DVG Series
Quick Start Guide
SRT caller/Listener

R1.1

Contents

1 Scope

This quick start guide provides fundamental information on how to configure a SRT protected stream between one Transmitter to a receiver for the purpose of sending a multicast transport stream over IP network like the Internet. This quick start guide is applicable for DVG software version 1.0 and above.

2 General

VideoFlow's solution is comprised at minimum with two elements Protector/Transmitter and Sentinel/Receiver. The sample system as illustrated below comprises from a Digital Video Gateway (DVG) Protector/Transmitter connected to the source (e.g., encoder) and acts as a transmitter of protected data stream. On the Receiving side another DVG Sentinel/Receiver is Tuned to receive the stream and output to the receiver (e.g., Integrated receiver decoder – IRD). The quick start guide provides an easy and systematic guide for setting up the Protector and the Sentinel using SRT reliable protection protocol. Both Protector and Sentinel require three steps setup:

1. Interfaces setup
2. Stream setup
3. SRT setup

A step by step procedure to connect a DVG Transmitter to a DVG Receiver is provided. The procedure includes the following sections:

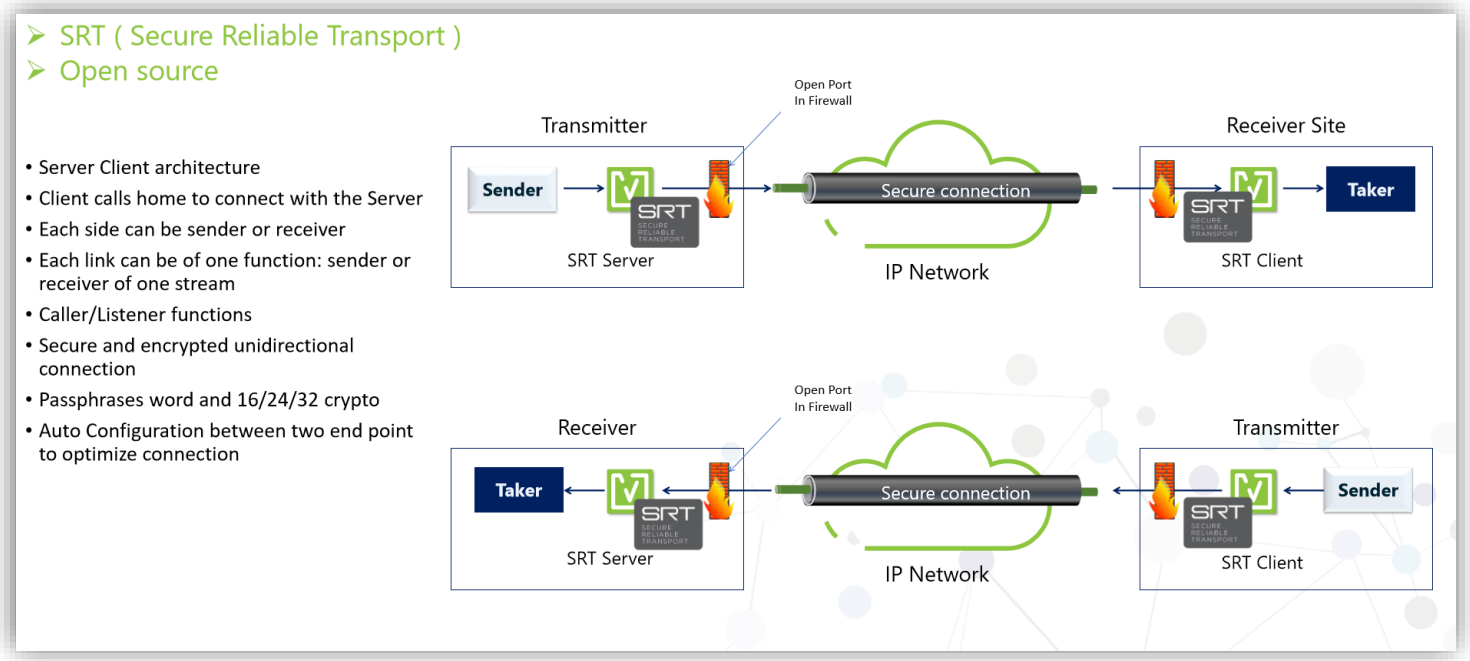
1. Receiver setup
    a. Interfaces
    b. Stream setup as an SRT Listener (server)
    c. Setup verification
2. Transmitter setup
    a. Interfaces
    b. Stream setup as an SRT Caller (client)
    c. Setup verification

NOTE
Both the DVG device may be capable of any function; transmitter, Receiver, Relay. The Functionality is user selectable on a stream by stream basis. The example given in this quick start guide is for setting up a contribution network. Therefore, the Receiver is configured as SRT Listener (Server) and the Transmitter as SRT Caller (Client).

At the end of the process, the two devices will communicate and will protect the quality of a multicast stream.

3 VideoFlow's SRT Solution

This section provides an introduction to VideoFlow's SRT implementation. The Secure Reliable Transport (SRT) is an open source protocol that is used by many companies to connect over unmanaged networks. The SRT provides ARQ functionality and encryption to the Stream. The Protocol is using a Server/Client architecture regardless of the transmission direction. Each session can carry only one stream in unicast or multicast. The DVG stream can have SRT input and SRT output. To Date VideoFlow implemented only Caller/Listener function, but the SRT includes a Rendezvous option as well. The SRT protocol allows other vendor solution supporting SRT to connect to a DVG as a transmitter or Receiver. Open source tools like VLC, OBS and FFMPEG come with built in SRT support.



The SRT includes its own buffering for the purpose of transmission and receiving. The user is allowed to set the delay configuration to the buffer.

The SRT is based on a client server architecture allowing a seamless traversal through firewalls and routers using a single UDP port. The SRT may require little IT support to configure and operate.

The Architecture is composed of two elements; An SRT Listener (server) and SRT Caller (client). The SRT Listener requires a reachable static IP address which is used as an anchor for the SRT caller wishing to establish connection with the Listener. The SRT Callers can use any interface or media to connect to the Listener. Each SRT session has a unique UDP port number assigned for it, and it may not be shared by other clients. The client server model is independent from the function that each VideoFlow instance is configured to use (transmitter or receiver).

NOTE

The SRT Listener should be set in a location where it can be reachable. Its IP address shall be static. The SRT Caller can be set anywhere.

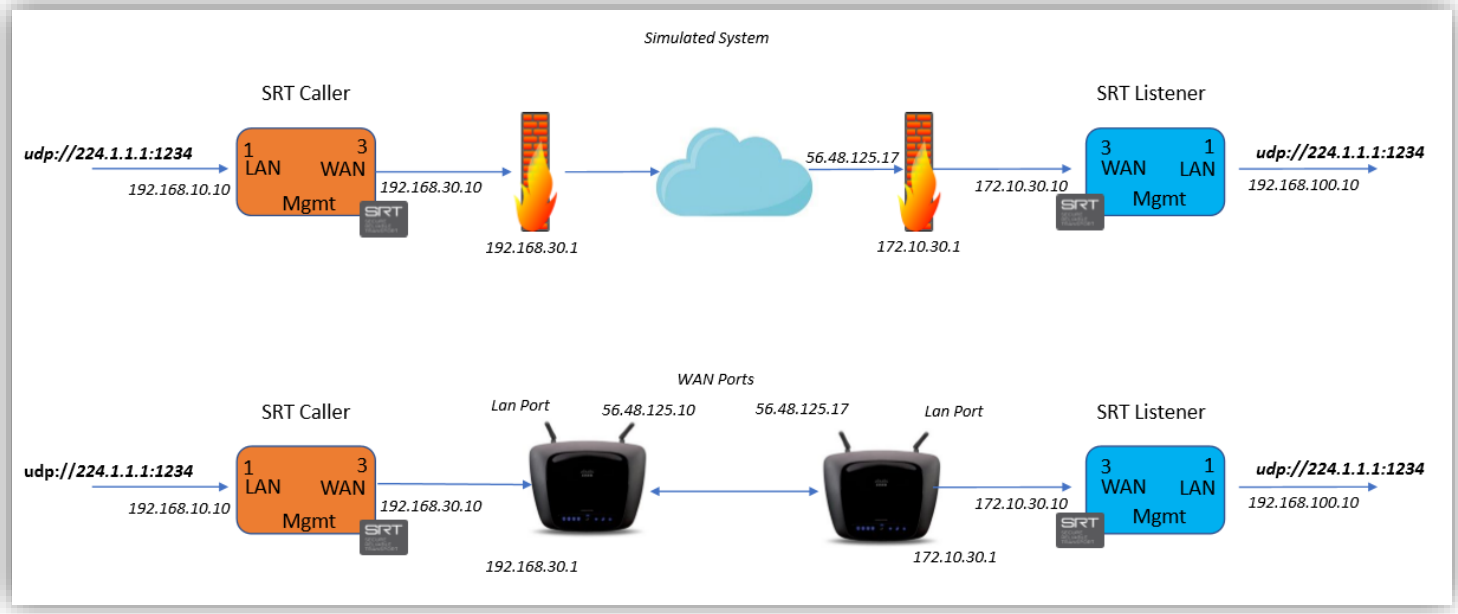
In a contribution network architecture will normally be multipoint-to-point were many Transmitters are connecting to a central Receiver. Therefore, SRT Listener will be set in the Receiver; the SRT Caller client in the Transmitter.

In a distribution network architecture will normally be point-to multipoint were one central Transmitter in connecting too many Receivers. Therefore, the SRT Listener will be set in the transmitter and many SRT Callers on the receivers.

3.1 Quick start desktop demo setup

For a simple benchtop demo, we propose to use a low cost Wifi Routers as a network simulation.

The following diagram ilustrates the Simulated System and its implementation oin the lab using off the self Wifi routers



3.1.1 Client-side Router setup

Local LAN: 192.168.30.1/24 Gateway: 192.168.30.1

WAN Address: 56.48.125.10/24 Gateway: 56.48.125.1

3.1.2 Server-side Router setup

Local LAN: 172.10.30.10/24 Gateway: 172.10.30.1

WAN Address: 56.48.125.17/24 Gateway: 56.48.125.1

In the Router Web management add forward rule of port 12000 to 172.10.30.10

Another option is to put 172.10.30.10 in the DMZ.

