Carrier Ethernet and IP VPNs  
with D-NFV

PoC Template #8

|  |  |
| --- | --- |
| Last Updated: | Sep 1, 2015 |
| Doc. Version: | 1.0 |
| Doc. Owner | Sarit Carmeli |

Contents

[1. Introduction 3](#_Toc429038577)

[1.1. Purpose 3](#_Toc429038578)

[1.2. Layout Overview 3](#_Toc429038579)

[1.2.1. Application Diagram 3](#_Toc429038580)

[1.2.2. Products Under Test 4](#_Toc429038581)

[1.2.3. BOM 4](#_Toc429038582)

[2. Preliminary Configuration and Management 5](#_Toc429038583)

[2.1. Preliminary Settings 5](#_Toc429038584)

[2.1.1. ETX-2 Preliminary Setting 5](#_Toc429038585)

[2.1.2. MiNID Preliminary Setting 6](#_Toc429038587)

[3. Building the RADview (Orchestrator) Map 7](#_Toc429038588)

[3.1. Add the Entities (ETXs, MiNID and Cloud) 7](#_Toc429038589)

[3.2. Creating VNF Instances and VNF Services 7](#_Toc429038590)

[3.2.1. VNF network configuration 7](#_Toc429038591)

[3.2.2. VNF Flavor Configuration 8](#_Toc429038593)

[3.2.3. VNF Image Repository Configuration 9](#_Toc429038595)

[3.2.4. Creating VNF Chaining Network: 10](#_Toc429038597)

[3.2.5. Fortigate FW Instance Configuration 12](#_Toc429038598)

[3.2.6. HPVSR Instance Configuration 12](#_Toc429038601)

[3.2.7. Fortigate Firewall Configuration: 13](#_Toc429038603)

[3.2.8. Fortigate Firewall Authentication and Registration 14](#_Toc429038606)

[3.2.9. VNF Service Configuration 14](#_Toc429038607)

[4. TWAMP Configuration and Testing 15](#_Toc429038609)

[4.1. ETX-2 and MiNID TWAMP Configuration 15](#_Toc429038610)

[4.1.1. ETX-2i D-NFV TWAMP Controller 15](#_Toc429038611)

[4.1.2. ETX-203AX TWAMP Responder 16](#_Toc429038612)

[4.1.3. MiNID-SA TWAMP Responder 18](#_Toc429038614)

[4.2. TWAMP Tests 21](#_Toc429038616)

[4.2.1. Status and Statistics 21](#_Toc429038617)

[4.2.2. L3 Service – End-to-End Traffic test 22](#_Toc429038618)

[4.2.3. Statistics Collection 23](#_Toc429038619)

[4.2.4. PM Portal 26](#_Toc429038620)

[5. ETH Service – Configuration, OAM and Y.1564 28](#_Toc429038621)

[5.1.1. Service Template and Configuration 28](#_Toc429038622)

[5.1.2. OAM Statistics 29](#_Toc429038625)

[5.1.3. L2 Service – End-to-End Traffic test 32](#_Toc429038626)

[5.1.4. Y.1564 Test 34](#_Toc429038628)

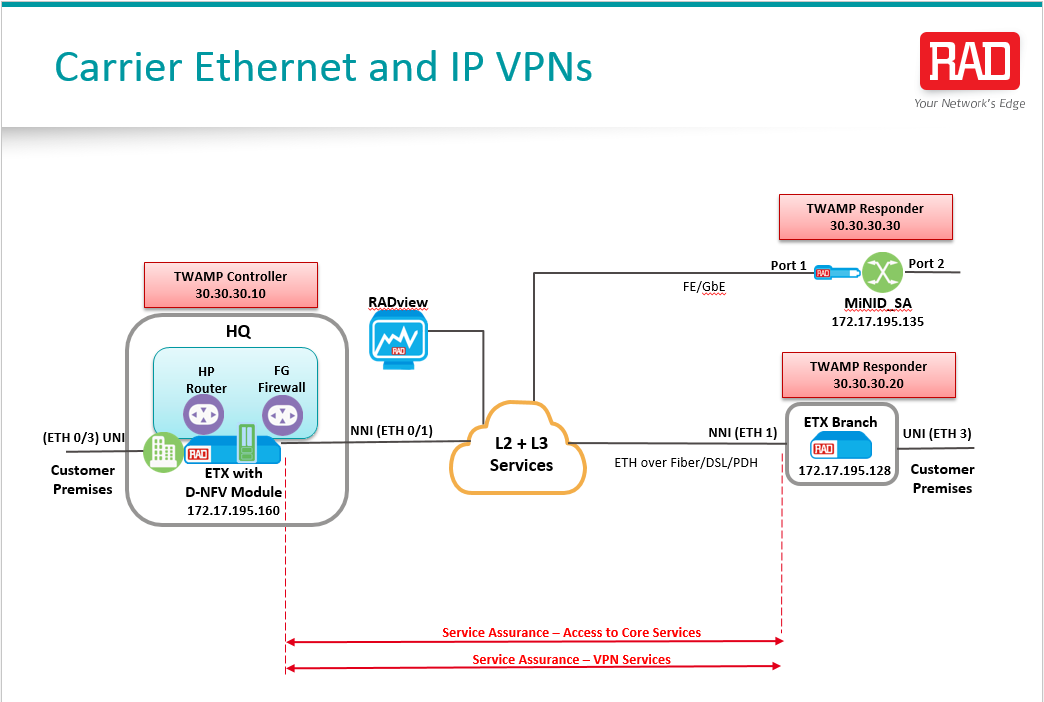
# Introduction

## Purpose

This document demonstrates the TWAMP and OAM capabilities together with L2 and D-NFV services.

## Layout Overview

### Application Diagram



### Products Under Test

|  |  |
| --- | --- |
| ETX-2i with D-NFV module  IP and Carrier Ethernet Demarcation Device with D-NFV  A next-generation hybrid L2 and L3 demarcation device for business and mobile applications. It is ideal for E-Line, E-LAN, E-Tree, and E-Access services, L3 VPNs, and value-added services using virtualization at the customer edge. The ETX-2i features an 8 Gbps forwarding engine for Carrier Ethernet and IP, with high capacity service provisioning, performance monitoring, Network Functions Virtualization (NFV), and application awareness capabilities. |  |
| ETX-203AX  Carrier Ethernet Demarcation Device  ETX-203AX delivers SLA-based Ethernet business services to the customer premises over native Ethernet access. It handles up to 5 Gbps of user traffic at wire-speed and is ideal for carriers, service providers, and wholesale operators requiring advanced Ethernet functionality at customer premises and multi-tenant units (MTUs). |  |
| MiNID  A field-programmable miniature L2/L3 network interface device (NID), available as an SFP sleeve and in a standalone enclosure. | Ethernet Demarcation SFP |

### BOM

The following tables contain the elements used in this PoC testing.

##### RAD POC Proposal BOM

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Product | Ordering Option | Description | QTY | SW Version |
| ETX-2i | ETX-2I/ACHP/19V |  | 1 | 5.9.0(0.18) |
| ETX-DNFV-M/I7/128S/8R | X86 – Compute node OS | 1 | dnfv-os\_1.1.0.007 |
| ETX-203AX | ETX-203AX\2SFP\4UTP | 6660020000 | 1 | 5.9.0(0.18) |
| MiNID | MINID/STU/GE/ACEX/CMB | 6790080000 |  | 2.1.0(0.45) |
| RADVIEW | RADview Front End GUI |  |  | Rel 5.0 (build 191) |
| Open Stack Controller |  |  | dnfv-os\_1.1.0.007-ctrl-win |
|  | RV-EMS server |  | 5.0.0(0.600) |
| RV-LIC/ENW |  |  |  |

##### Test Equipment

|  |  |  |
| --- | --- | --- |
| Function | Unit | Notes |
| ETH Generator | Spirent |  |
| Fiber Cable | SM Fiber for SFP-6 |  |
| Terminal Configuration Cable | RAD CBL-DB9-RJ45 | Supplied |

# Preliminary Configuration and Management

## Preliminary Settings

Creating the services between the different locations will be done via RADview. However there are several parameters which need to be configured via CLI before beginning to work with RADview.

Before starting to configure the ETX-2, each should be set to its default parameters.

### ETX-2 Preliminary Setting

1. Configure each ETX-2 according to the scripts in appendix A:

**Note**: Each of the scripts should be modified according to the IP address of the unit, RADview and Default Gateway.

* **ETX-2i/DNFV (HQ)** Queues and Management Configuration scripts –  
  refer to [Appendix A.1](#_B.1_ETX-205A_Tokyo)
* **ETX-203AX (Branch)** Queues and Management Configuration scripts –   
  refer to [Appendix A.2](#_B.2_ETX-203AX_New)

1. After running the scripts, verify ping replies from the management station towards each of the ETX-2 units.
2. Save the configuration for each ETX-2.
3. Login the ETX-2i and access the x86:

Configure chassis ve-module remote-terminal

User: **rad**

Password: **rad123**

**sudo –I 🡪 (pw is rad123)**

1. Use the following commands to set the IP address of the x86:

cd /home/rad

sudo -E work/scripts/mgmt/dnfv-conf.sh compute --ip=172.17.195.161 --mask=255.255.255.0 --gw=172.17.195.1 --ip-ctrl=172.17.230.138

Use this script in order to perform the operation:

dnfv-conf compute --ip=172.17.195.161 --mask=255.255.255.0 --gw=172.17.195.1 --ip-ctrl=172.17.230.138

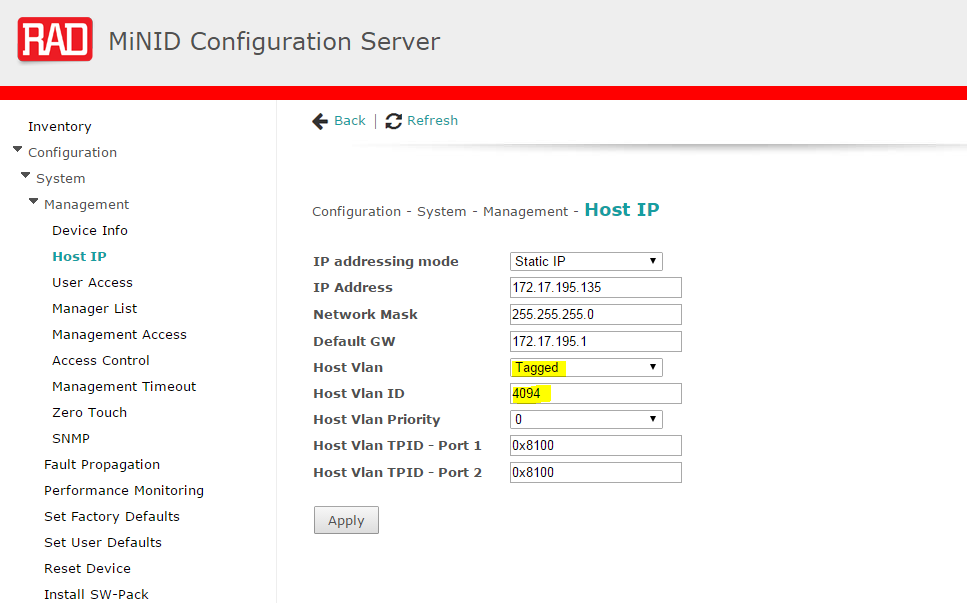
**Note**: **dnfv-conf --help** displays the full syntax of the script.

**Note:** An automatic compute node reboot will occur after the script is successfully completed.

1. Verify ping connectivity from the management station towards the x86.

### MiNID Preliminary Setting

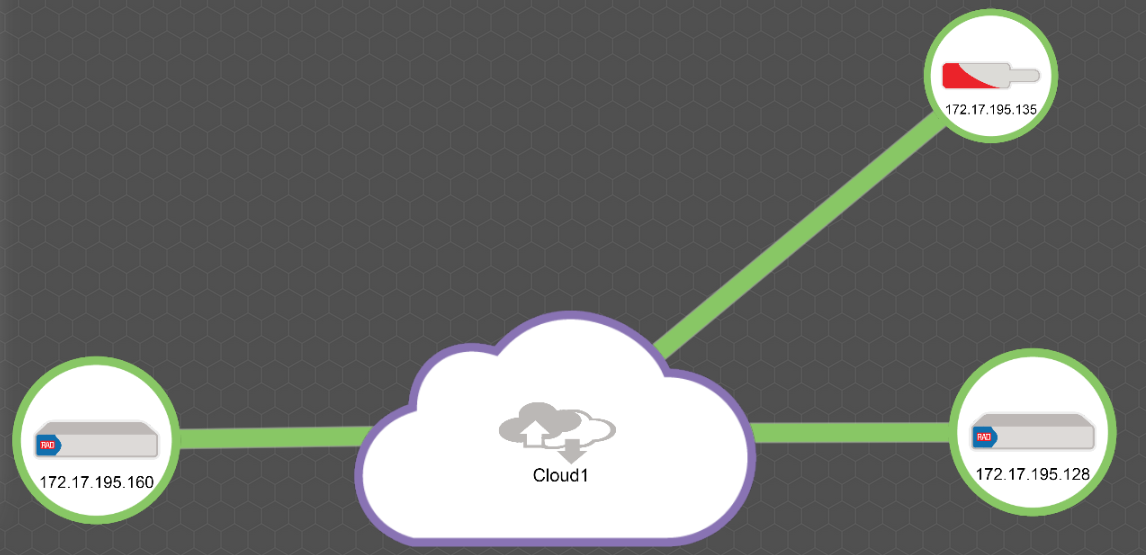
1. Enter the MiNID Web GUI (default IP 192.168.205.1), and configure the host IP parameters:



1. Verify ping connectivity from the management station towards the MiNID.

# Building the RADview (Orchestrator) Map

## Add the Entities (ETXs, MiNID and Cloud)



1. Add all entities to the RADview topology as illustrated above.
2. Verify that the color of each entity is green or orange.

|  |  |  |
| --- | --- | --- |
| NE Name | Product | IP Address (As defined under the Preliminary Setting) |
| ETX with D-NFV Module (HQ) | ETX-2i | 172.17.195.160 |
| ETX Branch | ETH-203AX | 172.17.195.128 |
| MiNID\_SA | MiNID-SA | 172.17.195.135 |

**Note**: The L2+L3 services cloud is implemented using ETX-205A, which is forwarding the correct VLANs for management and traffic as required.  
The ETX-205A has 5 ETH ports, three of which are connected to the ETXs and MiNID, and the other two connected to the LAN switch (untagged ingress).

