570NAT-HW-X19
High Density Network Address Translator
User Manual

EVERTZ MICROSYSTEMS LTD.
5292 John Lucas Drive
Burlington, Ontario
Canada L7L 5Z9

Phone:	+1 905-335-3700	
Sales:	sales@evertz.com	Fax: +1 905-335-3573
Tech Support:	service@evertz.com	Fax: +1 905-335-7571
Web Page:	http://www.evertz.com	

Version 1.0, August 2020

The material contained in this manual consists of information that is the property of Evertz Microsystems and is intended solely for the use of purchasers of the 570NAT-HW-X19 series product. Evertz Microsystems expressly prohibits the use of this manual for any purpose other than the operation of the 570NAT-HW-X19 series product. Due to on going research and development, features and specifications in this manual are subject to change without notice.

This page left intentionally blank

IMPORTANT SAFETY INSTRUCTIONS

⚡	The lightning flash with arrowhead symbol within an equilateral triangle is intended to alert the user to the presence of uninsulated “Dangerous voltage” within the product’s enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.
⚠	The exclamation point within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance (Servicing) instructions in the literature accompanying the product.

- Read these instructions
- Keep these instructions.
- Heed all warnings.
- Follow all instructions.
- Do not use this apparatus near water
- Clean only with dry cloth.
- Do not block any ventilation openings. Install in accordance with the manufacturer’s instructions.
- Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
- Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than other. A grounding-type plug has two blades and a third grounding prong. The wide blade or the third prong is provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
- Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles and the point where they exit from the apparatus.
- Only use attachments/accessories specified by the manufacturer
- Unplug this apparatus during lightning storms or when unused for long periods of time.
- Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.

WARNING
TO REDUCE THE RISK OF FIRE OR ELECTRIC – SHOCK, DO NOT EXPOSE THIS APPARATUS TO RAIN OR MOISTURE

WARNING
DO NOT EXPOSE THIS EQUIPMENT TO DRIPPING OR SPLASHING AND ENSURE THAT NO OBJECTS FILLED WITH LIQUIDS ARE PLACED ON THE EQUIPMENT

WARNING
TO COMPLETELY DISCONNECT THIS EQUIPMENT FROM THE AC MAINS, DISCONNECT THE POWER SUPPLY CORD PLUG FROM THE AC RECEPTACLE

WARNING
THE MAINS PLUG OF THE POWER SUPPLY CORD SHALL REMAIN READILY OPERABLE

INFORMATION TO USERS IN EUROPE

NOTE

CISPR 22 CLASS A DIGITAL DEVICE OR PERIPHERAL

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to the European Union EMC directive. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

EN60065	Safety
EN55103-1: 1996	Emission
EN55103-2: 1996	Immunity

EN504192 2005
Waste electrical products should not be disposed of with household waste.
Contact your Local Authority for recycling advice

INFORMATION TO USERS IN THE U.S.A.

NOTE

FCC CLASS A DIGITAL DEVICE OR PERIPHERAL

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

WARNING

Changes or Modifications not expressly approved by Evertz Microsystems Ltd. could void the user’s authority to operate the equipment.

Use of unshielded plugs or cables may cause radiation interference. Properly shielded interface cables with the shield connected to the chassis ground of the device must be used.

REVISION HISTORY

REVISION	DESCRIPTION	DATE
1.0	First Release	Aug 2020

Information contained in this manual is believed to be accurate and reliable. However, Evertz assumes no responsibility for the use thereof nor for the rights of third parties, which may be affected in any way by the use thereof. Any representations in this document concerning performance of Evertz products are for informational use only and are not warranties of future performance, either expressed or implied. The only warranty offered by Evertz in relation to this product is the Evertz standard limited warranty, stated in the sales contract or order confirmation form.

Although every attempt has been made to accurately describe the features, installation and operation of this product in this manual, no warranty is granted nor liability assumed in relation to any errors or omissions unless specifically undertaken in the Evertz sales contract or order confirmation. Information contained in this manual is periodically updated and changes will be incorporated into subsequent editions. If you encounter an error, please notify Evertz Customer Service department. Evertz reserves the right, without notice or liability, to make changes in equipment design or specifications.

This page left intentionally blank

TABLE OF CONTENTS

Figures

This page left intentionally blank

1. OVERVIEW

The 570NAT–X19–10G is a high–density, multi–port, multi–flow hardware Network Address Translation (NAT) engine with enhanced features including port aggregation, tunneling, packet replication and bandwidth capping, allowing service providers to seamlessly bridge across networks in multi–tenant environments.

The 570NAT–X19–10G is organized as 6 WAN–side ports plus 6 LAN–side ports, with a packet processing core between each WAN–LAN pair. Each processing core can sustain up to 256 data flows, configurable based on multicasts or VLAN Tags. This gives an exceptional product density of 12x

10GbE ports, with 1536 multicast/VLAN flows — all in the space–efficient Evertz 570 modular hardware platform.

Multiple processing cores can be configured to aggregate their Tx traffic to a single WAN Port. Correspondingly, Rx traffic from that WAN port is distributed to its contributing processing cores. WAN–side port aggregation allows network engineers to achieve functions such as port–based redundancy using the 570NAT–X19–10G.

The 570NAT–X19–10G is controlled by the industry–leading VistaLINK PRO, and via web interface.

The 12 Ethernet ports support 10GbE and offer full flexibility for LAN and WAN interfacing.

The 570NAT–X19–10G provides four modes of operation:

1. The One–to–One NAT Mode allows unicast/multicast IP streams from one network to be translated to different unicast/multicast IP addresses, on a flow–by–flow basis, up to 256 unique flows per processing core. Address translation is available in both directions, while an optional packet replication feature is provided in the WAN–to–LAN direction.

2. The tunneling (or Encapsulation or MC–in–MC) NAT Mode allows unicast/multicast addresses from the LAN side to be encapsulated into new multicasts for the WAN network, again, on a flow–by–flow basis, up to 128 unique settings per processing core. Correspondingly, traffic is de–encapsulated in the WAN–to–LAN direction.

3. The VLAN Mode allows VLAN–tagged datagrams from the LAN side to seamlessly enter a WAN after multicast encapsulation, similar to the tunneling NAT mode. In this mode, however, fl ows are based on VLAN tags, rather than unicasts/multicasts alone. Up to 256 unique flows can be configured per processing core, with independent encapsulation headers.

4. The port mode allows the user to encapsulate all incoming LAN traffic on a given physical port, on a port–by–port basis. There is no multicast or VLAN Tag filtering — all traffic on that physical LAN port is encapsulated out to the WAN and de–encapsulated in the reverse direction. This mode provides a bandwidth capping feature such that network operators can ensure that links do not over–subscribe their contribution limits to a WAN.

Features & Benefits

- One–to–one NAT with user configurable Packet Replication
- MC–in–MC NAT for tunneling flows based on multicast addresses
- VLAN based NAT for tunneling flows based on VLAN tag
- Port based NAT for tunneling all traffic (ingress/egress) on per port basis
- Port Aggregation (LAN–to–WAN direction)
- Port Redundancy on both WAN and LAN side (network path failure protection)
- Virtual interfaces for Unicast flows mapping or VLAN ID change
- IGMPv3 with SSM support
- Point–to–point and multi–point signal intra/inter–facility distribution/contribution
- Operates over a Dark fiber, Ethernet, IP, MPLS VPLS, core network
- In–band Management (Management Traffic transport over Multicast)
- Support for FEC Pro MPEG (forward error correction)
- 12x 10GbE (SFP10G–TR13–A)
- Control via 570FC Frame Controller
- Full integration with VistaLINK PRO and MAGNUM
- Standalone Web–based control interface

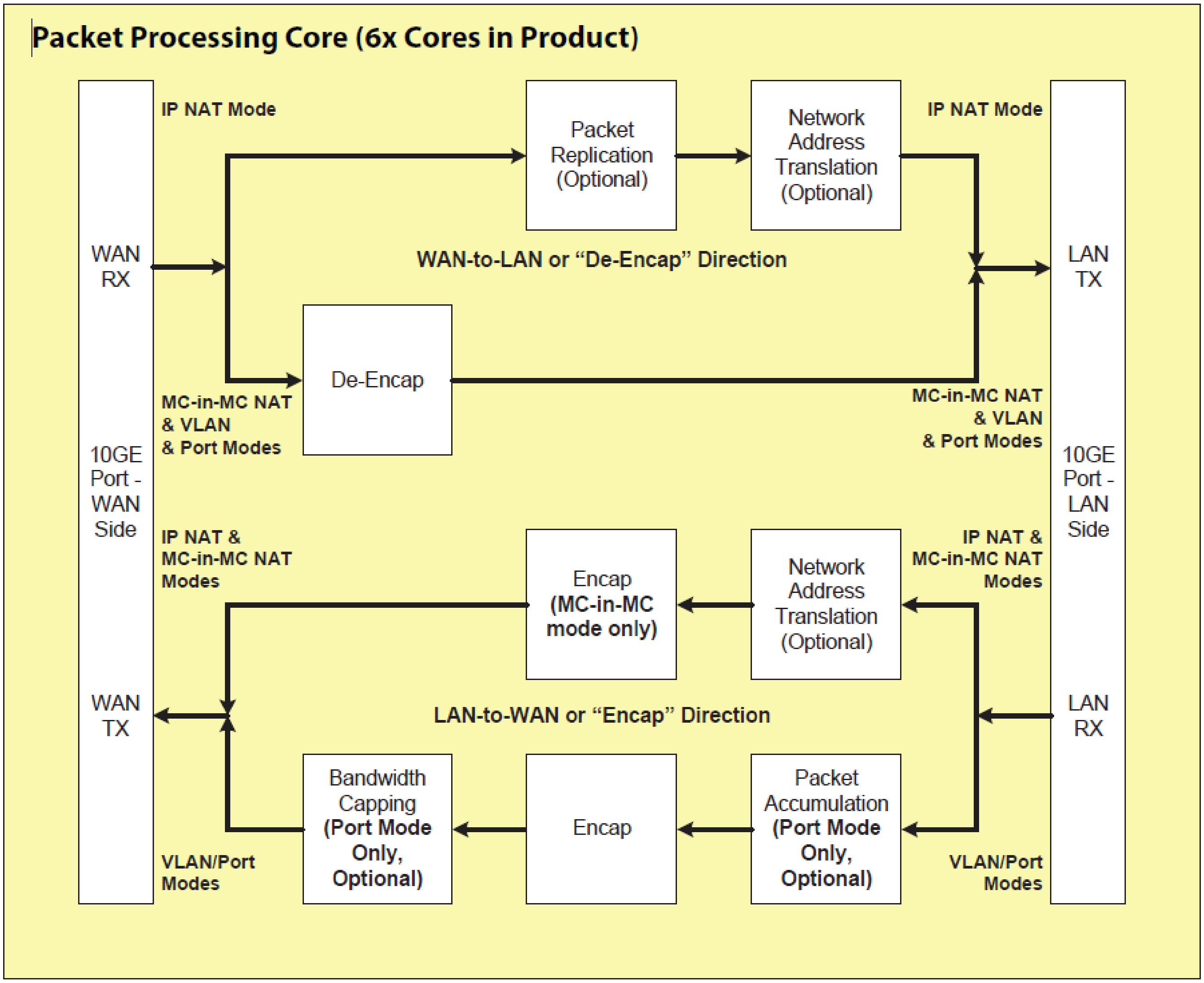

Packet Processing Core (6x Cores in Product)
WAN RX
10GE Port - WAN Side
WAN TX
IP NAT Mode
Packet Replication (Optional)
Network Address Translation (Optional)
IP NAT Mode
LAN TX
10GE Port - LAN Side
LAN RX
WAN-to-LAN or "De-Encap" Direction
De-Encap
MC-in-MC NAT & VLAN & Port Modes
MC-in-MC NAT & VLAN & Port Modes
IP NAT & MC-in-MC NAT Modes
Encap (MC-in-MC mode only)
Network Address Translation (Optional)
IP NAT & MC-in-MC NAT Modes
LAN-to-WAN or "Encap" Direction
Bandwidth Capping (Port Mode Only, Optional)
Encap
Packet Accumulation (Port Mode Only, Optional)
VLAN/Port Modes
VLAN/Port Modes

Figure 1-1: Single NAT Core Block Diagram

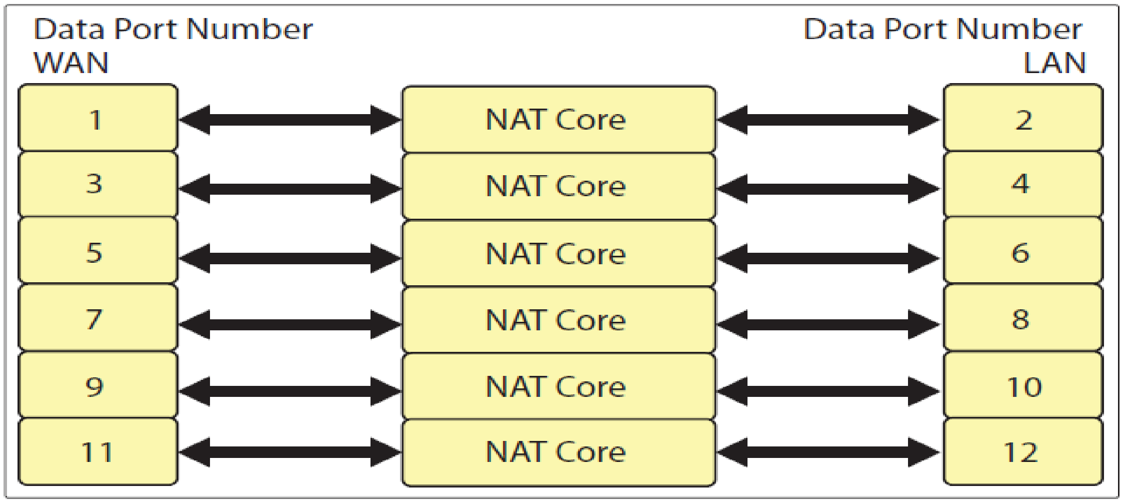


Figure 1-2 : 570NAT-HW-X19 Core Mapping Block Diagram

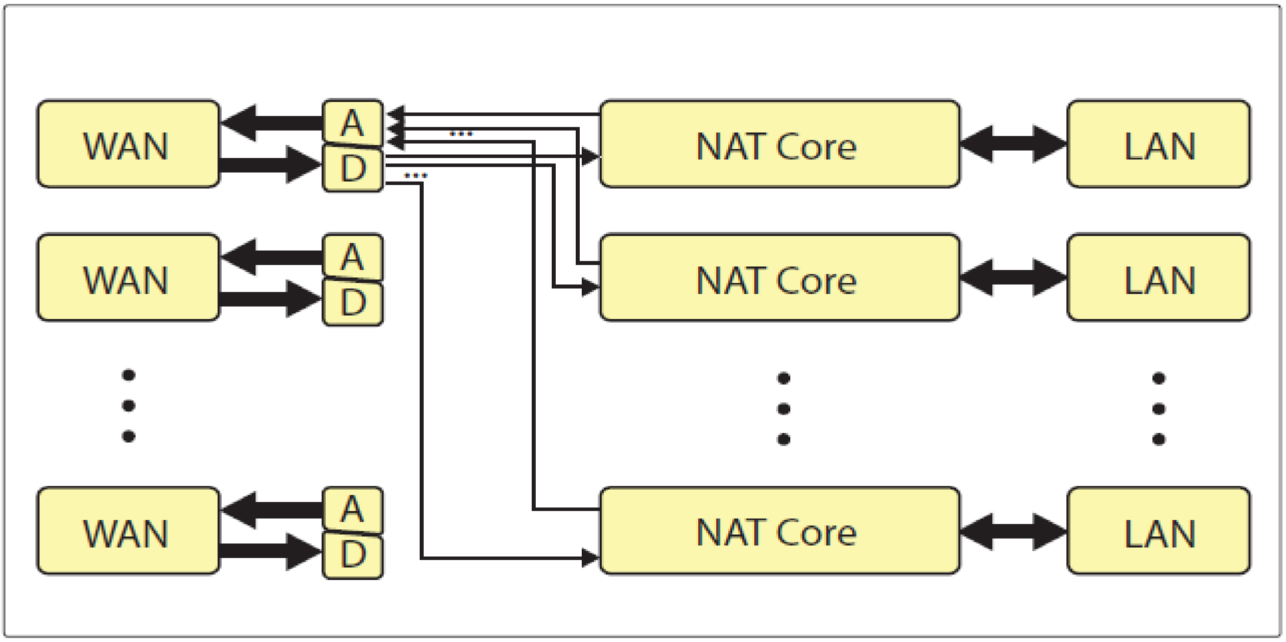


Figure 1-3: WAN-Side Port Aggregation and Demux (available in all modes)

2. GETTING STARTED

2.1. REAR PLATE DESCRIPTION

The 570NAT-HW-X19 comes standard with a companion rear plate. Figure 2-1 provides an illustration of the 570NAT-HW-X19 rear plate.

