



DVG Series

Quick Start Guide

RIST Server/Client

R1.2

Contents

1	SCOPE	3
2	GENERAL	3
3	VIDEOFLOW'S RIST SOLUTION.....	4
3.1	QUICK START DESKTOP DEMO SETUP	6
3.1.1	<i>Client-side Router setup</i>	<i>6</i>
3.1.2	<i>Server-side Router setup</i>	<i>6</i>
3.1.3	<i>RIST tunnel</i>	<i>6</i>
4	SETTING UP THE RECEIVER AT THE CENTER	7
4.1	SENTINEL PORT SETUP.....	7
4.1.1	<i>First Time Connection.....</i>	<i>7</i>
4.1.2	<i>New Management IP Address Setup.....</i>	<i>8</i>
4.1.3	<i>Receiver device Data Ports Setup.....</i>	<i>10</i>
4.2	CREATING A RIST SERVER	13
4.2.1	<i>Create a RIST server</i>	<i>13</i>
4.2.2	<i>Create Certificates.....</i>	<i>16</i>
4.3	ADDING A STREAM	19
4.3.1	<i>Steps.....</i>	<i>19</i>
4.3.2	<i>Set the Stream to RIST mode.....</i>	<i>23</i>
5	SETTING UP THE TRANSMITTER AT THE REMOTE SITE.....	24
5.1	DVG PORT SETUP	24
5.1.1	<i>First Time Connection.....</i>	<i>24</i>
5.1.2	<i>New Management IP Address Setup.....</i>	<i>25</i>
5.1.3	<i>DVG Data Ports Setup</i>	<i>26</i>
5.2	CREATING A RIST TUNNEL	30
5.2.1	<i>Create a RIST tunnel.....</i>	<i>30</i>
5.3	ADDING A STREAM	33
5.3.1	<i>Add Stream.....</i>	<i>33</i>
5.3.2	<i>Set the Stream to RIST mode.....</i>	<i>36</i>
5.3.3	<i>Verify Stream Configuration in the transmitter</i>	<i>38</i>
5.3.4	<i>Verify Stream Configuration in the Receiver</i>	<i>39</i>

1 Scope

This quick start guide provides fundamental information on how to configure a RIST 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 RIST reliable protection protocol. Both Protector and Sentinel require three steps setup:

1. Interfaces setup
2. Stream setup
3. Encrypted RIST tunnel 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 RIST Server
 - c. Setup verification
2. Transmitter setup
 - a. Interfaces
 - b. Stream setup as an RIST 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 RIST Server and the Transmitter as RIST Client .

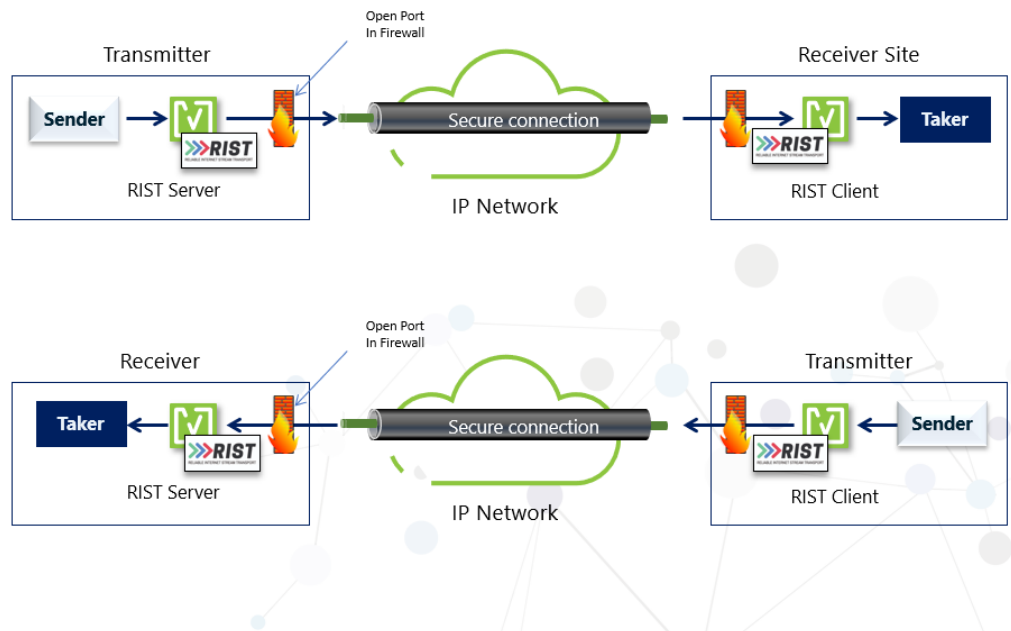
At the end of the process, the two devices will communicate and will protect the quality of a multicast stream.

3 VideoFlow's RIST Solution

This section provides an introduction to VideoFlow's RIST implementation. The Reliable Internet Secure Transport (RIST) is an open specification protocol spear headed by VideoFlow. This is a new protocol supported by many companies to connect over unmanaged networks. The RIST 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 RIST input and RIST output. To Date VideoFlow implemented two flavors: Simple RIST sender/receiver (no tunneling and encryption) and RIST MAIN profile DTLS encrypted tunnel. The RIST protocol allows other vendor solution supporting RIST to connect to a DVG as a transmitter or Receiver. Open source tools like VLC, OBS and FFMPEG will include built in RIST support.

➤ RIST (Reliable Internet Streaming Transport) ➤ Open Specification

- Server Client architecture
- Client calls home to connect with the Server
- Each side can be sender or receiver
- Caller/Listener functions
- Each link can be of may functions: sender, receiver and support multiple streams
- Secure and encrypted unidirectional connection
- Two Encryption options:
 - DTLS with AES-128/256 support
 - PSK with AES- 128/256 support
- Authentication
 - Certificates and optional SRP
- Took a lot of VideoFlow technology capabilities:
 - NPD
 - Inband traffic
 - Bi-directional streaming



The RIST includes its own buffering for the purpose of transmission and receiving. The user is allowed to set the delay configuration to the buffer. The basic underlined protocol of RIST is RTP for media and RTCP for command and communication, based on the guidance or TSovIP.

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

The Architecture is composed of two elements; An RIST server and RIST client. The RIST Server requires a reachable static IP address which is used as an anchor for the clients wishing to establish connection with the server. The RIST client can use any interface or media to connect to the Server. Each RIST 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).

A RIST main tunnel support full datagram, and requires the use of an internal Subnet and IP allocation for both sides.



NOTE

The RIST Server should be set in a location where it can be reachable. Its IP address shall be static. The RIST Client can be set anywhere.

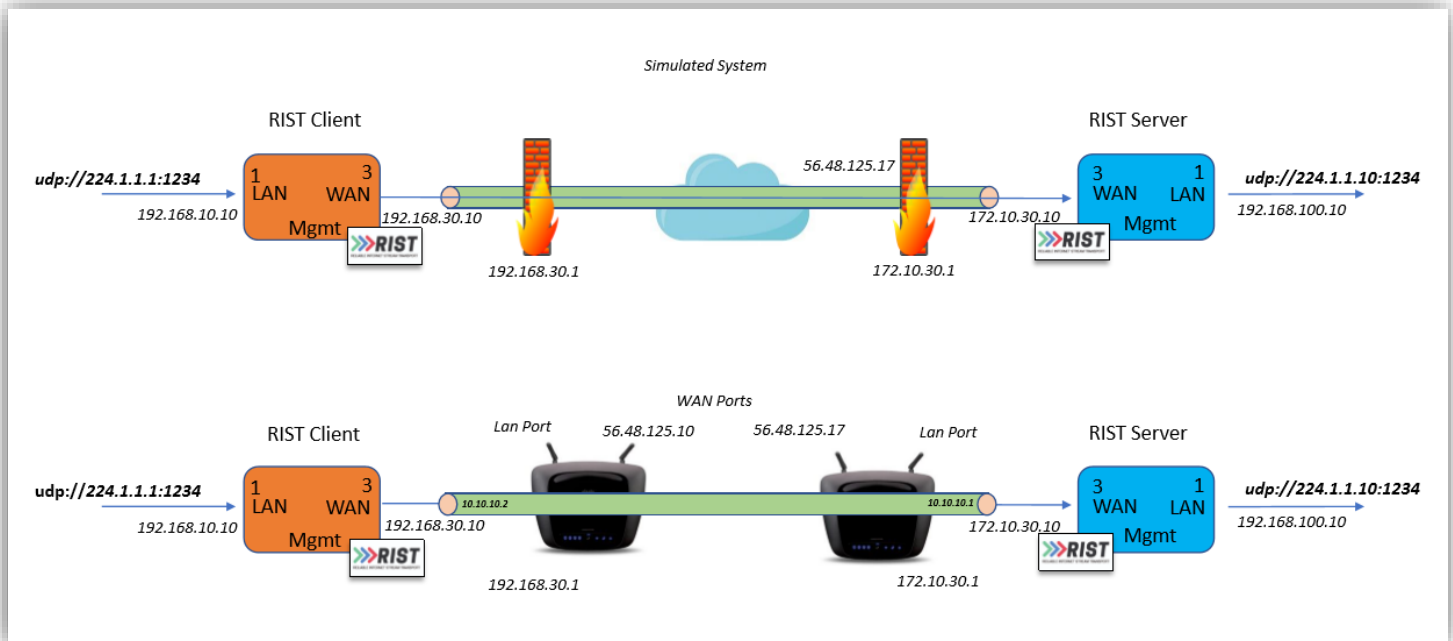
In a contribution network architecture will normally be multipoint-to-point where many Transmitters are connecting to a central Receiver. Therefore, RIST Server will be set in the Receiver; the RIST client in the Transmitter.

In a distribution network architecture will normally be point-to multipoint were one central Transmitter in connecting too many Receivers. Therefore, the RIST Server will be set in the transmitter and many RIST 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 illustrates the Simulated System and its implementation in the lab using of 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.

3.1.3 RIST tunnel

Client side inner IP address: 10.10.10.2

Server side Inner IP address: 10.10.10.1

4 Setting Up the Receiver at the Center

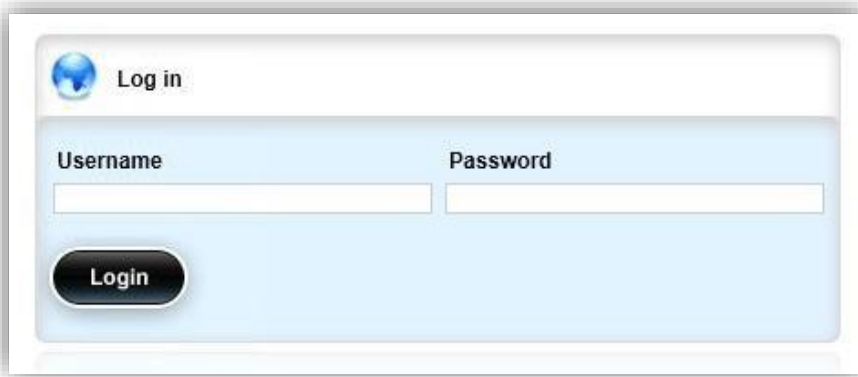
This section will describe the procedure required for configuring the Sentinel/Receiver at the center. The Receiver will act as the Server to the transmitters connecting to it from remote location.

