equipment (if applicable).

This RFP comprises requirements to the equipment and services that shall be supplied by the successful Supplier to the Purchaser under the conditions stated in the Contract. The Supplier is encouraged to supply better or equivalent equipment and services to the specified in the current document. Under the Contract the Supplier shall provide system engineering, manufacture, supply equipment, hardware, software and Services, test , in accordance with the Technical Requirements and Specifications and meet the required delivery schedule.

5. Concepts and general overview

Terminology note: for the sake of the current presentation the terms “automation” and “orchestration” will be used interchangeably throughout this document.

Neterra engages in this project with a specific goal – finding an optimal solution for a set of relatively simple, practical and well known challenges. The idea however is while finding the proper solution to those immediate needs, a foundation of much more robust and scalable platform to be laid down, capable of meeting our demands in the foreseeable future.

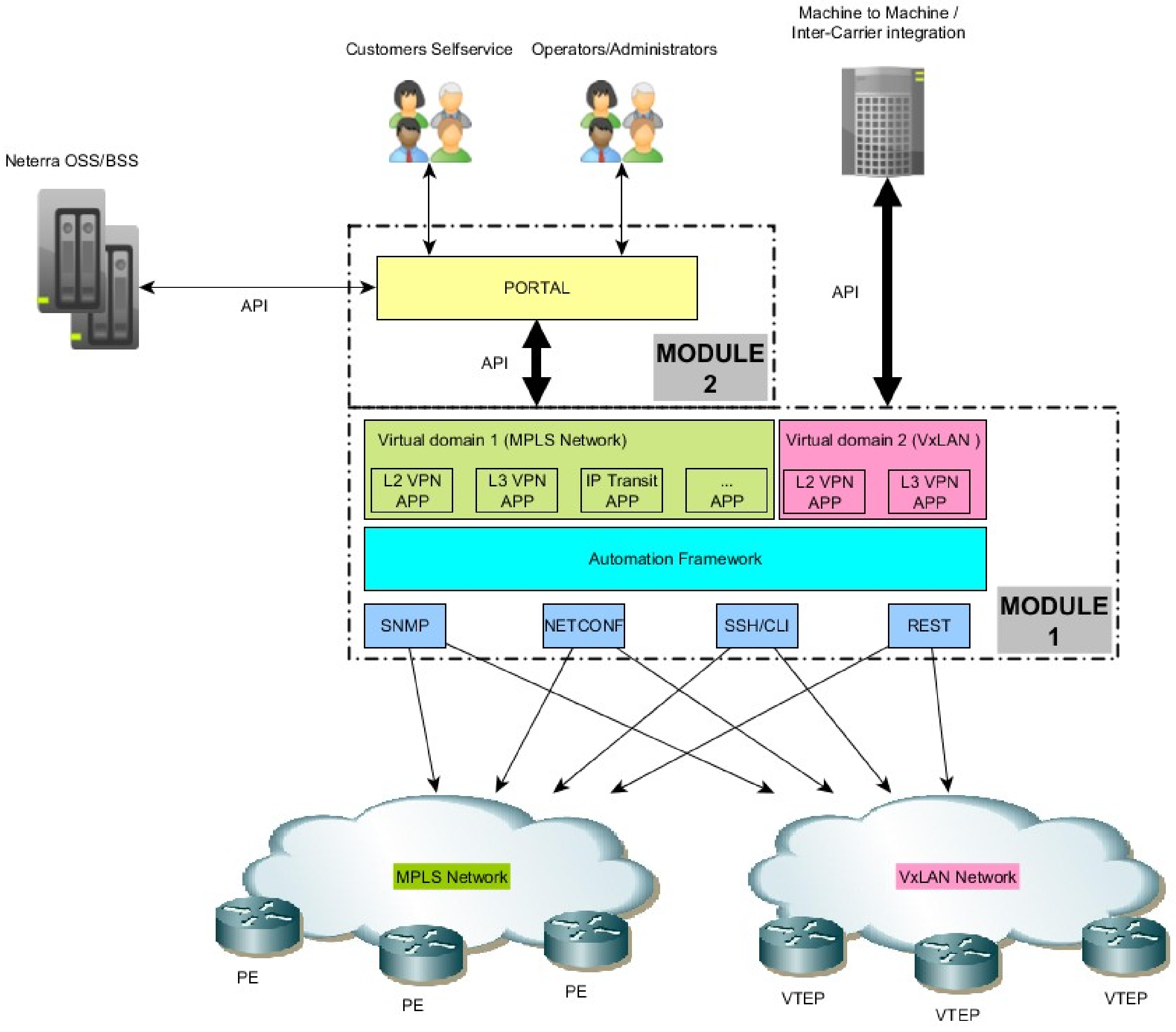
Neterra is a telco operator. We perform our operations in a complex networking environment (topologically- and technologically-wise). Still, we are a traditional player doing most of the configurational work required for delivering our services – manually, by human operators. We would like to start a migration towards a more automated and programmatic approach of provisioning of our services in the spirit of the recent SDN and NFV paradigm developments.