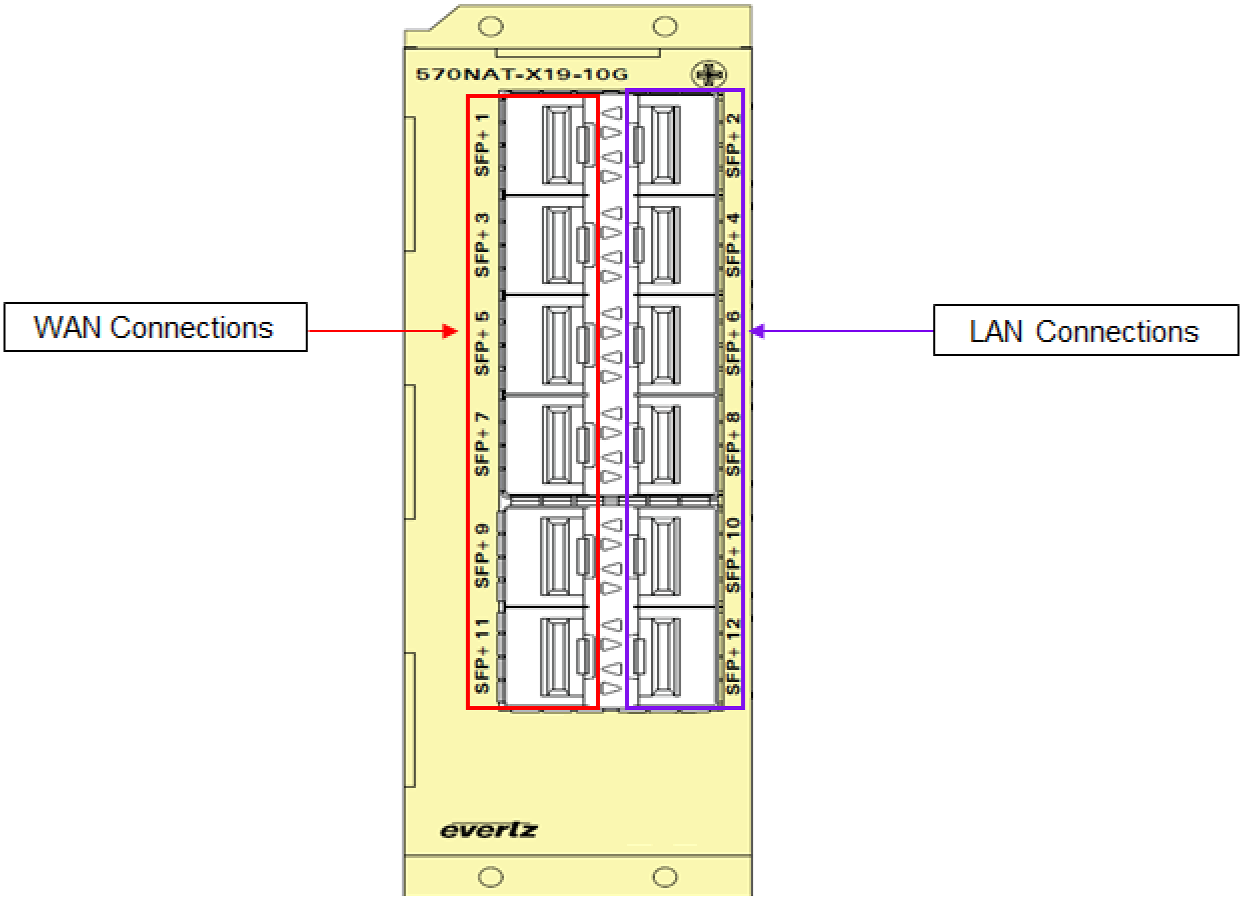


Figure 2-1: 570NAT-X19-10G Rear Plate

1GigE or 10GigE Input / Output: There are 12 SFP bi-directional connections used for the 1GE or 10GE input and output.

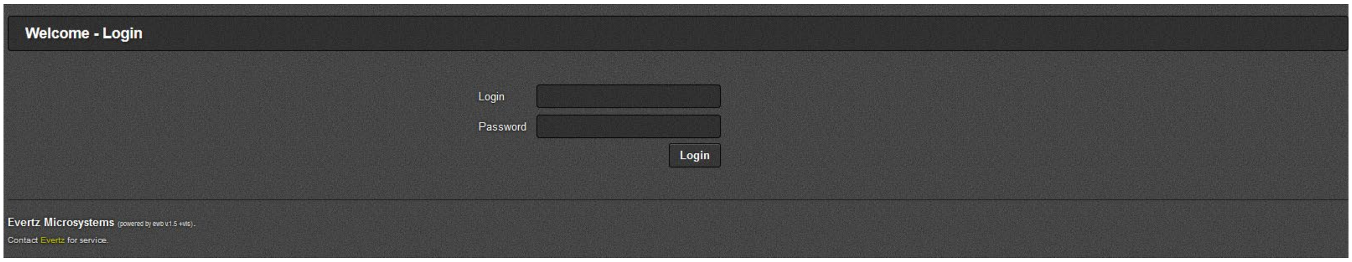
2.2. CARE AND HANDLING OF OPTICAL FIBER

✍ **Never touch the end face of an optical fiber. Always keep dust caps on optical fiber connectors when not connected and always remember to properly clean the optical end face of a connector before making a connection.**

The transmission characteristics of the fiber are dependent on the shape of the optical core and therefore care must be taken to prevent fiber damage due to heavy objects or abrupt fiber bending. Evertz recommends that the user maintains a minimum bending radius of 5 cm to avoid fiber-bending loss that will decrease the maximum attainable distance of the fiber cable. The Evertz fiber optic modules come with cable lockout devices, to prevent the user from damaging the fiber by installing a module into a slot in the frame that does not have a suitable I/O module.

2.3. SETTING DEVICE IP

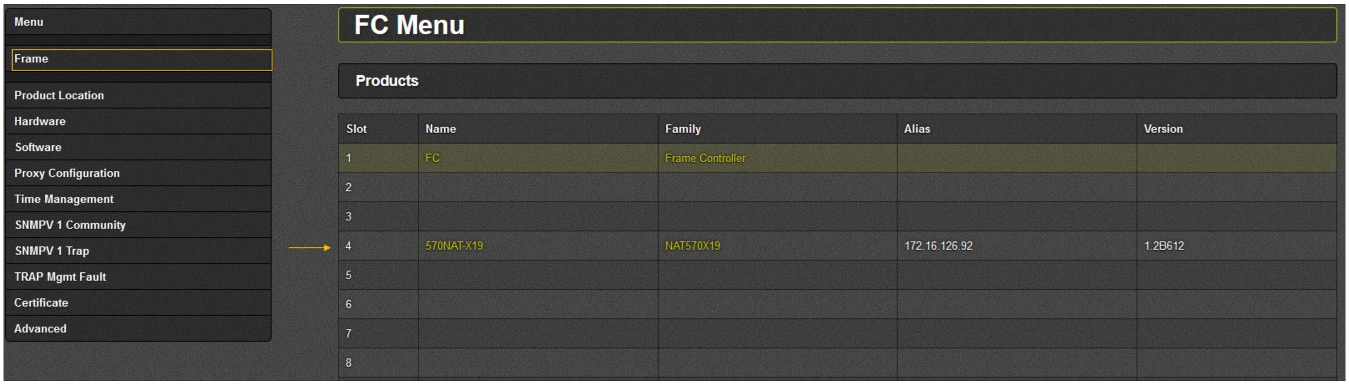
The 570NAT-HW-X19 must first be configured through the frame controller. To do so, open a web browser and type the IP address of the frame controller. You will be presented with the login menu,



Evertz Microsystems (powered by ewb v.1.5 +vis).
Contact Evertz for service.

Figure 2-2 : WebEASY® - Frame Controller Login

The default login/password combination is admin/admin.
After successfully logging into the frame controller, you will be presented with the FC Menu. If not, you can access the FC menu by selecting 'Frame' from the side menu (highlighted below in Figure 2-3)



Slot	Name	Family	Alias	Version
1	FC	Frame Controller		
2				
3				
4	570NAT-X19	NAT570X19	172.16.126.92	1.2B612
5				
6				
7				
8				

Figure 2-3 : WebEASY® - Frame Controller - FC Menu

Once in the FC Menu, take note of which slot the 570NAT-X19 card you are looking to configure.
To set the IP address for this card, proceed by selecting 'proxy configuration' in the side menu.

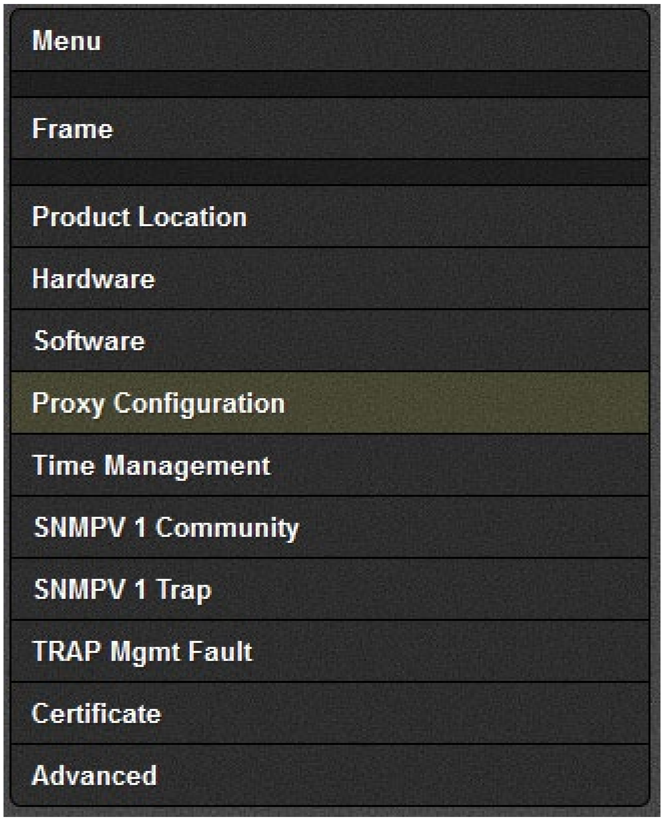
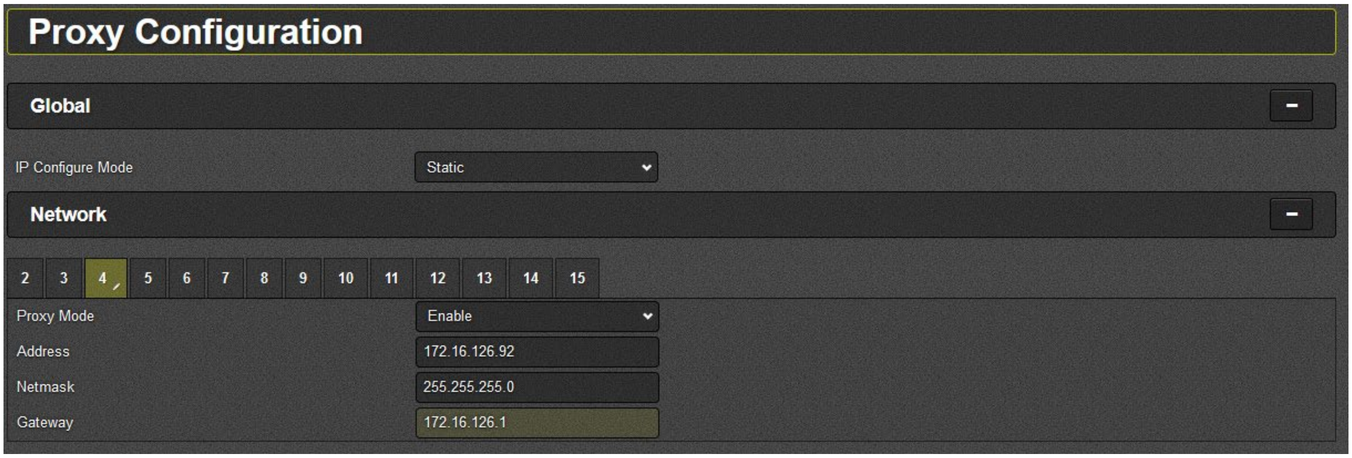


Figure 2-4: WebEASY® - Frame Controller – Side Menu

Once selected, the proxy configuration page will load.



IP Configure Mode: Static

Proxy Mode: Enable

Address: 172.16.126.92

Netmask: 255.255.255.0

Gateway: 172.16.126.1

Figure 2-5 : WebEASY® - Frame Controller – Proxy Configuration

Once in the proxy configuration, select the slot number for your 570NAT-X19 card in the frame controller. Slot selection is displayed just below ‘Network’, here slot #4 has been selected.

Enable proxy mode and set an IP, netmask and gateway for the 570NAT-X19 card.

3. TECHNICAL SPECIFICATIONS

3.1. ONE-TO-ONE NAT

- 1536x static mapping
- Packet Replication (WAN-to-LAN direction)
- VLAN ID change
- Ingress traffic filtering based on VLAND ID option

3.2. MC-IN-MC NAT

- 1536x Multicast Mapping

3.3. VLAN-BASED NAT

- 1536x VLAN ID Mapping

3.4. PORT-BASED NAT

- 12x datagram flow mapping (from 12x 10GbE)

3.5. VIRTUAL INTERFACES

- 15x interfaces per data port (both WAN and LAN side)
- VLAN ID change (One-to-One NAT mode)

3.6. SFP MODULES

12x SFP Modules

- 100GbE optical 850nm, MMF (+SFP10G-TR85-A)
- 10GbE optical 1310nm, SMF, 2Km (+SFP10G-TR13S)
- 10GbE optical 1310nm, SMF, 10Km (+SFP10G-TR13-A)
- 10GbE optical 1550nm, SMF, 40Km (+SFP10G-TR15S)
- 10GbE optical 1550nm, SMF, 80Km (+SFP10G-TR15H)
- 10GbE optical CWDM (SFP10G-TRCxxH) and DWDM (SFP10G-TRDxxxH)

3.7. ORDERING INFORMATION

570NAT-X19-10G	High Density NAT

Enclosures:

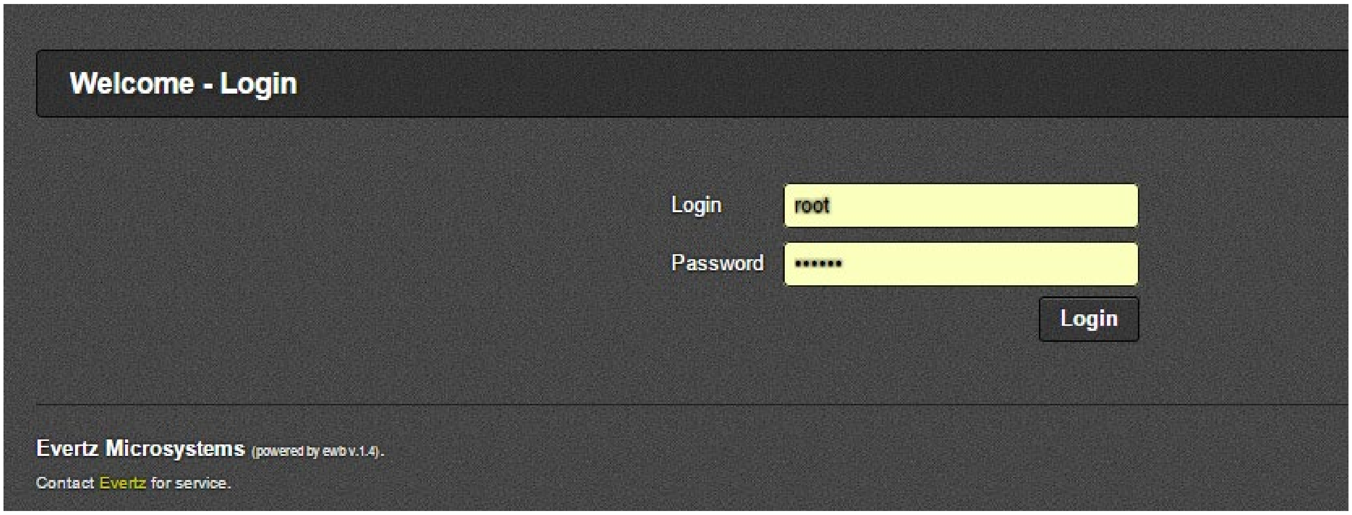
570FR	3RU chassis
S570FR	1RU chassis

This page left intentionally blank

4. WEB INTERFACE

The 570NAT-HW-X19 provides a built-in web interface, WebEASY®, which allows a user to interact with using a standard Internet web browser. The 570NAT-HW-X19 web interface can be accessed by entering the IP address of the control port of the 570NAT-HW-X19 into the address bar of an Internet web browser. Refer to section **Error! Reference source not found.** for setting the network configurations.