4 Setting Up the Receiver at the Center

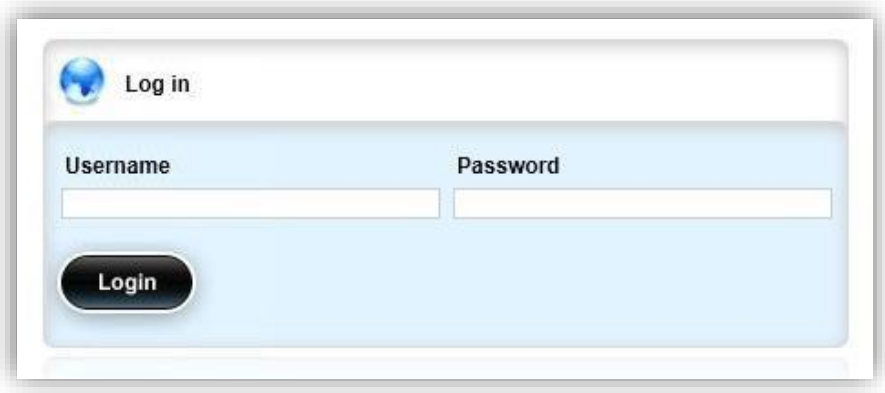
This section will describe the procedure required for configuring the Sentinel/Receiver at the center. The Receiver will act as the Server to the transmitters connecting to it from remote location.

4.1 Sentinel Port Setup

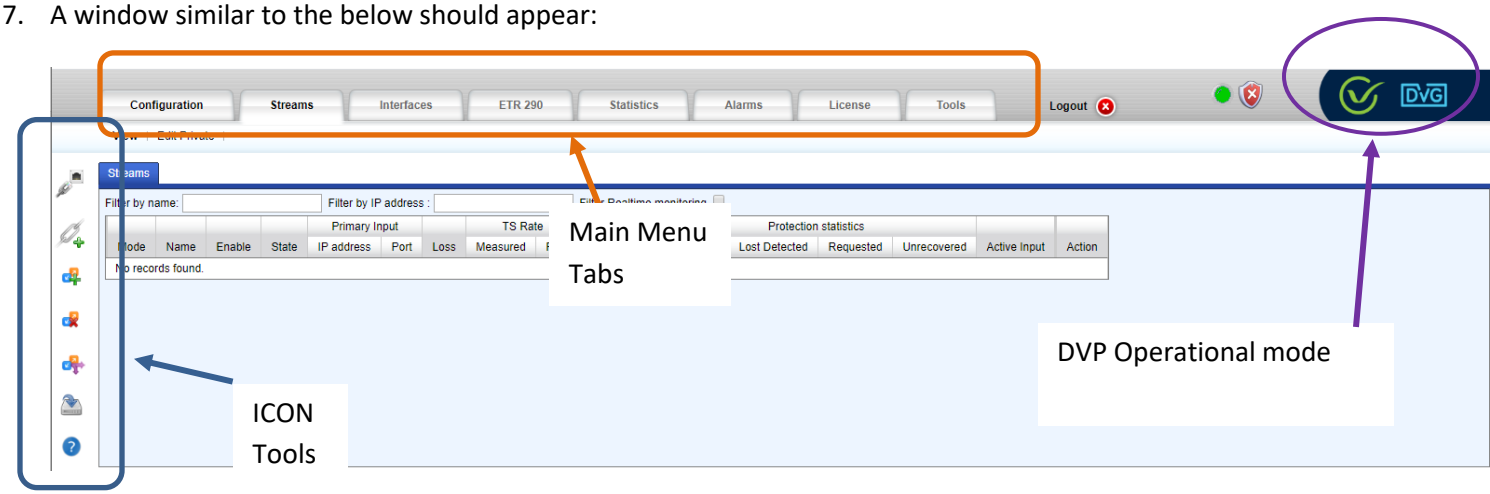
The default DVP factory management IP address is: 10.0.0.200.

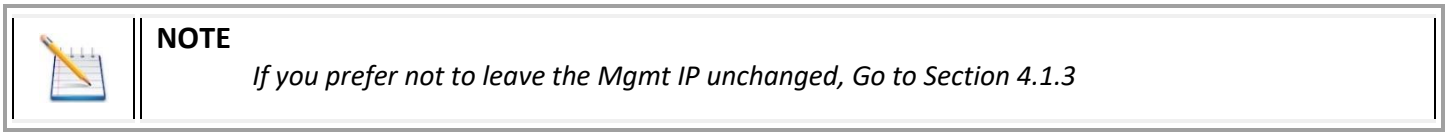
4.1.1 First Time Connection

1. Connect an Ethernet cable between a computer running a browser program to a port labeled Mgmt in the DVP's front panel.
2. Change the local LAN settings in your PC to manual IP address
3. Select IP address from the same subnet (e.g., 10.0.0.120, Subnet Mask: 255.255.255.0)
4. Browse the Sentinel's management IP address. A login window similar to the below will appear:



5. Type the default Username: oper
6. Type the default Password: oper
7. A window similar to the below should appear:



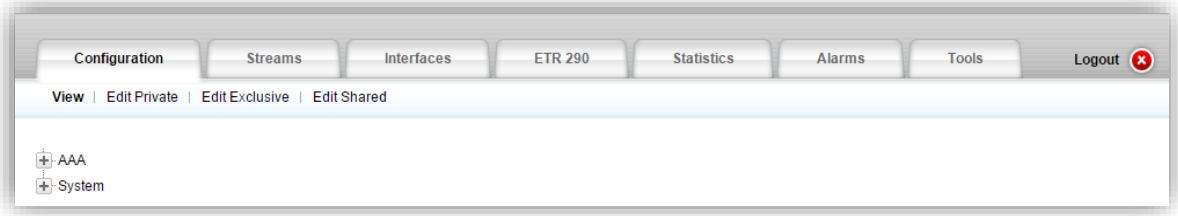


NOTE

If you prefer not to leave the Mgmt IP unchanged, Go to Section 4.1.3

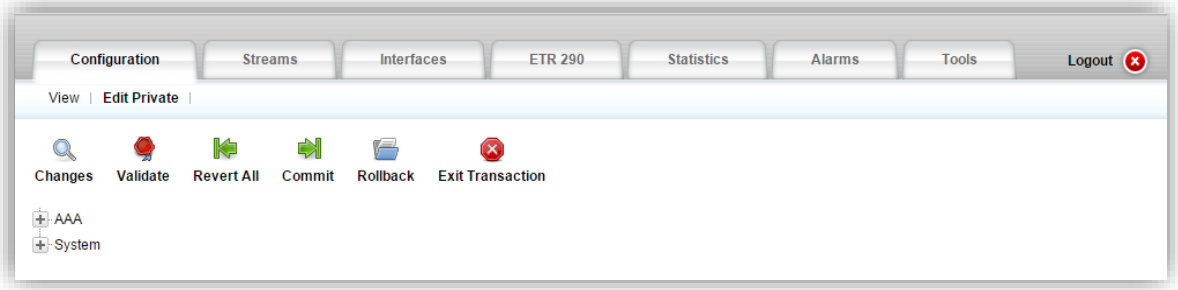
8. Click on the Configuration tab

9. A new page will appear:

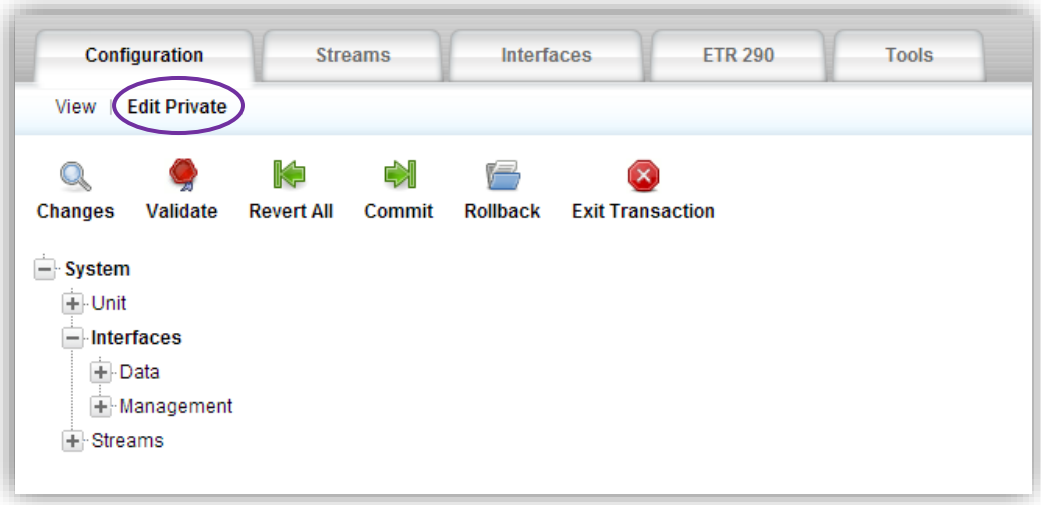


4.1.2 New Management IP Address Setup

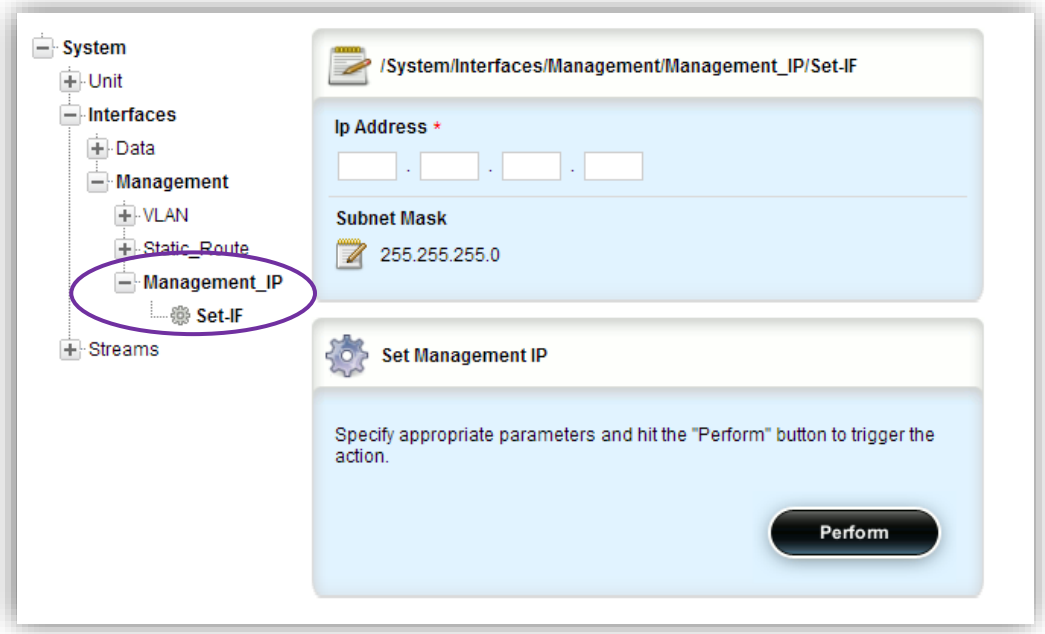
1. Click on the **Edit Private** mode



2. Clicking on the '+' expand a menu tree item. Click on System→Interfaces→Management



3. Click on Management_IP→Set-IF to setup the management interface's IP address



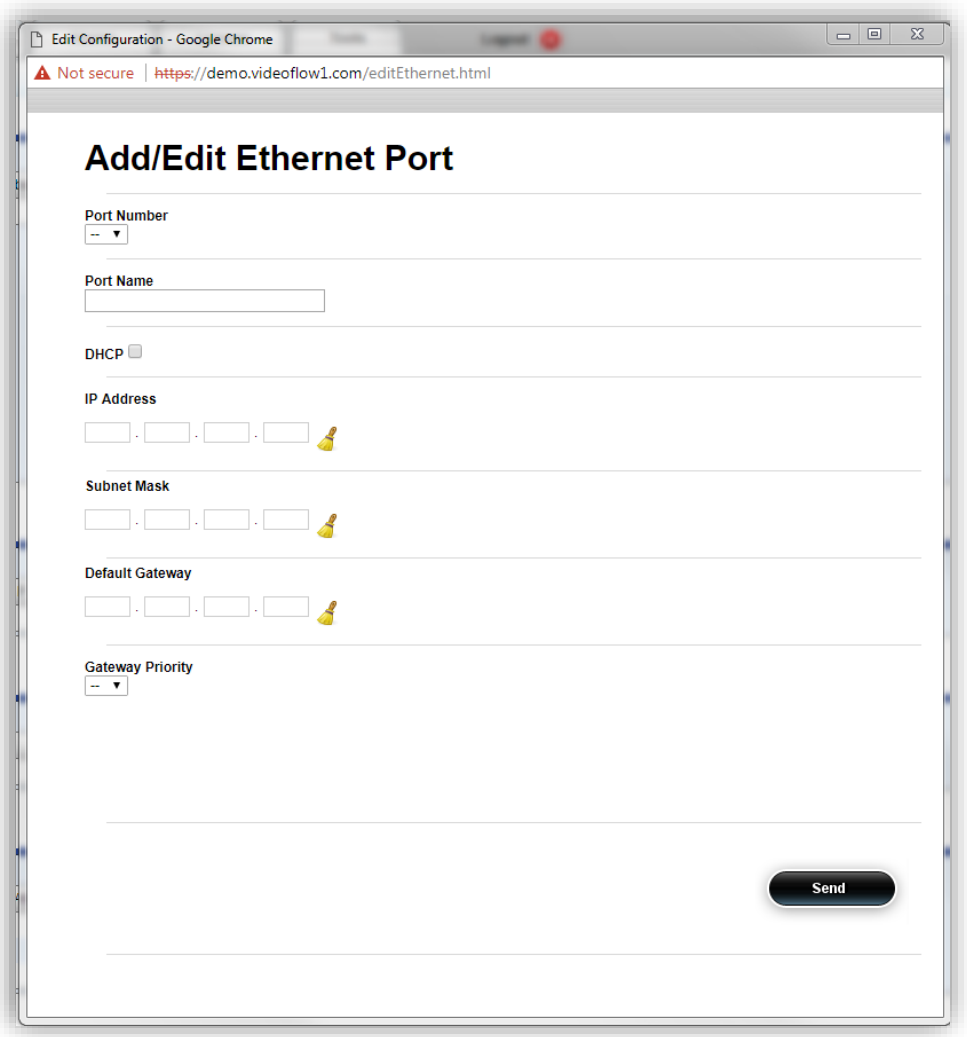
4. Type a new management IP address if required
5. Modify the management Subnet Mask if required
6. Click on the Perform button to apply the changes

7. The PC and the DVG will disconnect in the case of management IP and/or subnet mask change. Follow the below procedure to reconnect:
   a. *Close the browser window*
   b. *Change the IP address in the PC to be in the same subnet as the new management IP address*
   c. *Open the browser and browse the new management IP address*
8. Once the connection with the Sentinel is resumed, continue to the next section

4.1.3 Receiver device Data Ports Setup

This section describes how to Add and assign IP addresses to the DVP interfaces. The ports are used for connecting the DVP to either the local network (LAN) or to the external network (WAN).

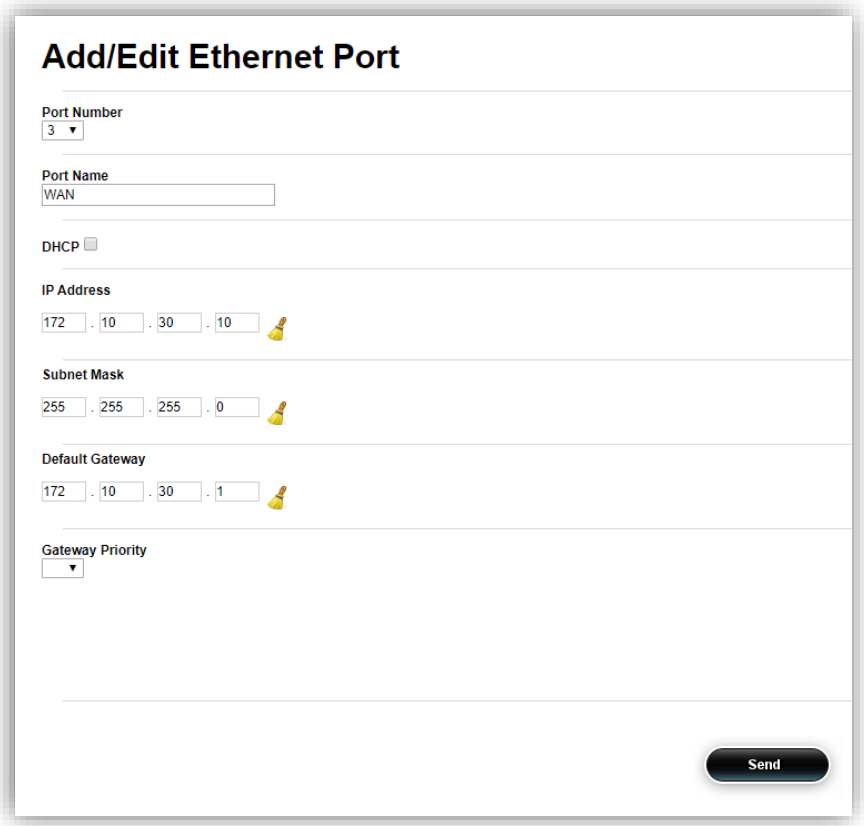
1. Press on the  icon to bring the IP configuration



Select the interface Id number from the pull down list.

In this guide's network example the external network (the public Internet in this example) is connected to Port3 and the local network is connected to Port 1.

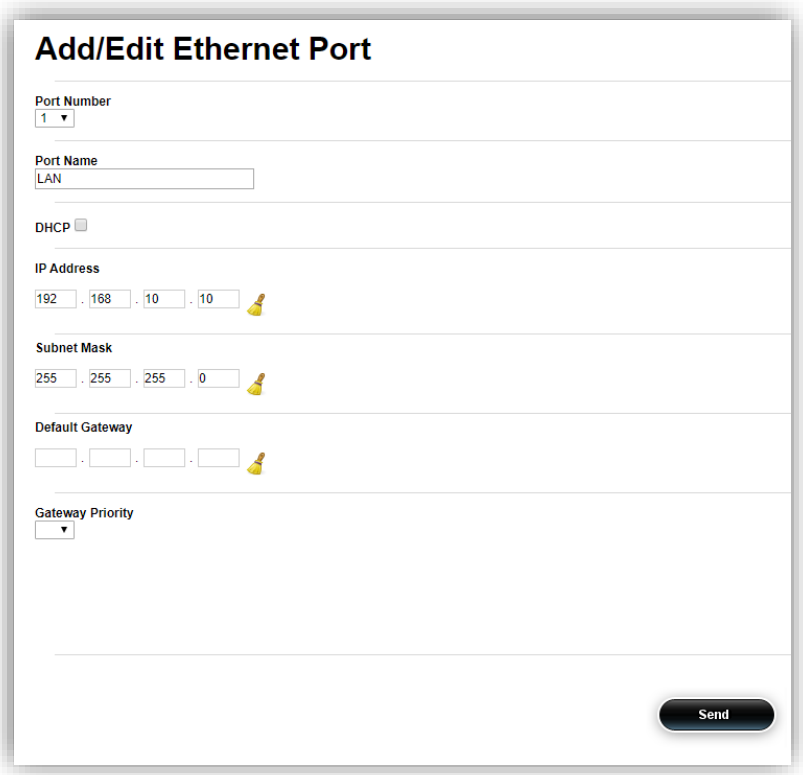
2. Port 3 (to external network) configuration (In this example:):
   Check the 'Enable' check box to enable the Port
   Set the Name field to 'WAN'
   configure IP Address: 172.10.30.10
   configure Subnet Mask: 255.255.255.0
   Configure Default Gateway: 172.10.30.1



To complete configuration click on the ‘Send’ button to apply the configuration changes

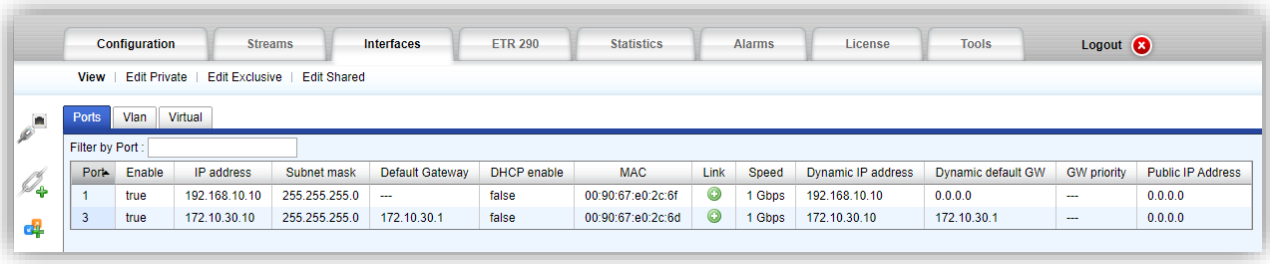
3. Repeat the same steps to configure Por1 (to local network) configuration:

Set the Name field to ‘LAN’
configure IP Address: 192.168.10.10
Subnet Mask: 255.255.255.0
Note that there is no need to configure default gateway to ports connecting to the local network



4. Check the stream connectivity

Press the Interfaces TAB to expose:



Port	Enable	IP address	Subnet mask	Default Gateway	DHCP enable	MAC	Link	Speed	Dynamic IP address	Dynamic default GW	GW priority	Public IP Address
1	true	192.168.10.10	255.255.255.0	---	false	00:90:67:e0:2c:6f		1 Gbps	192.168.10.10	0.0.0.0	---	0.0.0.0
3	true	172.10.30.10	255.255.255.0	172.10.30.1	false	00:90:67:e0:2c:6d		1 Gbps	172.10.30.10	172.10.30.1	---	0.0.0.0

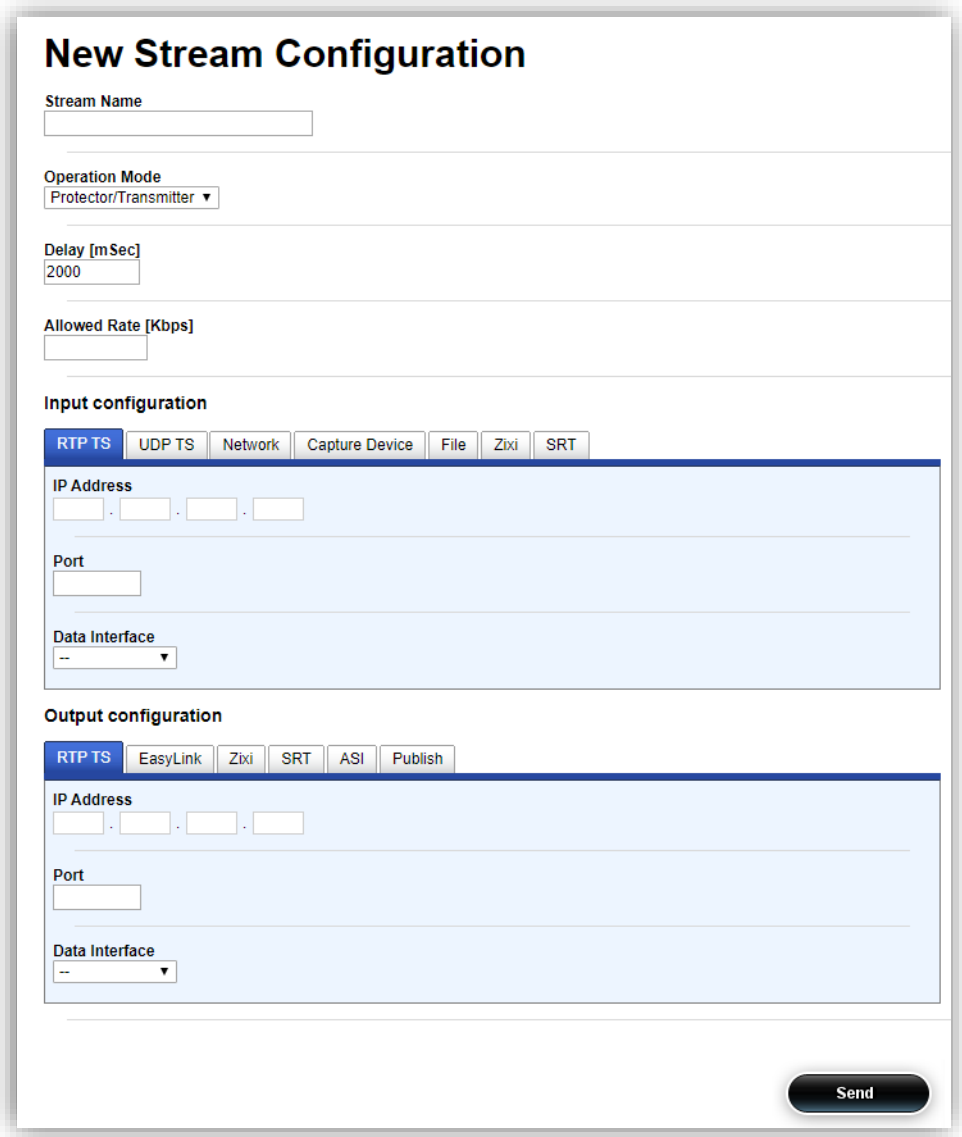
4.2 Adding a Stream

At this stage, we are going to be Adding a stream which is comprised of three steps:

1. Adding stream
2. Setup the stream's input interface and properties
3. Setup the stream's SRT output and interface properties Add Stream