Our vision is to start the process of implementing the platform around a specific set of services - traditional services like L2VPNs. But the platform must be developed with modularity and seamless expansion in mind for supporting other different kind of services in the future. So we envision the project development split in the following 3 modules:

- MODULE 1 - that would cover the development of the platform CORE/FRAMEWORK and the minimum set of additional components (APPs, HW interface modules and APIs) that would allow us to automate the provisioning of L2VPN services (EPL, EVPL, E-access) in two types of underlay networks – MPLS based and VxLAN based. In this module we would also like to have BGP peering service APP developed. At this stage the platform must be capable of accepting a request for provisioning a service (via northbound API) from a simple internal administrator operated WebGUI and generate and execute the appropriate workflow over it's southbound interfaces (APIs, direct HW interfacing agents etc.) which will lead to a proper service manipulation (new deployment, change, suspend or termination).

- MODULE 2 – concerns the development of full blown web based portal to be used by the internal staff (noc, operators, administrators) as well as the end customers themselves for the purposes of self service.
- MODULE 3 – NMS integration. The orchestrated services must be properly associated with the existing (or newly developed) NMS monitoring activities and objects.

The following Is a general overview diagram, illustrating the concept:



6. Technical requirements

IMPORTANT: This is not a software development RfP. Neterra assumes the solution vendors have already a well developed products which only needs certain adaptation to the actual customer environment.

All the abstractions presented bellow in the requirements (like mentioning of “plugins”, “modules”, “software environments” etc.) are more of a “pseudo-code” examples used for better illustrating our needs. The vendor is expected to demonstrate his existing approaches serving the same purposes.

IMPORTANT: The vendors are allowed to go beyond the scope of this RfP and suggest particular networking hardware to be used by the customer if that is the only reliable way to deliver the functionality needed in the terms defined in article 7.

6.1. General requirements

6.1.1. Modular design – the platform must be built allowing standardized extension of functionality by the addition or upgrade of software modules (apps, plugins, Network HW connectors etc.). That must also increase the availability of the system as changes in given app would not affect any other.

6.1.2. Carrier grade reliability – The platform must be built using all the best practices for designing HA IT systems.

6.1.3. Multivendor environment – the platform must support or be easily and seamlessly adaptable to support systems and hardware from arbitrary vendors.

6.1.4. Multiuser operations (parallel operations) – the platform must be built in such a way allowing multiple operators, administrators and customers to interact with it and request provisioning of services. That would also mean that appropriate mechanisms for dealing with collisions and incompatible interferences must be implemented for the sake of the system stability.

6.1.5. Security

- Encrypted Communication – both user-machine and machine-machine
- extensive Authentication, Authorization and Accounting subsystem, detailed user/groups right management
- detailed event logging

6.1.6. Standards compliance - every operational aspect of the platform must be in compliance to the relevant standards (if any) or at least in compliance to the best practices and recommendations.