When first visiting the 570NAT-HW-X19 web interface, the user will be asked to enter a Login and Password. Enter "***root***" for Password and "***evertz***" for Login to get administrator privileges. When viewing only the configurations, "*customer*" for both Login and Password.



Welcome - Login

Login: root

Password: ••••••

Evertz Microsystems (powered by ewb v.1.4).

Contact Evertz for service.

Figure 4-1: WebEASY® - Login Screen

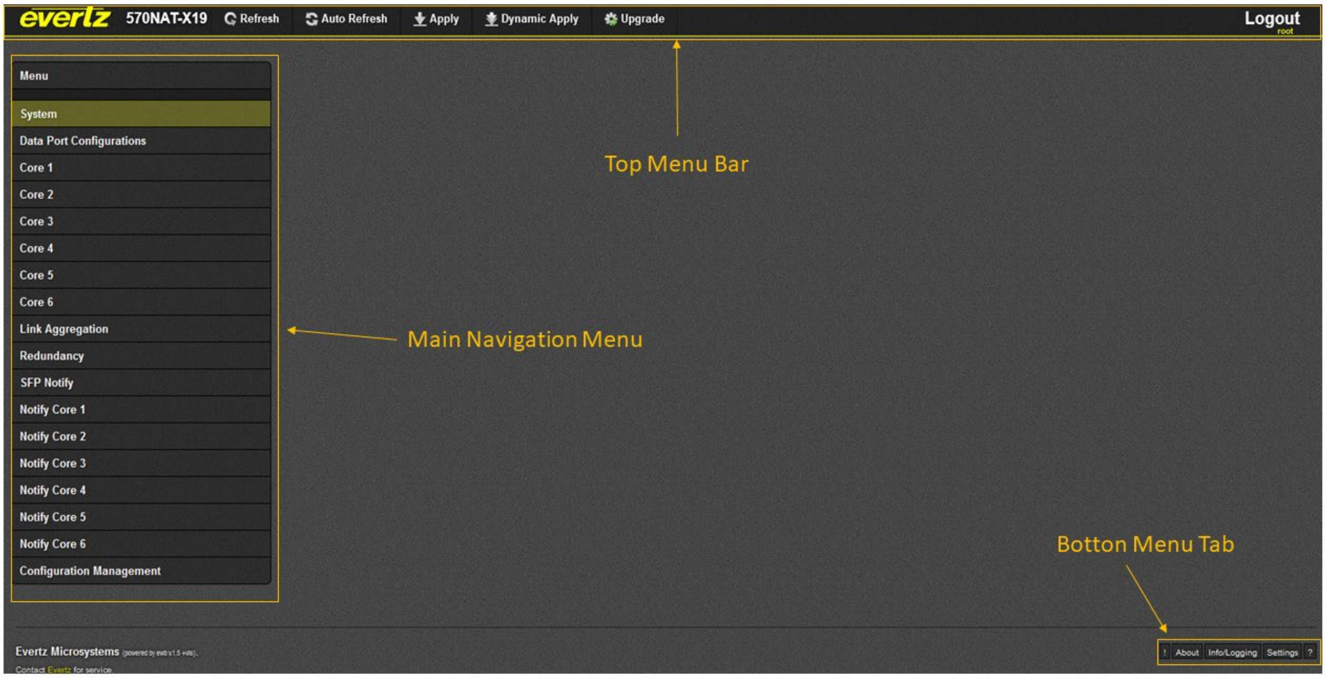


Figure 4-2 : WebEASY® - Main Menu

Once logging into the Evertz WebEASY® interface for your device, you may navigate to different useful pages using the main navigation menu, the top menu bar and the bottom menu tab.

Main Navigation Menu

This menu contains every page specific to the operation of the 570NAT-HW-X19. Here you can change a variety of device settings and monitor the device status.

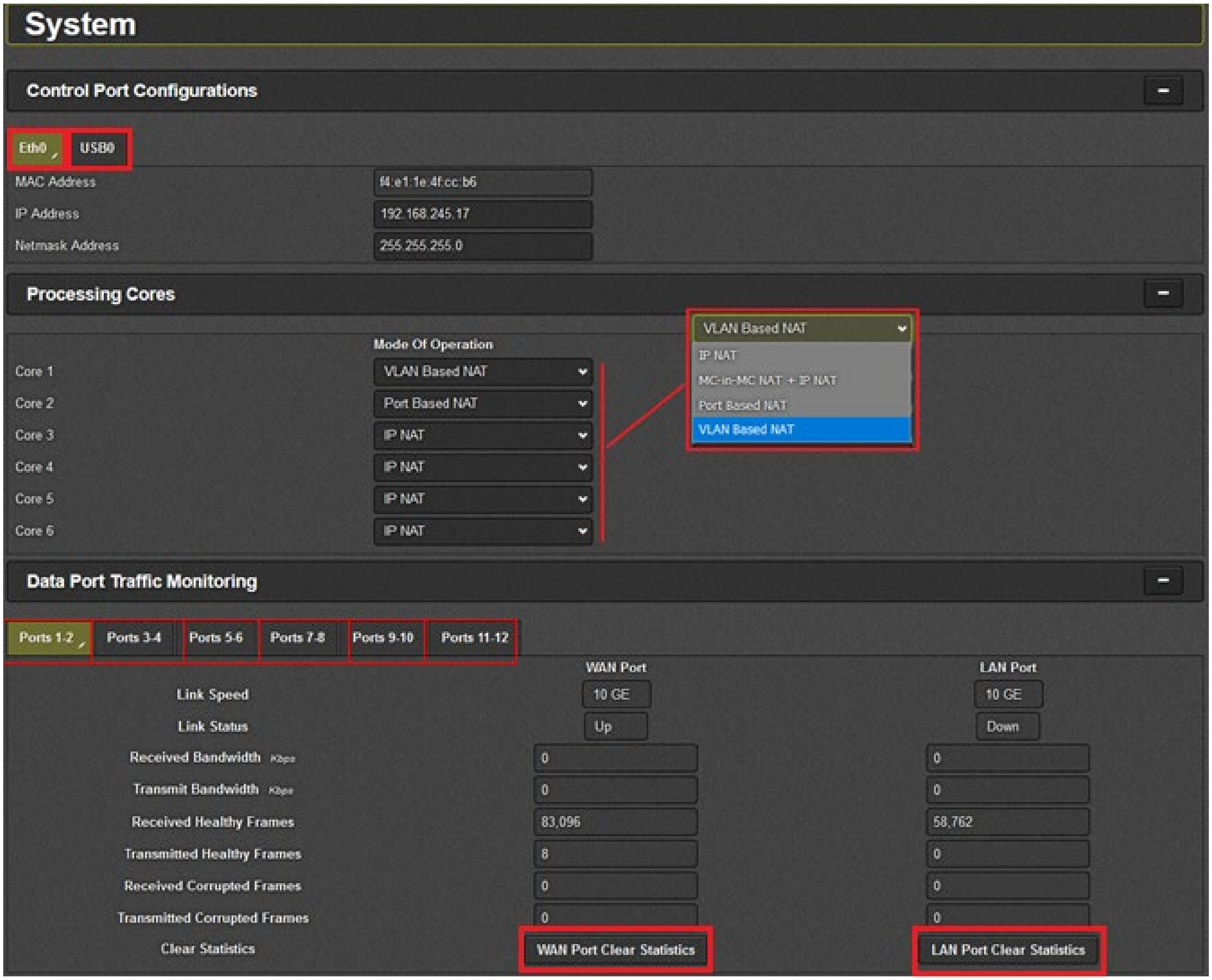
Top Menu Bar

The top menu bar allows the user to refresh the page, apply settings and upgrade the firmware of the 570NAT-HW-X19. Note that applying some settings requires a system reset for changes to take place.

Bottom Menu Tab

The bottom menu tab allows the user to view the event log (**!**), view WebEASY and device build information (**About**), view device hardware information and set up remote logging (**Info/Logging**), change settings in WebEASY, manage roles and user accounts (**Settings)** as well as enable descriptive tooltips for the device settings (**?**).

4.1. SYSTEM TAB


System
Control Port Configurations
Eth0
USB0
Processing Cores
Data Port Traffic Monitoring
Ports 1-2
Ports 3-4
Ports 5-6
Ports 7-8
Ports 9-10
Ports 11-12
WAN Port Clear Statistics
LAN Port Clear Statistics

MAC Address: f4:e1:1e:4f:cc:b6
IP Address: 192.168.245.17
Netmask Address: 255.255.255.0

	Mode Of Operation
Core 1	VLAN Based NAT
Core 2	Port Based NAT
Core 3	IP NAT
Core 4	IP NAT
Core 5	IP NAT
Core 6	IP NAT

VLAN Based NAT
- IP NAT
- MC-in-MC NAT + IP NAT
- Port Based NAT
- VLAN Based NAT

	WAN Port	LAN Port
Link Speed	10 GE	10 GE
Link Status	Up	Down
Received Bandwidth Kbps	0	0
Transmit Bandwidth Kbps	0	0
Received Healthy Frames	83,096	58,762
Transmitted Healthy Frames	8	0
Received Corrupted Frames	0	0
Transmitted Corrupted Frames	0	0
Clear Statistics	WAN Port Clear Statistics	LAN Port Clear Statistics

Figure 4-3: WebEASY® - System Tab – Part 1

4.1.1. Control Port Configuration

For Eth0 or USB0

MAC Address: This field displays the MAC Address of the 570NAT-HW-X19.

IP Address: This field allows the user to enter the IP address to be assigned to control port of the 570NAT-HW-X19.

Netmask Address: This field allows the user to enter the netmask address for the device control port.

4.1.2. Processing Cores

The 570NAT-X19 allows for customizing mode of operation for each core. Mode of operation is set through the dropdown available in the system menu.

Mode of Operation: Within this drop down menu the user can configure the desired mode of operation for each core of the 570NAT-HW-X19.

The NAT can be set to: *IP NAT*, *MC-In-MC NAT + IP NAT*, *Port Based NAT*, *VLAN Based NAT.*

Once a core has been set to a mode of operation, the settings for the mode of operation on that core can be set by selecting that core on the WebEASY® main menu sidebar (shown in Figure 4-2).

Each mode of operation can be found in the following sections: Port Based NAT [Section 4.3], VLAN Based NAT [Section 4.4], IP NAT [Section 4.5], MC-in-MC NAT + IP NAT [Section 4.6].

4.1.3. Data Port Traffic Monitoring

For each of the 12 Data ports (6 pairs) the following parameters can be monitored. Port are selected as WAN-LAN pairs.

Link Speed: This monitor will automatically detect the link speed of the SFP module installed.

Link Status: This field displays the physical link status of the associated data port as either *Up* or *Down*.

Received Bandwidth (kbps): This field displays the bit rate received by the associated data port in kbps.

Transmit Bandwidth (kbps): This field returns the bit rate transmitted by the associated data port in kbps.

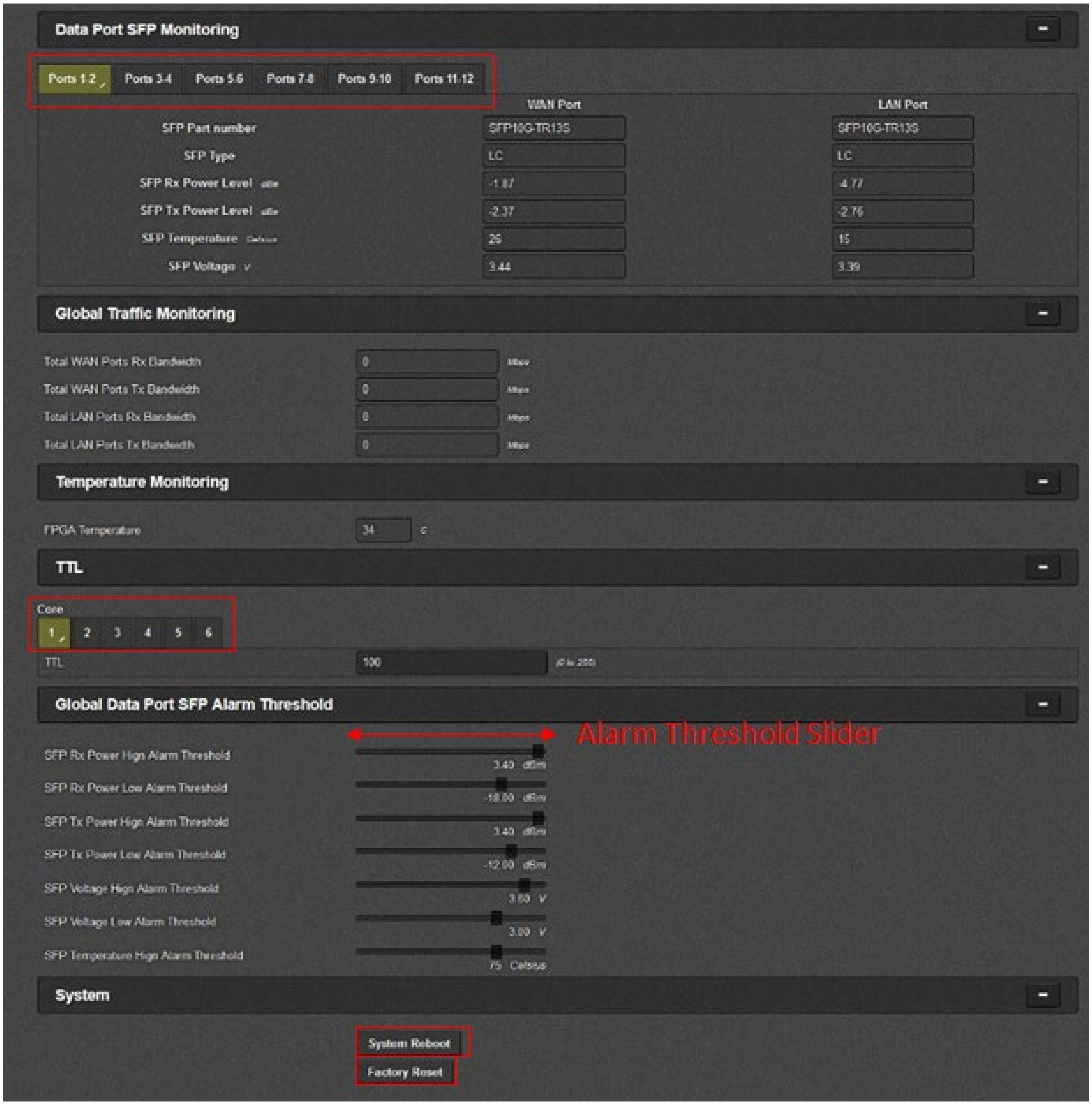
Received Healthy Frames: This parameter displays number of good Ethernet packets received.

Transmitted Healthy Frames: This parameter displays number of good Ethernet packets transmitted.

Received Corrupted Frames: This parameter displays number of Ethernet packets received with errors

Transmitted Corrupted Frames: This parameter displays number of Ethernet packets transmitted with errors.

Clear All Statistics: This control button allows the user to clear all the statistics.



Data Port SFP Monitoring

	WAN Port	LAN Port
SFP Part number	SFP10G-TR13S	SFP10G-TR13S
SFP Type	LC	LC
SFP Rx Power Level dBm	-1.87	-4.77
SFP Tx Power Level dBm	-2.37	-2.76
SFP Temperature Celsius	26	15
SFP Voltage V	3.44	3.39

Global Traffic Monitoring

Total WAN Ports Rx Bandwidth	0	Mbps
Total WAN Ports Tx Bandwidth	0	Mbps
Total LAN Ports Rx Bandwidth	0	Mbps
Total LAN Ports Tx Bandwidth	0	Mbps

Temperature Monitoring

FPGA Temperature 34 C

TTL

TTL 100 (0 to 255)

Global Data Port SFP Alarm Threshold

SFP Rx Power High Alarm Threshold	3.40 dBm
SFP Rx Power Low Alarm Threshold	-18.00 dBm
SFP Tx Power High Alarm Threshold	3.40 dBm
SFP Tx Power Low Alarm Threshold	-12.00 dBm
SFP Voltage High Alarm Threshold	3.60 V
SFP Voltage Low Alarm Threshold	3.00 V
SFP Temperature High Alarm Threshold	75 Celsius

System

Figure 4-4: WebEASY® - System Tab – Part 2

4.1.4. Data Port SFP Monitoring

For Ports 1 to 12

SFP Part Number: This field displays the SFP part number detected.

SFP Type: This field displays the part number detected for the SFP.

SFP Rx Power Level (dbm): This field displays the receiving power level on the SFP.

SFP TX Power Level (dbm): This field displays the transmitting power level for the SFP

4.1.5. Global Traffic Monitoring

Total WAN Ports Rx Bandwidth (Mbps): This parameter displays the total received bandwidth for all WAN Ethernet ports.

Total WAN Ports Tx Bandwidth (Mbps): This parameter displays the total sent bandwidth for WAN Ethernet ports.