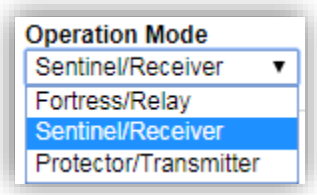
4.2.1 Steps

1. Click on the  ICON, a 'New Stream Configuration' Window will appear:

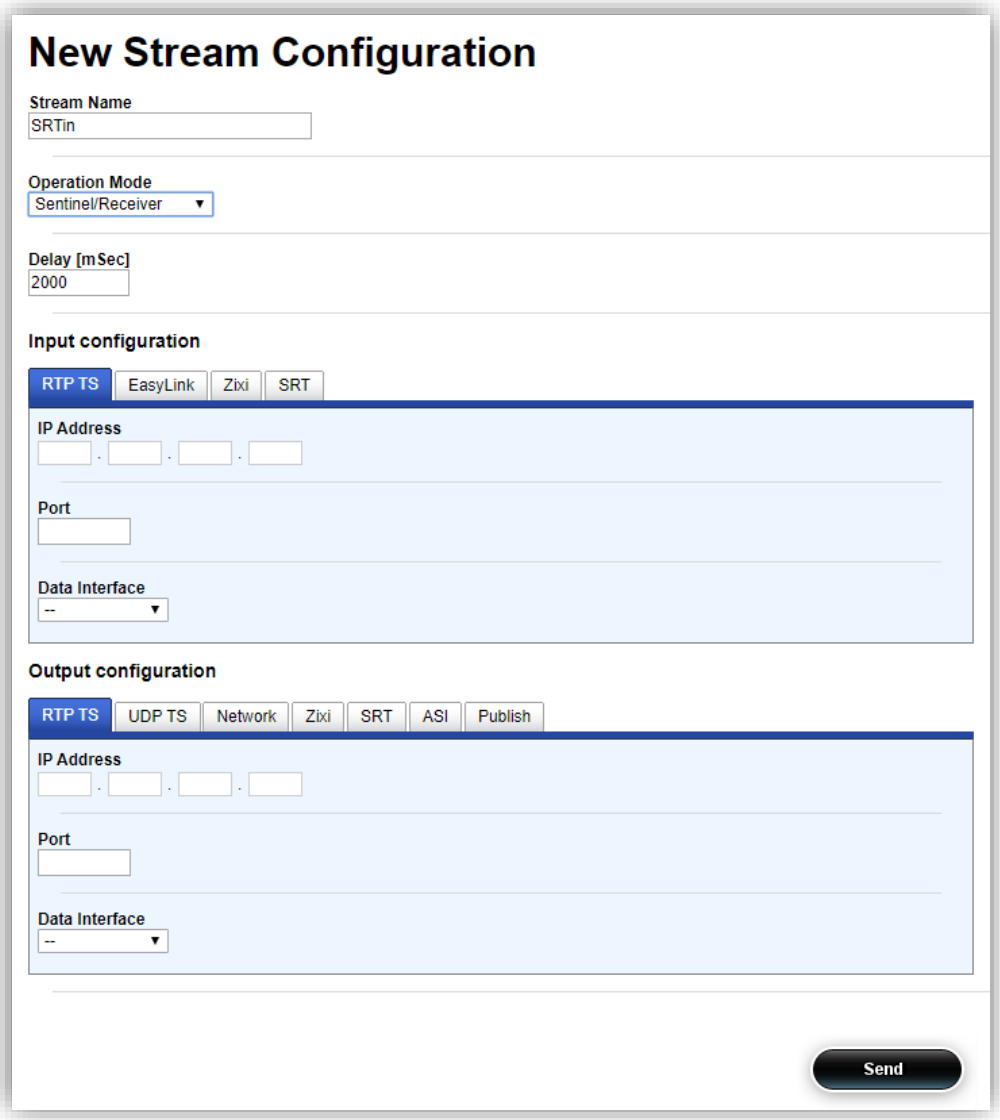


2. Set a name for the stream, in this case 'SRTin'

3. Select the stream function Protector/Sentinel/Fortress from a drop down menu. In our example **Sentinel**

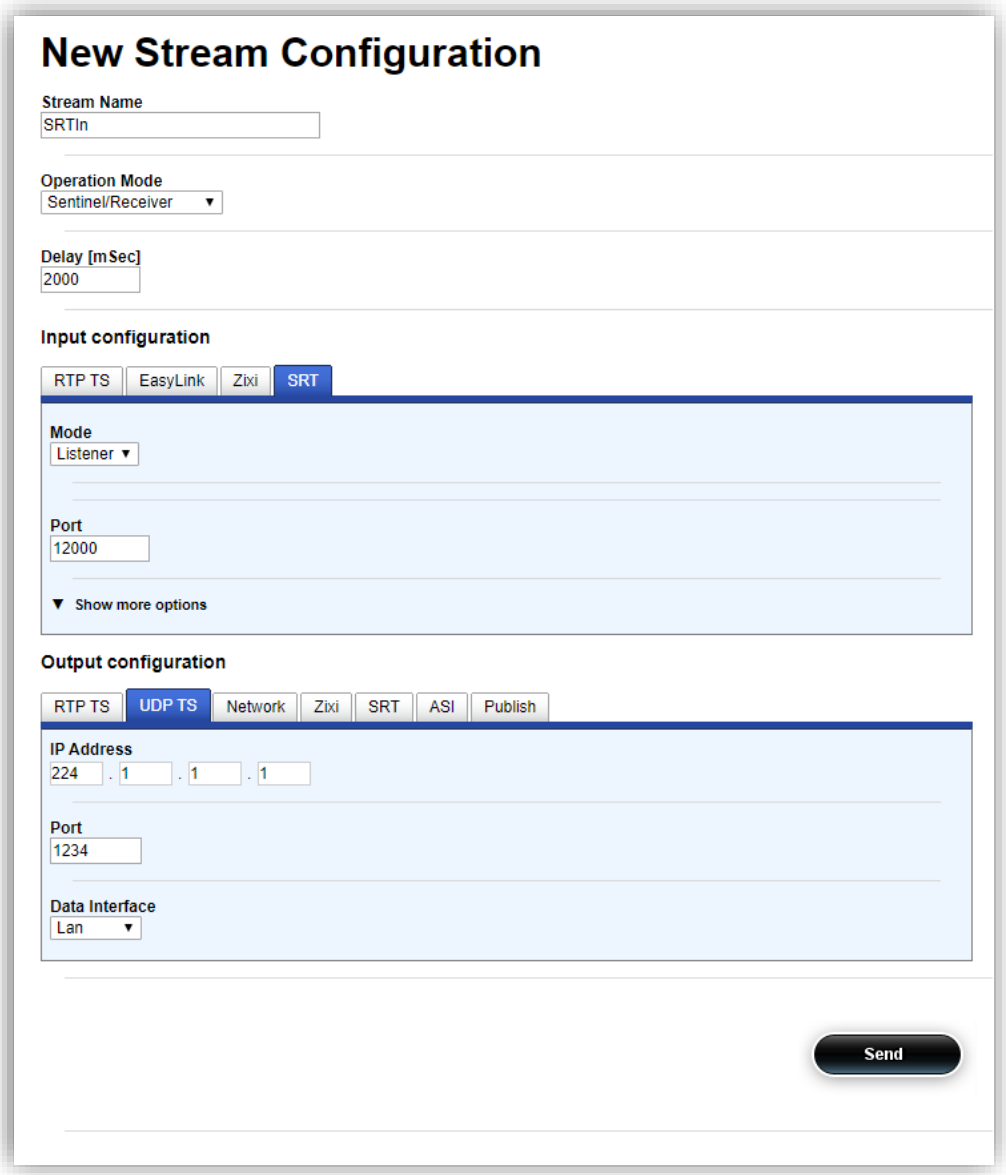


4. The Window will change its appearance to;



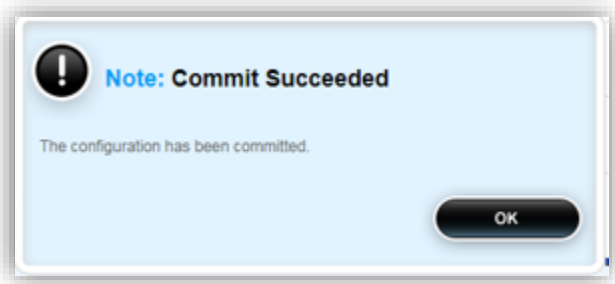
5. Configure the stream's **Input configuration** parameters:
    a. Select the **SRT** TAB
    b. Select the Mode to **Listener**
    c. Type a UDP Port number for the session
6. Configure the stream's **Output configuration** parameters:
    a. Select the **UDP** TAB
    b. Set the IP address to **224.1.1.1**
    c. Set the Port to **1234**

d. Select the output interface from a pull-down menu, in this example select the **Lan**

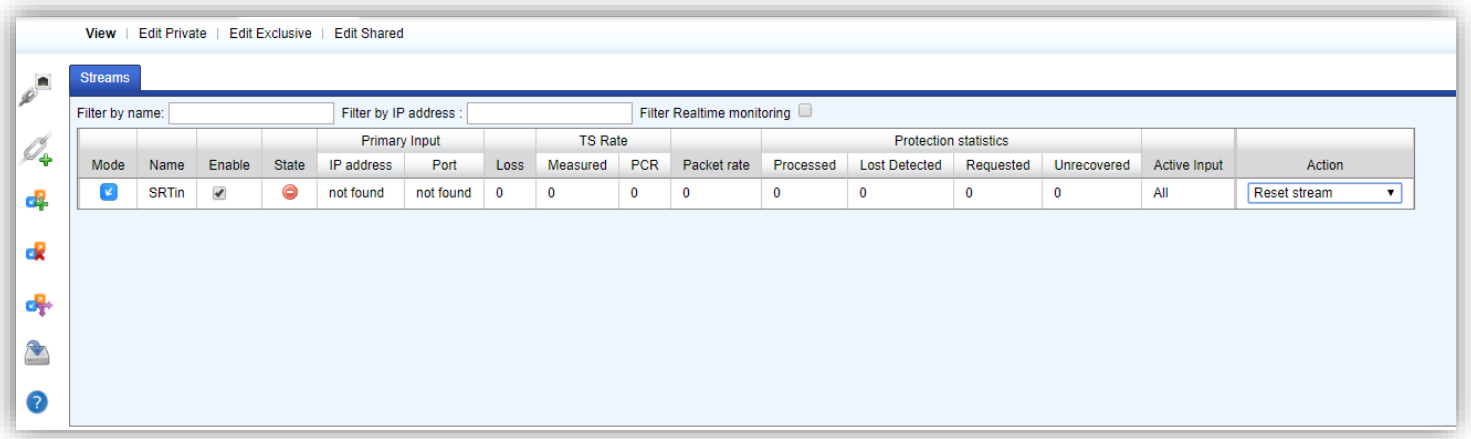


e. Press Send when done

7. Wait for the 'Commit Succeeded' window to appear:



8. Close the window
9. A new stream should appear:



At this time the Stream is not available yet (as the Transmitter is not configured).

5 Setting Up the Transmitter at the Remote Site

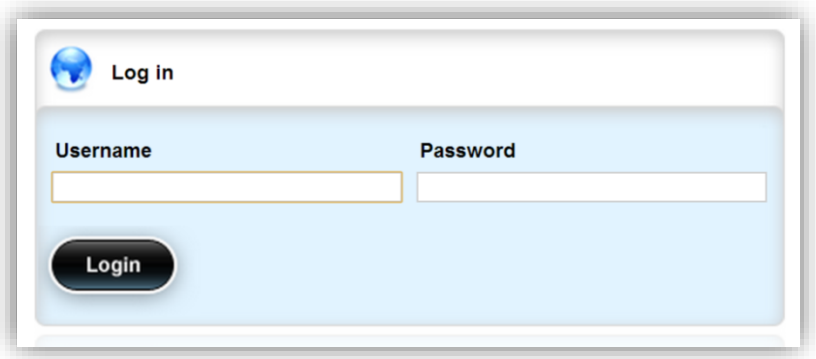
This section will describe the procedure required for configuring the Protector at the remote site. The DVG will act as the Client to connect to the remote peer DVG device.

5.1 DVG Port Setup

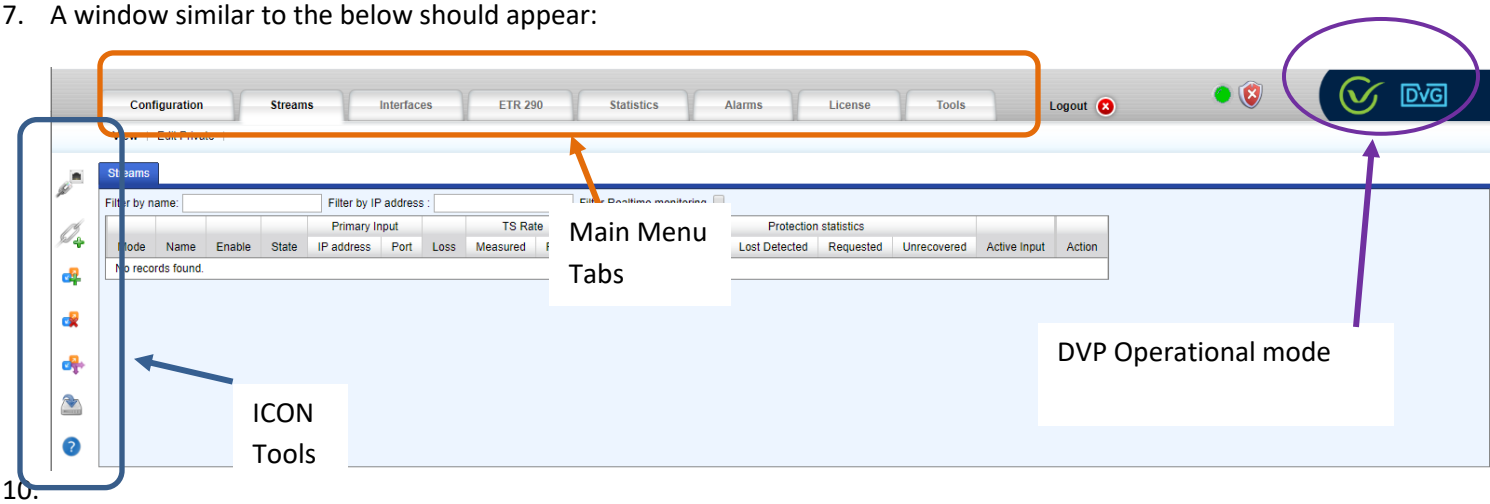
The default device factory management IP address is: 10.0.0.200.

5.1.1 First Time Connection

1. Connect an Ethernet cable between a computer running a browser program to the port labeled Mgmt in the DVP's front panel
2. Change the local LAN settings in your PC to manual IP address
3. Select IP address that is in the same subnet (e.g., 10.0.0.140, Subnet Mask: 255.255.255.0)
4. Browse the Protector's management IP address. A login window similar to the below will appear:



5. Type the default Username: oper
6. Type the default Password: oper
7. A window similar to the below should appear:

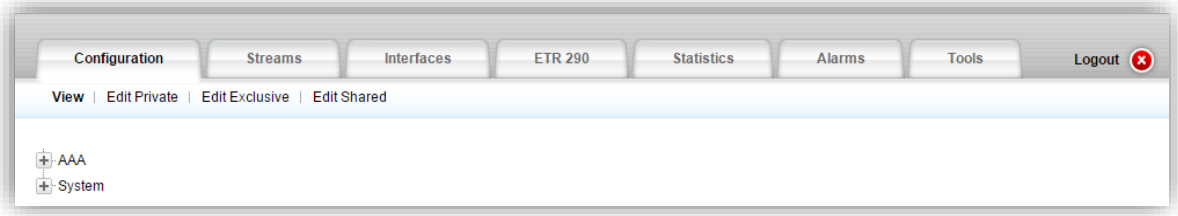


10.