4.1 Sentinel Port Setup

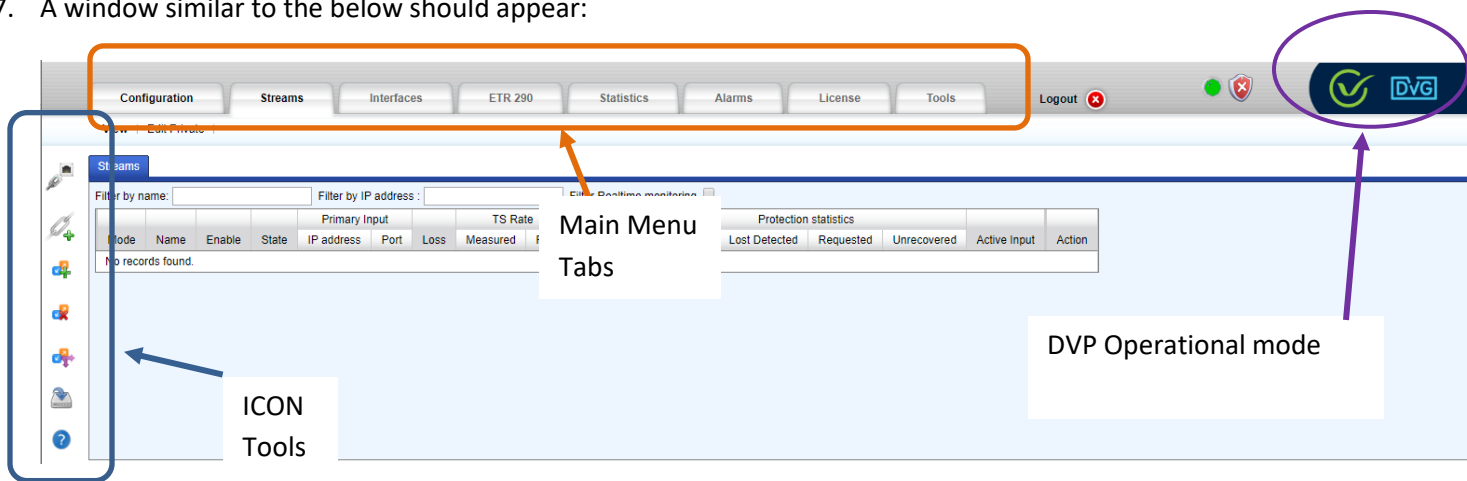
The default DVP factory management IP address is: 10.0.0.200.

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:

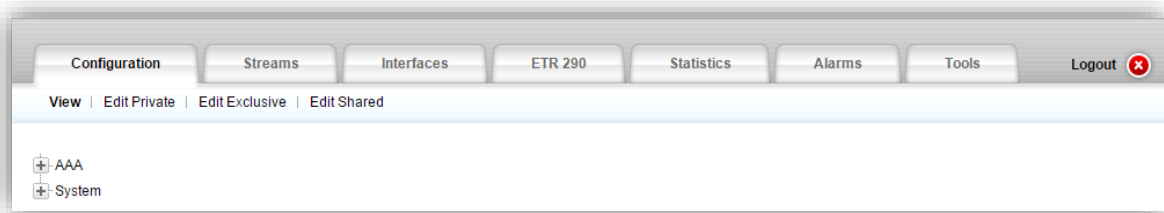


NOTE

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

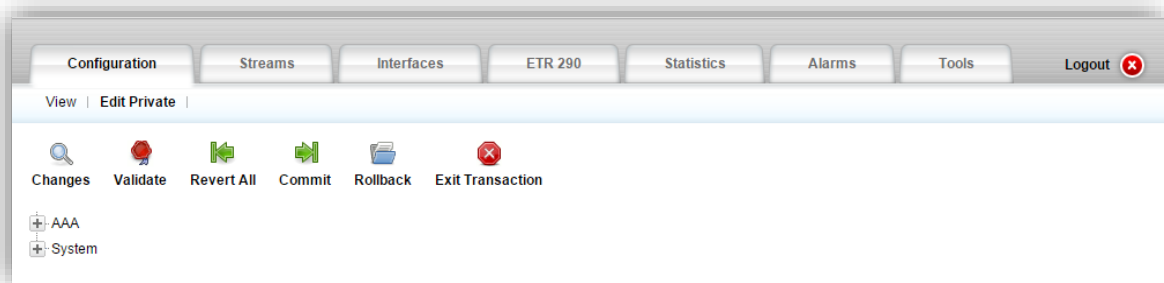
8. Click on the Configuration tab

9. A new page will appear:

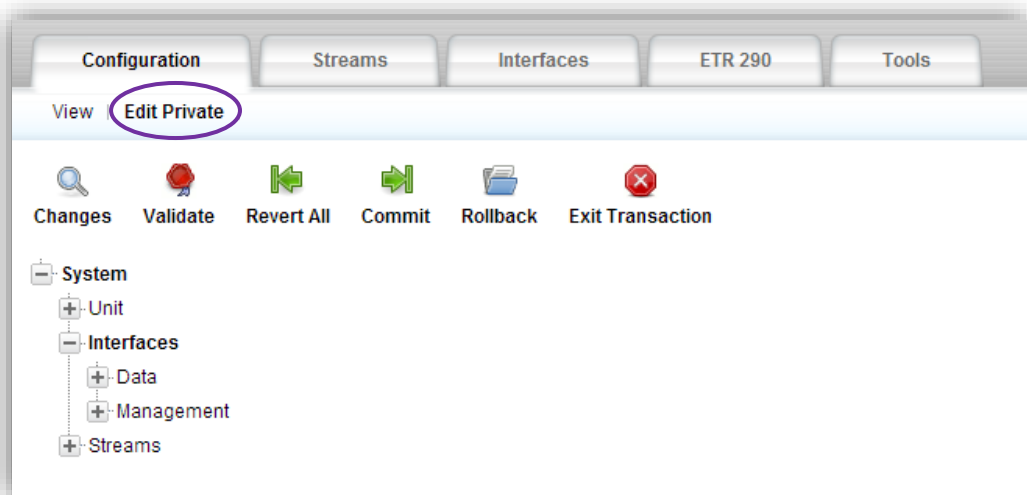


4.1.2 New Management IP Address Setup

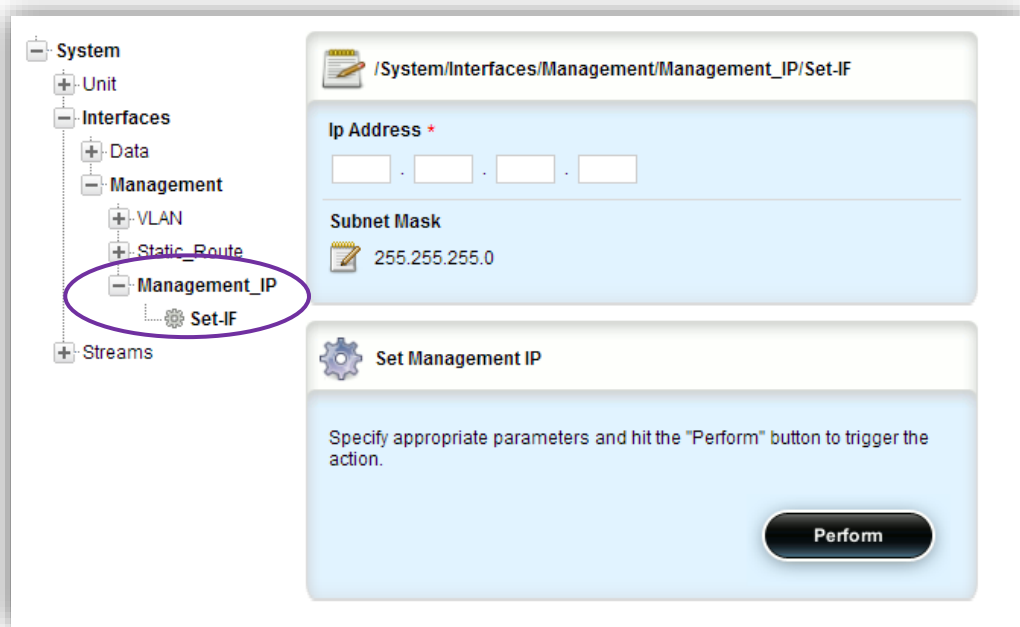
1. Click on the **Edit Private** mode



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

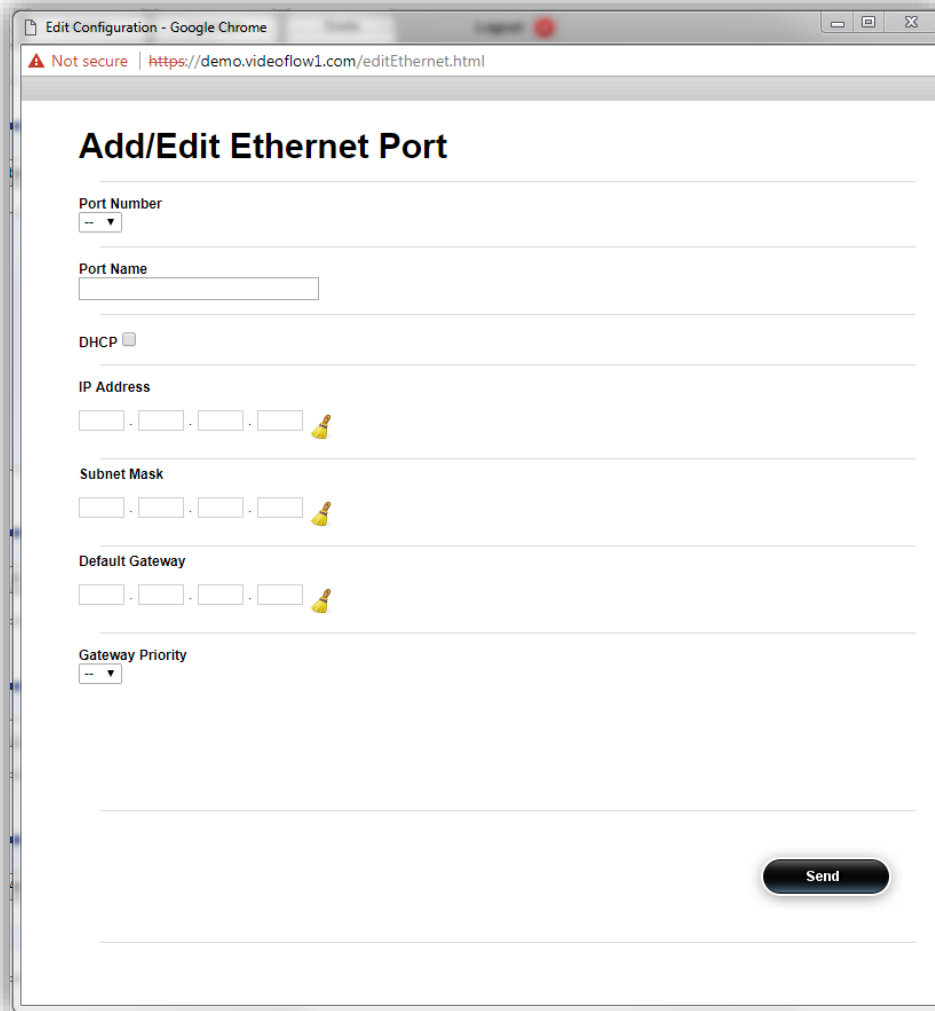


4. Type a new management IP address if required
5. Modify the management Subnet Mask if required
6. Click on the Perform button to apply the changes
7. The PC and the DVG will disconnect in the case of management IP and/or subnet mask change. Follow the below procedure to reconnect:
 - a. Close the browser 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