Total LAN Ports Rx Bandwidth (Mbps): This parameter displays the total received bandwidth for all LAN Ethernet ports.

Total LAN Ports Tx Bandwidth (Mbps): This parameter displays the total sent bandwidth for LAN Ethernet ports.

4.1.6. Temperature Monitoring

FPGA Temperature: This monitor will display the temperature of the FPGA.

4.1.7. TTL

TTL: This field allows the user to enter the Time To Live (TTL) to be used on each separate core of the NAT.

4.1.8. Global Data Port SFP Alarm Threshold

Use sliders to set alarm thresholds for Rx, Tx, Voltage and Temperature conditions of SFPs.

It is recommended users consult with the documentation for their SFPs and use their operational specifications as a guideline for setting the SFP alarms.

SFP Rx Power High Alarm Threshold (dBm): Alarm will trigger if SFP Rx exceeds this threshold.

SFP Tx Power Low Alarm Threshold (dBm): Alarm will trigger if SFP Rx falls below this threshold.

SFP Rx Power High Alarm Threshold (dBm): Alarm will trigger if SFP Tx exceeds this threshold.

SFP Tx Power Low Alarm Threshold (dBm): Alarm will trigger if SFP Tx falls below this threshold.

SFP Voltage High Alarm Threshold (V): Alarm will trigger if SFP voltage exceeds this threshold.

SFP Voltage Low Alarm Threshold (V): Alarm will trigger if SFP voltage falls below this threshold.

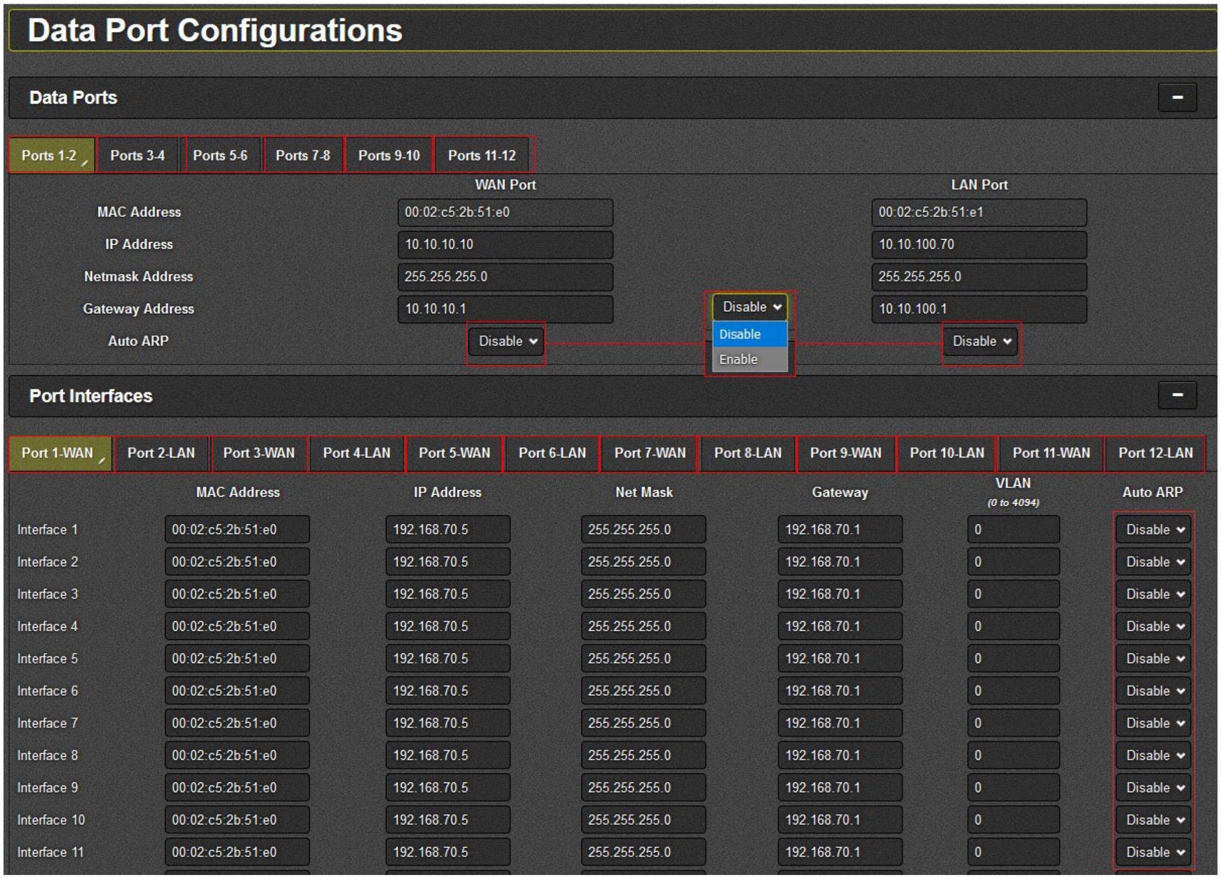
SFP Temperature High Alarm Threshold (°C): Alarm will trigger if SFP temperature exceeds this threshold.

4.1.9. System

System Reboot: This button allows the user to reboot the 570NAT-HW-X19 module, doing this will result in the connection being lost temporarily while the unit resets. A warning pop-up may appear in WebEASY® during this time, wait for the unit to reset.

Factory Reset: This button will reset the 570NAT-HW-X19 unit to factory default settings and firmware.

4.2. DATA PORT CONFIGURATIONS



Data Port Configurations

Data Ports

	WAN Port	LAN Port
MAC Address	00:02:c5:2b:51:e0	00:02:c5:2b:51:e1
IP Address	10.10.10.10	10.10.100.70
Netmask Address	255.255.255.0	255.255.255.0
Gateway Address	10.10.10.1	10.10.100.1
Auto ARP	Disable	Disable

Port Interfaces

	MAC Address	IP Address	Net Mask	Gateway	VLAN (0 to 4094)	Auto ARP
Interface 1	00:02:c5:2b:51:e0	192.168.70.5	255.255.255.0	192.168.70.1	0	Disable
Interface 2	00:02:c5:2b:51:e0	192.168.70.5	255.255.255.0	192.168.70.1	0	Disable
Interface 3	00:02:c5:2b:51:e0	192.168.70.5	255.255.255.0	192.168.70.1	0	Disable
Interface 4	00:02:c5:2b:51:e0	192.168.70.5	255.255.255.0	192.168.70.1	0	Disable
Interface 5	00:02:c5:2b:51:e0	192.168.70.5	255.255.255.0	192.168.70.1	0	Disable
Interface 6	00:02:c5:2b:51:e0	192.168.70.5	255.255.255.0	192.168.70.1	0	Disable
Interface 7	00:02:c5:2b:51:e0	192.168.70.5	255.255.255.0	192.168.70.1	0	Disable
Interface 8	00:02:c5:2b:51:e0	192.168.70.5	255.255.255.0	192.168.70.1	0	Disable
Interface 9	00:02:c5:2b:51:e0	192.168.70.5	255.255.255.0	192.168.70.1	0	Disable
Interface 10	00:02:c5:2b:51:e0	192.168.70.5	255.255.255.0	192.168.70.1	0	Disable
Interface 11	00:02:c5:2b:51:e0	192.168.70.5	255.255.255.0	192.168.70.1	0	Disable

Figure 4-5 : WebEASY® - Data Port Configurations

This page allows users to set address information for data ports and port interfaces attached to each port. For an explanation of the port assignments see Figure 1-2.

4.2.1. Data Ports

Data ports are set in WAN – LAN pairs (port numbers: WAN : odd #, LAN : even #), the dataports menu allows users to set the following:

MAC Address: MAC set by hardware displayed here.

IP Address: This allows user to set the IP Address to be assigned to this port.

Netmask Address: This allows the user to enter the netmask for this port

Gateway Address: This allows the user to enter the gateway address of this port.

Auto ARP: Enabling this allows for automatic address resolution for conflicting IPs assigned to this port. Disabling this will prevent ARP rerouting.

4.2.2. Port Interfaces

Port interfaces allow the NAT interface for each port to be set individually.

MAC Address: MAC set by hardware displayed here for each port.

IP Address (WAN): This allows the user to enter the IP address this port pair will use to communicate to the WAN.

IP Address (LAN): This allows user to set the IP Address to be assigned to this port through the LAN.

Netmask Address (WAN): This allows the user to enter the netmask this port pair will use to communicate to the WAN.

Netmask Address (LAN): This allows the user to enter the netmask this port will use over the LAN.

Gateway Address (WAN): This allows the user to enter the address of the gateway used to communicate to the WAN.

Gateway Address (LAN): This allows the user to enter the address of the gateway used to communicate to the LAN.

Auto ARP: Enabling this allows for automatic address resolution for conflicting IPs assigned to this port. Disabling this will prevent ARP rerouting.

4.3. PORT BASED NAT

Port Mode allows the user to encapsulate all incoming LAN traffic on a given physical port, on a port-by-port basis. There is no multicast or VLAN Tag filtering – All traffic on that physical LAN port is encapsulated out to the WAN, and de-encapsulated in the reverse direction. This mode provides a Bandwidth Capping feature such that network operators can ensure that links do not over-subscribe their contribution limits to a WAN.

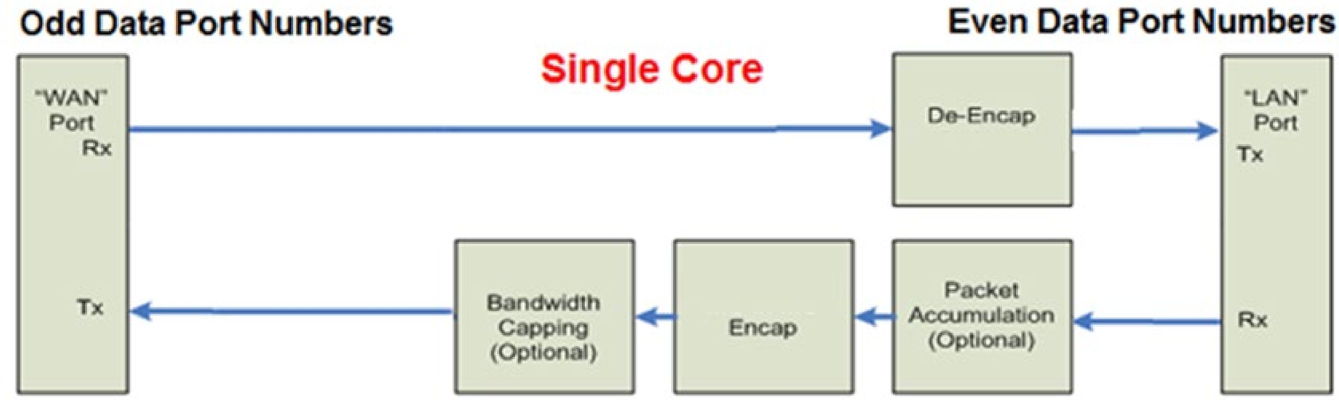
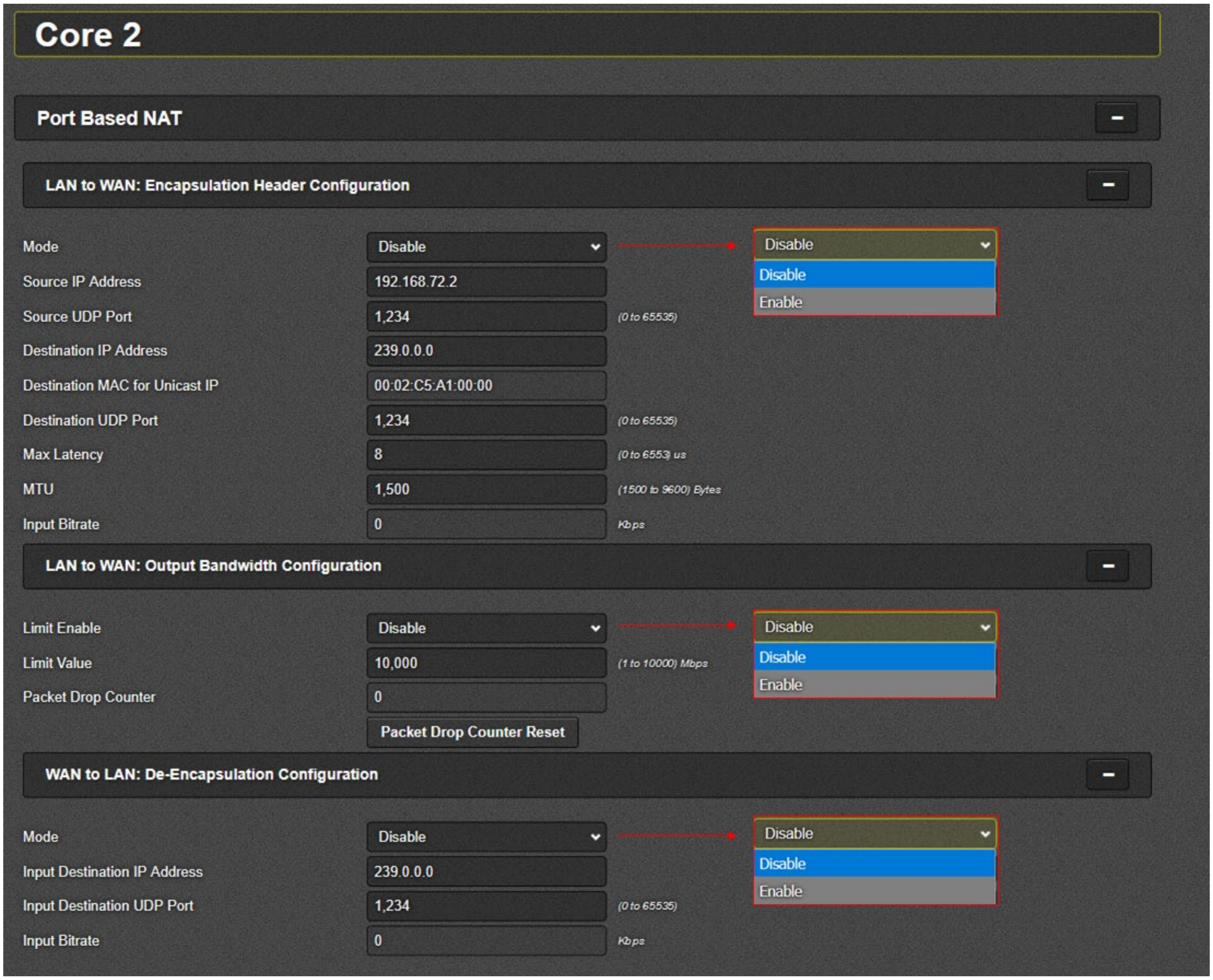


Figure 4-6 : Port Based NAT Mode Block Diagram



Core 2

Port Based NAT

LAN to WAN: Encapsulation Header Configuration

Mode	Disable	
Source IP Address	192.168.72.2	
Source UDP Port	1,234	(0 to 65535)
Destination IP Address	239.0.0.0	
Destination MAC for Unicast IP	00:02:C5:A1:00:00	
Destination UDP Port	1,234	(0 to 65535)
Max Latency	8	(0 to 6553) us
MTU	1,500	(1500 to 9600) Bytes
Input Bitrate	0	Kbps

LAN to WAN: Output Bandwidth Configuration

Limit Enable	Disable	
Limit Value	10,000	(1 to 10000) Mbps
Packet Drop Counter	0	

WAN to LAN: De-Encapsulation Configuration

Mode	Disable	
Input Destination IP Address	239.0.0.0	
Input Destination UDP Port	1,234	(0 to 65535)
Input Bitrate	0	Kbps

Figure 4-7 : WebEASY® - Port Based NAT

4.3.1. LAN to WAN: Encapsulation Header Configuration

For cores 1 to 6

Mode: This control allows the user to enable or disable the output.

Source IP Address: This control allows the user to set the physical source IP address of the incoming traffic.

Source UDP Port: This control allows the user to set the physical source UDP port of the incoming IP traffic.

Destination IP Address: This control is used to configure the output header on encapsulation with the desired Destination IP Address.

Destination MAC for Unicast IP: This control is used to configure the output header on the encapsulation with the desired Destination MAC address.

Destination UDP Port: This control is used to configure the output header on encapsulation with the desired Destination UDP Port.

Max Latency (0 to 6553 µs): This is a timeout on how long the Core waits while accumulating MTU bytes. If the timeout expires, the Core will transmit whatever packets it has accumulated, even if much less than MTU. If the Core is midway through receiving a packet, it must wait till that packet is done, then transmit the accumulated data. This means, the latency can sometimes exceed the user value, if the Core has a large incoming packet when the latency timeout expires.

MTU (1500 to 9600 bytes): This is the upper limit of the packet length that the network can tolerate. MTU is predictable, in the sense that the Core will never produce packets larger than MTU. The Core will accumulate input packets till it collects close to MTU bytes, but not greater. The exception is when input packets are larger than the specified MTU size, because the product does not fragment packets.