	NOTE *If you prefer not to leave the Mgmt IP unchanged, Go to Section 5.1.3*

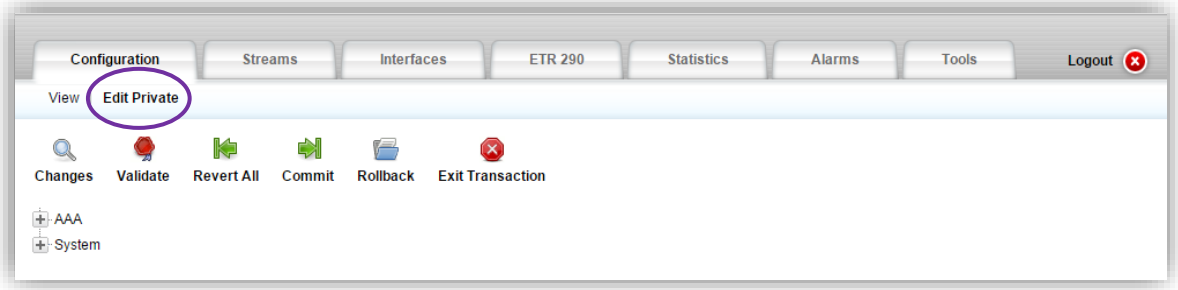
8. Click on the Configuration tab

9. A new page will appear:

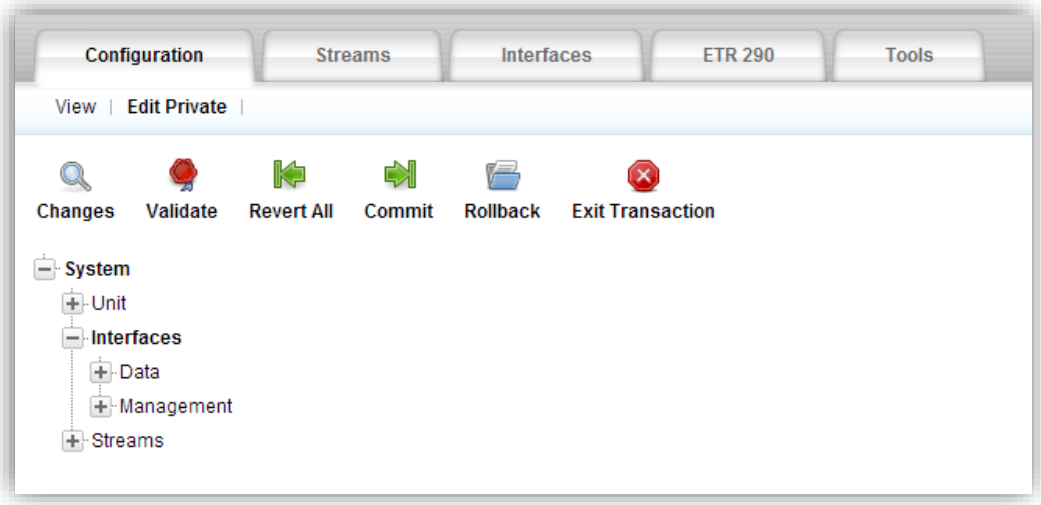


5.1.2 New Management IP Address Setup

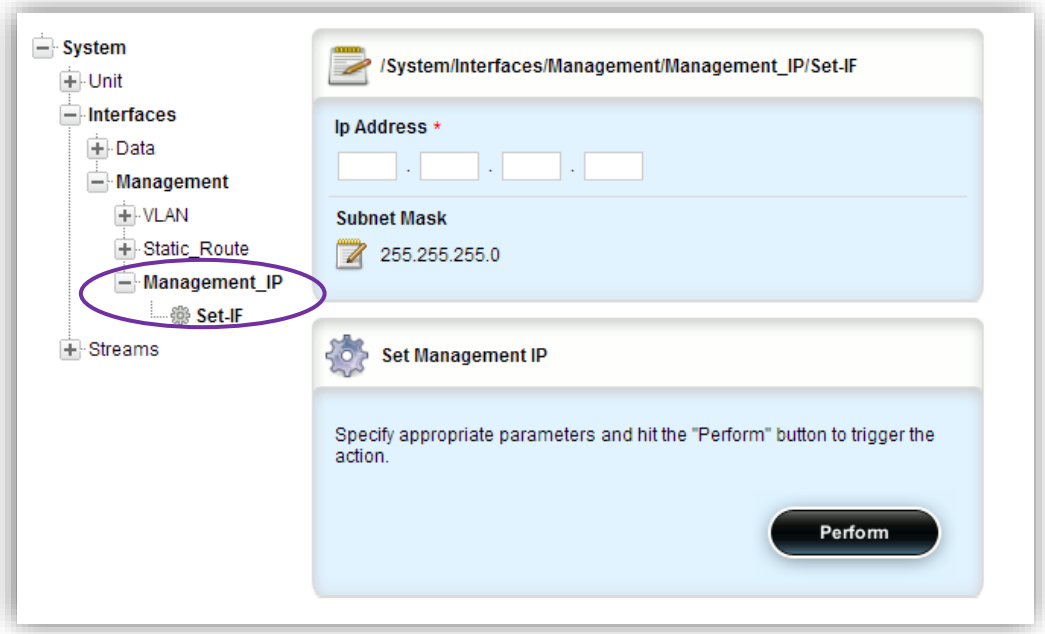
1. Click on the Edit Private mode.



2. Click on the '+' to expand the menu tree. Expand the menu tree further by clicking on Management



3. Click on Management_IP→Set-IF to setup the management interface's IP address.

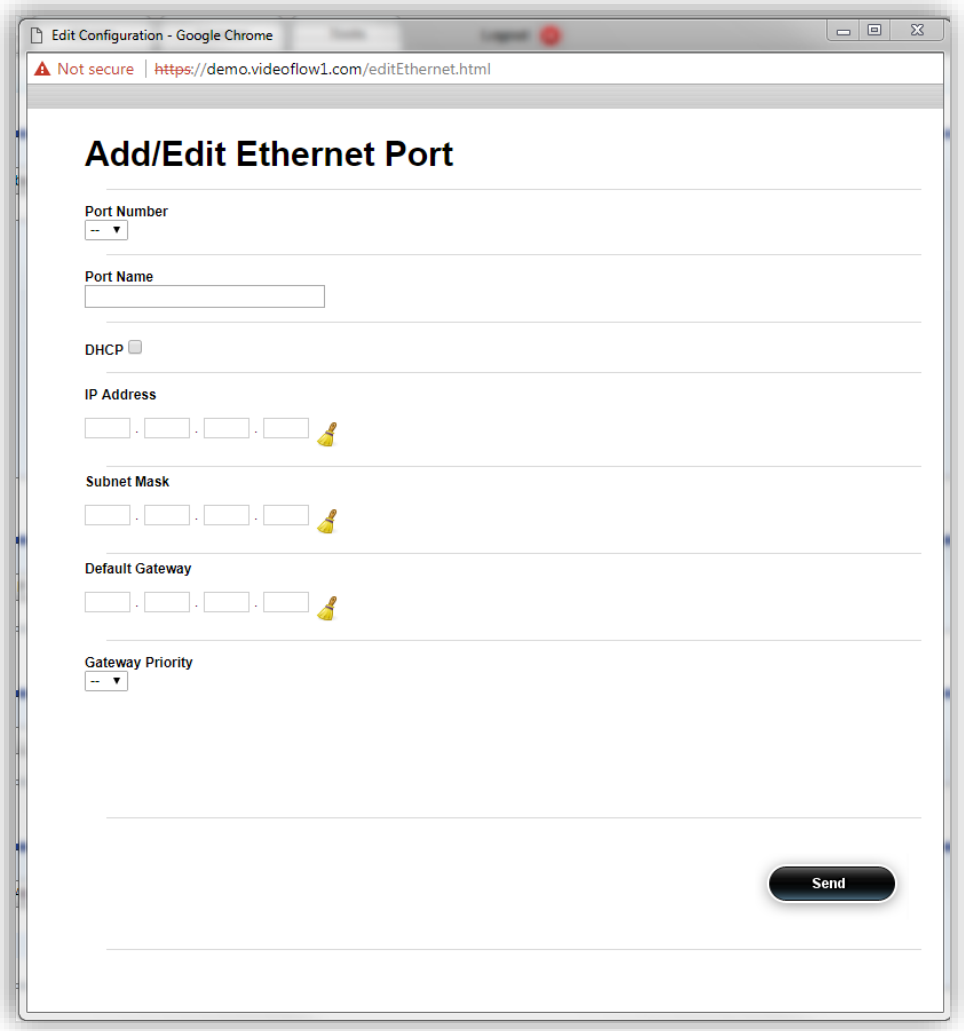


4. Type a new management IP address if required.
5. Modify the management Subnet Mask if required.
6. Click on Perform to apply the changes.
7. The PC and the DVP will disconnect in the case of management IP and/or subnet mask change. Follow the below procedure to reconnect:
    a. *Close the browser window.*
    b. *Change the IP in the PC to the same subnet as the new management IP address.*
    c. *Open the browser and browse the new management IP address.*
8. Once connection with the Protector is resumed, continue to the next section.

5.1.3 DVG Data Ports Setup

This section describes how to Add and assign IP addresses to the DVG interfaces. The ports are used for connecting the DVP to either the local network (LAN) or to the external network (WAN).

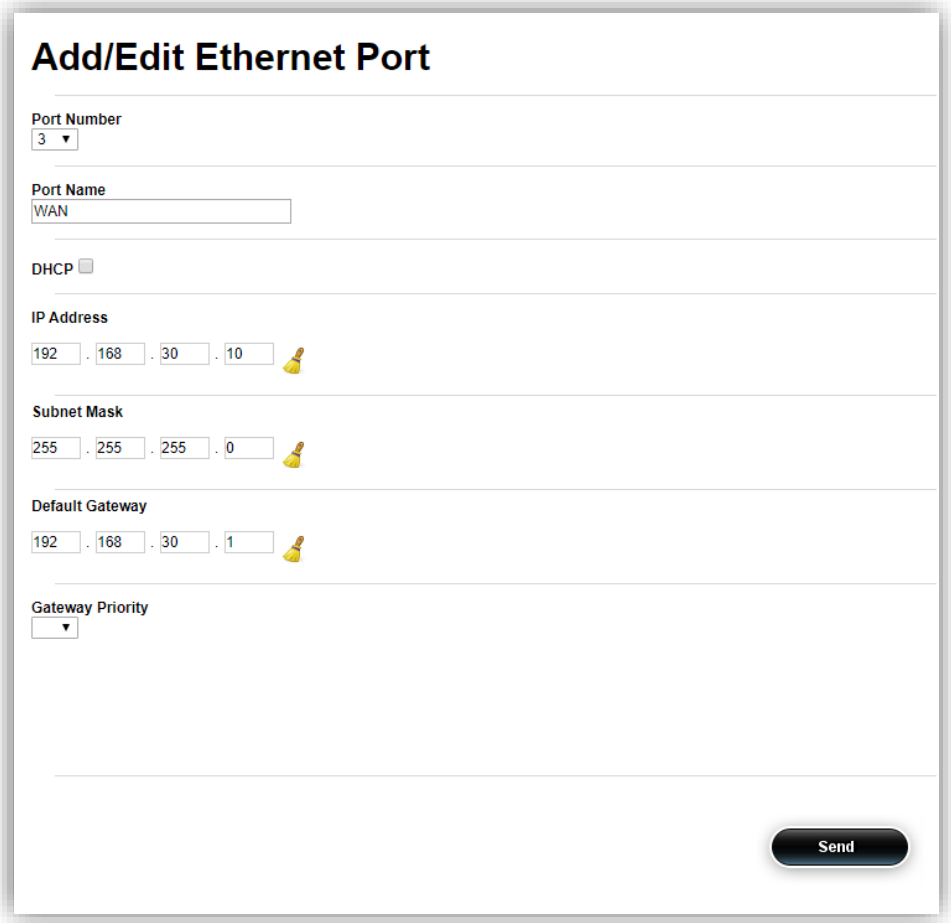
1. Press on the  icon to bring the IP configuration



Select the interface Id number from the pull down list.