## Creating VNF Instances and VNF Services

### VNF network configuration

VNF Networks are the logical ports within the instance, and they required in order to attach a vNIC to the VNF.

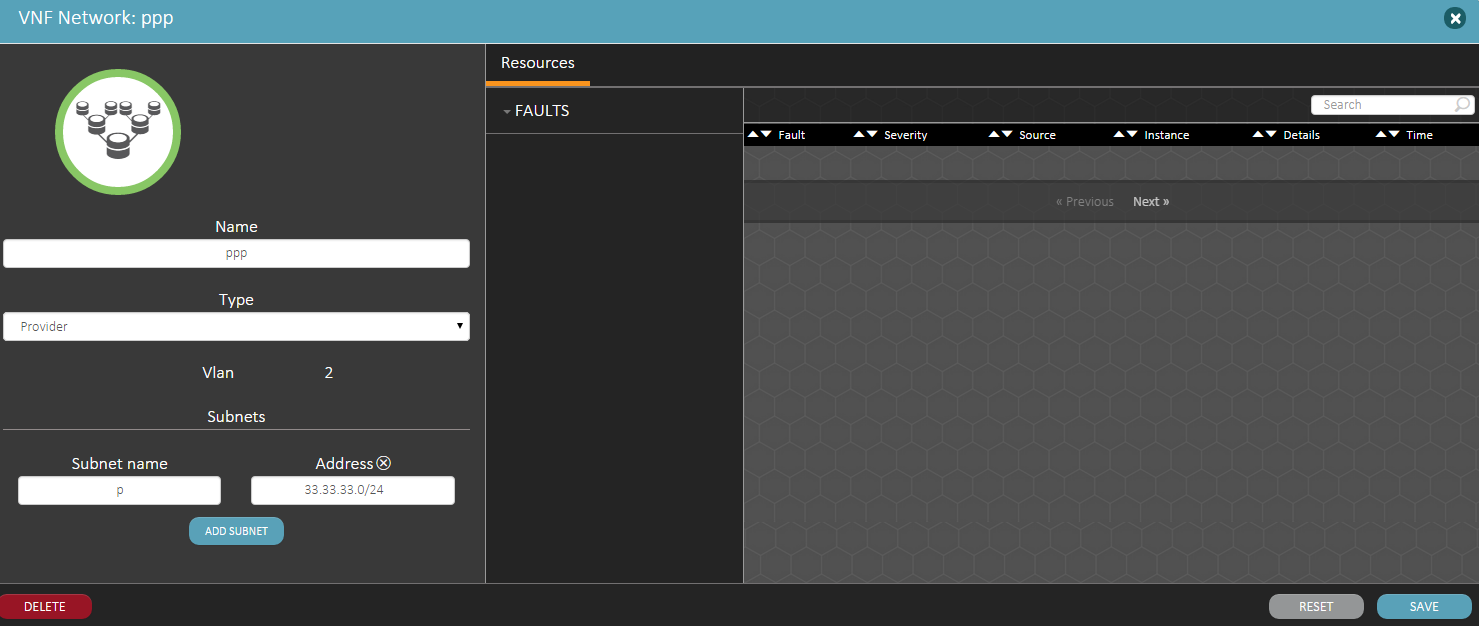
* To create new VNF Network:

1. Navigate to *Virtualization🡪 VNF Networks 🡪 Add new (+)*.  
   OR

Use the ‘create new’ drop down menu 🡪 Virtualization 🡪 VNF Network.

1. Set the mandatory parameters:

* **Name** – must be unique
* **Type**: NNI ports - Network Interface, UNI ports - User Network Interface or Management Network Ports
* **Subnet name** – must be unique
* **Address of the subnet** (subnet IP/mask) – must be valid.



The VNF network is assigned automatically to the VNF Instance, allowing the instance to connect to the user/ network side accordingly and also allow the user to manage and to configure the instance.

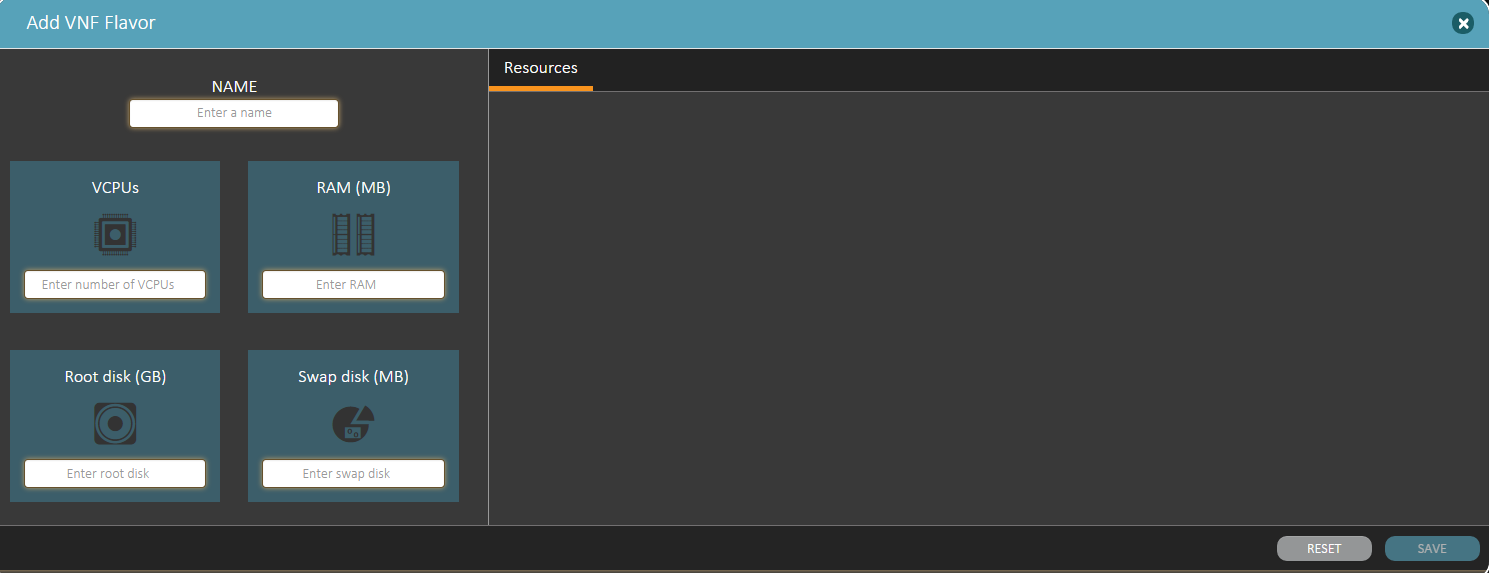
### VNF Flavor Configuration

Flavor configuration sets the resources within the x86 that will be used by the Instance. These resources will be used to hold and manage the image, all its subservices and processes that are running on the x86.

* To create a new VNF Flavor:

1. Navigate to *Virtualization🡪 VNF Flavors 🡪 Add new (+).*  
   OR

Use the ‘create new’ drop down menu 🡪 Virtualization 🡪 VNF Flavor.



1. Enter the following parameters and press on the Save button.

* Name
* VCPU-The number of CPU’s uses for the Instance
* RAM (MB)
* Root Disk- Instances Hard Disk size
* Swap Disk –Not supported yet, default value must be 0MB.

### VNF Image Repository Configuration

The following configuration creates the VNF image in the repository. At this step the minimum hardware parameters are set in addition to the format and the container for the image.

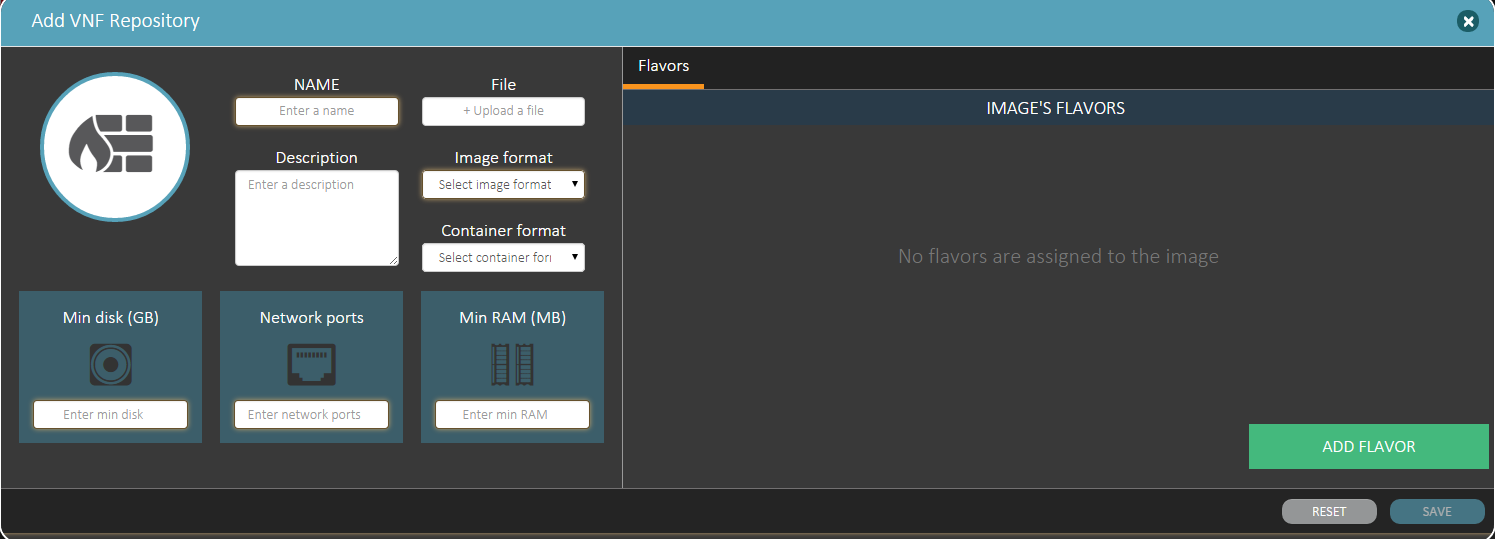
VNF Flavor/s should also be assigned to the Image.

* To create new VNF Image:

1. Navigate to the left menu Virtualization🡪 VNF Repository🡪 Add new (+).

OR

Use the ‘create new’ drop down menu 🡪 Virtualization 🡪 VNF Repository.



1. Enter the following parameters and press on the Save button:

* Name
* File- Upload the Instance image file.  
  The file contains the D-NFV application that will be loaded to the x86 processor.
* Description
* Image format - Choose image format from the drop list
* Container format - Not supported yet

1. Press the *“Add Flavor”* button – Add the instance flavor.   
   The user can assign multiple flavors to the same image, but during the instance configuration it can use only one of them.
2. Min disk, Network ports, Min RAM- these values **must be smaller than the same values configured in the assigned VNF flavors**

### Creating VNF Chaining Network:

The Orchestrator can create multiple VNF instances using the concatenated form, and then assign them VNF services. The result is a Service that contains multiple L2/L3 applications. For example:

* HPVSR + Fortigate firewall
* Fortigate + Certes vCEP

The configuration of that mode requires first to create another VNF network (the 4th network) – **chaining network**. This network will be the L3 network entity used in order to connect the VNF instances.