Input Bit rate (kbps): This monitor will display the bit rate coming in on the port**.**

Points to Note:

1. MTU is a 'hard limit', while MAX LATENCY is a 'soft limit'.
2. If LATENCY is set too low, output packets will be much smaller than MTU. But if LATENCY is set very high, there is no danger of output packets exceeding MTU - Packets will always be less than MTU.

Deciding Values:

1. Set MTU to whatever max packet length (or slightly less) that your network can tolerate, for example, 5000 bytes.
2. How long does it take for 5000 bytes to arrive at 10Gbps rate? That's 4us. You can double that value and use LATENCY of 8us, as an example.
3. This means, if data rate stays between 5Gbps-10Gbps, then the Core will wait to accumulate close to 5000 bytes. If data rate drops below 5Gbps, the LATENCY will kick-in, and output packets will be <5000 bytes, and link efficiency will get lower. Usually lower link efficiency is not a problem at lower data rates.

✍ **Max Latency and MTU work together to determine the size of the output frame.**

4.3.2. LAN to WAN: Output Bandwidth Configuration

Limit Enable: This control allows the user to enable or disable Output Bandwidth Control.

Limit Value: This control allows the user a set limit for the maximum output bandwidth allowed on the data port.

Packet Drop Counter: This monitor will display the number of packets dropped due to exceeding the *Limit Value*.

Packet Drop Counter Reset (click button): This button allows the user to reset Packet Drop Counter.

4.3.3. WAN to LAN: De-Encapsulation Configuration

Mode: This control allows the user to enable or disable the input stream which is going to be decapsulated.

Input Destination IP Address: This control allows the user to set the IP address of the packet to be received.

Input Destination UDP Port: This control allows the user to set the UDP Port number to be received.

Input Bit rate: This monitor will display the bit rate coming in on the port**.**

4.4. VLAN BASED NAT

The VLAN Mode allows VLAN-tagged datagrams from the LAN side to enter a WAN after multicast encapsulation, similar to the Tunnelling NAT mode. In this mode, however, flows are based on VLAN Tags, rather than unicasts/multicasts alone. Up to 256 unique flows can be configured per processing core, with independent encapsulation headers.

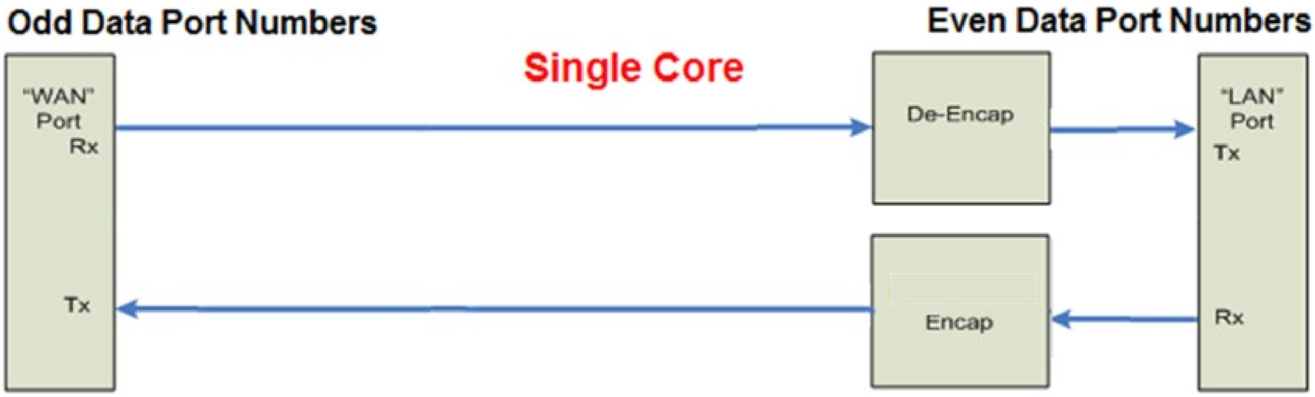
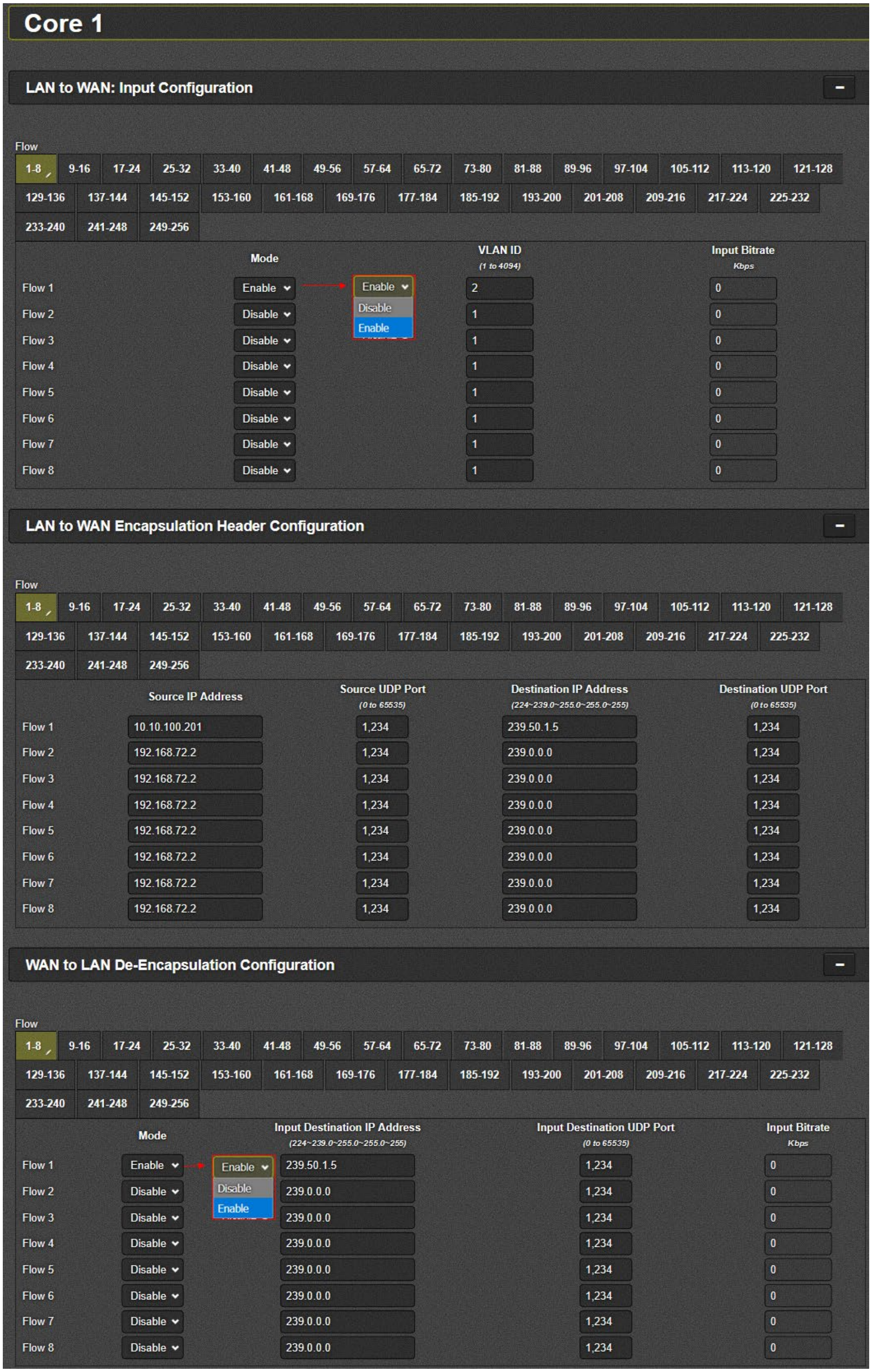


Figure 4-8 : VLAN Based NAT Mode Block Diagram

Each VLAN flow must have a unique Tag value. Two or more flows cannot share the same VLAN Tag because there is no '*Packet Replication'* in VLAN Mode.

VLAN Mode does not support nested VLAN Tags. The 570NAT-HW-X19 only supports Ether Type=0x8100 traffic.



Core 1

LAN to WAN: Input Configuration

	Mode	VLAN ID (1 to 4094)	Input Bitrate Kbps
Flow 1	Enable	2	0
Flow 2	Disable	1	0
Flow 3	Disable	1	0
Flow 4	Disable	1	0
Flow 5	Disable	1	0
Flow 6	Disable	1	0
Flow 7	Disable	1	0
Flow 8	Disable	1	0

LAN to WAN Encapsulation Header Configuration

	Source IP Address	Source UDP Port (0 to 65535)	Destination IP Address (224~239.0~255.0~255.0~255)	Destination UDP Port (0 to 65535)
Flow 1	10.10.100.201	1,234	239.50.1.5	1,234
Flow 2	192.168.72.2	1,234	239.0.0.0	1,234
Flow 3	192.168.72.2	1,234	239.0.0.0	1,234
Flow 4	192.168.72.2	1,234	239.0.0.0	1,234
Flow 5	192.168.72.2	1,234	239.0.0.0	1,234
Flow 6	192.168.72.2	1,234	239.0.0.0	1,234
Flow 7	192.168.72.2	1,234	239.0.0.0	1,234
Flow 8	192.168.72.2	1,234	239.0.0.0	1,234

WAN to LAN De-Encapsulation Configuration

	Mode	Input Destination IP Address (224~239.0~255.0~255.0~255)	Input Destination UDP Port (0 to 65535)	Input Bitrate Kbps
Flow 1	Enable	239.50.1.5	1,234	0
Flow 2	Disable	239.0.0.0	1,234	0
Flow 3	Disable	239.0.0.0	1,234	0
Flow 4	Disable	239.0.0.0	1,234	0
Flow 5	Disable	239.0.0.0	1,234	0
Flow 6	Disable	239.0.0.0	1,234	0
Flow 7	Disable	239.0.0.0	1,234	0
Flow 8	Disable	239.0.0.0	1,234	0

Figure 4-9 : WebEASY® - VLAN Based NAT

4.4.1. LAN to WAN: Input Configuration

Flows 1 to 256

Mode: This control allows the user to enable the associated input stream for encapsulation.

VLAN ID: This control allows the user to assign a VLAN ID to the associated flow; incoming packets of the flow with the specified VLAN ID will then be encapsulated.

Input Bit rate: This monitor will display the bit rate coming in on the port**.**

4.4.2. LAN to WAN: Encapsulation Header Configuration

Flows 1 to 256

Source IP Address: This control allows the user to set the physical source IP address of the incoming streams.

Source UDP Port: This control allows the user to set the physical source UDP port of the incoming streams.

Destination IP Address: This control is used to configure the output header encapsulation with the desired destination IP address.

Destination UDP Port: This control is used to configure the output header encapsulation with the desired destination UDP Port number.

4.4.3. WAN to LAN: De-Encapsulation Configuration

Flows 1 to 256

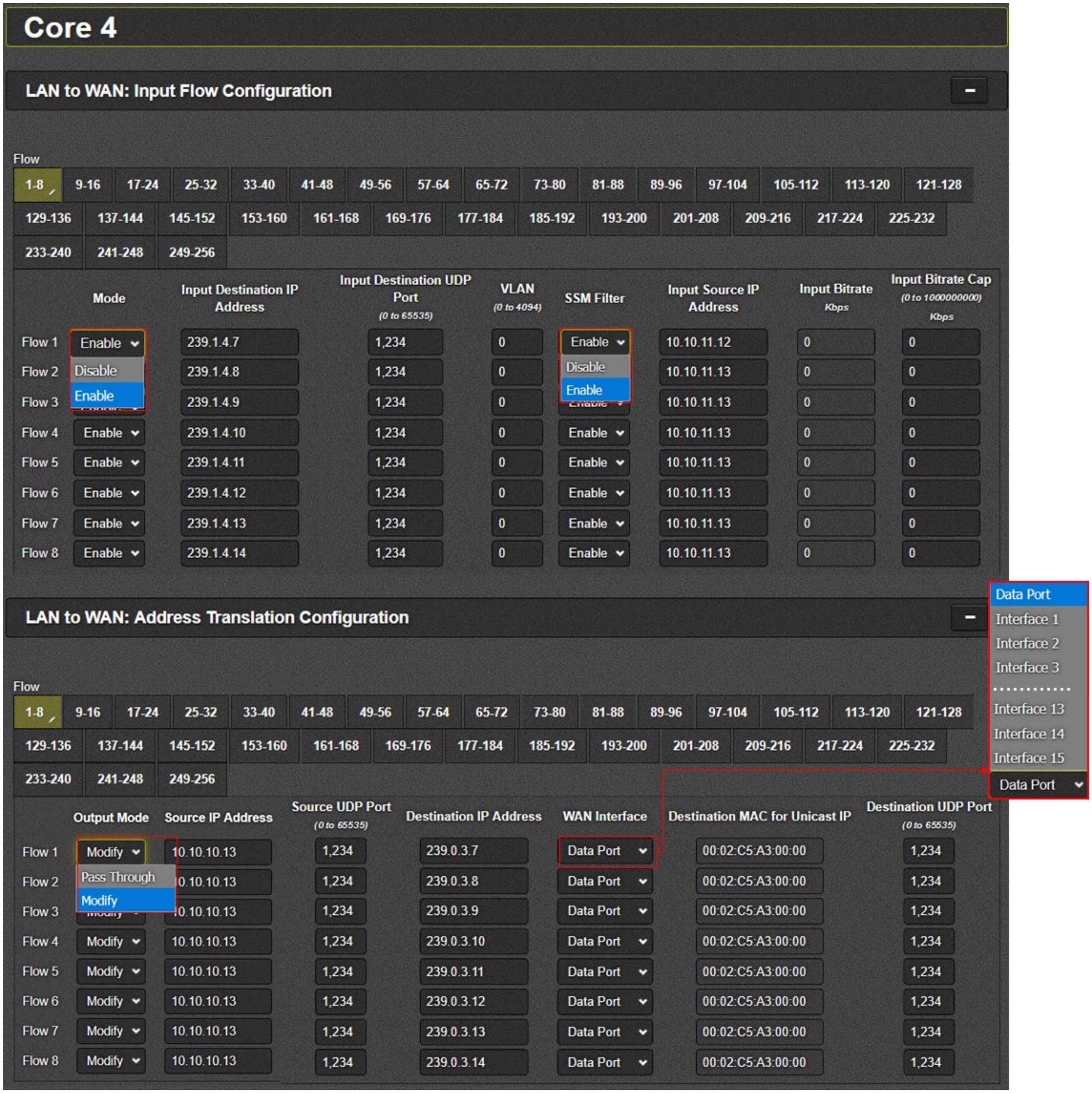
Mode: This control allows the user to enable the associated input stream which is going to be de-encapsulated.

Input Destination IP Address: This control allows the user to set the IP address of the packet to be received for de-encapsulation.

Input Destination UDP Port: This control allows the user to set the UDP Port number to be received for de-encapsulation.

Input Bit rate: This monitor will display the bit rate coming in on the port**.**

4.5. IP NAT



Core 4

LAN to WAN: Input Flow Configuration

	Mode	Input Destination IP Address	Input Destination UDP Port (0 to 65535)	VLAN (0 to 4094)	SSM Filter	Input Source IP Address	Input Bitrate Kbps	Input Bitrate Cap (0 to 1000000000) Kbps
Flow 1	Enable	239.1.4.7	1,234	0	Enable	10.10.11.12	0	0
Flow 2		239.1.4.8	1,234	0		10.10.11.13	0	0
Flow 3		239.1.4.9	1,234	0		10.10.11.13	0	0
Flow 4	Enable	239.1.4.10	1,234	0	Enable	10.10.11.13	0	0
Flow 5	Enable	239.1.4.11	1,234	0	Enable	10.10.11.13	0	0
Flow 6	Enable	239.1.4.12	1,234	0	Enable	10.10.11.13	0	0
Flow 7	Enable	239.1.4.13	1,234	0	Enable	10.10.11.13	0	0
Flow 8	Enable	239.1.4.14	1,234	0	Enable	10.10.11.13	0	0

LAN to WAN: Address Translation Configuration

	Output Mode	Source IP Address	Source UDP Port (0 to 65535)	Destination IP Address	WAN Interface	Destination MAC for Unicast IP	Destination UDP Port (0 to 65535)
Flow 1	Modify	10.10.10.13	1,234	239.0.3.7	Data Port	00:02:C5:A3:00:00	1,234
Flow 2		10.10.10.13	1,234	239.0.3.8	Data Port	00:02:C5:A3:00:00	1,234
Flow 3		10.10.10.13	1,234	239.0.3.9	Data Port	00:02:C5:A3:00:00	1,234
Flow 4	Modify	10.10.10.13	1,234	239.0.3.10	Data Port	00:02:C5:A3:00:00	1,234
Flow 5	Modify	10.10.10.13	1,234	239.0.3.11	Data Port	00:02:C5:A3:00:00	1,234
Flow 6	Modify	10.10.10.13	1,234	239.0.3.12	Data Port	00:02:C5:A3:00:00	1,234
Flow 7	Modify	10.10.10.13	1,234	239.0.3.13	Data Port	00:02:C5:A3:00:00	1,234
Flow 8	Modify	10.10.10.13	1,234	239.0.3.14	Data Port	00:02:C5:A3:00:00	1,234

Figure 4-10 : WebEASY® - Core Configured as IP NAT (Part 1 – LAN to WAN)

There is up to 256 transport streams that can be specified to be configured based on its multicast address and is sectioned into flow groups. Each flow group will display eight flows for configuration. There are 32 flow groups in total.