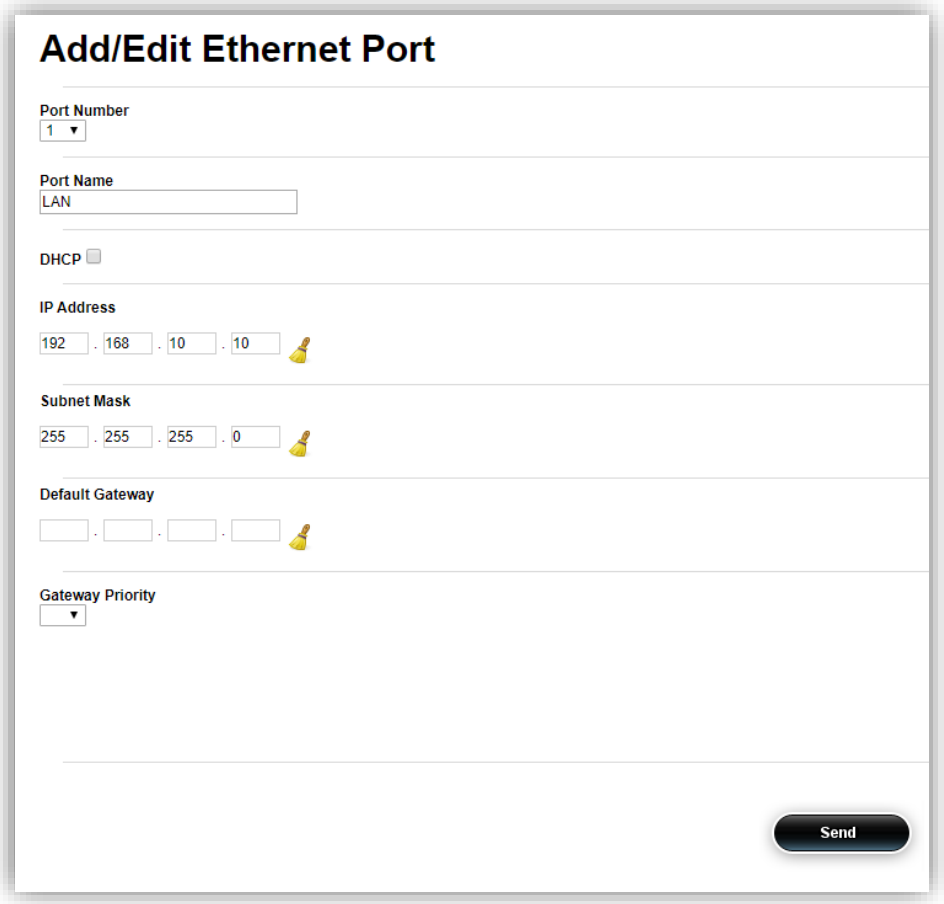
In this guide's network example the external network (the public Internet in this example) is connected to Port3 and the local network is connected to Port 1.

2. Port 1 (to external network) configuration (In this example:):
   Check the 'Enable' check box to enable the Port
   Set the Name field to 'WAN'
   configure IP Address: 192.168.30.10
   configure Subnet Mask: 255.255.255.0
   Configure Default Gateway: 192.168.30.10



To complete configuration click on the ‘Send’ button to apply the configuration changes

3. Repeat the same steps to configure Port 2 (to local network) configuration:

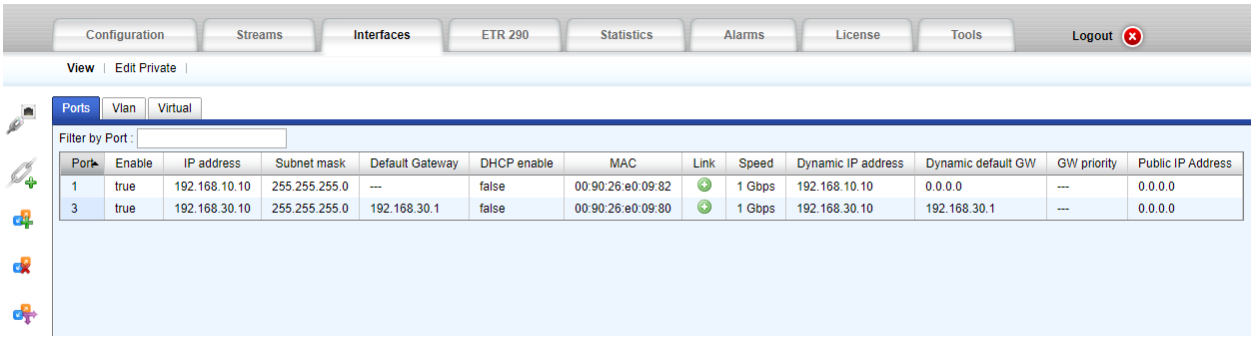


Set the Name field to 'LAN'

IP Address: 192.168.10.10
Subnet Mask: 255.255.255.0
Note that there is no need to configure default gateway to ports connecting to the local network

Close the window when done.

4. Check the connectivity,



Port	Enable	IP address	Subnet mask	Default Gateway	DHCP enable	MAC	Link	Speed	Dynamic IP address	Dynamic default GW	GW priority	Public IP Address
1	true	192.168.10.10	255.255.255.0	---	false	00:90:26:e0:09:82		1 Gbps	192.168.10.10	0.0.0.0	---	0.0.0.0
3	true	192.168.30.10	255.255.255.0	192.168.30.1	false	00:90:26:e0:09:80		1 Gbps	192.168.30.10	192.168.30.1	---	0.0.0.0

5.2 Adding the Stream

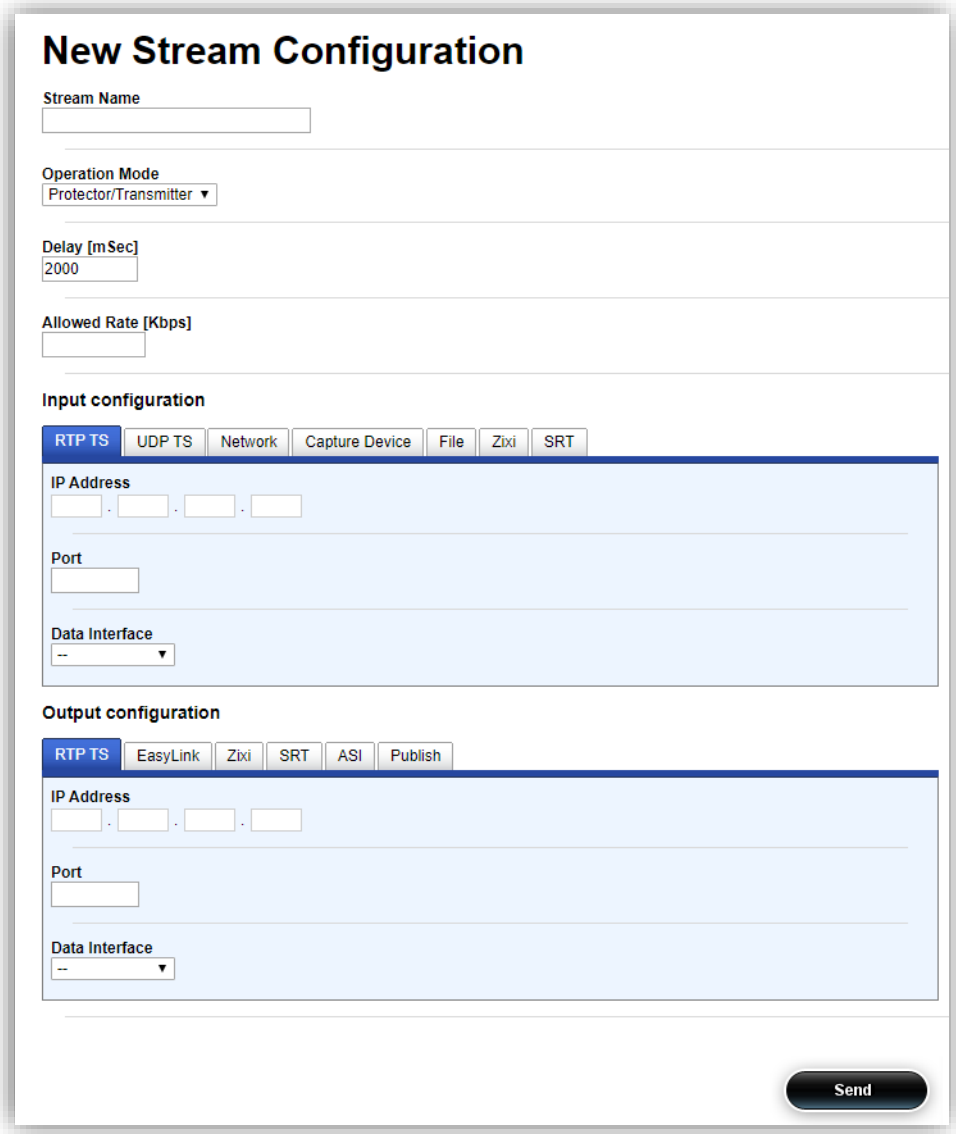
5.3 Adding a Stream

At this stage, we need to add streams to our setup. Adding a stream is comprised of three steps:

1. Adding stream
2. Setup the stream's input interface and properties
3. Setup the stream's output interface and properties