* To create a VNF chaining network:

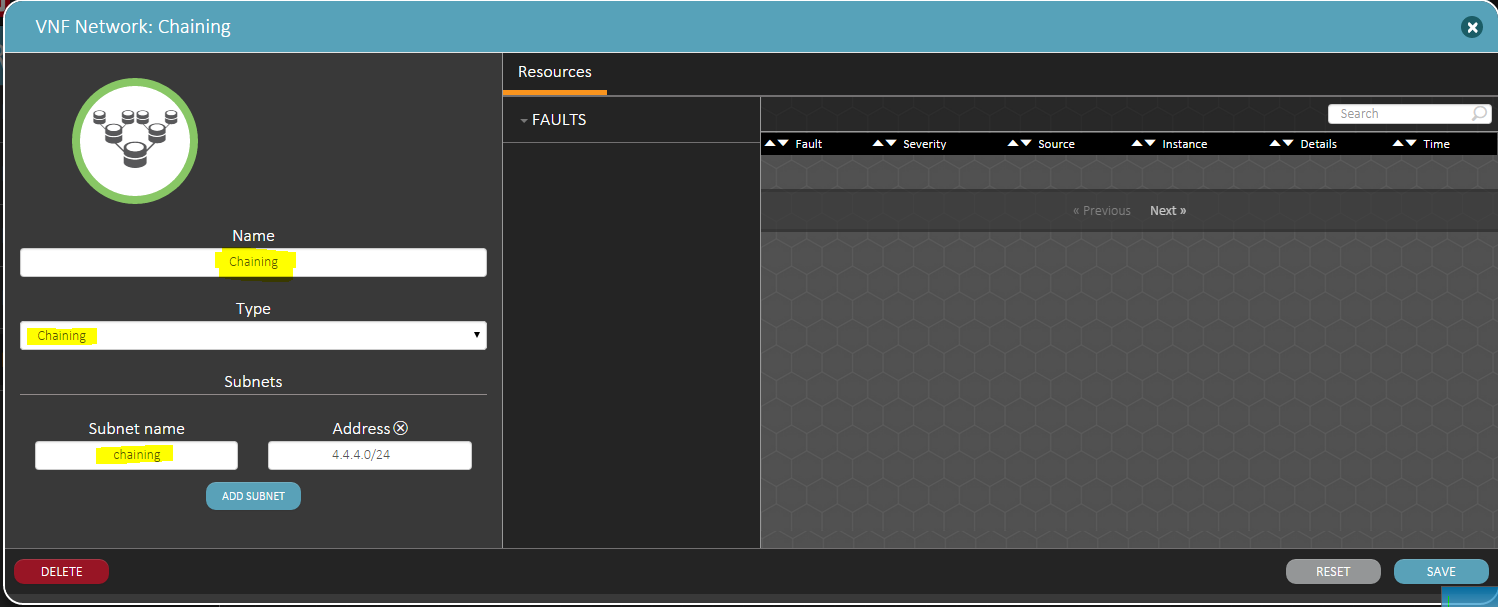
1. Navigate to Virtualization🡪VNF networks

**OR**

Use the drop down menu 🡪 Virtualization🡪VNF networks.

1. The following parameters should be set:

* **Name** – must be unique
* **Type**: use the drop down menu and select – **“Chaining”**
* **Subnet name** – must be unique
* **Address of the subnet (subnet IP/mask)** – must be valid.



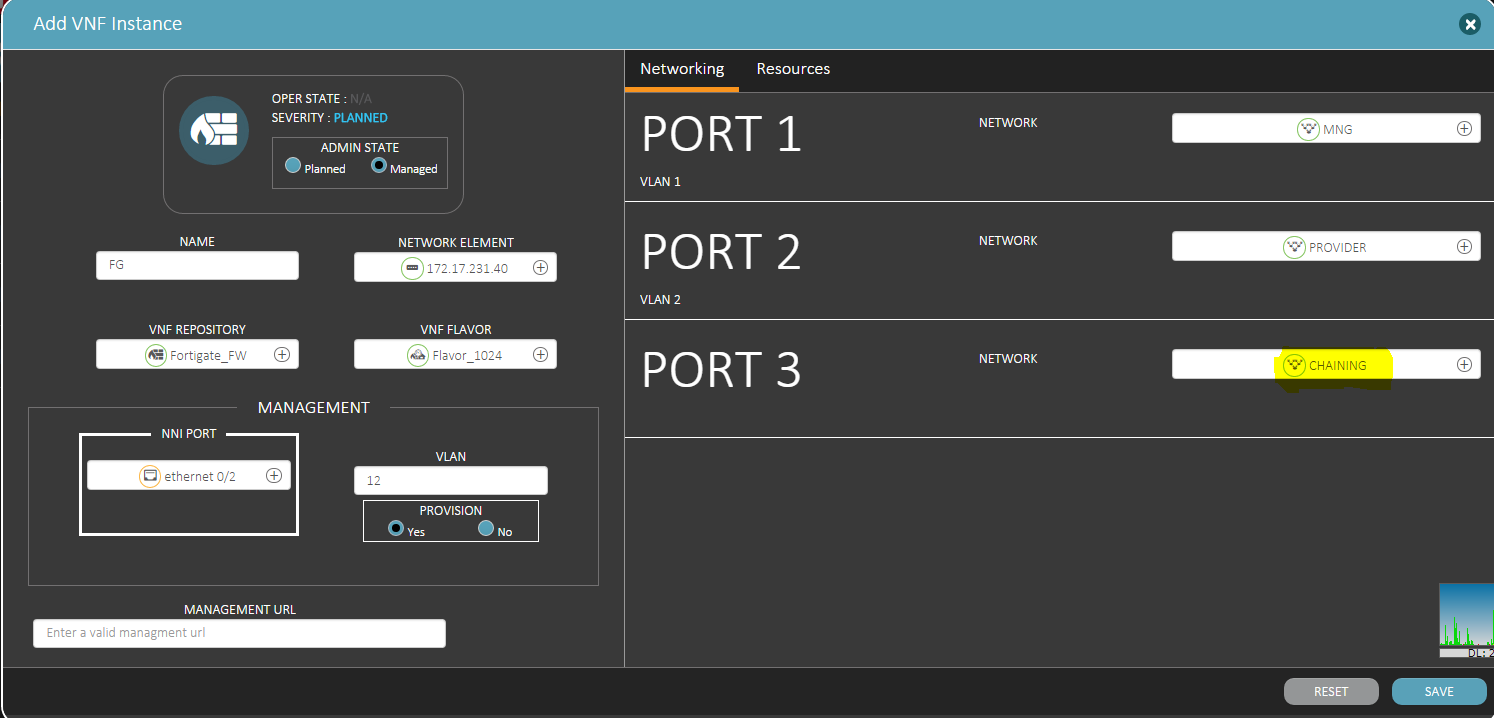
The Instance configuration depends on the network configuration and deployment method. Deploying two concatenated instances require a chaining network between them (User and Provider networks) in order to transmit/receive traffic and management network in order to manage the VNF instances.

This document describes how to configure HPVSR and Fortigate FW in a chaining mode. Similar configuration can be used in order to concatenate any other two instances.

**Notes:**

* Theoretically, concatenating three or more instances requires two or more chaining networks (for N concatenated instances, N-1 chaining networks are needed). The VNF chaining network **MUST be unique** between any two instances.

### Fortigate FW Instance Configuration

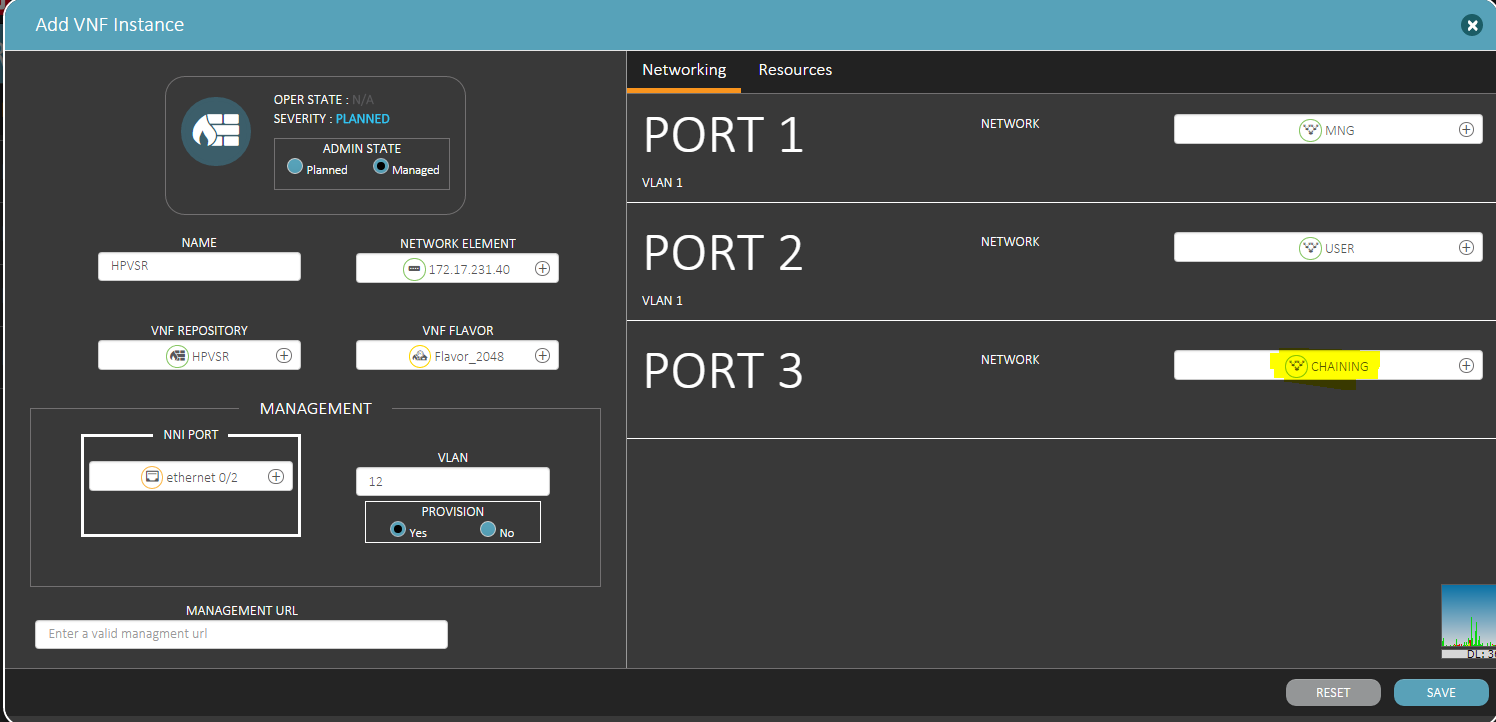


Assign the ports in the following order:

1. Port 1 to MNG network,
2. Port 2 to the user/provider network
3. Port 3 to the chaining network.

Note: This order determines the IP configuration of the VNF Instance virtual port.

### HPVSR Instance Configuration



1. Log in to the instance console, and configure the management IP parameters:

System-view  
interface gi 1/0  
ip address 172.17.195.82 255.255.255.0  
quit  
ip route-static 0.0.0.0 0.0.0.0 gi 1/0 172.17.195.1  
local-user admin  
password simple admin   
authorization-attribute user-role network-admin  
quit  
telnet server enable  
line vty 0 4   
user-role network-admin  
authentication-mode none  
quit  
user-interface vty 0 4   
quit  
save force

1. Once management configuration is ready – configure the port IPs:  
   Note that the purpose of IP route-static marked in Yellow, is to establish a IP path connection between the Instances, forwarding the packets to the User/Provider networks through the chaining network.

interface gi 2/0  
ip address 10.10.10.1 255.255.255.0   
description UNI  
quit  
interface gi 3/0  
ip address 20.20.20.1 255.255.255.0   
description Chaining  
quit  
undo ip route-static 0.0.0.0 0.0.0.0 172.17.191.1  
undo ip route-static 20.0.0.0 24 GigabitEthernet2/0 20.0.0.254  
undo ip route-static 30.0.0.0 24 GigabitEthernet3/0 30.0.0.254  
ip route-static 10.10.10.0 24 GigabitEthernet 2/0 10.10.10.1

ip route-static 20.20.20.0 24 GigabitEthernet 3/0 20.20.20.1

ip route-static 30.30.30.0 24 GigabitEthernet 3/0 20.20.20.2

quit  
save force

### Fortigate Firewall Configuration:

Note that the purpose of second static route marked in Yellow, is to establish an IP path connection between the Instances, forwarding the packets to the User/Provider networks through the chaining network.

Username: admin / {No password is required}

config system interface  
edit port1   
set mode static

set description Management   
set ip 172.17.195.XXX 255.255.255.0  
end

config system interface

edit port2   
set mode static

set description NNI  
set ip 30.30.30.1 255.255.255.0  
end

config system interface

edit port3   
set mode static

set description chaining  
set ip 20.20.20.2 255.255.255.0  
end

config router static  
edit 1   
set gateway 172.17.195.1  
set dst 0.0.0.0 0.0.0.0   
set device port1

set comment Management\_Default\_GW  
end

config router static  
edit 2   
set gateway 20.20.20.1  
set dst 10.10.10.0 255.255.255.0   
set device port3

set comment Static\_route\_to\_UNI\_network  
end

### Fortigate Firewall Authentication and Registration

1. Check the connectivity with the Fortigate firewall (ping its management IP address). If the connectivity test to the image is successful – move on to license loading. In the CLI of the image, enter:

execute update-now  
execute reboot  
y (the image will reboot itself).