6.2. MODULE 1 requirements

6.2.1. Highly performing, highly reliable, highly modular and highly customizable framework to serve as a core of the platform. It is admissible the framework to be based on recognized open source solutions. The following summary metrics:

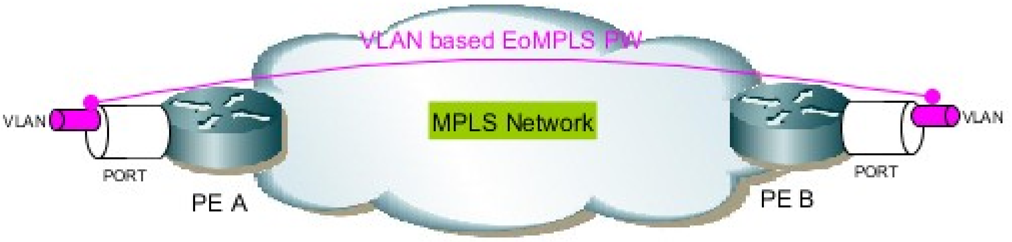
- Maximum number controlled network nodes – virtually unlimited. The system must be capable of increasing the scale of operation by simply adding new nodes (server hardware resources)
- Beginning of life network node management capacity - 1000 devices

- Maximum number of provisioned and active services - virtually unlimited. The system must be capable of increasing the scale of operation by simply adding new nodes (server hardware resources)
- Beginning of life capacity for service provisioning – 10 000 services.

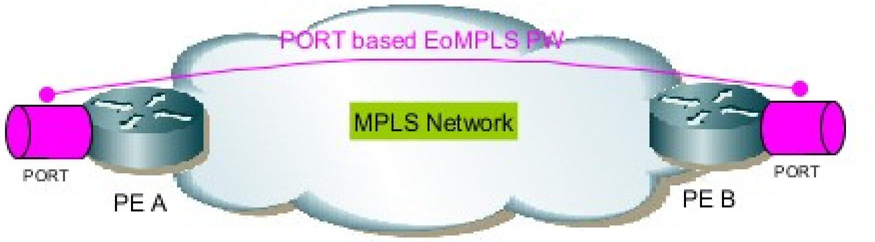
6.2.2. L2 VPN APP – The system must be equipped with application module running on top of the framework and capable of provisioning L2VPN services on networks using the following technologies - VxLAN + EVPN and MPLS/VPLS.

The immediate goal is the development of an app to be capable of provisioning the following P-t-P services:

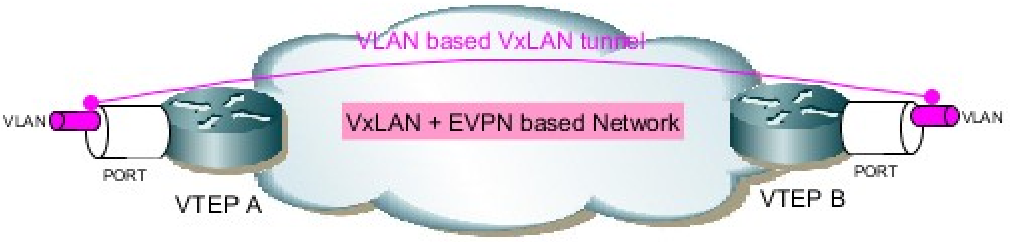
- EoMPLS (Martini/Kompella) VLAN based EVPL service



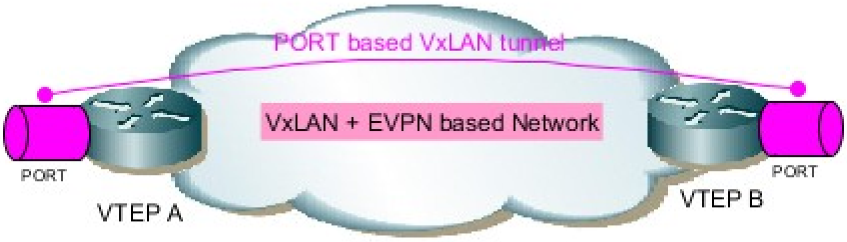
- EoMPLS (Martini/Kompella) PORT based EPL service



- VxLAN+EVPN VLAN based EVPL service



- VxLAN+EVPN PORT based EPL service



The MPLS network PE nodes comprise of the following equipment:

- HPE 5510 HI routing switches (Comware 7)
- HPE 5500 HI routing switches (Comware 5)
- HPE 5940 routing switches (Comware 7)
- HUAWEI s6720 routing switches
- CISCO Catalyst 6500 routing switches

The VxLAN+EVPN network VTEP nodes comprise of the following equipment:

- HPE 5940 routing switches (Comware 7)
- HUAWEI s6720 routing switches
- HUAWEI CE6860 routing switches

The MPLS and VxLAN networks NNI connectivity is fully configured and operational. The general idea is the platform to perform the configuration tasks ONLY on the PE and VTEP nodes terminating the service.

The platform must be capable of deploying the service based on a minimal set of input data including:

- Service type
- Virtual domain
- A-end device, port, vlan
- B-end device, port, vlan
- Bandwidth allocation
- etc.

6.2.3. BGP peering service APP - The system must be equipped with application module running on top of the framework and capable of provisioning BGP peering configurations on a BIRD BGP daemon based border routers.

The service here wold conclude in a set of configuration fragments based on a predefined templates and concerning protocols and attributes related to a customer BGP peering session.

The documentation of the BIRD software → https://bird.network.cz

An important functionality of this APP is the ability to queue, aggregate and schedule the service configuration requests, so that they do not happen asynchronously and chaotically. A configurable control of the interval of deploying the accumulated request is required.

6.2.4. Network hardware control – the system must be capable of controlling the network hardware by the means of separate software modules (agents, plugins) attached to the framework which can be further developed and expanded. Initially required are the following methods:

- SNMP
- NETCONF
- CLI (Telnet/SSH)

The southbound interface must be developed in such a way allowing also the attachment of modules providing API based communication with systems like SDN controllers, SD-WAN platforms etc.

6.2.5. Virtualization (domain virtualization, logical partitioning) – the platform must provide the means of controlling the services in multiple different networks by allocating and separating resources in different virtual domains. Thus securing isolation and allowing for the platform to be reused (by different telcos for example) and utilized efficiently.

6.2.6. Fully customizable – the system must allow the operator to define the attributes of the actual object of automation - the service. Attributes like (but not limited to):

- Object/Service ID
- Service type
- Name and description
- Virtual domain associations
- End customer associations
- OSS/BSS identifiers
- etc.

6.2.7. Service consistency by following definable and customizable Internal rules and policies – during the process of service manipulation a system of guiding rules/policies must exist under the control of the administrator. For example things like eligibility of certain devices and ports to serve as service end points must be

6.2.8. Service tracking – the system must keep record of the services configured in the network (state, history) and be able to generate reports.

6.2.9. Service sanity checking – the platform must check continuously and detect inconsistencies like changed (manually or by means other than the platform itself) or missing configurations etc. And then report appropriately.

6.2.10. Standard API - the platform must provide Restful API for it's Northbound interface allowing the system to interact with:

- Gui web portals (and hence operators and customers)
- partnering systems (machine to machine communication) for the sake of solution integration between carriers

6.2.11. Proper documentation and examples for the development of customer own apps and southbound modules/plugins.

6.3. MODULE 2 requirements

Will be discussed on a later stage based on the results of MODULE 1 proposal.

6.4. MODULE 3 requirements

Will be discussed on a later stage based on the results of MODULE 1 proposal.

7. Solution development and implementation

Neterra assumes the solution has to be custom tailored to the specific operational environment and that would require an iterative development and implementation process.

Neterra will assign a responsible engineer who will be in charge of assisting the developer.

7.1. Terms and dates

- MODULE 1 - Neterra expects the platform to be delivered in production condition **3 months** after contract signing.

8. Technical support and warranty

a) Neterra requires a three year period of advanced 24x7 technical support to be provided as warranty, after the solution is activated (ready for service). That must cover:

- Initial training for the operators and administrators
- issuing bugfixes upon request
- operational assistance
- remote access and troubleshooting
- sending support engineer on field if required on the expanse of the vendor

b) The vendor must commit to offer support services for the platform for at least 10 years after the initial contract signing.