Edit Configuration - Google Chrome


Not secure | <https://demo.videoflow1.com/editEthernet.html>


Add/Edit Ethernet Port


Port Number
-- ▾

Port Name

DHCP ☐

IP Address
 . . . 

Subnet Mask
 . . . 

Default Gateway
 . . . 

Gateway Priority
-- ▾

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

Add/Edit Ethernet Port

Port Number

3 ▼

Port Name

WAN

DHCP ☐

IP Address

172 . 10 . 30 . 10 🔔

Subnet Mask

255 . 255 . 255 . 0 🔔

Default Gateway

172 . 10 . 30 . 1 🔔

Gateway Priority

▼

Send

To complete configuration click on the 'Send' button to apply the configuration changes

- Repeat the same steps to configure Port1 (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

Add/Edit Ethernet Port

Port Number: 1

Port Name: LAN

DHCP: ☐

IP Address: 192 . 168 . 10 . 10

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: . . .

Gateway Priority:

Send

- Check the stream connectivity

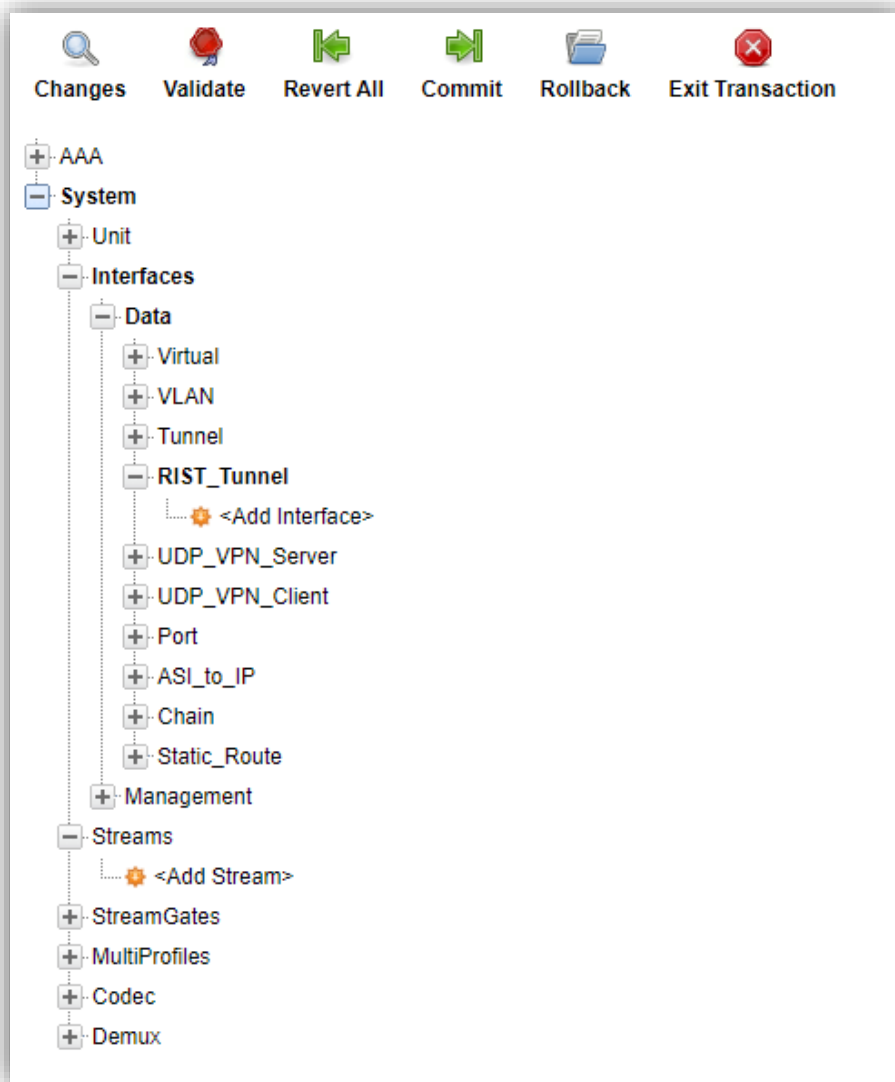
Press the Interfaces TAB to expose:

Configuration Streams Interfaces ETR 290 Statistics Alarms License Tools Logout											
View Edit Private Edit Exclusive Edit Shared											
Ports Vlan Virtual											
Filter by Port:											
Port	Enable	IP address	Subnet mask	Default Gateway	DHCP enable	MAC	Link	Speed	Dynamic IP address	Dynamic default GW	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

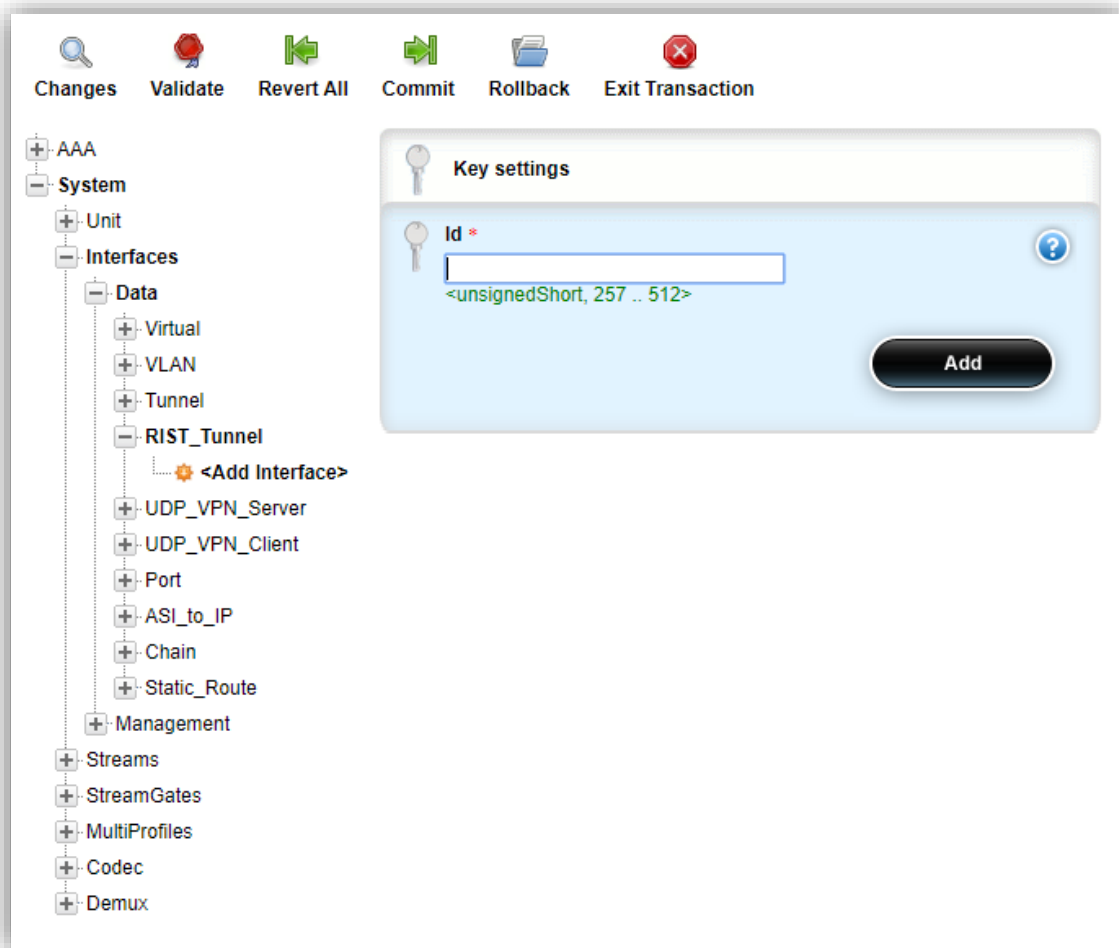
4.2 Creating a RIST Server

4.2.1 Create a RIST server

Go to the Configuration Tab, expand the Interfaces followed by **RIST_Tunnel**



Press **Add interface**,



Type an IF between 257 to 512, in this example we will use **257** and press the **Add button** to continue.