1. Log in to https://{fortigate\_image\_management\_IP} (user: admin no pw needed). Load the license file and click OK.
2. Log in to the CLI and type:

execute update-now

At this point the image is communicating with Fortinet servers and authenticating using the serial number and license parameters.

1. Wait for the CLI message: \*ATTENTION\* Admin sessions removed because license registration status changed to “VALID”.
2. Log in to https://{fortigate\_image\_management\_IP} and open the web GUI to the firewall.

### VNF Service Configuration

1. Configure the VNF service and add the two instances to it in a chaining mode, where the HPVSR is connected to the UNI side, and the Fortigate firewall connected to the NNI side.
2. Use VLAN 100 as the classifier to that service in the user side, Swapped by VLAN 1010.



# TWAMP Configuration and Testing

## ETX-2 and MiNID TWAMP Configuration

### ETX-2i D-NFV TWAMP Controller

1. Configure the ETX-2i as TWAMP controller as follows:

######## Enabling the TWAMP Configuration ####################

exit all

admin license  
license-enable twamp  
exit all

######## TWAMP svi and interface Configuration ####################

configure port

svi 2 twamp

no shutdown

exit

exit all

configure router 1

interface 2

address 30.30.30.10/24

bind svi 2

management-access allow-ping

dhcp-client

client-id mac

exit

no shutdown

exit

exit all

######## pm-collection Reporting configuration ######

Configure reporting

pm-collection twamp interval 60

exit

exit all

###### TWAMP controller and OAM configuration ########

configure oam

##### Configure TWAMP

twamp

##### TWAMP - Profile Configuration

profile "1" 1

transmit-rate 1

exit

##### TWAMP - Controller Configuration

controller "1" 1 light l2-probe

bind ethernet 0/1

vlan-tag vlan 1010

router-entity 1

local-ip-address 30.30.30.10

no shutdown

##### TWAMP - Controller Peer Configuration

peer 30.30.30.20

test-session 1 name "1" udp-port 500 test-profile "1" dscp 21

activate continuous

exit

peer 30.30.30.30

test-session 2 name "2" udp-port 600 test-profile "1" dscp 21

activate continuous

exit

exit

exit all

1. Save the configuration

### ETX-203AX TWAMP Responder

1. Configure the ETX-203AX as TWAMP responder as follows:

######## Enabling the TWAMP Configuration ####################

exit all

admin license  
license-enable twamp  
exit all

save

######## SVI Port Configuration ####################

configure port

svi 2 twamp

no shutdown

exit

exit all

####### Classifier Profile Configuration ##########

configure flows

classifier-profile "vlan\_1010" match-any

match vlan 1010

exit

classifier-profile "vlan\_100" match-any

match vlan 100

exit

####### DATA + TWAMP Flows ##########

flow "3\_to\_1"

classifier "vlan\_100"

policer profile "Policer1"

mark all

vlan 1010

exit

ingress-port ethernet 3

egress-port ethernet 1 queue 0 block 0/1

no shutdown

exit

flow "1\_to\_3"

classifier "vlan\_1010"

policer profile "Policer1"

mark all

vlan 100

exit

ingress-port ethernet 1

egress-port ethernet 3 queue 0 block 0/1

no shutdown

exit

exit all

####### Router Interface Configuration ##########

configure router 1

# interface 2 for TWAMP

interface 2

address 30.30.30.20/24

name TWAMP\_Interface

bind svi 2

dhcp-client

client-id mac

exit

no shutdown

exit

static-route 0.0.0.0/0 address 172.17.195.1 metric 1

exit all

####### TWAMP - Responder Configuration #######

configure oam twamp

responder "1" 1 light l2-probe

bind ethernet 1

vlan-tag vlan 1010

router-entity 1

local-ip-address 30.30.30.20

test-session 1 name "1" udp-port 500

no shutdown

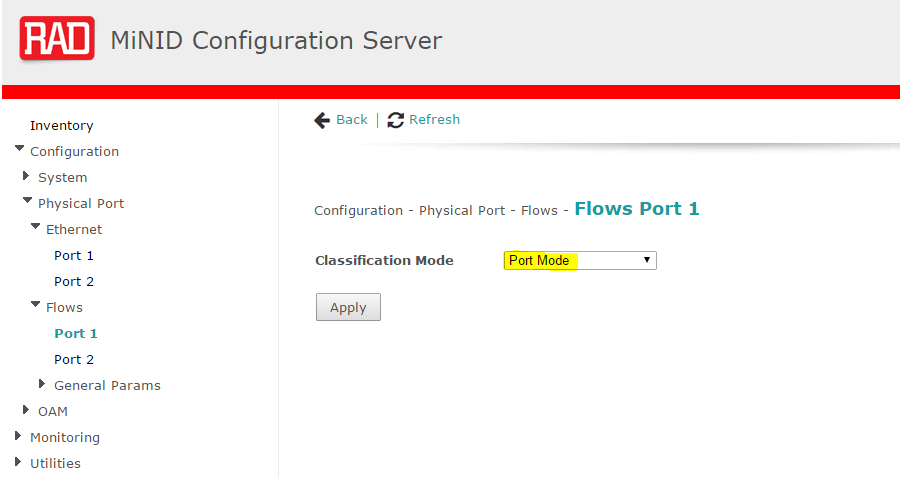
exit

exit all

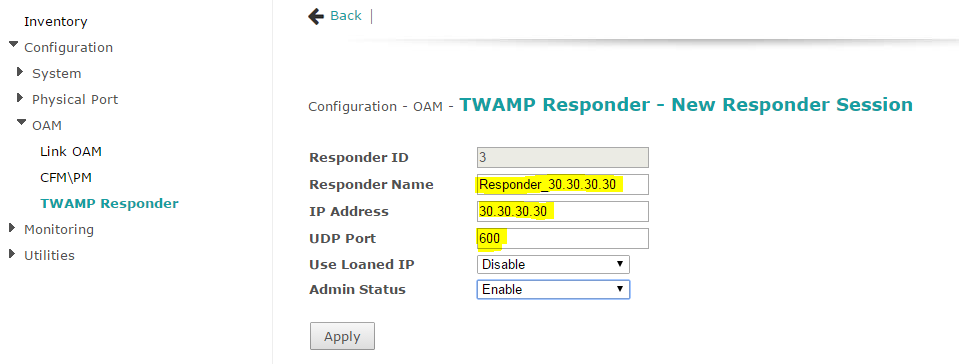
1. Save the configuration

### MiNID-SA TWAMP Responder

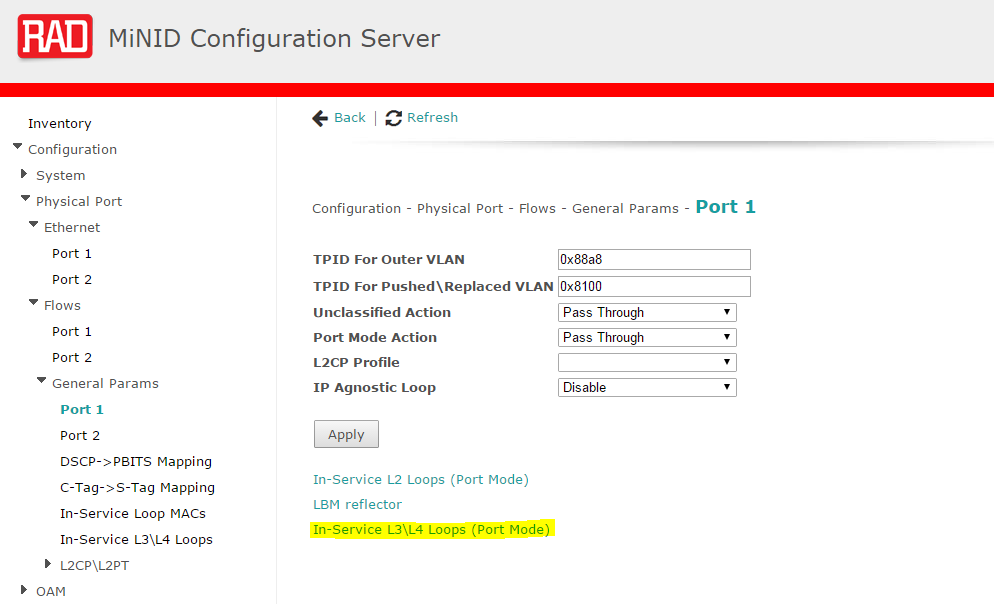
1. Enter the MiNID web GUI.
2. Navigate to *configuration>Physical port>flows>flows port 1*, and change the classification mode to **port mode.**



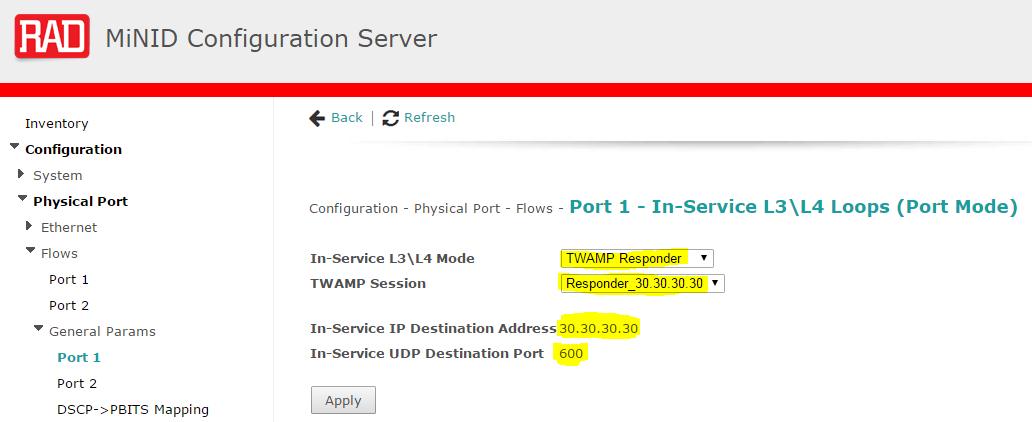
1. Navigate to *Configuration>oam>TWAMP responder* and add new TWAMP responder:



1. Navigate to *Configuration>Physical Port>Flows>General Params>Port 1*  
   and click on “In-service L3/L4 Loops (port mode)”



1. Enable the responder in the Loop and assign the configured TWAMP responder from previous step:



* Ngf
* Nf
* Ngf
* Ngfn
* f

## TWAMP Tests

### Status and Statistics

1. Access the **ETX-2i** (TWAMP *controller*) and verify the status of each of the TWAMP peers is *“In Progress”* and the Tx Packets are equal to the Rx Packets:

configure oam twamp controller 1 1 light l2-probe

peer 30.30.30.20

show status

IPPM Type : TWAMP Light

Activation Mode : Continuous

Calculation Mode : round-trip

Start Time : 1970-01-01 06:28:48

Controller Test Name Peer UDP Status Tx Packets Rx Packets

-----------------------------------------------------------------------------

1 500 In Progress 277 277

configure oam twamp controller 1 1 light l2-probe

peer 30.30.30.30

show status

IPPM Type : TWAMP Light

Activation Mode : Continuous

Calculation Mode : round-trip

Start Time : 1970-01-01 06:55:36

Controller Test Name Peer UDP Status Tx Packets Rx Packets

-----------------------------------------------------------------------------

2 600 In Progress 194 194

1. Access the **ETX-203AX**(TWAMP *responder*) and verify the status of the TWAMP peer is *“Ready”* and the Tx Packets are equal to the Rx Packets. Check also the TWAMP report.