4.5.1. LAN to WAN: Input Flow Configuration

Flows 1 to 256

Mode: This control allows the user to enable or disable the input associated with that flow.

Input Destination IP Address: This control allows the user to set the Input Destination IP address of the packets to be received.

Input Destination UDP Port: This control allows the user to set the Destination UDP Port number to be received.

VLAN: This control allows the user to assign this flow to a VLAN.

SSM Filter: This control allows the user to enable Source Specific Multicast (SSM) channel based filtering.

Input Source IP Address: This control is used in NAT mode to configure the output header with the desired source IP address.

Input Bitrate: This monitor will display the bit rate of the streams that are being received in kbps.

Input Bitrate Cap: This control allows the user to set a cap on the bitrate for each flow in Kbps.

4.5.2. LAN to WAN: Address Translation Configuration

Flows 1 to 256

Output Mode: This control is used to set the output mode on the flow stream. Options are *Pass Through* or *Modify. Pass Through* will enable the stream to pass through without making any changes to the headers while *Modify* enables changes to the headers.

Source IP Address: This control is used in NAT mode to configure the output header with the desired source IP address.

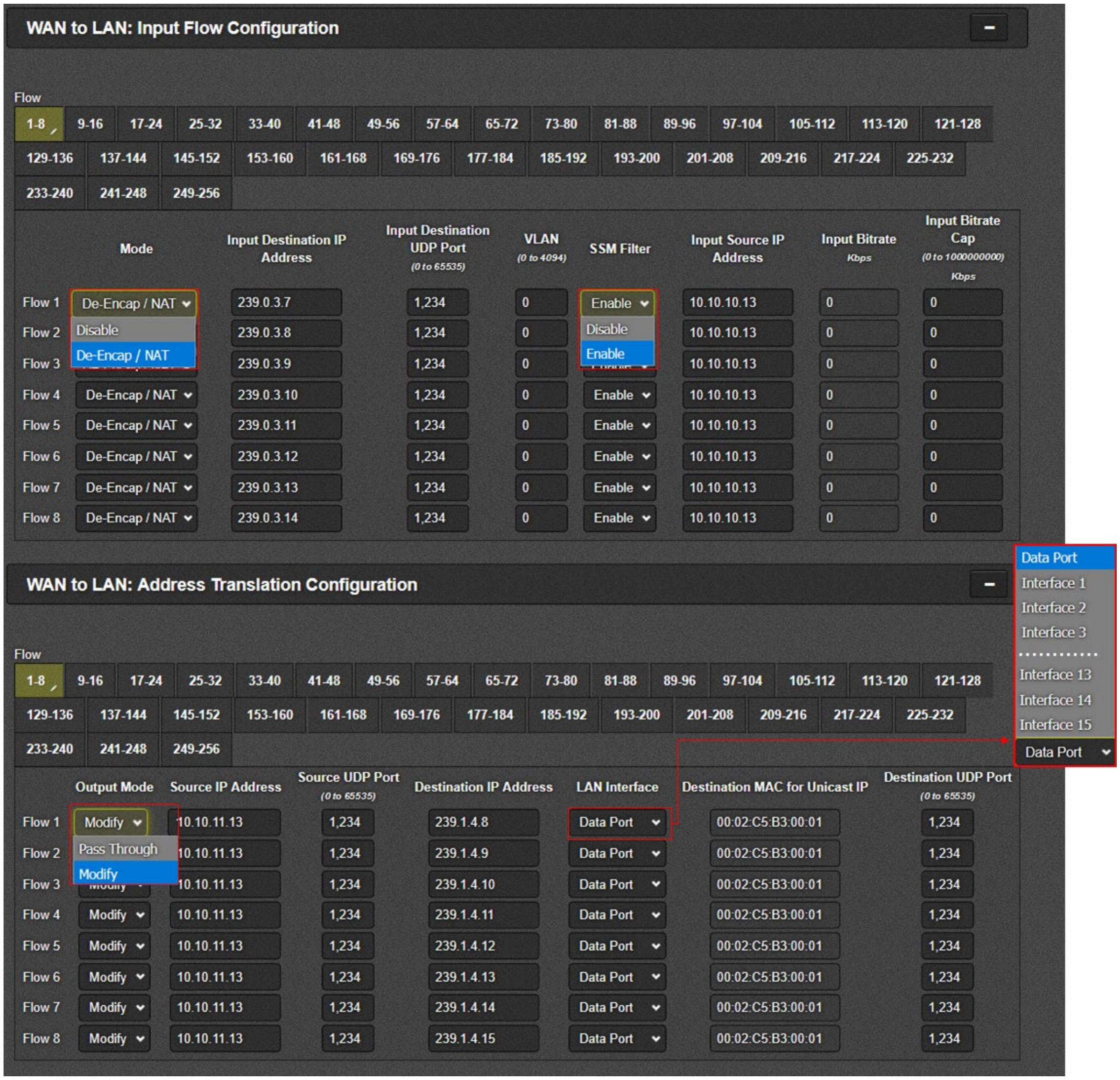
Source UDP Port: This control is used in NAT mode to configure the output header with the desired source UDP Port.

Destination IP Address: This control is used in NAT mode to configure the output header with the desired destination IP address.

WAN Interface: This control allows the user to set the WAN interface this flow passed through in LAN to WAN, the options given are to flow directly through data port or through a NAT virtual interface (Interfaces 1-15, Figure 4-10 shows an abbreviated menu).

Destination MAC for Unicast IP: This field displays the destination MAC.

Destination UDP Port: This control is used to enter the destination UDP port.



WAN to LAN: Input Flow Configuration

	Mode	Input Destination IP Address	Input Destination UDP Port (0 to 65535)	VLAN (0 to 4094)	SSM Filter	Input Source IP Address	Input Bitrate Kbps	Input Bitrate Cap (0 to 1000000000) Kbps
Flow 1	De-Encap / NAT	239.0.3.7	1,234	0	Enable	10.10.10.13	0	0
Flow 2		239.0.3.8	1,234	0		10.10.10.13	0	0
Flow 3		239.0.3.9	1,234	0		10.10.10.13	0	0
Flow 4	De-Encap / NAT	239.0.3.10	1,234	0	Enable	10.10.10.13	0	0
Flow 5	De-Encap / NAT	239.0.3.11	1,234	0	Enable	10.10.10.13	0	0
Flow 6	De-Encap / NAT	239.0.3.12	1,234	0	Enable	10.10.10.13	0	0
Flow 7	De-Encap / NAT	239.0.3.13	1,234	0	Enable	10.10.10.13	0	0
Flow 8	De-Encap / NAT	239.0.3.14	1,234	0	Enable	10.10.10.13	0	0

WAN to LAN: Address Translation Configuration

	Output Mode	Source IP Address	Source UDP Port (0 to 65535)	Destination IP Address	LAN Interface	Destination MAC for Unicast IP	Destination UDP Port (0 to 65535)
Flow 1	Modify	10.10.11.13	1,234	239.1.4.8	Data Port	00:02:C5:B3:00:01	1,234
Flow 2		10.10.11.13	1,234	239.1.4.9	Data Port	00:02:C5:B3:00:01	1,234
Flow 3		10.10.11.13	1,234	239.1.4.10	Data Port	00:02:C5:B3:00:01	1,234
Flow 4	Modify	10.10.11.13	1,234	239.1.4.11	Data Port	00:02:C5:B3:00:01	1,234
Flow 5	Modify	10.10.11.13	1,234	239.1.4.12	Data Port	00:02:C5:B3:00:01	1,234
Flow 6	Modify	10.10.11.13	1,234	239.1.4.13	Data Port	00:02:C5:B3:00:01	1,234
Flow 7	Modify	10.10.11.13	1,234	239.1.4.14	Data Port	00:02:C5:B3:00:01	1,234
Flow 8	Modify	10.10.11.13	1,234	239.1.4.15	Data Port	00:02:C5:B3:00:01	1,234

Figure 4-11 : WebEASY® - IP NAT (Part 2 – WAN to LAN)

4.5.3. WAN to LAN: Input Flow Configuration

Flows 1 to 256

Mode: This control allows the user to enable De-Encap/NAT or disable WAN to LAN for this flow.

Input Destination IP Address: This control allows the user to set the Input Destination IP address of the packets to be received.

Input Destination UDP Port: This control allows the user to set the Destination UDP Port number to be received.

VLAN: This control allows the user to assign this flow to a VLAN.

SSM Filter: This control allows the user to enable Source Specific Multicast (SSM) channel based filtering.

Input Source IP Address: This control is used in NAT mode to configure the output header with the desired source IP address.

Input Bitrate: This monitor will display the bit rate of the streams that are being received in kbps.

Input Bitrate Cap: This control allows the user to set a cap on the bitrate for each flow in Kbps.

4.5.4. WAN to LAN: Address Translation Configuration

Flows 1 to 256

Output Mode: This control is used to set the output mode on the flow stream. Options are *Pass Through* or *Modify. Pass Through* will enable the stream to pass through without making any changes to the headers while *Modify* enables changes to the headers.

Source IP Address: This control is used in NAT mode to configure the output header with the desired source IP address.

Source UDP Port: This control is used in NAT mode to configure the output header with the desired source UDP Port.

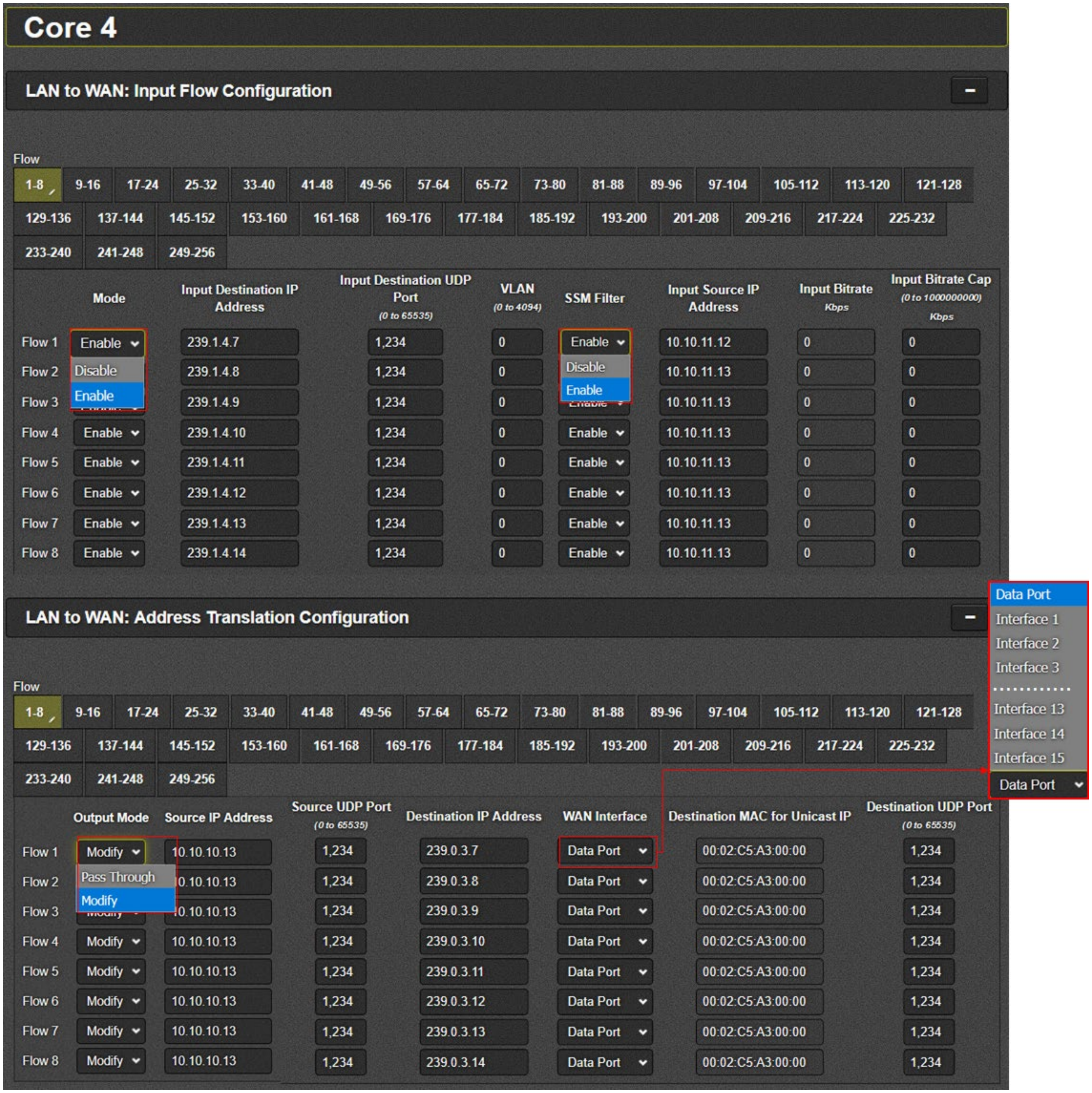
Destination IP Address: This control is used in NAT mode to configure the output header with the desired destination IP address.

LAN Interface: This control allows the user to set the LAN interface this flow passed through in WAN to LAN, the options given are to flow directly through data port or through a NAT virtual interface (Interfaces 1-15, Figure 4-11 shows an abbreviated menu).

Destination MAC for Unicast IP: This control is used to enter the Destination MAC address.

Destination UDP Port: This control is used in NAT mode to configure the output header with the desired destination UDP Port.

4.6. MC-IN-MC NAT + IP NAT



LAN to WAN: Input Flow Configuration

	Mode	Input Destination IP Address	Input Destination UDP Port (0 to 65535)	VLAN (0 to 4094)	SSM Filter	Input Source IP Address	Input Bitrate Kbps	Input Bitrate Cap (0 to 1000000000) Kbps
Flow 1	Enable	239.1.4.7	1,234	0	Enable	10.10.11.12	0	0
Flow 2		239.1.4.8	1,234	0		10.10.11.13	0	0
Flow 3		239.1.4.9	1,234	0		10.10.11.13	0	0
Flow 4	Enable	239.1.4.10	1,234	0	Enable	10.10.11.13	0	0
Flow 5	Enable	239.1.4.11	1,234	0	Enable	10.10.11.13	0	0
Flow 6	Enable	239.1.4.12	1,234	0	Enable	10.10.11.13	0	0
Flow 7	Enable	239.1.4.13	1,234	0	Enable	10.10.11.13	0	0
Flow 8	Enable	239.1.4.14	1,234	0	Enable	10.10.11.13	0	0

LAN to WAN: Address Translation Configuration

	Output Mode	Source IP Address	Source UDP Port (0 to 65535)	Destination IP Address	WAN Interface	Destination MAC for Unicast IP	Destination UDP Port (0 to 65535)
Flow 1	Modify	10.10.10.13	1,234	239.0.3.7	Data Port	00:02:C5:A3:00:00	1,234
Flow 2		10.10.10.13	1,234	239.0.3.8	Data Port	00:02:C5:A3:00:00	1,234
Flow 3		10.10.10.13	1,234	239.0.3.9	Data Port	00:02:C5:A3:00:00	1,234
Flow 4	Modify	10.10.10.13	1,234	239.0.3.10	Data Port	00:02:C5:A3:00:00	1,234
Flow 5	Modify	10.10.10.13	1,234	239.0.3.11	Data Port	00:02:C5:A3:00:00	1,234
Flow 6	Modify	10.10.10.13	1,234	239.0.3.12	Data Port	00:02:C5:A3:00:00	1,234
Flow 7	Modify	10.10.10.13	1,234	239.0.3.13	Data Port	00:02:C5:A3:00:00	1,234
Flow 8	Modify	10.10.10.13	1,234	239.0.3.14	Data Port	00:02:C5:A3:00:00	1,234

Figure 4-12 : WebEASY® - MC-in-MC NAT + IP NAT (Part 1)

There are up to 256 transport streams that can be specified to be configured based on its multicast address and is sectioned into flow groups. Each flow group will display eight flows for configuration. There are 32 flow groups in total.

4.6.1. LAN to WAN: Input Flow Configuration

Flows 1-256

Mode: This control allows the user to enable or disable the input associated with that flow.