A new window will open:

The screenshot displays a network configuration interface. On the left is a tree view with the following structure:

- AAA
- System
 - Unit
 - Interfaces
 - Data
 - Virtual
 - VLAN
 - Tunnel
 - RIST_Tunnel
 - <Add Interface>
 - 257
 - UDP_VPN_Server
 - UDP_VPN_Client
 - Port
 - ASI_to_IP
 - Chain
 - Static_Route
 - Management
 - Streams
 - StreamGates
 - MultiProfiles
 - Codec
 - Demux

The main panel on the right shows the configuration for the selected interface, `/System/Interfaces/Data/RIST_Tunnel/Interface`. It includes a 'Key settings' section at the top and a list of configuration parameters below:

- Key settings**
 - Id**: 257
- Enable**: ☒ Enabled (false)
- Name**: VPN257
- Mode ***: RIST_Server
- Port ***: 35000
- Bind Ip Address**: 172.10.30.10
- Peer Inner Ip Address**: 10.10.10.2
- Local Inner Ip Address**: 10.10.10.1
- Encryption Mode**: DTLS (None)
- Encryption**: AES-256/AES-128 (AES-256/AES-128)

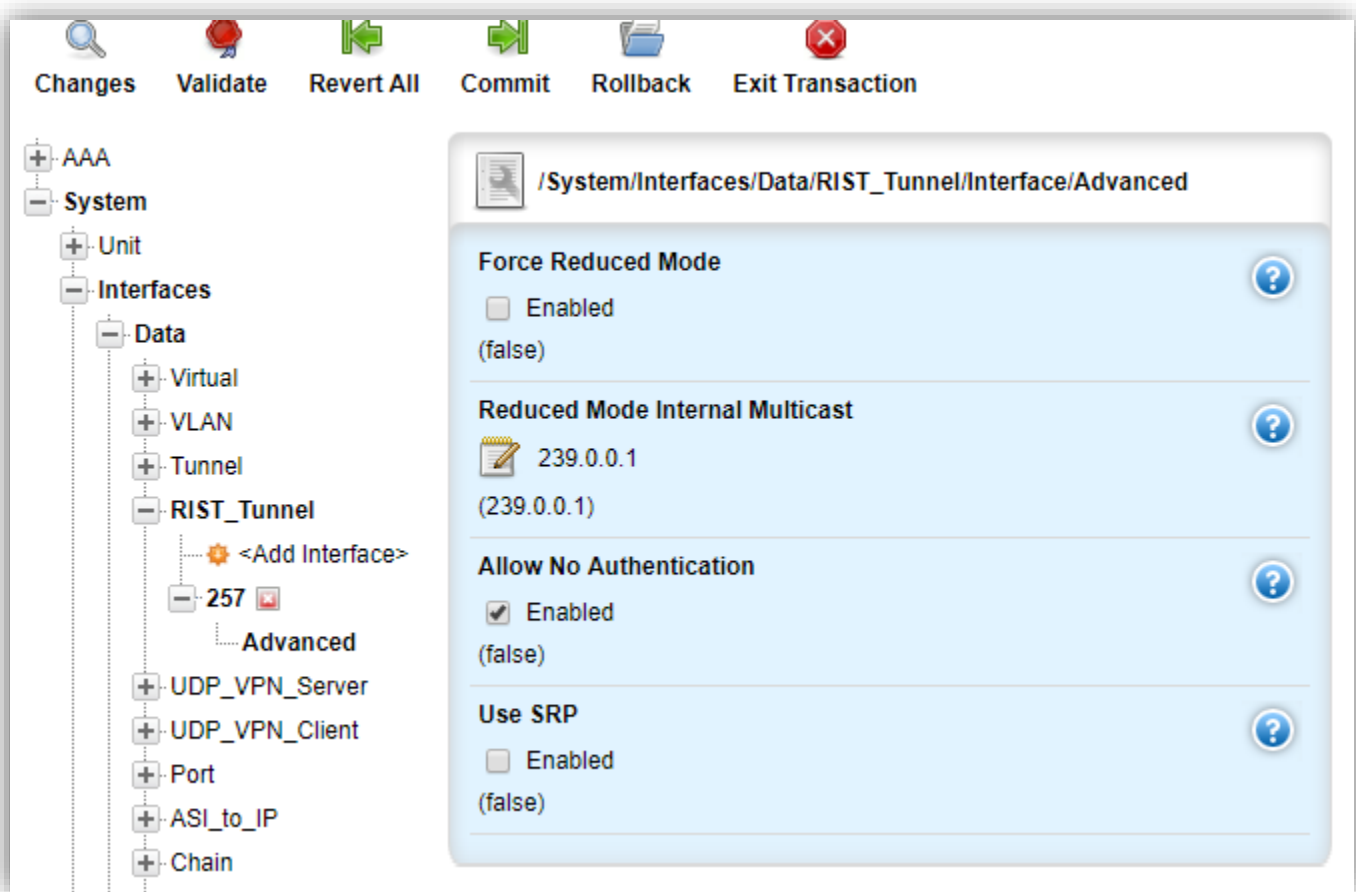
4.2.1.1 Configure the tunnel:

1. Set Enable
2. Configure a Name : **VPN257**
3. Set Mode to **RIST_Server**
4. Configure Port to be **35000** (for this setup)
5. Configure a Bind IP address to use the WAN port in this setup: **172.10.30.10**
6. Configure Peer Inner IP address: **10.10.10.2**
7. Configure Peer Inner IP address: **10.10.10.1**
8. Set encryption mode to be **DTLS**
9. Set encryption mode to be **AES-256/AES-128**

4.2.1.2 Configure Advance features

For this setup we will not authenticate the client certificates, and so the user is advised to expand the **Advanced** leaf

And select the 'Allow No Authentication'



Press **Commit**

4.2.2 Create Certificates

With DTLS encryption we need to create Server and Client self-Signed certificates.

4.2.2.1 Certificate creation

Open the Create certificate page: Go to **Tools** TAB, Select **File Operations** followed by **RIST Tunnel**, Select **generate certificates**.

The following window will open:

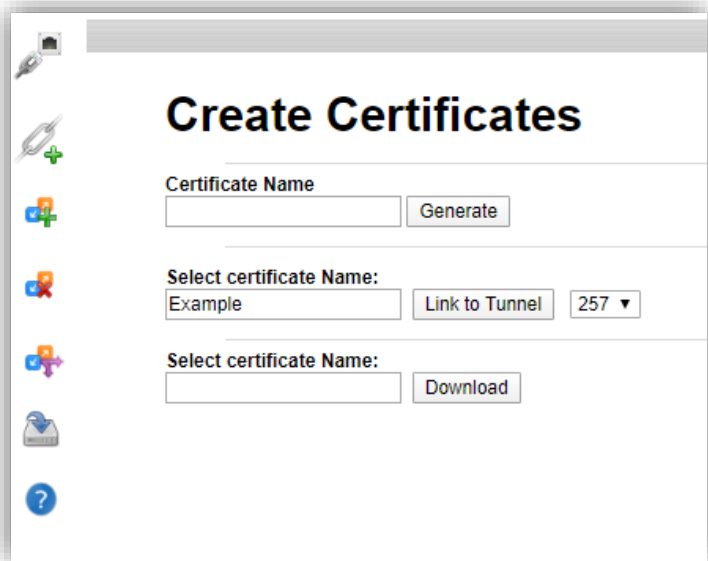
Assign a name to the certificate under the **Certificate Name**, in this example we will use 'Example' as the name

And Press the **Generate button**, the SW will create an internal certificate.

4.2.2.2 *Linking to Tunnel*

Return to the same location.

Under the **Select certificate Name**, re-enter the Name 'Example' and select ID 257



The image shows a web browser window with a title bar and a sidebar on the left containing several icons: a key, a plus sign, a plus sign with a checkmark, a plus sign with a red X, a plus sign with a checkmark and a plus sign, a folder, and a question mark. The main content area has a heading "Create Certificates". Below the heading, there are three sections. The first section is labeled "Certificate Name" and contains a text input field and a "Generate" button. The second section is labeled "Select certificate Name:" and contains a text input field with the value "Example", a "Link to Tunnel" button, and a dropdown menu with the value "257" and a downward arrow. The third section is labeled "Select certificate Name:" and contains a text input field and a "Download" button.

Create Certificates

Certificate Name
 [Generate](#)

Select certificate Name:
 [Link to Tunnel](#) 257 ▼

Select certificate Name:
 [Download](#)


And Press the Link to Tunnel, the SW will tie the certificates to the 257 tunnel.

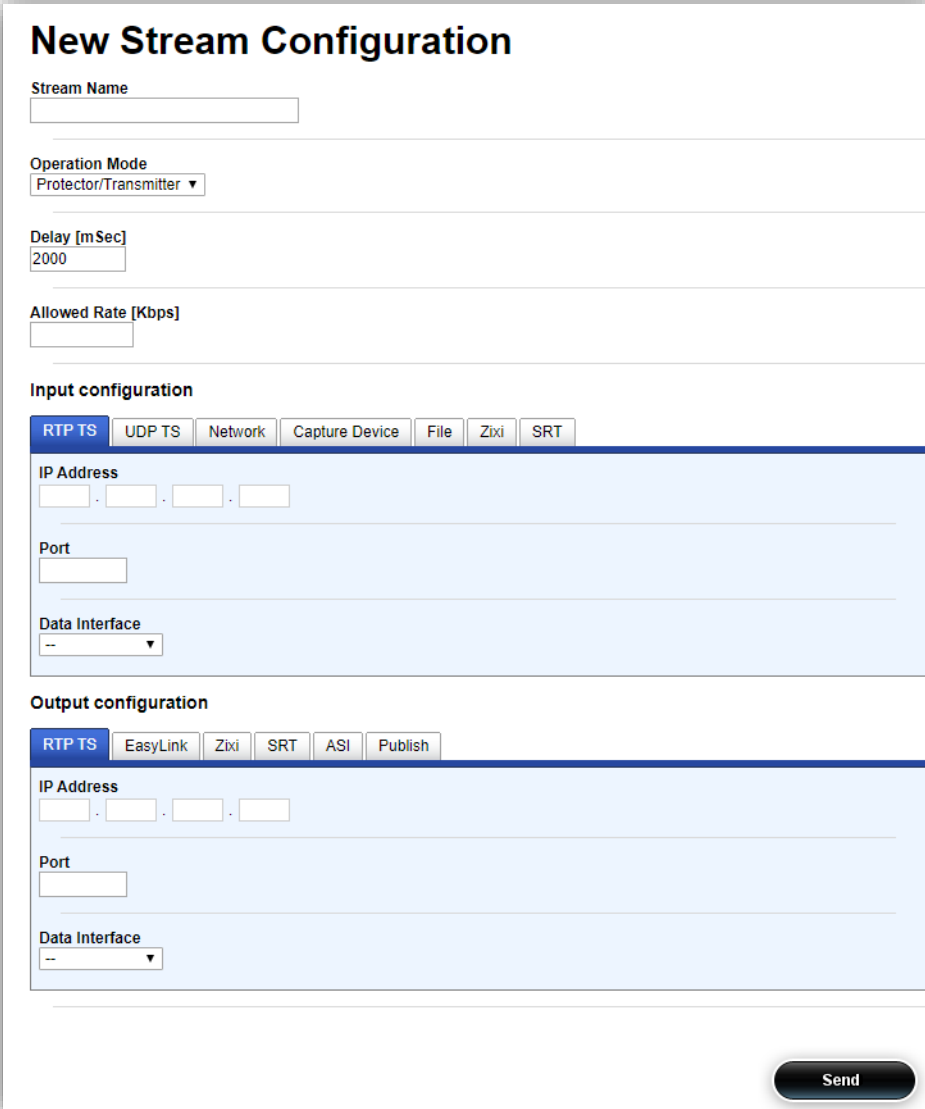
4.3 Adding a Stream

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 RIST output and interface properties Add Stream

4.3.1 Steps

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



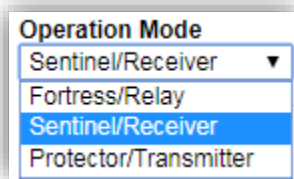
The 'New Stream Configuration' window is a form for setting up a new stream. It has a title bar and a main content area. The form is divided into several sections:

- Stream Name:** A text input field.
- Operation Mode:** A dropdown menu with 'Protector/Transmitter' selected.
- Delay [mSec]:** A text input field with '2000' entered.
- Allowed Rate [Kbps]:** A text input field.
- Input configuration:** A section with a tabbed interface. The 'RTP TS' tab is selected. It contains:
 - IP Address:** Four text input fields for IP address components.
 - Port:** A text input field.
 - Data Interface:** A dropdown menu with '--' selected.
- Output configuration:** A section with a tabbed interface. The 'RTP TS' tab is selected. It contains:
 - IP Address:** Four text input fields for IP address components.
 - Port:** A text input field.
 - Data Interface:** A dropdown menu with '--' selected.