configure oam twamp responder 1 1 light

show status

PPM Type : TWAMP Light

Router Entity : 1

Router Interface : 2

Router Interface oper status : UP

Responder Status : Ready

Responder Test Name UDP Port Tx Packets Rx Packets

-----------------------------------------------------------------------------

1 500 8651 8651

configure oam twamp

controller 1 1 light l2-probe

peer 30.30.30.20

show report 1 current

Test Name : 1

IPPM Type : TWAMP Light

Controller IP Address : 30.30.30.10 / 59667

Responder IP Address : 30.30.30.20 / 500

IP DSCP : 21

Payload Length (bytes) : 256

Calculation Mode : round-trip

Start Time : 1970-01-01 06:28:48

Test Interval : Current

Time Stamp : 1970-01-02 00:00:00

Elapsed Time (sec): 240

Tx Packets : 240

Loss Packets : 0

Loss Ratio : 0

Availability Count (sec): 240

Duplicate Packets Fwd / Back : 0 0

Duplicate Ratio Fwd / Back : 0 0

Reordered Packets Fwd / Back : 0 0

Reordered Ratio Fwd / Back : 0 0

Fragmented Packets Fwd / Back : 0 0

Delay Threshold Crossing Count : 0

Delay Min / Max / Average (ms) : 0.098 0.119 0.101

PDV Max / Average (ms) : 0.021 0.003

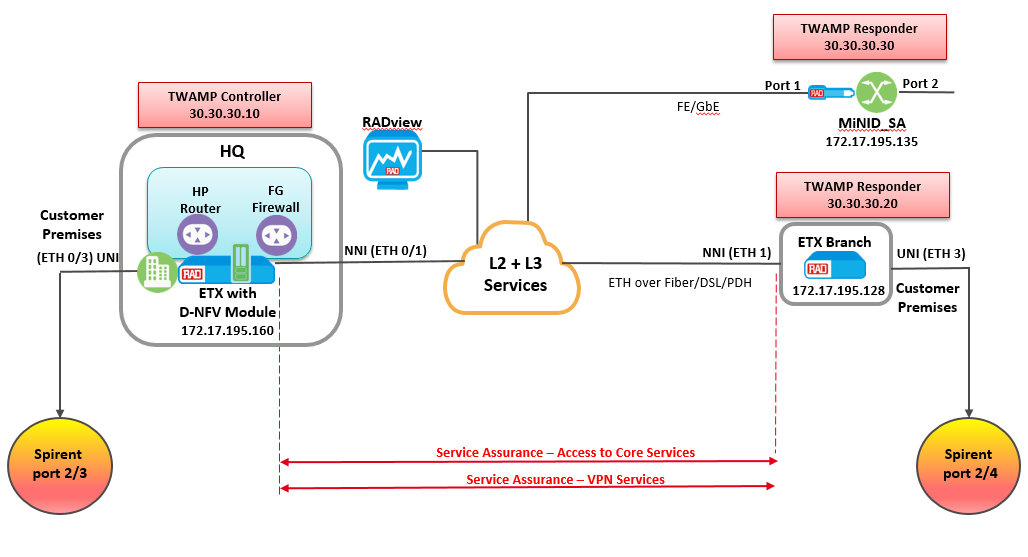
IPDV Max / Average (ms) : 0.020 0.001

IPDV-Fwd Max / Average (ms) : 0.024 0.005

IPDV-Back Max / Average (ms) : 0.022 0.005

### L3 Service – End-to-End Traffic test

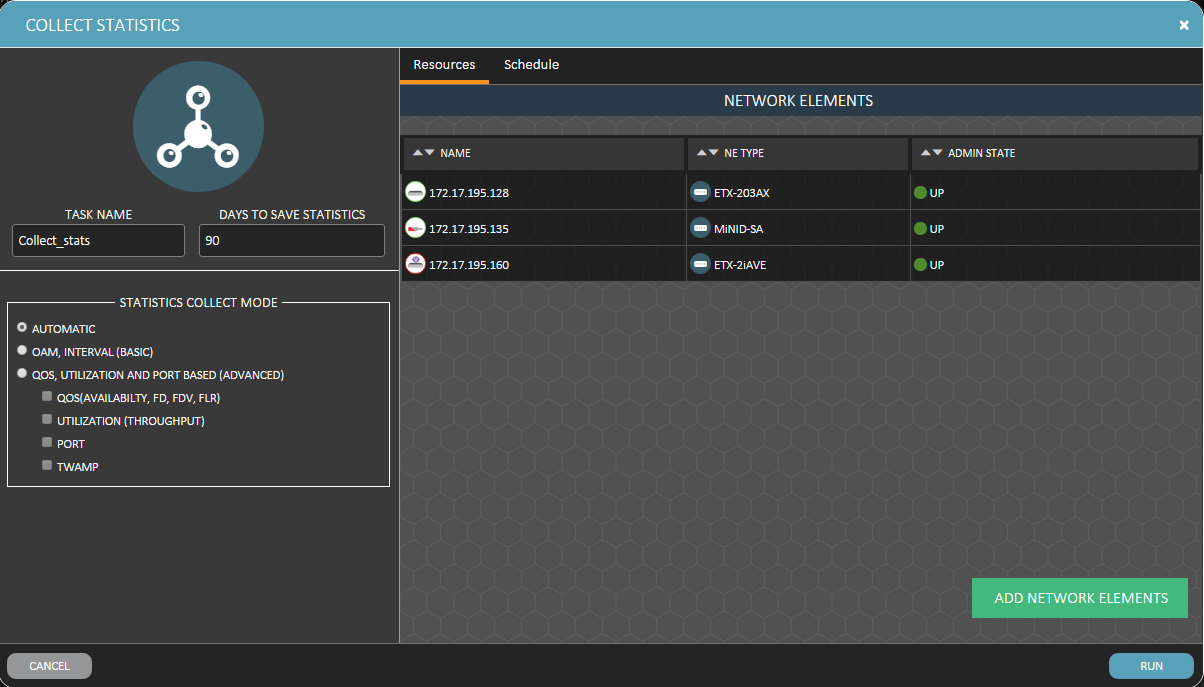
1. Connect an ETH generator to the ETX-2i and the ETX-203AX:



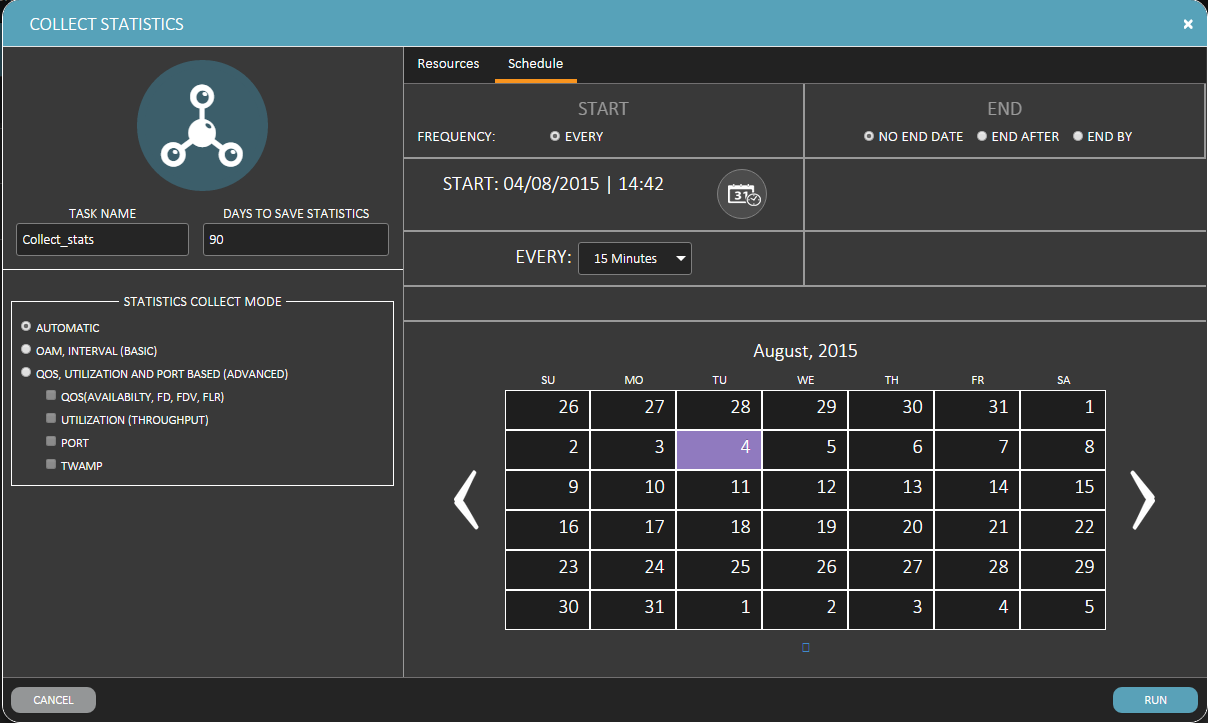
1. Configure the ETH generator to transmit L3 traffic End-to-End and verify traffic transmit and receive accordingly (verify ARP connectivity before start generating traffic).

### Statistics Collection

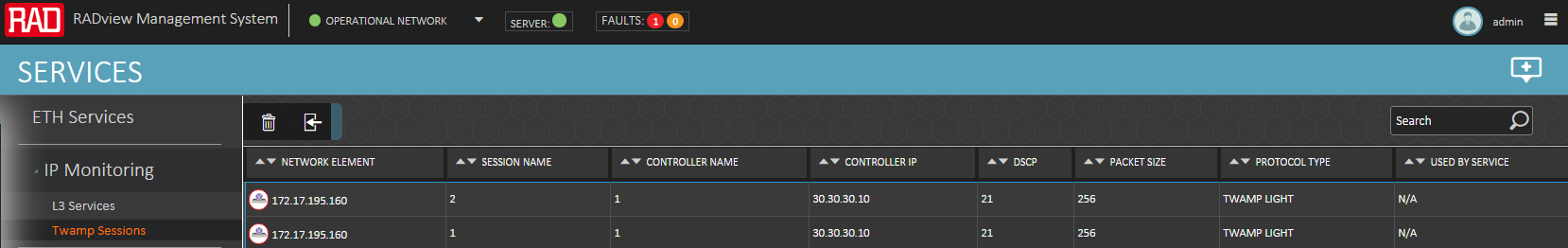
1. At the Collect Statistics menu in RADview, start task to collect statistics and add the required NEs (ETX-2i, ETX-203AX and MiNID).



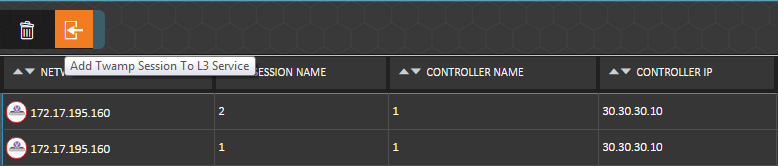
1. Under the “Schedule” tab set the task to run every 15 minutes:



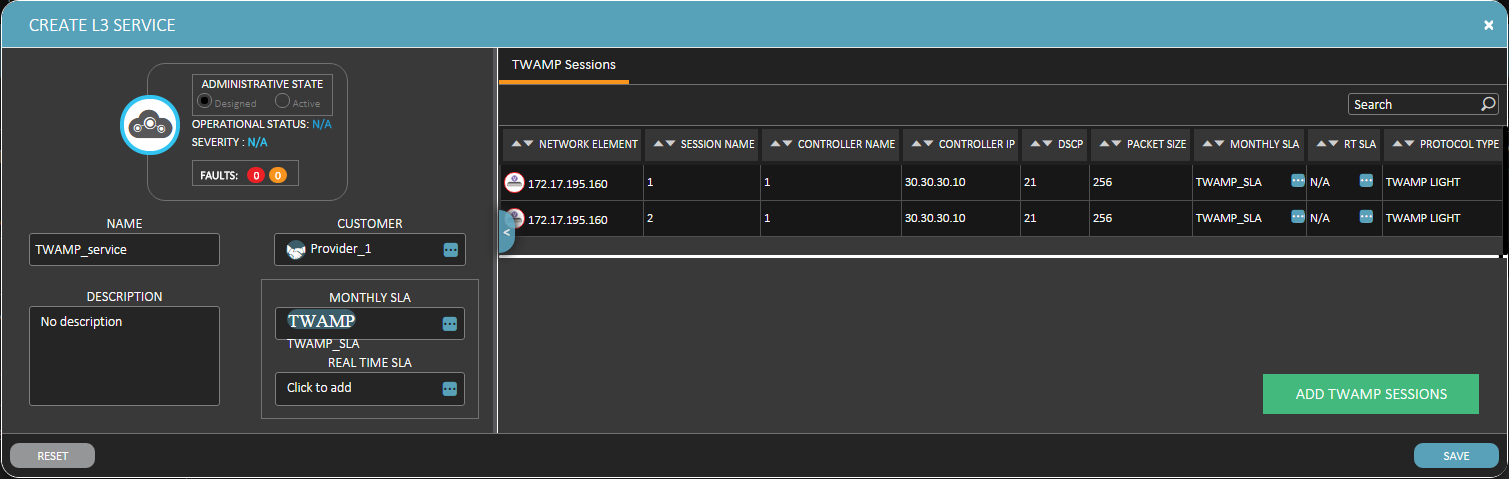
1. Once the first task is completed, you can see the TWAMP session was collected from the controller:



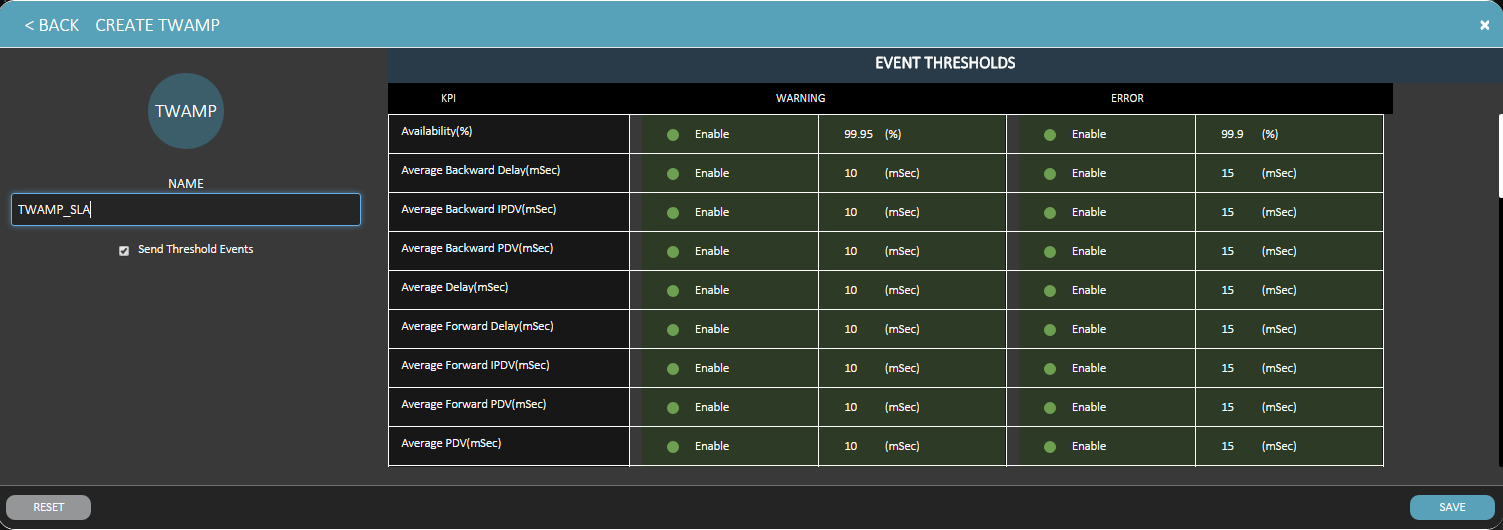
1. Mark the required sessions and click on “Add TWAMP session To L3 Service”:



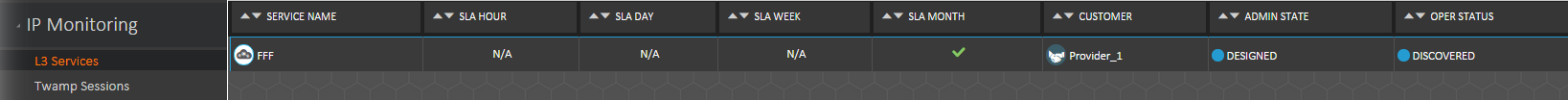
1. Configure the L3 TWAMP service and assign the monthly/real-time SLA:



1. Configure the TWAMP\_SLA and set all measurement parmeters as required:



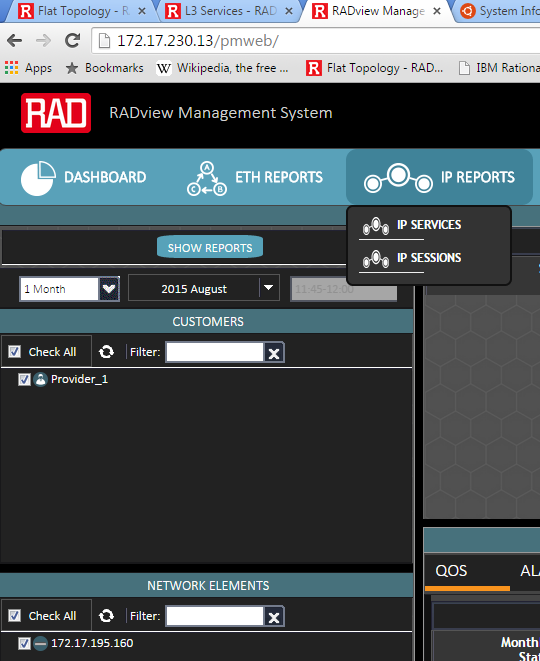
1. Save and verify it was added successfully to the L3 service list:



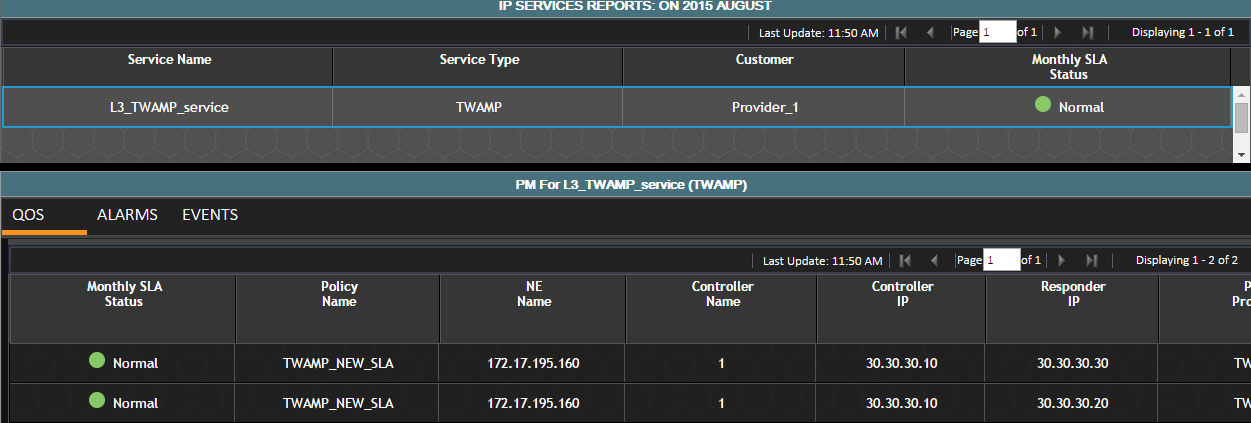
### PM Portal

All TWAMP statistics can be collected using the PM Portal:

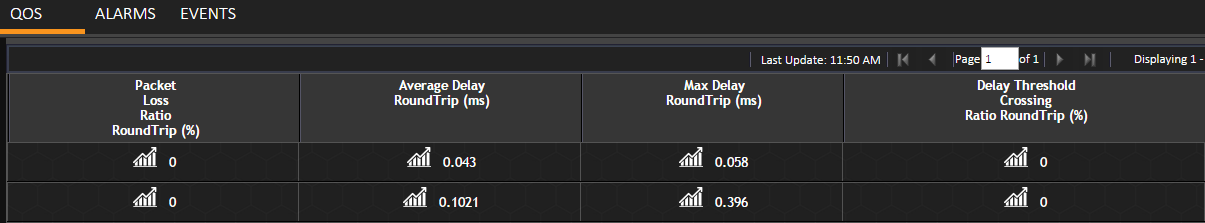
1. Under the Web browser type the IP address of the RV server.
2. PM portal login page will be opened – user/password: root/root.
3. Go to *IP Reports>IP services*, select the required costumer and the NE you would like to monitor and click the *“SHOW REPORTS”* button.



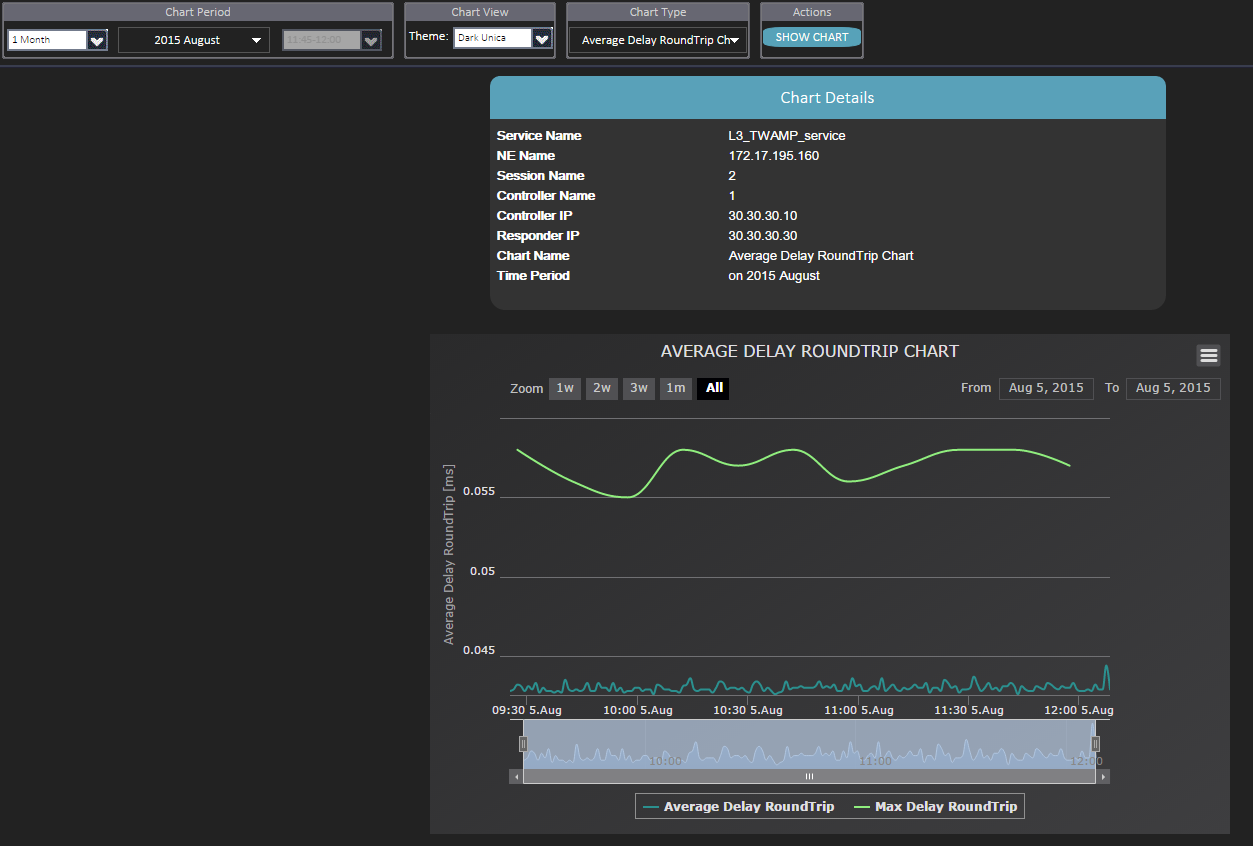
1. IP services reports and PM table with all measured parameters of the session will be displayed at the right side of the PM portal screen:



1. Obtain the parameters in the table by scrolling the bottom bar to the right



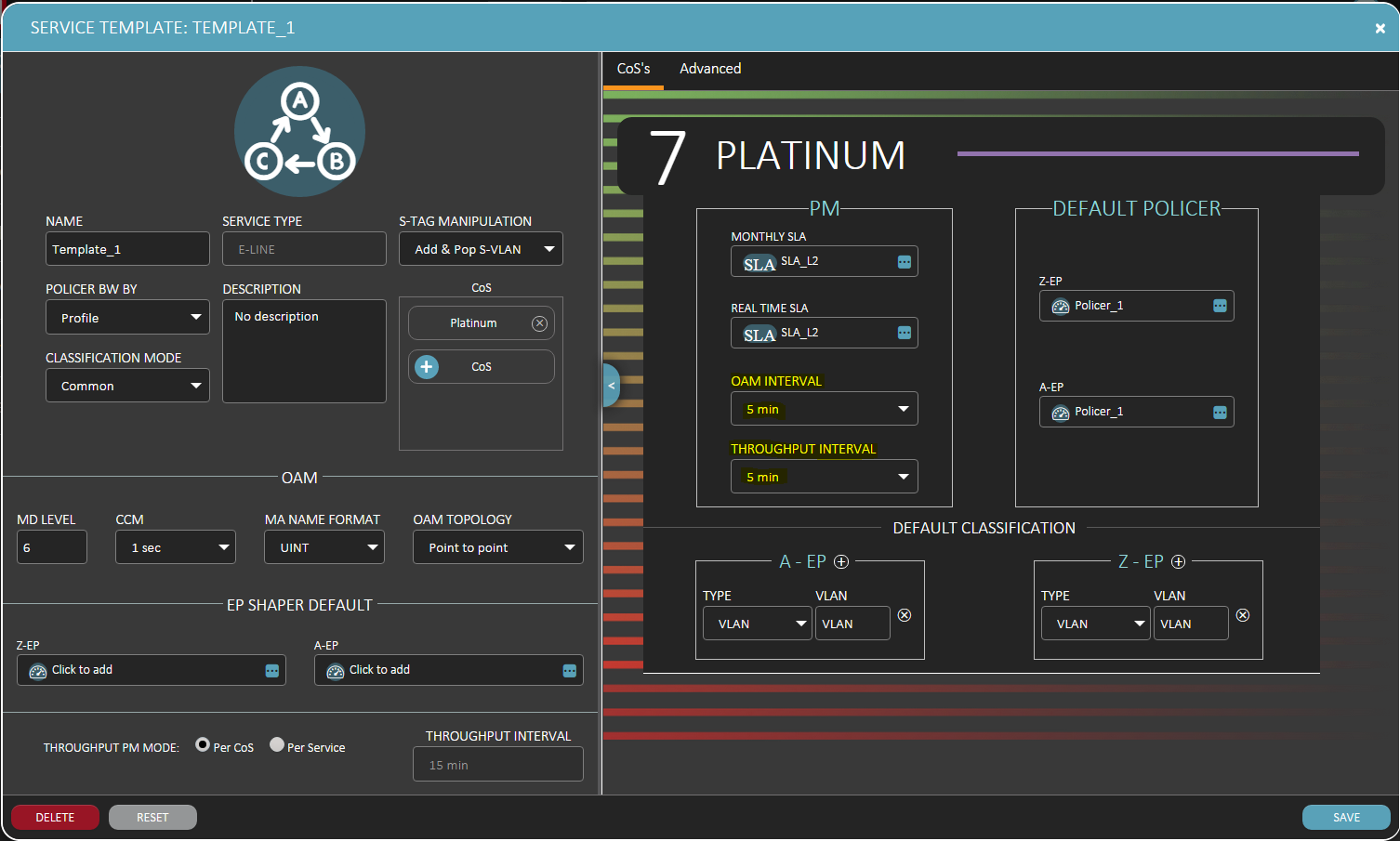
1. Click on the graph icon ( ) to open a new browser and display the measured parameter in a graphical form:



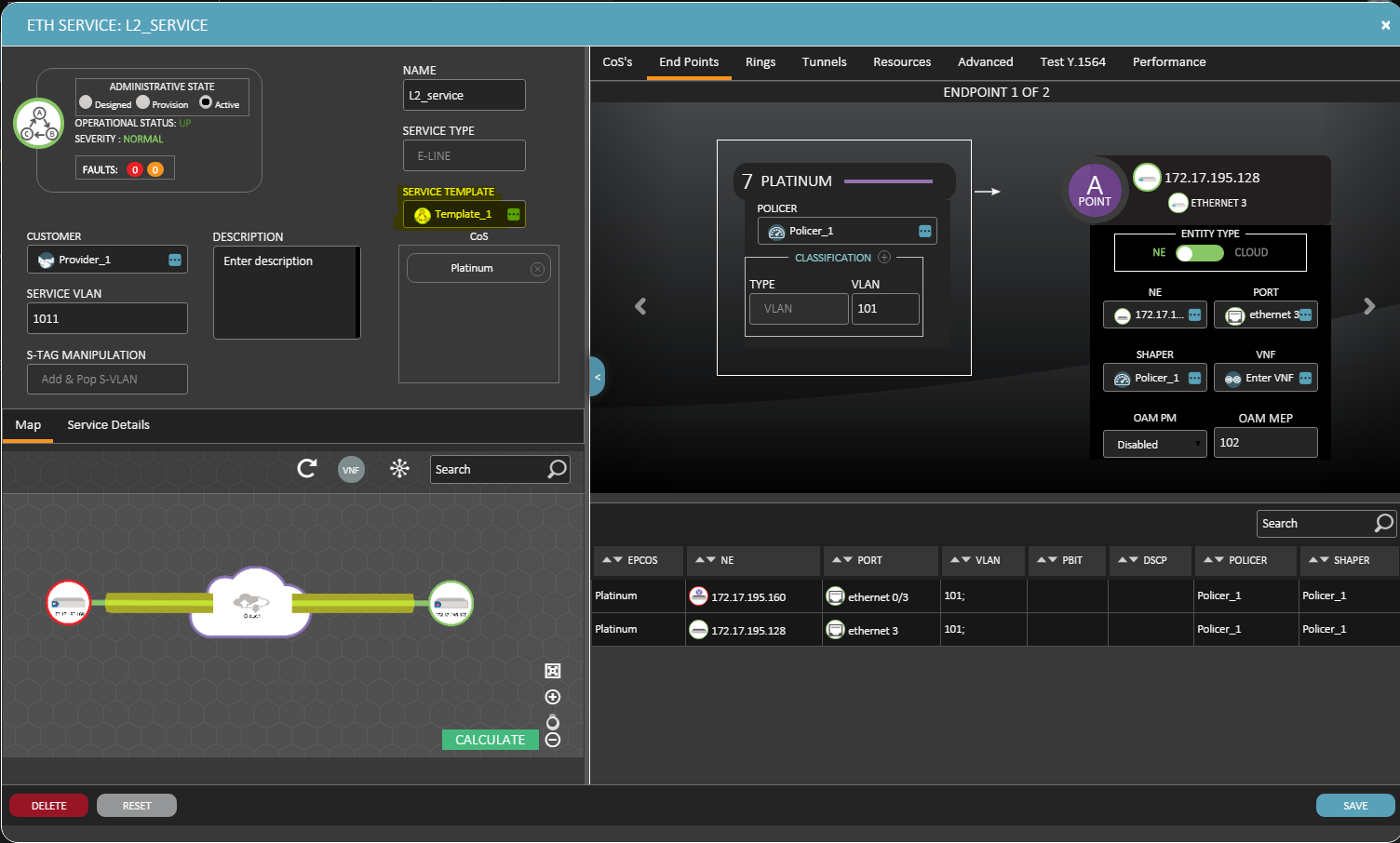
# ETH Service – Configuration, OAM and Y.1564

### Service Template and Configuration

1. Configure the service template, and enable the OAM Parameters:



1. Create a new service between ETX-2i ETH Port 0/3 and ETX-203AX ETH Port 3:



### OAM Statistics

1. Login both ETX-2 via cli and verify the Remote MEP and Remote MAC presented properly and the OAM status is *“OK”*:

Configure>oam>cfm>maintenance-domain 1>maintenance-association 1>mep 101>show status

Ingress Port : Ethernet 0/1

Direction : Down

Classification Profile : S.40.1\_L2\_service\_1

CCM Priority : 7

MD Name :

MA Name : 1011

Administrative Status : Up

Test Status : Off

MEP Defect : Status

Rx LCK : Off

Rx AIS : Off

Cross Connected CCM (Mismatch; Unexpected MD Level) : Off

Invalid CCM (Unexpected MEP; Unexpected CCM Period) : Off

Remote MEP Remote MEP Address Operational Status

-----------------------------------------------------------------------------

102 00-20-D2-53-E9-DC OK

1. Check the OAM Statistics:

Configure>oam>cfm>maintenance-domain 1>maintenance-association 1>mep 101>service 1>dest-ne 1>show statistics running

Running Counters

-----------------------------------------------------------------------------

Forward Backward

Tx Frames : 479499 479343

Rx Frames : 479499 479343

Frames Loss : 0 0

Unavailable Seconds : 0 0

Available Seconds : 385 385

Two Way Delay (mSec) : 0.021

Two Way IFDV (mSec) : 0.000

Current Forward IFDV (mSec) : 0.000

Current Backward IFDV (mSec) : 0.000

Frames Above Delay Threshold : 0

Frames Above IFDV Threshold : 0Elapsed Time (sec) : 385

Loss and Delay Measurements Messages

-----------------------------------------------------------------------------

Tx Rx

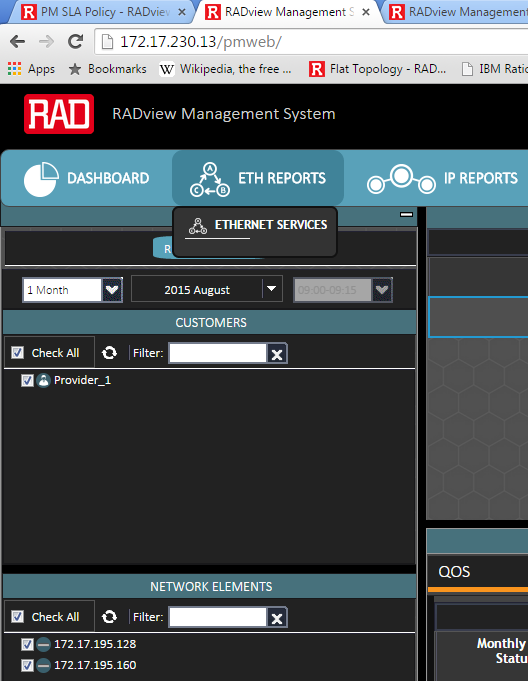
LMMs : 386 LMRs : 386

DMMs : 386 DMRs : 386Traffic Test

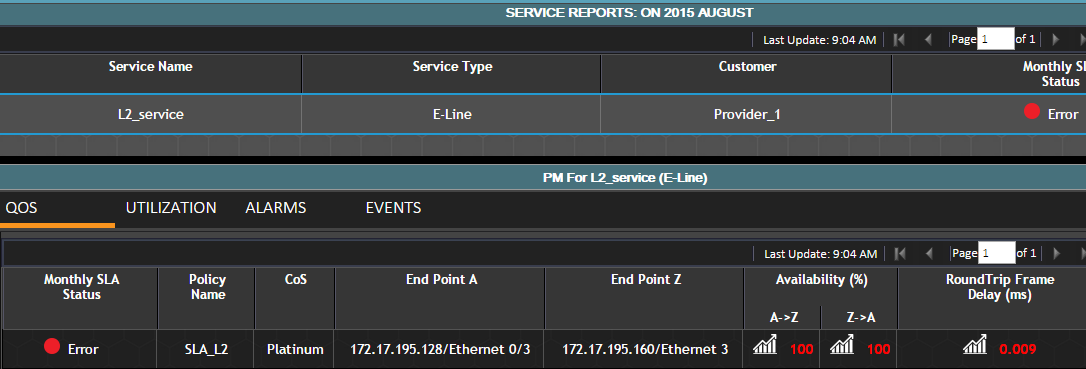
1. Open a web browser, type the IP address of the RV server and click Enter.

PM portal login page will be opened – user password is root/root.

1. Go to *ETH Reports>Ethernet Services*, select the required costumer name and the specific NE to monitor and click on the *“Show Reports”* button:



1. ETH services reports and PM table with all measured parameters from the service will be displayed at the right side of the PM portal screen:

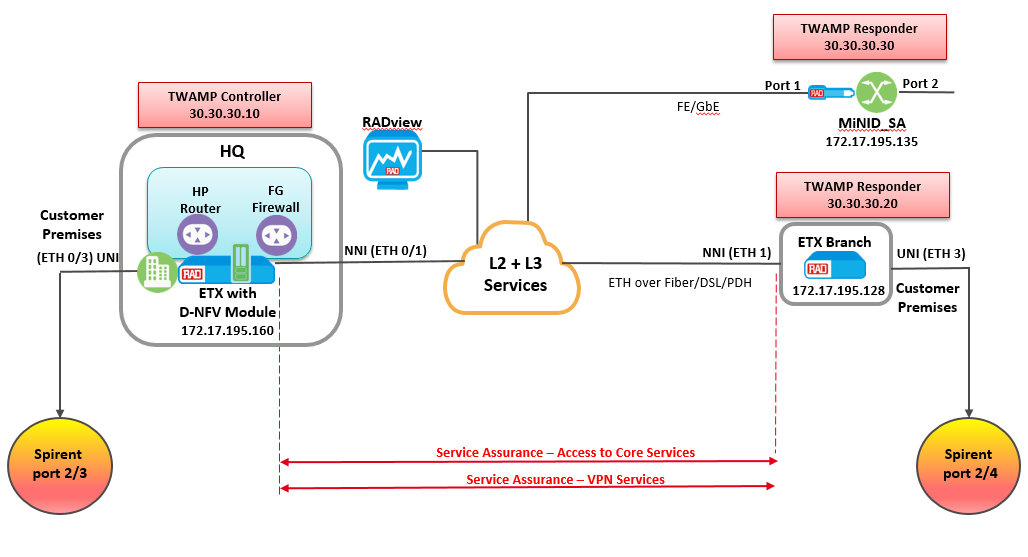


1. Click the graph icon ( ) to open a new browser and display the measured parameter in a graphical form:

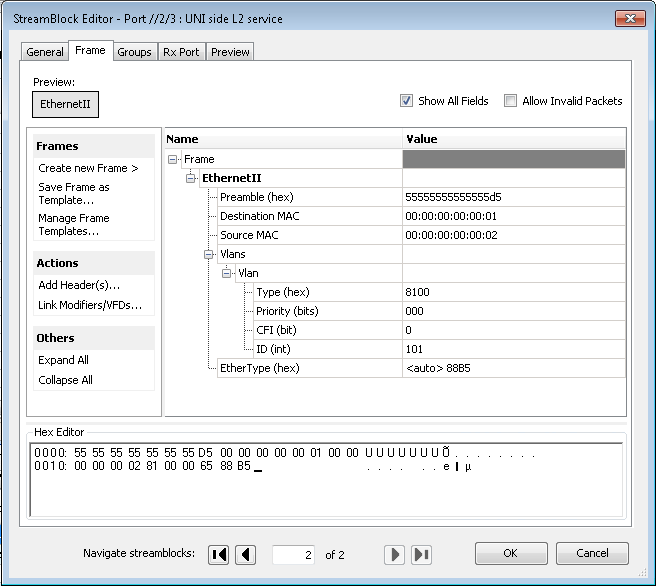


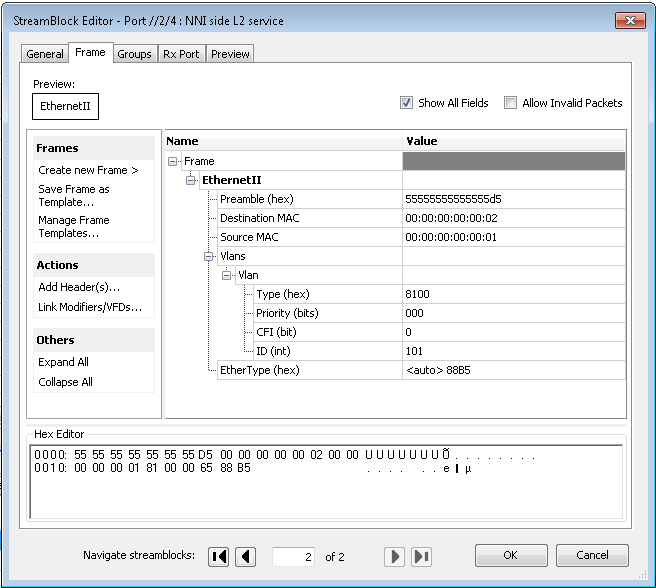
### L2 Service – End-to-End Traffic test