Input Destination IP Address: This control allows the user to set the Input Destination IP address of the packets to be received.

Input Destination UDP Port: This control allows the user to set the Destination UDP Port number to be received.

VLAN: This control allows the user to assign this flow to a VLAN.

SSM Filter: This control allows the user to enable Source Specific Multicast (SSM) channel based filtering.

Input Source IP Address: This control is used in NAT mode to configure the output header with the desired source IP address.

Input Bitrate: This monitor will display the bit rate of the streams that are being received in kbps.

Input Bitrate Cap: This control allows the user to set a cap on the bitrate for each flow in Kbps.

4.6.2. LAN to WAN: Address Translation Configuration

NAT Cores (1-6) and Flows 1 to 256

Output Mode: This control is used to set the output mode on the flow stream. Options are *Pass Through* or *Modify. Pass Through* will enable the stream to pass through without making any changes to the headers while *Modify* enables changes to the headers.

Source IP Address: This control is used in NAT mode to configure the output header with the desired source IP address.

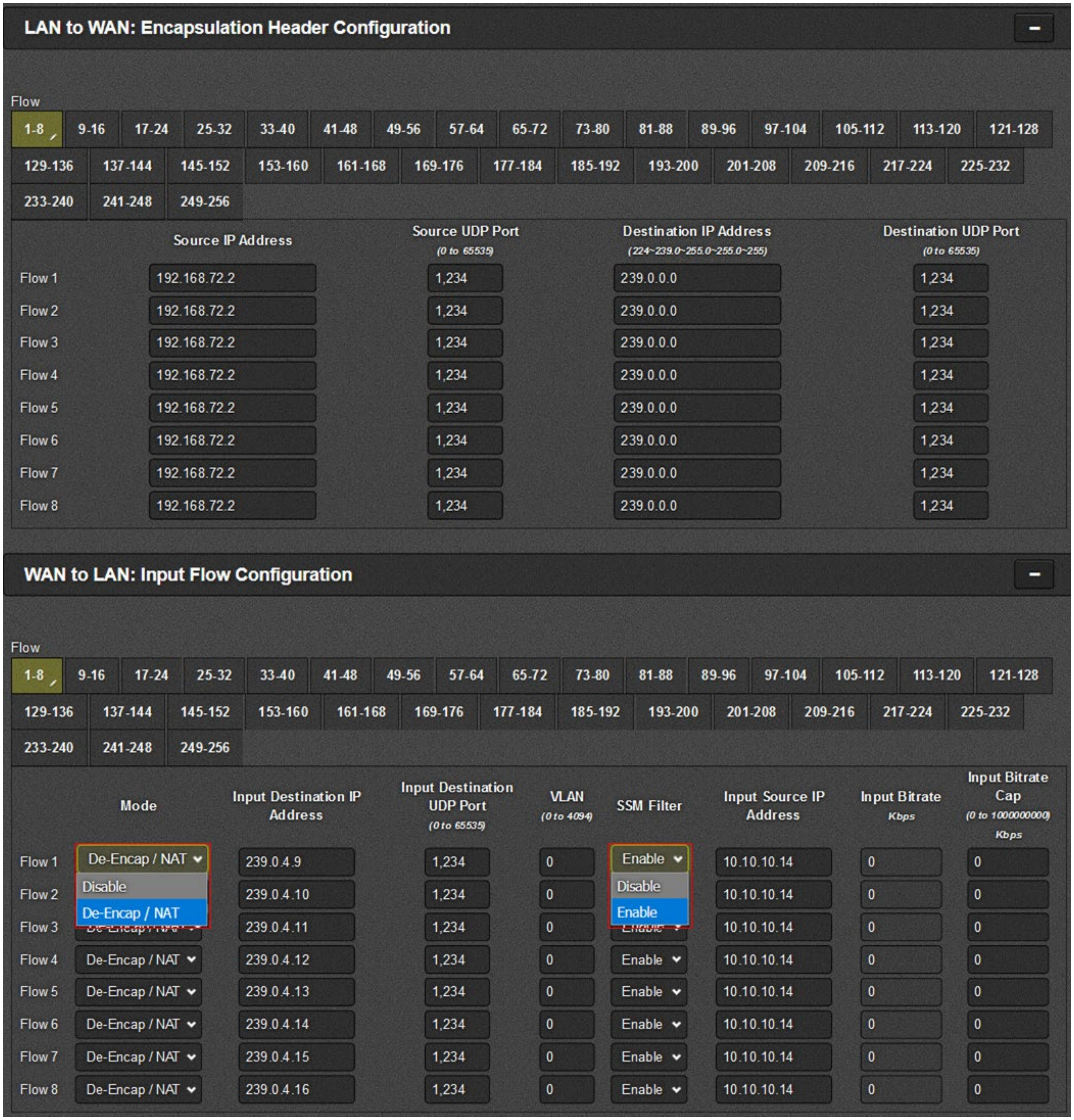
Source UDP Port: This control is used in NAT mode to configure the output header with the desired source UDP Port.

Destination IP Address: This control is used in NAT mode to configure the output header with the desired destination IP address.

WAN Interface: This control allows the user to set the WAN interface this flow passed through in LAN to WAN, the options given are to flow directly through data port or through a NAT virtual interface (Interfaces 1-15, Figure 4-12 shows an abbreviated menu).

Destination MAC for Unicast IP: This field displays the destination MAC.

Destination UDP Port: This control is used to enter the destination UDP port.



LAN to WAN: Encapsulation Header Configuration

Flow

	Source IP Address	Source UDP Port *(0 to 65535)*	Destination IP Address *(224~239.0~255.0~255.0~255)*	Destination UDP Port *(0 to 65535)*
Flow 1	192.168.72.2	1,234	239.0.0.0	1,234
Flow 2	192.168.72.2	1,234	239.0.0.0	1,234
Flow 3	192.168.72.2	1,234	239.0.0.0	1,234
Flow 4	192.168.72.2	1,234	239.0.0.0	1,234
Flow 5	192.168.72.2	1,234	239.0.0.0	1,234
Flow 6	192.168.72.2	1,234	239.0.0.0	1,234
Flow 7	192.168.72.2	1,234	239.0.0.0	1,234
Flow 8	192.168.72.2	1,234	239.0.0.0	1,234

WAN to LAN: Input Flow Configuration

Flow

	Mode	Input Destination IP Address	Input Destination UDP Port *(0 to 65535)*	VLAN *(0 to 4094)*	SSM Filter	Input Source IP Address	Input Bitrate Kbps	Input Bitrate Cap *(0 to 1000000000)* Kbps
Flow 1	De-Encap / NAT	239.0.4.9	1,234	0	Enable	10.10.10.14	0	0
Flow 2	Disable De-Encap / NAT	239.0.4.10	1,234	0	Disable Enable	10.10.10.14	0	0
Flow 3	De-Encap / NAT	239.0.4.11	1,234	0	Enable	10.10.10.14	0	0
Flow 4	De-Encap / NAT	239.0.4.12	1,234	0	Enable	10.10.10.14	0	0
Flow 5	De-Encap / NAT	239.0.4.13	1,234	0	Enable	10.10.10.14	0	0
Flow 6	De-Encap / NAT	239.0.4.14	1,234	0	Enable	10.10.10.14	0	0
Flow 7	De-Encap / NAT	239.0.4.15	1,234	0	Enable	10.10.10.14	0	0
Flow 8	De-Encap / NAT	239.0.4.16	1,234	0	Enable	10.10.10.14	0	0

Figure 4-13 : WebEASY® - MC-in-MC NAT + IP NAT (Part 2)

4.6.3. LAN to WAN : Encapsulation Header Configuration

Flows 1-256

Source IP Address: Allows user to designate source IP for encapsulation header.

Source UDP Port: Allows user to designate source UDP Port for encapsulation.

Destination IP Address: Allows user to designate the destination IP for encap.

Destination UDP Port: Allows user to designate the destination UDP port for encap.

4.6.4. WAN to LAN: Input Flow Configuration

Flows 1 to 256

Mode: This control allows the user to enable De-Encap/NAT or disable WAN to LAN for this flow.

Input Destination IP Address: This control allows the user to set the Input Destination IP address of the packets to be received.

Input Destination UDP Port: This control allows the user to set the Destination UDP Port number to be received.

VLAN: This control allows the user to assign this flow to a VLAN.

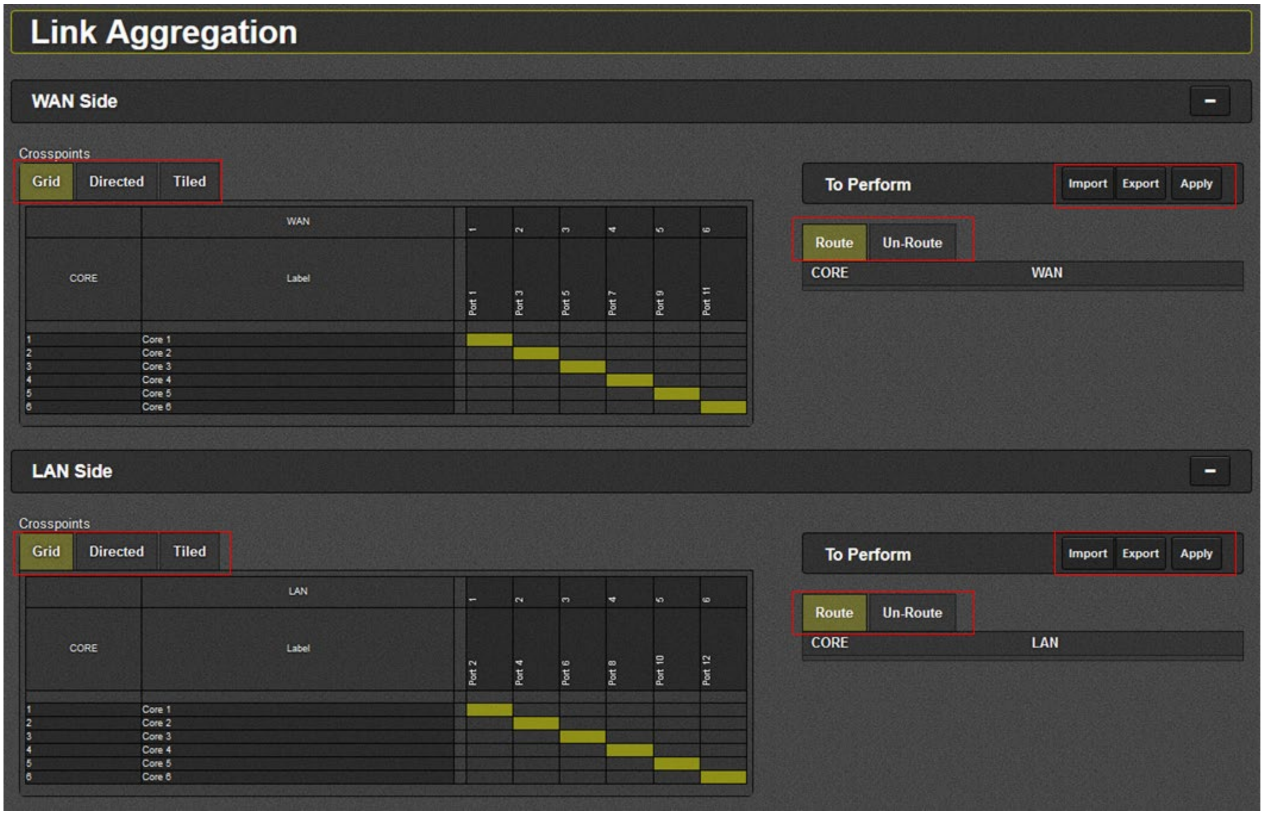
SSM Filter: This control allows the user to enable Source Specific Multicast (SSM) channel based filtering.

Input Source IP Address: This control is used in NAT mode to configure the output header with the desired source IP address.

Input Bitrate: This monitor will display the bit rate of the streams that are being received in kbps.

Input Bitrate Cap: This control allows the user to set a cap on the bitrate for each flow in Kbps.

4.7. LINK AGGREGATION



	WAN	1	2	3	4	5	6
CORE	Label	Port 1	Port 3	Port 5	Port 7	Port 9	Port 11
1	Core 1	🟨					
2	Core 2		🟨				
3	Core 3			🟨			
4	Core 4				🟨		
5	Core 5					🟨	
6	Core 6						🟨

	LAN	1	2	3	4	5	6
CORE	Label	Port 2	Port 4	Port 6	Port 8	Port 10	Port 12
1	Core 1	🟨					
2	Core 2		🟨				
3	Core 3			🟨			
4	Core 4				🟨		
5	Core 5					🟨	
6	Core 6						🟨

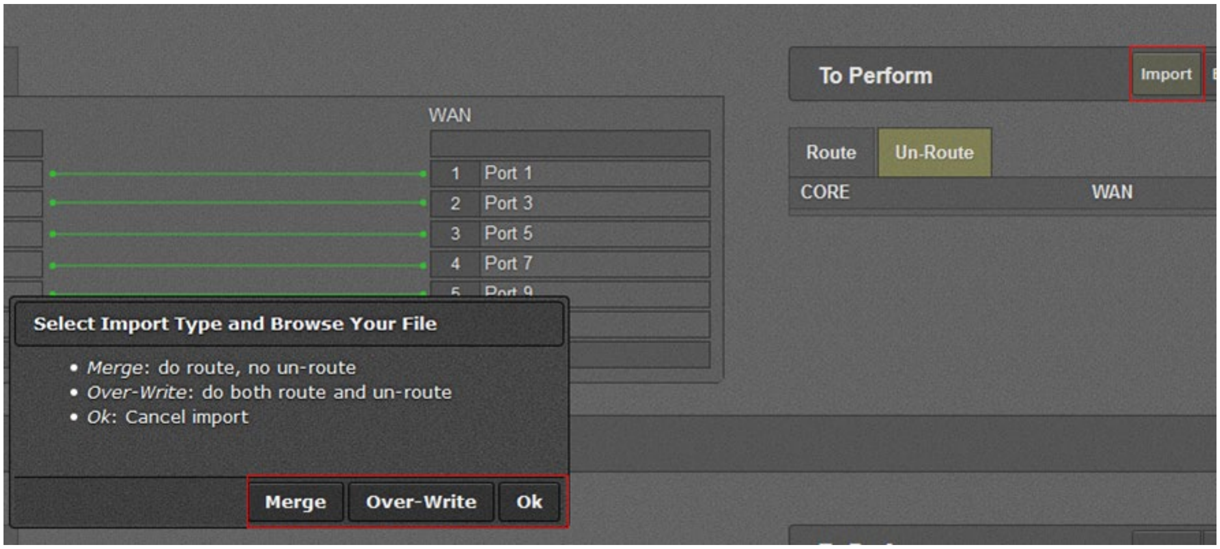
Figure 4-14: WebEASY® - Link Aggregation

Link aggregation allows users to direct the flow of data through WAN port – CORE – LAN port by assigning which WAN port is assigned to each core, and which LAN port is assigned to each core. This allows users to change the routing from the default shown in Figure 1-2. This routing can be done using ‘grid’, ‘directed’ and ‘tiled’ views, descbired below.

A given processing core cannot contribute its Tx traffic to more than one WAN port. Correspondingly, a given processing core cannot receive traffic from more than one WAN port.

When changing routes, it is important to select ‘Apply’ in the ‘To Perform’ menu for the changes to be applied.

To import a route from compatible router settings file (in .json format), select ‘Import’ from the ‘To Perform’ menu.

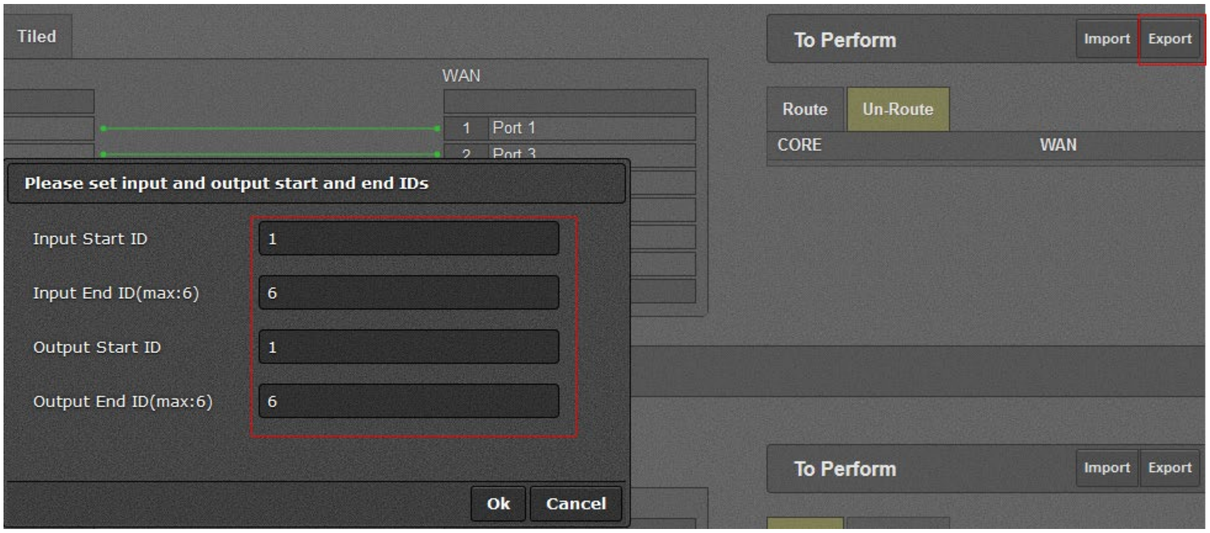


Select Import Type and Browse Your File

- *Merge*: do route, no un-route
- *Over-Write*: do both route and un-route
- *Ok*: Cancel import

Figure 4-15 : WebEASY® - Link Aggregation \ Import Route

Selecting ‘Import’ will open an options menu prompting the user to select how existing routes are handled. ‘Merge’ will add imported routes but will not un-route current routes, in cases of conflicting routes the current route will be kept and the imported route ignored. ‘Over-Write’ will both route and un-route, all existing routes will be unrouted and the routing will be set exactly as it is in the imported router settings file. Selecting ‘Ok’ will cancel import.