A 'Send' button is located at the bottom right of the window.

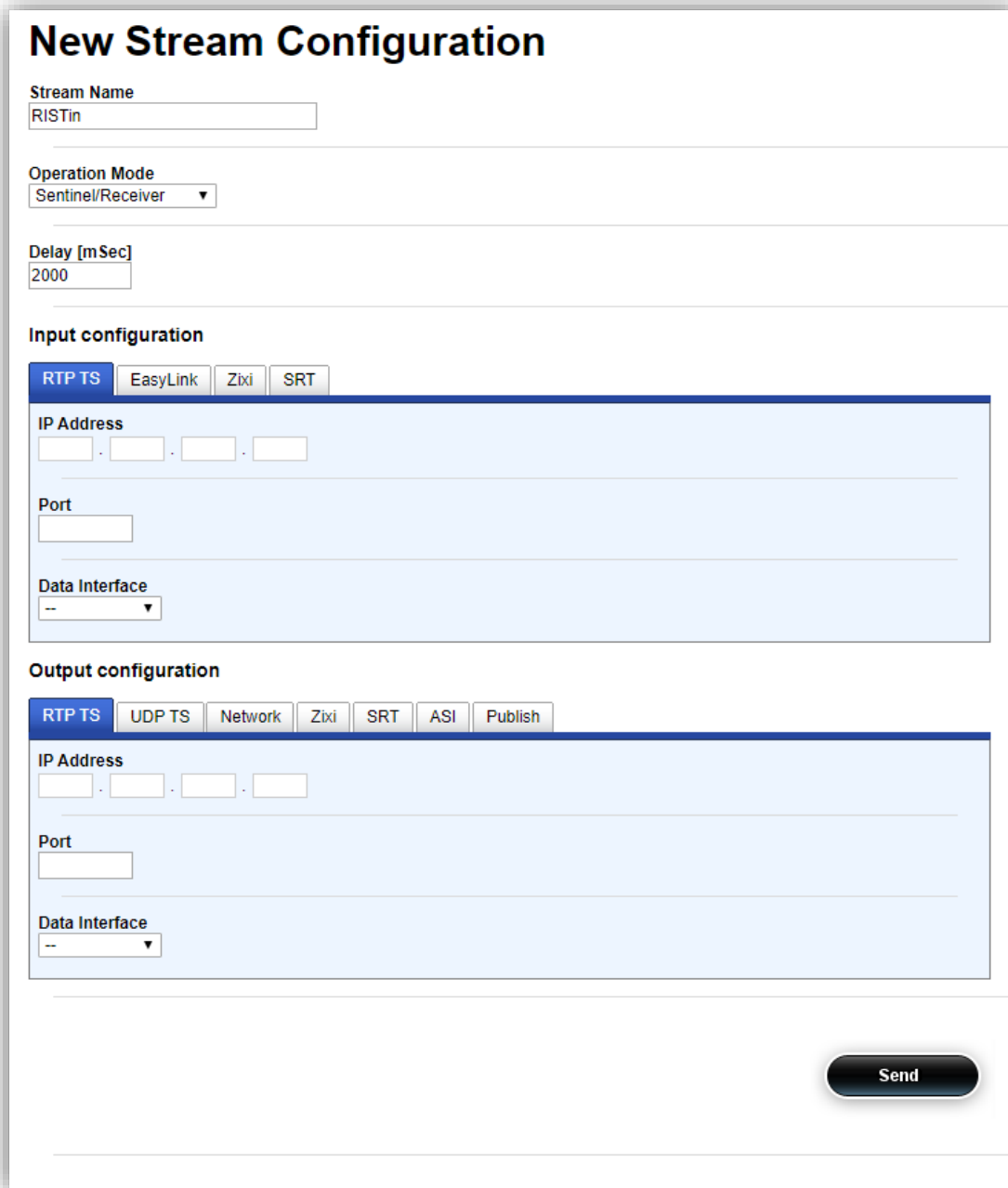
2. Set a name for the stream, in this case 'RISTin'

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



A dropdown menu titled "Operation Mode" with four options: "Sentinel/Receiver", "Fortress/Relay", "Sentinel/Receiver", and "Protector/Transmitter". The "Sentinel/Receiver" option is highlighted in blue.

4. The Window will change its appearance to;



A screenshot of the "New Stream Configuration" window. The window has a title bar and a main content area. The title "New Stream Configuration" is in large, bold, black font. Below the title, there are several input fields and a dropdown menu. The "Stream Name" field contains "RISTin". The "Operation Mode" dropdown menu is set to "Sentinel/Receiver". The "Delay [mSec]" field contains "2000". Below these fields, there are two sections: "Input configuration" and "Output configuration". Each section has a tabbed interface with "RTP TS" selected. The "Input configuration" section has fields for "IP Address" (four empty boxes), "Port" (one empty box), and "Data Interface" (a dropdown menu). The "Output configuration" section has fields for "IP Address" (four empty boxes), "Port" (one empty box), and "Data Interface" (a dropdown menu). At the bottom right of the window, there is a "Send" button.

5. Configure the stream's **Input configuration** parameters:
 - a. Select the **RTP** TAB
 - b. Configure the incoming IP address to 224.1.1.1
 - c. Configure the incoming RTP port to 1234

- d. Configure the Data Interface to be **VPN257**
- 6. Configure the stream's **Output configuration** parameters:
 - a. Select the **UDP TS** TAB
 - b. Set the IP address to **224.1.1.10**
 - c. Set the Port to **1234**
 - d. Select the output interface from a pull-down menu, in this example select the **LAN**

New Stream Configuration

Stream Name

RISTIn

Operation Mode

Sentinel/Receiver

Delay [mSec]

2000

Input configuration

RTP TS

EasyLink

Zixi

SRT

IP Address

224

.

1

.

1

.

1

Port

1234

Data Interface

VPN257

Output configuration

RTP TS

UDP TS

Network

Zixi

SRT

ASI

Publish

IP Address

224

.

1

.

1

.

10

Port

1234

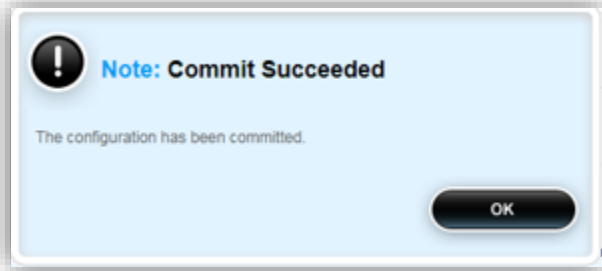
Data Interface

LAN

Send

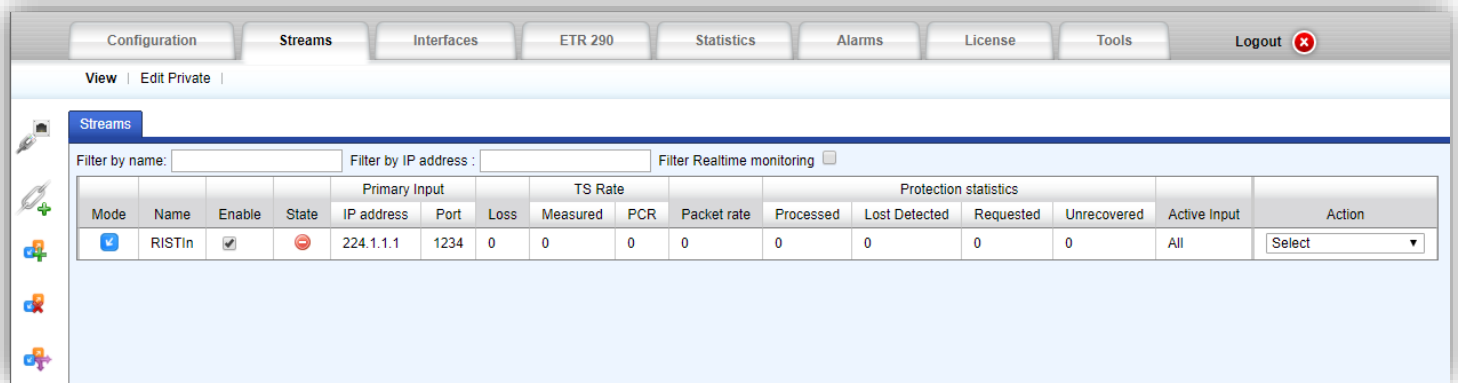
- e. Press Send when done

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).

4.3.2 Set the Stream to RIST mode

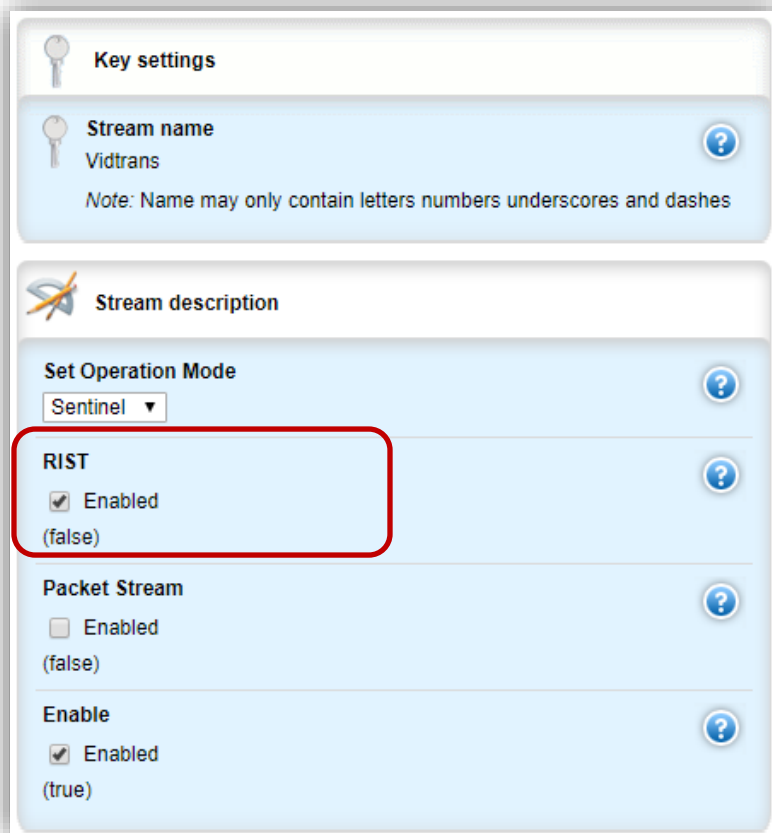
One last step is to set the Stream to work in RIST mode.