1. Connect an ETH generator to the ETX-2i and the ETX-203AX:



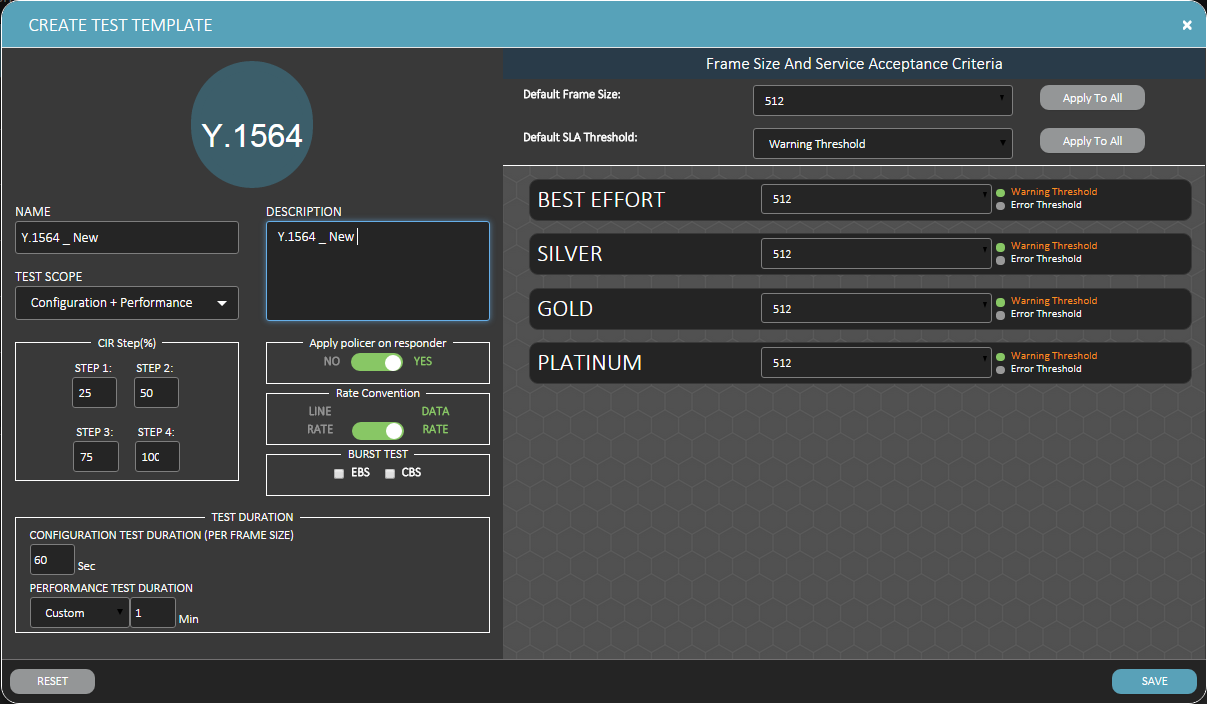
1. Configure the ETH generator to transmit L2 traffic End-to-End and verify traffic transmit and receive according **to the configured policer in the service**:





### Y.1564 Test

1. Go to Service>Test Template> Y.1564 and click on the  icon to create a new Y.1564 test template.
2. Configure all required test parameters of the test template and click *“Save”*:



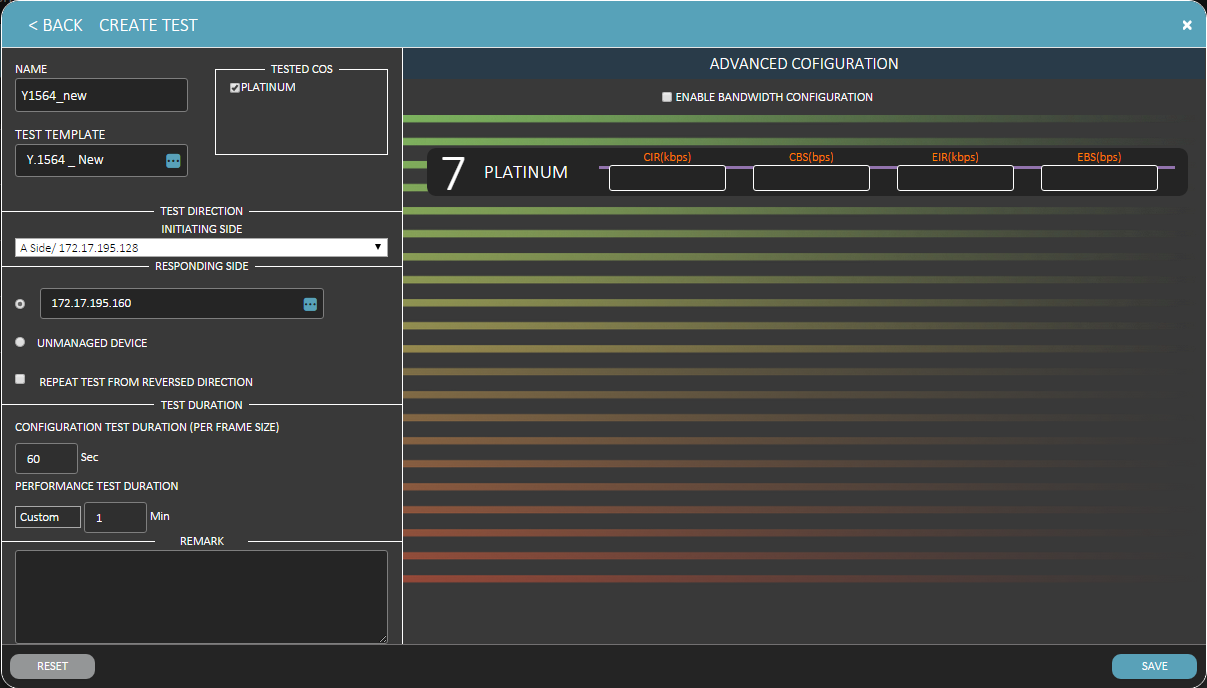
1. Navigate to service and select the required service to test and click on *Edit/View* button
2. At the Service window go to the Y.1564 tab and click on the  icon.

A new *“Create test”* window will be opened.

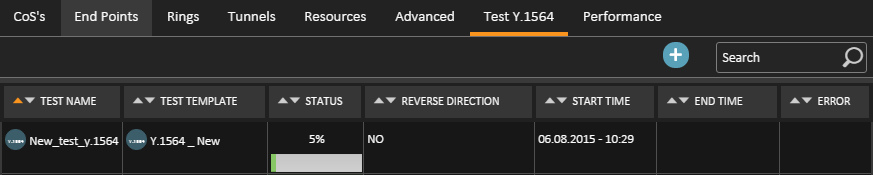
1. Configure all test parameters as displayed below:

* Test Name
* Test direction
* Test Template
* Test Duration
* Tested CoS in the service
* Enable/Disable Bandwidth configuration

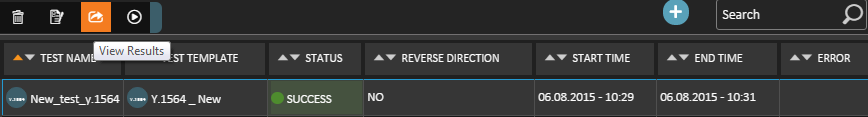
1. Click on “Save” to run the test.



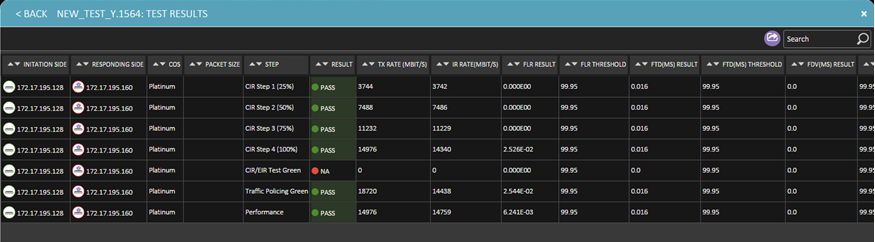
1. Press the *Test Y.1564* tab and verify test is in progress (status percentage should increase).



1. Once test is completed, mark the test line and click on the View results icon:



1. “Test Results” screen will be opened. Scroll the bottom horizontal bar to see all tests results:



1. All PDF reports saved on the server under: C:\Program Files (x86)\RADview\ui\server\uploads
2. Appendix A - ETX-2 Preliminary Setting
   1. ETX-2i/DNFV

##### Queues and Management Configuration

|  |
| --- |
| #\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*QUEUE\_GROUP\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  exit all  config qos queue-group-profile QGN1  exit all  config port eth 0/1 queue-group profile QGN1  exit all  config qos queue-group-profile QGN2  exit all  config port eth 0/2 queue-group profile QGN2  exit all  config qos queue-group-profile QGN3  exit all  config port eth 0/3 queue-group profile QGN3  exit all  config qos queue-group-profile QGN4  exit all  config port eth 0/4 queue-group profile QGN4  exit all  #\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*QUEUE\_GROUP END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  #\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*MANAGEMENT\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  config management snmp  target-params p1  message-processing-model snmpv3  version usm  security name initial level no-auth-no-priv  no shutdown  exit  #put target logical name  target p1  target-params p1  #put NMS server ip address  address udp-domain 172.17.230.13  no shutdown  tag-list "unmasked"  #put NMS server trap sync group (default is 1)  trap-sync-group 1  exit all  configure management snmp  config-change-notification  ##### connection between ETX-2i to X86 #######  exit all  configure port  svi 1  no shutdown  exit all  configure bridge 1  port 1  no shutdown  exit  port 2  no shutdown  exit  port 3  no shutdown  exit  exit all  configure flows  classifier-profile "all" match-any  match all  exit  classifier-profile "v100" match-any  match vlan 100  exit  classifier-profile "v4094" match-any  match vlan 4094  exit  classifier-profile "unt" match-any  match untagged  exit all  configure flows  flow "mng\_host\_x86"  classifier "v100"  no policer  ingress-port int-ethernet 0/8  egress-port bridge-port 1 3  reverse-direction block 0/1  no shutdown  exit  flow "mng\_all"  classifier "v4094"  no policer  mark all  vlan 100  exit  ingress-port ethernet 0/1  egress-port bridge-port 1 1  reverse-direction block 0/1  no shutdown  exit  flow "mng\_etx"  classifier "unt"  no policer  vlan-tag push vlan 100 p-bit fixed 0  ingress-port svi 1  egress-port bridge-port 1 2  reverse-direction  no shutdown  exit all  configure router 1  interface 1  address 172.17.195.160/24  bind svi 1  no shutdown  exit  static-route 0.0.0.0/0 address 172.17.195.1  exit all  #\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* |

* 1. ETX-203AX

##### Queues and Management Configuration

|  |
| --- |
| #\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*QUEUE\_GROUP\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  exit all  config qos queue-group-profile QGN1  exit all  config port eth 1 queue-group profile QGN1  exit all  config qos queue-group-profile QGN2  exit all  config port eth 2 queue-group profile QGN2  exit all  config qos queue-group-profile QGN3  exit all  config port eth 3 queue-group profile QGN3  exit all  config qos queue-group-profile QGN4  exit all  config port eth 4 queue-group profile QGN4  exit all  config qos queue-group-profile QGN5  exit all  config port eth 5 queue-group profile QGN5  exit all  config qos queue-group-profile QGN6  exit all  config port eth 6 queue-group profile QGN6  exit all  #\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* QUEUE\_GROUP END \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  #\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*MANAGEMENT\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  config management snmp  target-params p1  message-processing-model snmpv3  version usm  security name initial level no-auth-no-priv  no shutdown  exit  #put target logical name  target p1  target-params p1  #put NMS server ip address  address udp-domain 172.17.230.13  no shutdown  tag-list "unmasked"  #put NMS server trap sync group (default is 1)  trap-sync-group 1  exit all  configure management snmp  config-change-notification  ######## SVI Port Configuration ####################  configure port  svi 1  no shutdown  exit  exit all  ####### Classifier Profile Configuration ##########  configure flows  classifier-profile "v4094" match-any  match vlan 4094  exit  classifier-profile "all" match-any  match all  exit  ####### InBand MNG Flows ##########  flow "MNG\_In"  classifier "v4094"  policer profile "Policer1"  vlan-tag pop vlan  ingress-port ethernet 1  egress-port svi 1 queue 1  no shutdown  exit  flow "MNG\_out"  classifier "all"  policer profile "Policer1"  vlan-tag push vlan 4094 p-bit fixed 0  ingress-port svi 1  egress-port ethernet 1 queue 0 block 0/1  no shutdown  exit all  ####### Router Interface Configuration ##########    configure router 1  # interface 1 for MNG  interface 1  address 172.17.195.128/24  name MNG\_Interface  bind svi 1  dhcp-client  client-id mac  exit  no shutdown  exit  static-route 0.0.0.0/0 address 172.17.195.1 metric 1  exit all  #\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* |