5.3.1 Add Stream

1. Click on the  ICON, a 'New Stream Configuration' Window will appear:

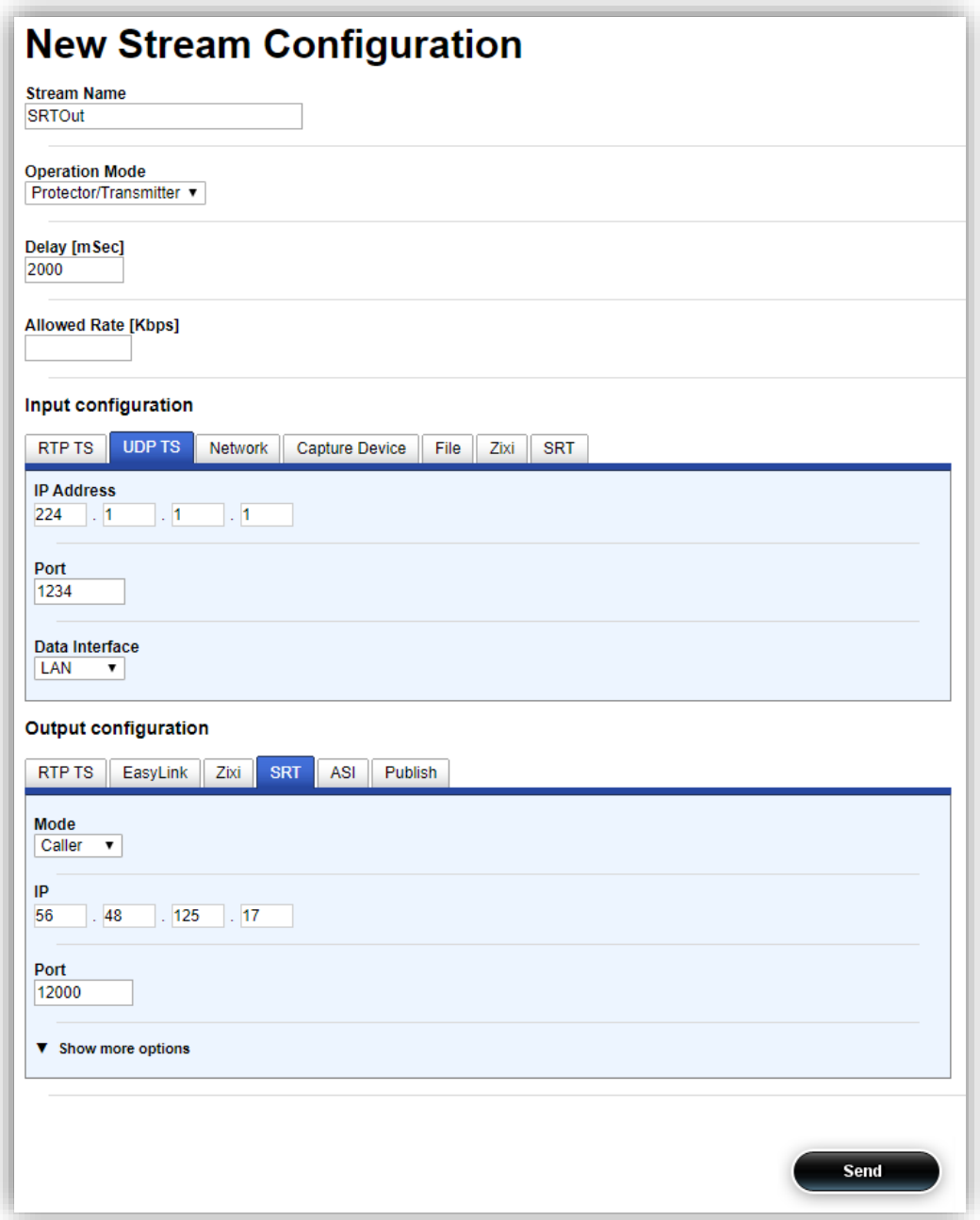


2. Set a name for the stream, in this case 'SRTin'

3. Configure the stream's **Input configuration** parameters:
   a. Configure Listen Ip according to the stream's destination IP address (224.1.1.1 in this example)
   b. Configure Listen Port according to the stream's UDP port (1234 in this example)

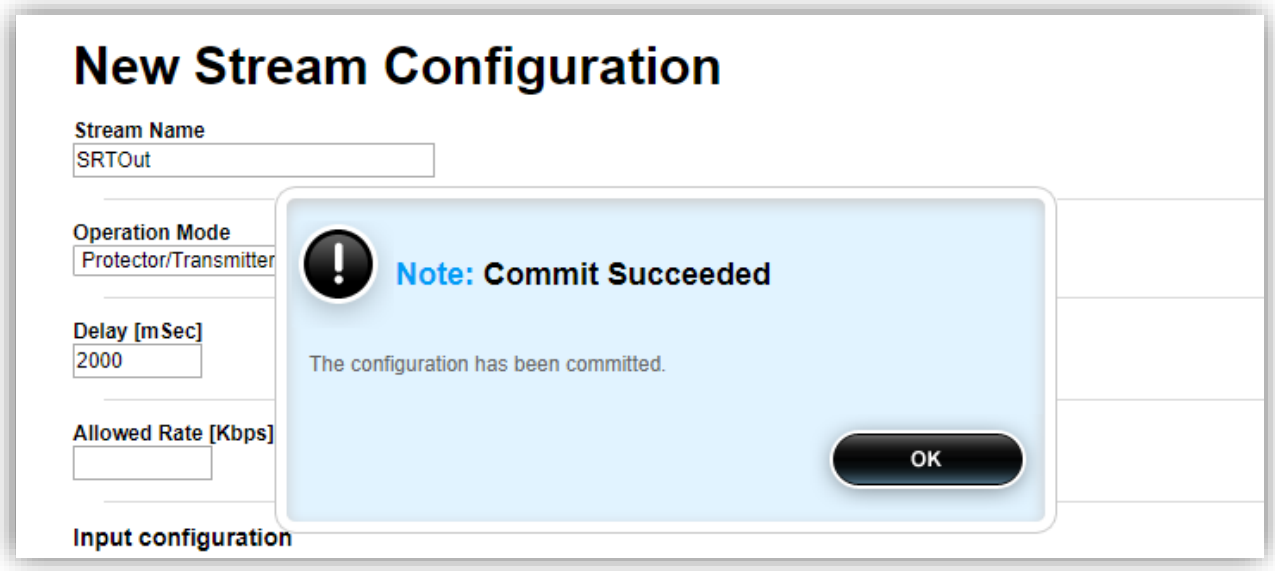
c. Select the Data interface from the Input Interface Name drop down menu (**LAN** in our example)

4. Configure the stream's **Output configuration SRT TAB** parameters:
   a. Select the Mode to be **Caller**
   b. Configure the Listening Port of the Server in this example: 56.48.125.17
   c. Configure the UDP port : 12000

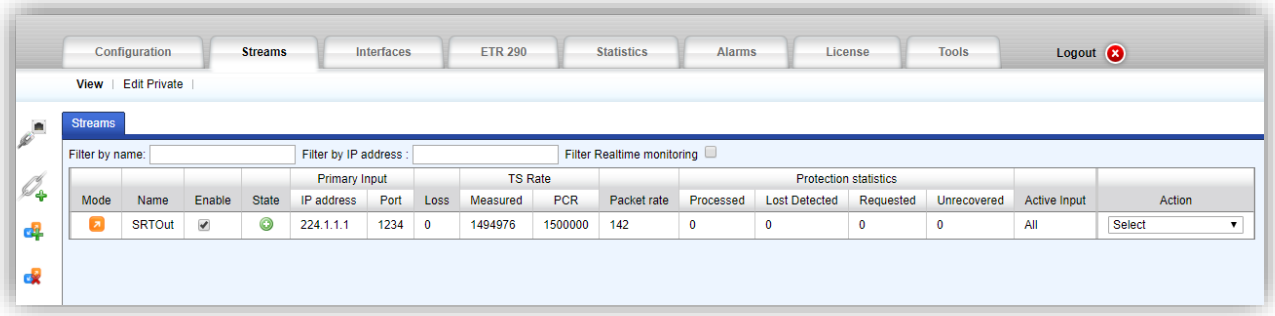


   d. Press **Send** button when done

10. Wait for the 'Commit Succeeded' window to appear:

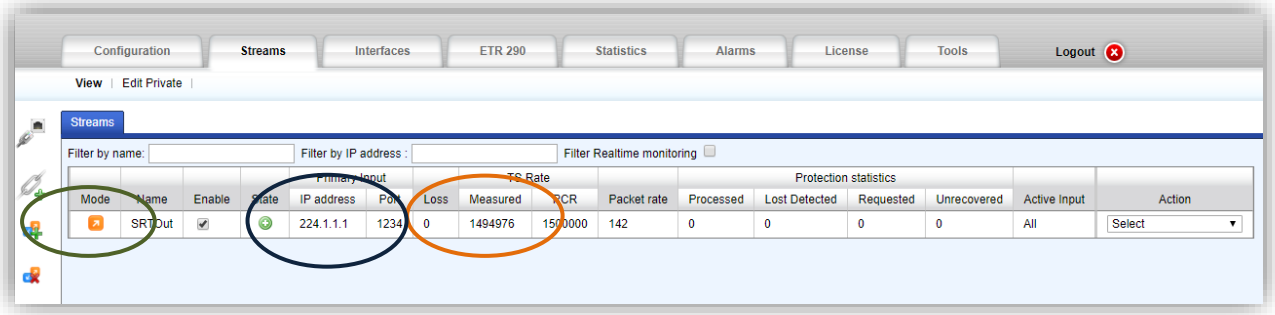


11. Close the window
12. A new stream should appear:



5.3.2 Verify Stream Configuration in the transmitter

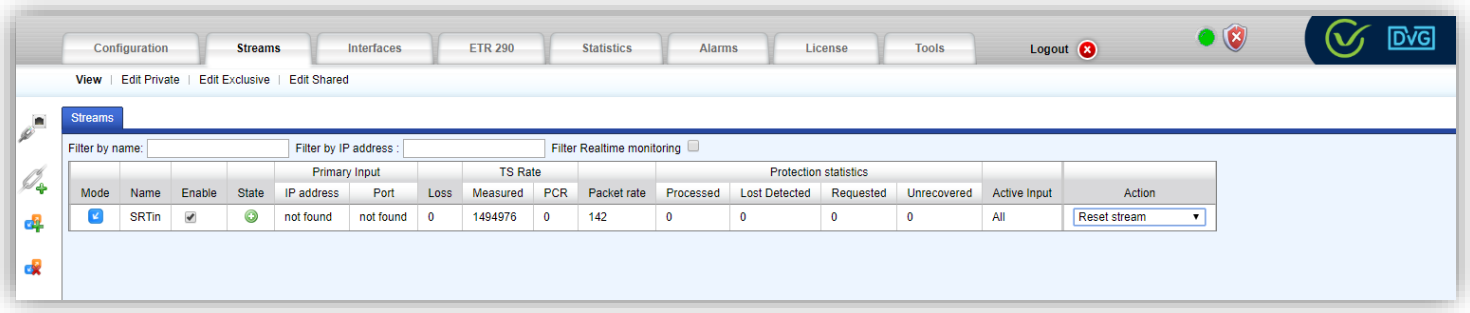
1. Click on the Streams Tab from the Main Menu:



2. Verify
    a. The stream shown
    b. Packet rate is shown and valid
    c. Both measured and PCR TS rate are shown and valid

5.3.3 Verify Stream Configuration in the Receiver

Click on the Streams Tab from the Main Menu:



2. Verify
    a. The stream shown
    b. Packet rate is shown and valid
    c. Both measured and PCR TS rate are shown and valid