To do that go to the Configuration Tab

Press '**Edit Private**'

Expand the **Unit, Streams** and press the '**RISTin**' stream name to expose the stream configuration window:

Check the RIST check box



The image shows a configuration window for a stream named 'Vidtrans'. It is divided into two main sections: 'Key settings' and 'Stream description'. In the 'Key settings' section, the 'Stream name' is 'Vidtrans'. In the 'Stream description' section, there are three settings: 'Set Operation Mode' (a dropdown menu currently set to 'Sentinel'), 'RIST' (a checkbox that is checked, with '(false)' below it), and 'Packet Stream' (a checkbox that is unchecked, with '(false)' below it). At the bottom of the 'Stream description' section, there is an 'Enable' checkbox that is checked, with '(true)' below it. A red rectangle highlights the 'RIST' checkbox and its label.

Section	Setting	Value
Key settings	Stream name	Vidtrans
	Note	Name may only contain letters numbers underscores and dashes
Stream description	Set Operation Mode	Sentinel
	RIST	<input checked="" type="checkbox"/> Enabled (false)
	Packet Stream	<input type="checkbox"/> Enabled (false)
	Enable	<input checked="" type="checkbox"/> Enabled (true)



Finish by pressing the Commit Icon **Commit** on Top

5 Setting Up the Transmitter at the Remote Site

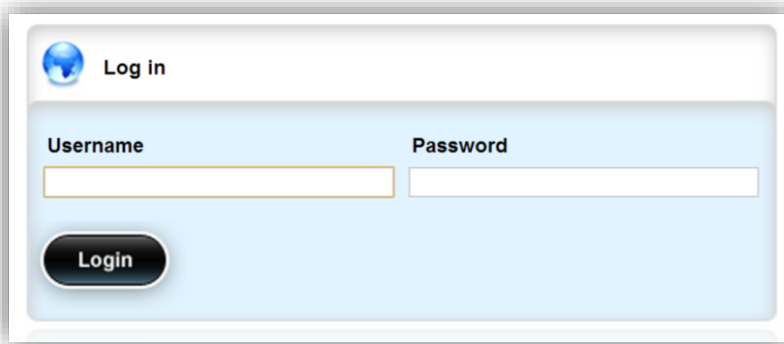
This section will describe the procedure required for configuring the Protector at the remote site. The DVG will act as the Client to connect to the remote peer DVG device.

5.1 DVG Port Setup

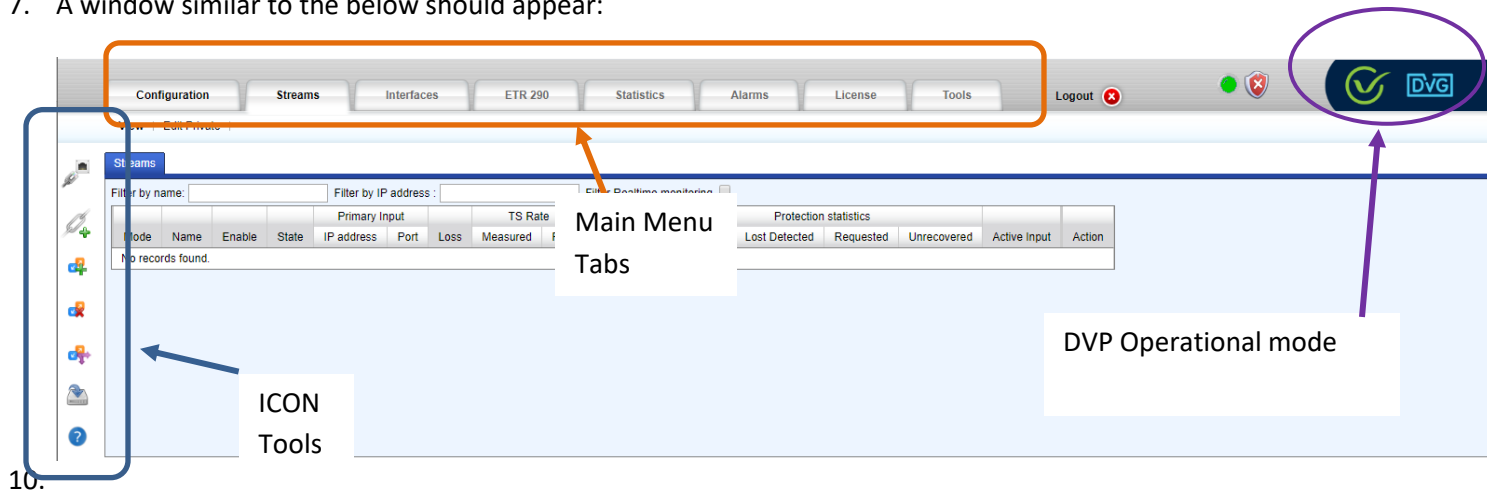
The default device factory management IP address is: 10.0.0.200.

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.

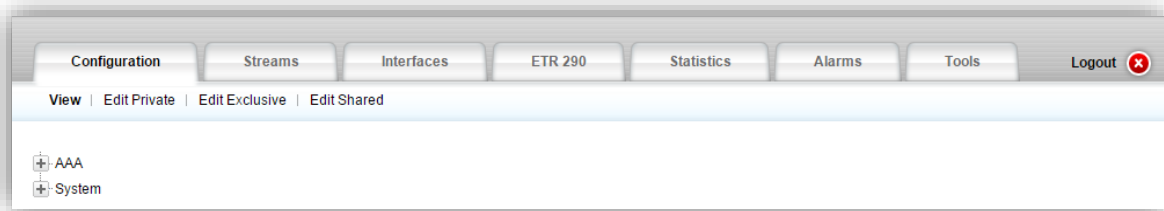


NOTE

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

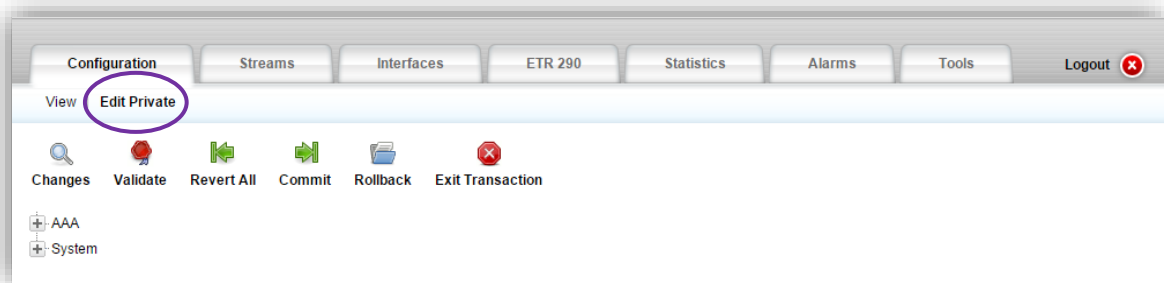
8. Click on the Configuration tab

9. A new page will appear:

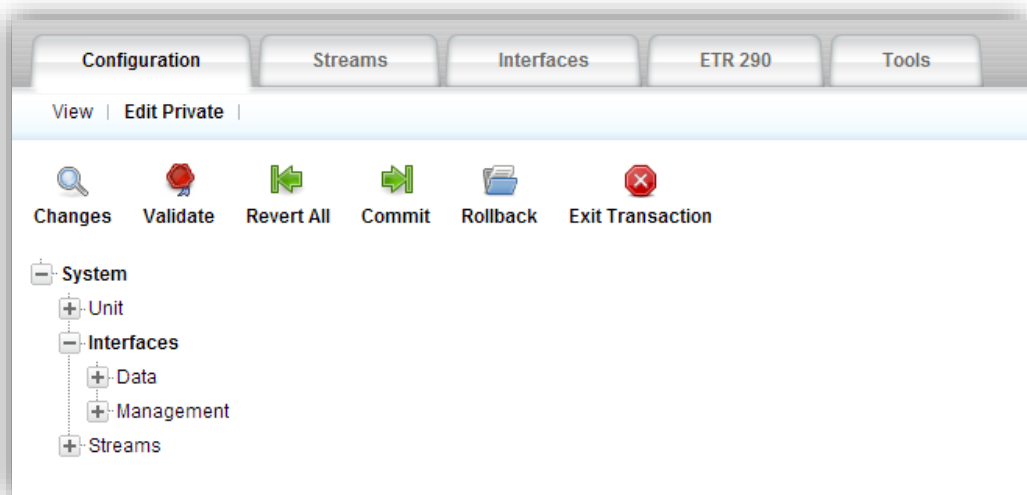


5.1.2 New Management IP Address Setup

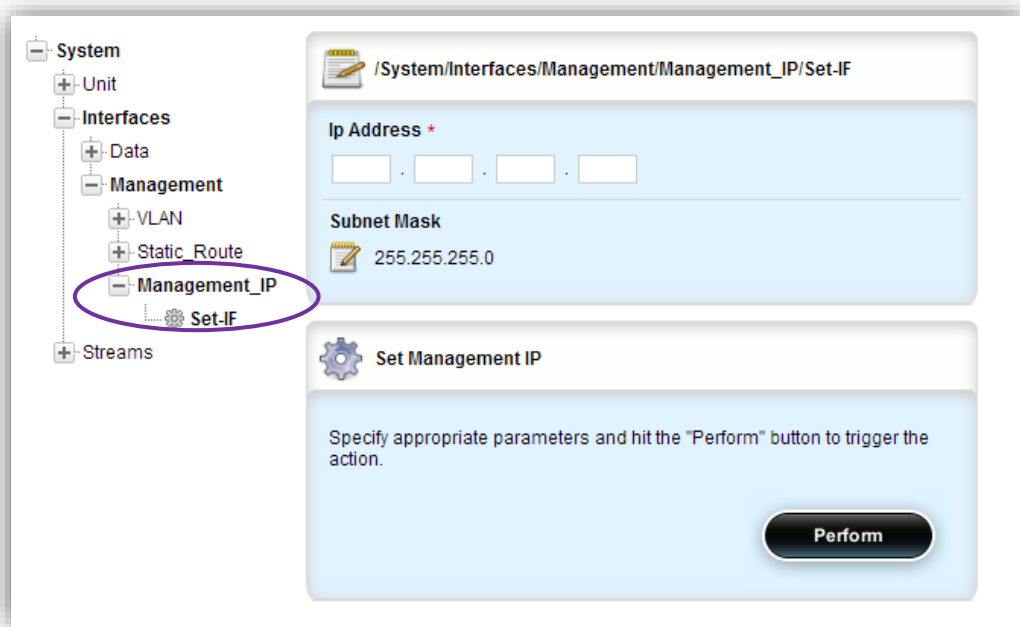
1. Click on the Edit Private mode.



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

Edit Configuration - Google Chrome

Not secure | <https://demo.videoflow1.com/editEthernet.html>

Add/Edit Ethernet Port

Port Number
-- ▾

Port Name

DHCP ☐

IP Address
 . . . 🔔

Subnet Mask
 . . . 🔔

Default Gateway
 . . . 🔔

Gateway Priority
-- ▾

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

Add/Edit Ethernet Port

Port Number

3 ▼

Port Name


WAN

DHCP ☐

IP Address

192 . 168 . 30 . 10 

Subnet Mask

255 . 255 . 255 . 0 

Default Gateway

192 . 168 . 30 . 1 

Gateway Priority

▼

Send

To complete configuration click on the 'Send' button to apply the configuration changes

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

Add/Edit Ethernet Port

Port Number
1 ▼

Port Name
LAN

DHCP ☐

IP Address
192 . 168 . 10 . 10 🔔

Subnet Mask
255 . 255 . 255 . 0 🔔

Default Gateway
 . . . 🔔

Gateway Priority
▼

Send

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.

- Check the connectivity,

Configuration

Streams

Interfaces

ETR 290

Statistics

Alarms

License

Tools

Logout

View

Edit Private

Ports

Vlan

Virtual

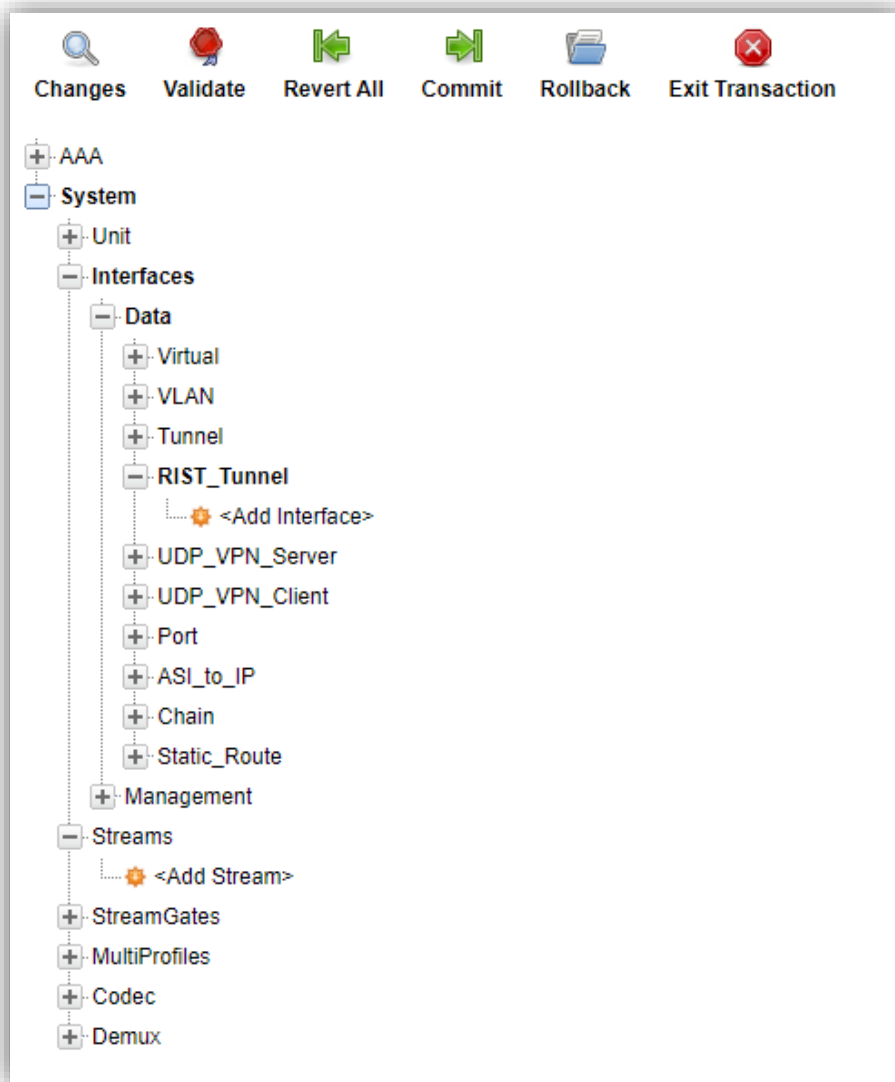
Filter by Port:

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

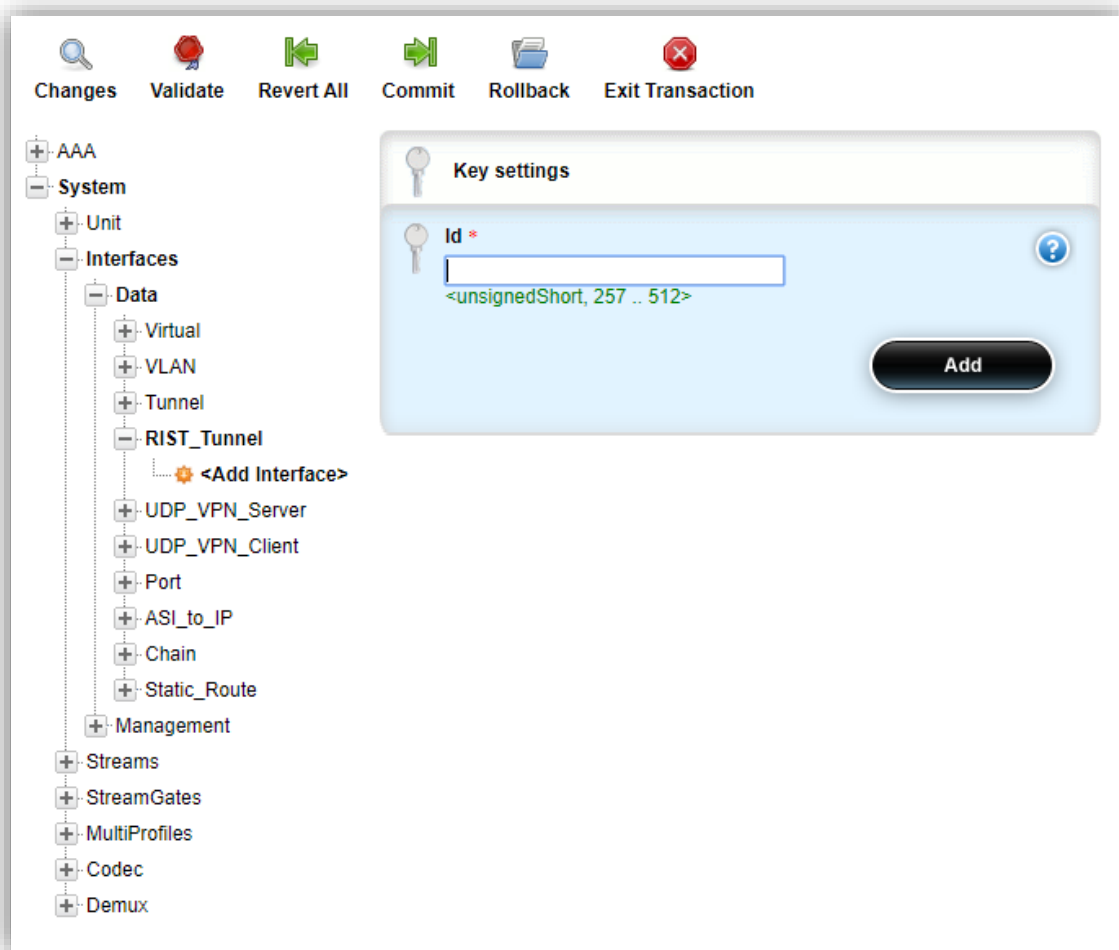
5.2 Creating a RIST Tunnel

5.2.1 Create a RIST tunnel

Go to the Configuration Tab, expand the Interfaces followed by **RIST_Tunnel**

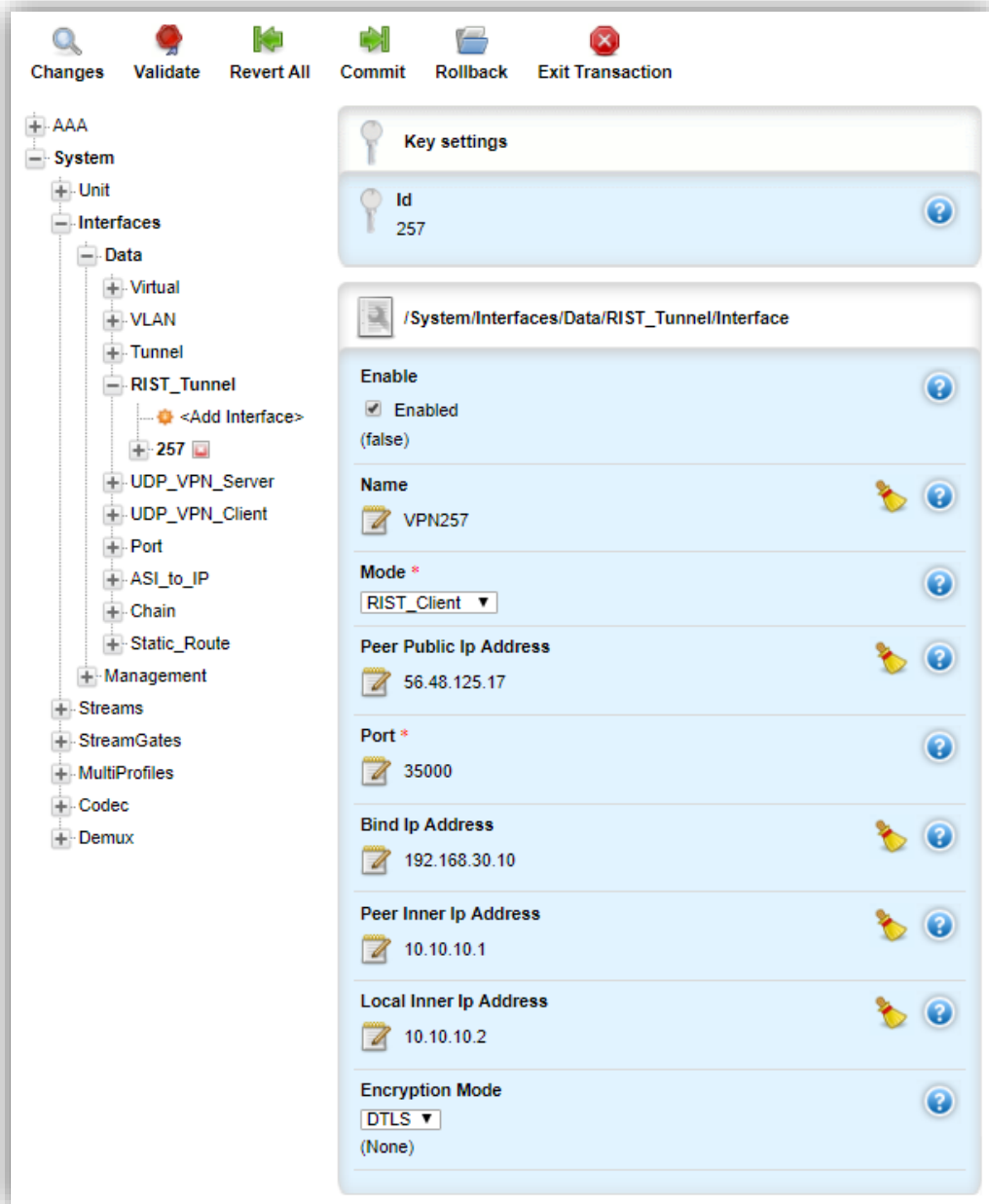


Press **Add interface**,



Type an IF between 257 to 512, in this example we will use **257** and press the **Add button** to continue.

A new window will open:



Configure the tunnel:

1. Set Enable
2. Configure a name : **VPN257**
3. Set Mode to **RIST_Client**
4. Configure IP to be **56.48.125.17**
5. Configure Port to be **35000** (for this setup)
6. Configure a Bind IP address to use the WAN port in this setup: **192.168.30.10**
7. Configure Peer Inner IP address: **10.10.10.1**
8. Configure Peer Inner IP address: **10.10.10.2**
9. Set encryption mode to be **DTLS**


Press **Commit**

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:

New Stream Configuration

Stream Name

Operation Mode

Protector/Transmitter ▾

Delay [mSec]

2000

Allowed Rate [Kbps]

Input configuration

RTP TS

UDP TS

Network

Capture Device

File

Zixi

SRT

IP Address

Port

Data Interface

-- ▾

Output configuration

RTP TS

EasyLink

Zixi

SRT

ASI

Publish

IP Address

Port

Data Interface

-- ▾

Send

2. Set a name for the stream, in this case 'RISTout'
3. Configure the stream's **Input configuration** parameters:
 - a. Select **UDP TS** TAB
 - b. Configure Ip according to the stream's destination IP address (**224.1.1.1** in this example)
 - c. Configure Port according to the stream's UDP port (1234 in this example)
 - d. Select the Data interface from the Input Interface Name drop down menu (**LAN** in our example)
4. Configure the stream's **Output configuration RTP TAB** parameters:
 - a. Configure the IP address: **224.1.1.1**
 - b. Configure the UDP port: **1234**
 - c. Date Interface: **VPN257**

New Stream Configuration

Stream Name

RISTout

Operation Mode

Protector/Transmitter ▼

Delay [mSec]

2000

Allowed Rate [Kbps]

Input configuration

RTP TS

UDP TS

Network

Capture Device

File

Zixi

SRT

IP Address

224 . 1 . 1 . 1

Port

1234

Data Interface

LAN ▼

Output configuration

RTP TS

EasyLink

Zixi

SRT

ASI

Publish

IP Address

224 . 1 . 1 . 1

Port

1234

Data Interface

VPN257 ▼

Send

- d. Press **Send** button when done

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

New Stream Configuration

Stream Name
RISout

Operation Mode
Protector/Transmitter

Delay [mSec]
2000

Allowed Rate [Kbps]

Input configuration:

RTP TS **UDP TS** Network Capture Device File Zixi SRT

IP Address
224 . 1 . 1 . 1

Port
1234

Data Interface
LAN

Output configuration

RTP TS EasyLink Zixi SRT ASI Publish

IP Address
224 . 1 . 1 . 1

Port
1234

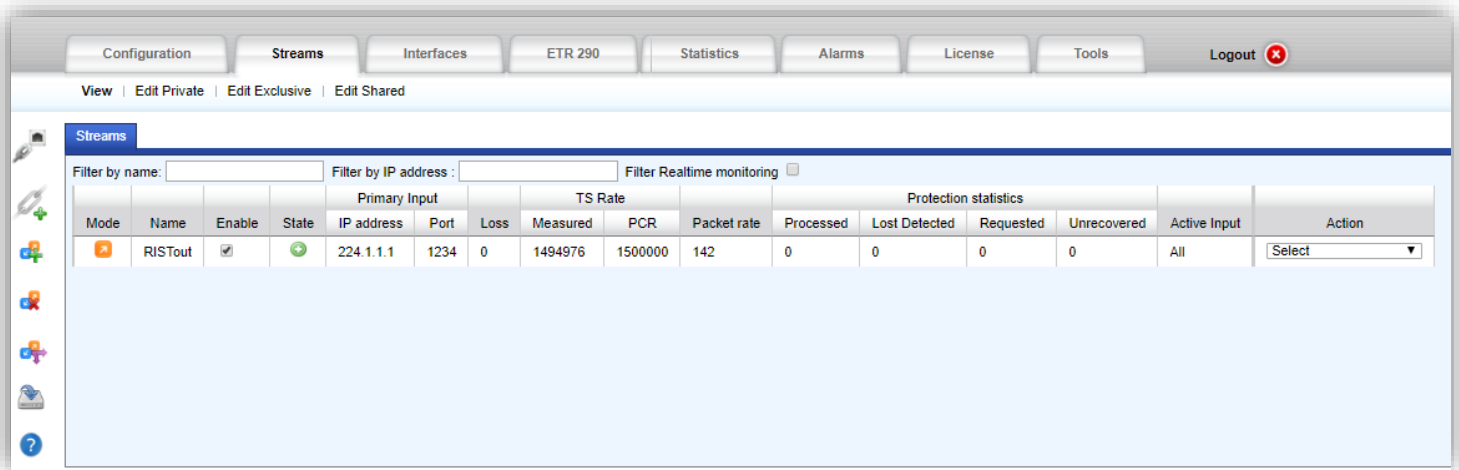
Data Interface
VPN257

Note: Commit Succeeded
The configuration has been committed.
OK

Send

11. Close the window

12. A new stream should appear:



5.3.2 Set the Stream to RIST mode


One last step is to set the Stream to work in RIST mode.


To do that go to the Configuration Tab

Press '**Edit Private**'

Expand the **Unit, Streams** and press the '**RISTout**' stream name to expose the stream configuration window:


Check the RIST check box

**Key settings**

**Stream name**

Vidtrans

Note: Name may only contain letters numbers underscores and dashes

**Stream description**

Set Operation Mode

Protector ▾

RIST

☒ Enabled

(false)

Packet Stream


☐ Enabled

(false)

Enable

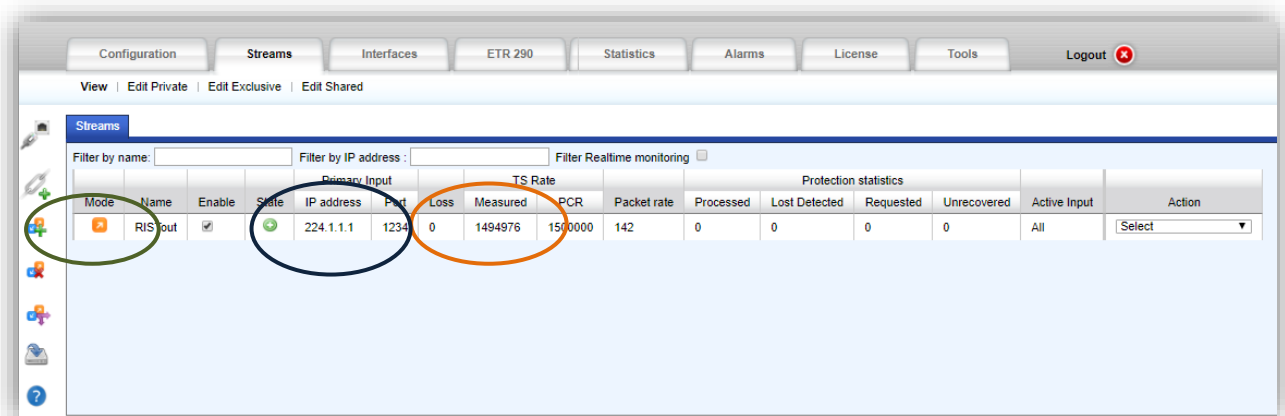
☒ Enabled

(true)

Finish by pressing the Commit Icon  **Commit** on Top

5.3.3 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

5.3.4 Verify Stream Configuration in the Receiver

Click on the Streams Tab from the Main Menu:

The screenshot shows a web-based interface for managing streams. At the top, there is a navigation bar with tabs: Configuration, Streams (selected), Interfaces, ETR 290, Statistics, Alarms, License, and Tools. A Logout button with a red 'x' icon is on the right. Below the navigation bar, there is a sub-header with 'View' and 'Edit Private' links. The main content area is titled 'Streams' and contains a table of stream configurations. Above the table, there are filters: 'Filter by name:', 'Filter by IP address:', and 'Filter Realtime monitoring' (with a checkbox). The table has columns for Mode, Name, Enable, State, Primary Input (IP address, Port), Loss, TS Rate (Measured, PCR), Packet rate, Protection statistics (Processed, Lost Detected, Requested, Unrecovered), Active Input, and Action. A single stream named 'RISTin' is listed with the following values: Mode: RISTin, Enable: checked, State: green circle with a checkmark, IP address: 224.1.1.1, Port: 1234, Loss: 0, Measured: 1484448, PCR: 1500000, Packet rate: 141, Processed: 0, Lost Detected: 8, Requested: 8, Unrecovered: 0, Active Input: All, and Action: Select (dropdown). Below the table, a status bar indicates 'Total streams bitrate is 2 Mbit/s out of 45 Mbit/s, in 1 streams.'

Mode	Name	Enable	State	Primary Input		Loss	TS Rate		Packet rate	Protection statistics				Active Input	Action
				IP address	Port		Measured	PCR		Processed	Lost Detected	Requested	Unrecovered		
RISTin	RISTin	<input checked="" type="checkbox"/>		224.1.1.1	1234	0	1484448	1500000	141	0	8	8	0	All	Select ▼

Total streams bitrate is 2 Mbit/s out of 45 Mbit/s, in 1 streams.

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