Please set input and output start and end IDs

Input Start ID: 1

Input End ID(max:6): 6

Output Start ID: 1

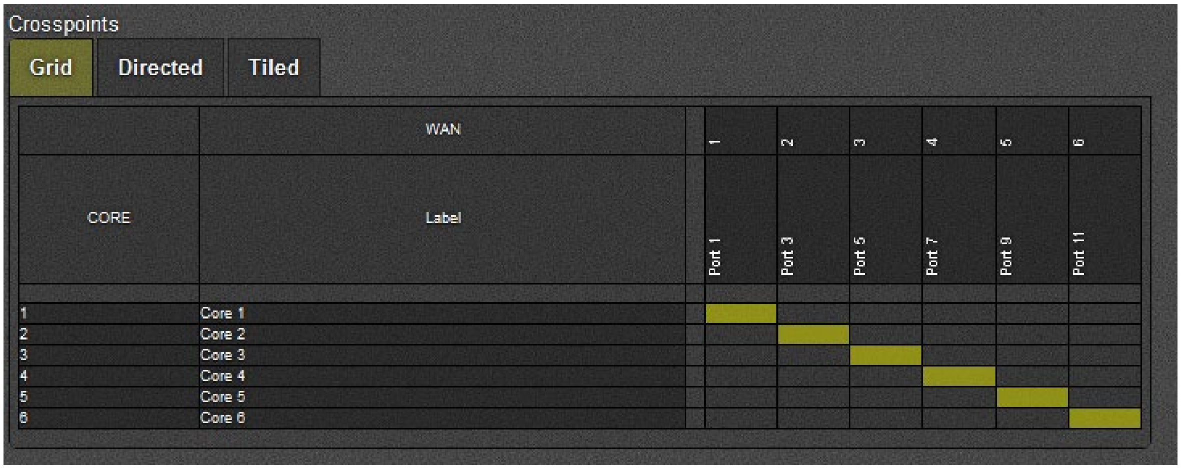
Output End ID(max:6): 6

Figure 4-16 : WebEASY® - Link Aggregation \ Export Route

To export the currently set route to a router settings file, select ‘Export’ from the ‘To Perform’ menu. A menu will appear prompting the user to set the range of inputs and outputs to be exported. Selecting ‘Ok’ will bring up a save file menu in the browser (this is the browser ‘save file’ menu and will vary by browser).

In the link aggregation page, the ‘Route’and ‘Un-Route’ menus (See Figure 4-14) pull up the que of routes the user has selected to be added, and the que of routes to be un-routed’, respectively. This allows the user to track the routes that are being added or removed before selecting ‘Apply’ and changes take effect.

4.7.1. Link Aggregation - Grid



CORE	WAN Label	1 Port 1	2 Port 3	3 Port 5	4 Port 7	5 Port 9	6 Port 11
1	Core 1	🟨					
2	Core 2		🟨				
3	Core 3			🟨			
4	Core 4				🟨		
5	Core 5					🟨	
6	Core 6						🟨

Figure 4-17 : WebEASY® - Link Aggregation\Grid View

The grid view allows users to set routes for both LAN side and WAN side (separately, as shown in Figure 4-14) by matching a port to a core insid the grid. For example, Port 1 is currently mapped to Core 1. If I wanted to link Port 9 to Core 1 instead, I would select the intersecting grid box for Core 1 and Port 9 (shown below in Figure 4-18).

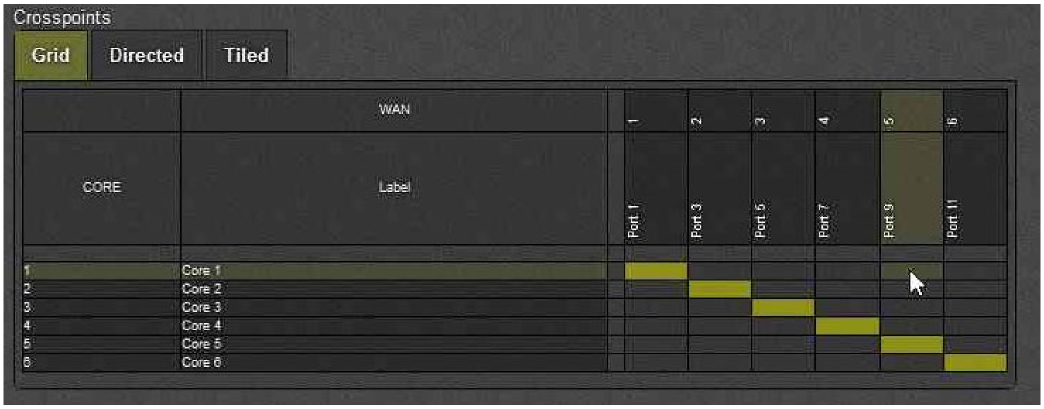
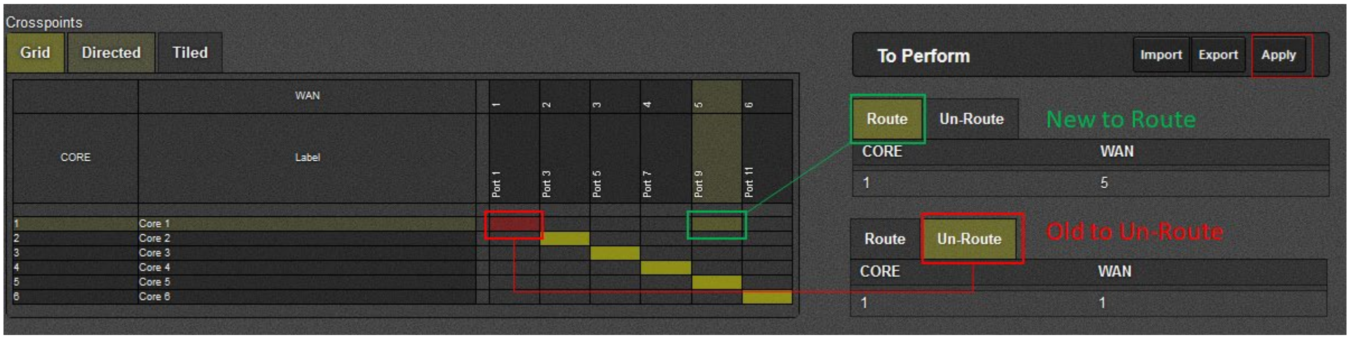


Figure 4-18 : WebEASY® - Link Aggregation\Grid View\Linking in Grid

Once this new route is selected in grid, it will be placed in the 'To Perform' que as shown below in Figure 4-19. Here, the old route will be shown in red on the grid, and the route to be Un-Routed will appear in the 'Un-Route' menu selection. The new route will be shown in beige green on the grid, and the new route to be routed will appear in the 'route' menu selection. Multiple route changes can be qued into the 'To Perform' menu. To apply the changes shown in the 'To Perform' que, select 'Apply'.

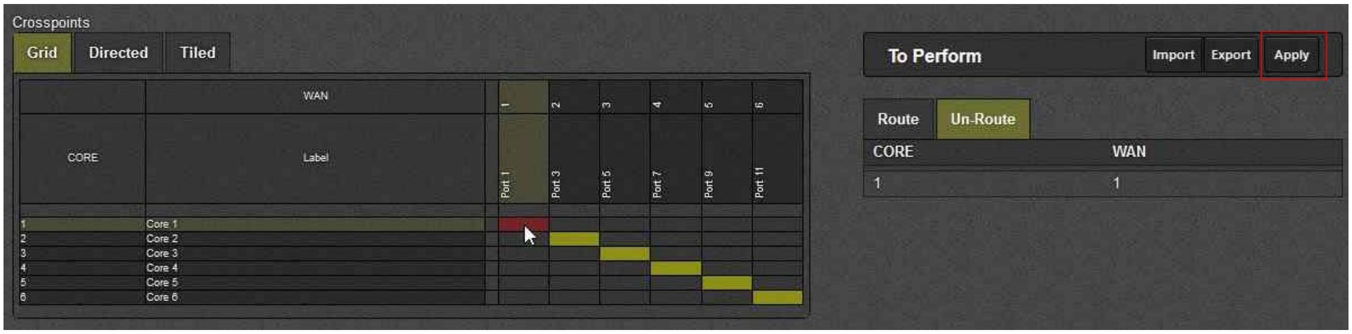


CORE	WAN
1	5

CORE	WAN
1	1

Figure 4-19 : WebEASY® - Link Aggregation\Grid View\To Perform in Grid

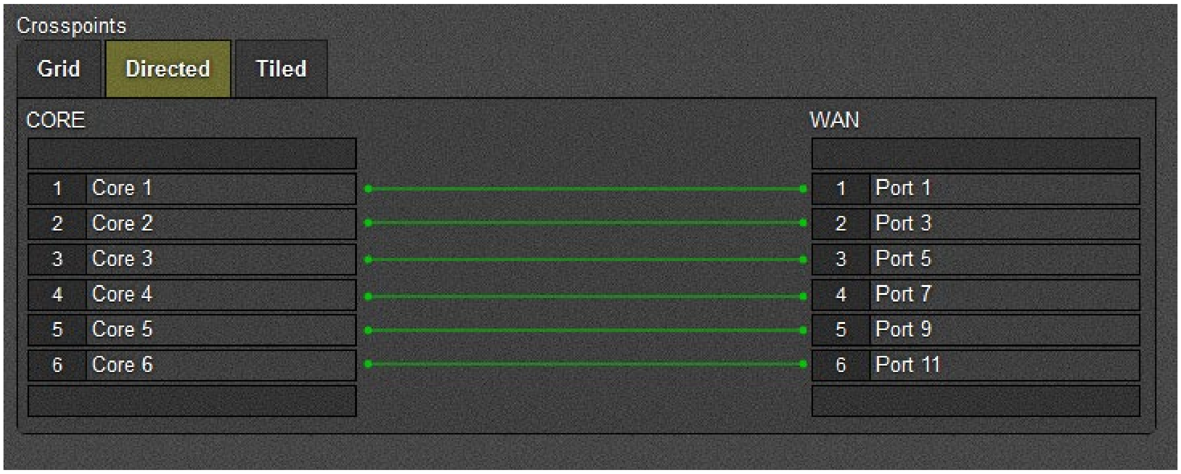
To Un-Route without creating any new route to override, simply select the assigned core-port pair grid space and click on it. This will turn that grid space red and the route will be added to the Un-Route que in 'To Perform', select 'Apply' for changes to take effect.



CORE	WAN
1	1

Figure 4-20 : WebEASY® - Link Aggregation\Grid View\Removing Links in Grid

4.7.2. Link Aggregation – Directed



CORE		WAN	
1	Core 1	1	Port 1
2	Core 2	2	Port 3
3	Core 3	3	Port 5
4	Core 4	4	Port 7
5	Core 5	5	Port 9
6	Core 6	6	Port 11

Figure 4-21 : WebEASY® - Link Aggregation\Directed View

The directed view allows users to assign routes in a drag-and-drop manner by selecting a core from the 'Core' column and dragging it to the port it is to be assigned. The example shown below in Figure 4-22 shows how to map Core 1 to Port 9 using drag-and-drop in directed view.

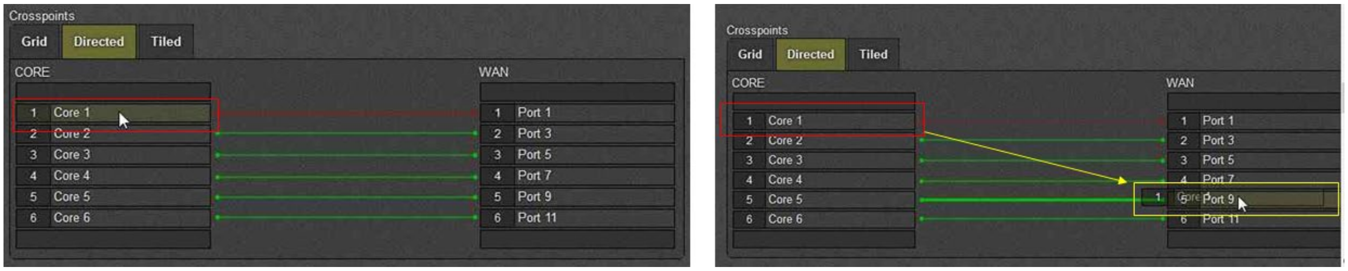
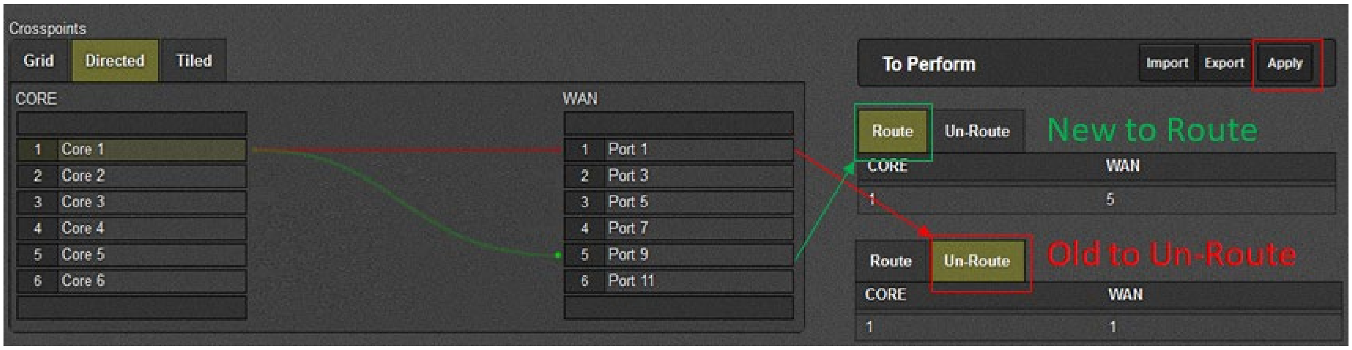


Figure 4-22 : WebEASY® - Link Aggregation\Directed View\Linking in Directed

When the new link is created, the old route to be unrouted will appear as a line in red and the old route will appear in the 'Un-Route' table of the 'To Perform' menu, as shown below in Figure 4-23. The new link will appear in green and will be displayed in the 'Route' table of the To Perform menu. Select 'Apply' in the 'To Perform' menu for route changes to be implemented.



Route:

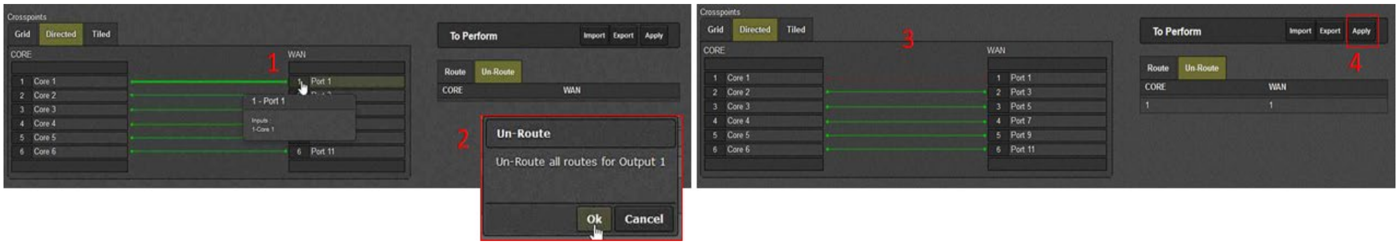
CORE	WAN
1	5

Un-Route:

CORE	WAN
1	1

Figure 4-23 : WebEASY® - Link Aggregation\Directed View\To Perform in Directed

Directed view also allows for unmapping without creating a new route (shown below in Figure 4-24). To do so, select the port to be unmapped (1), this will bring up a menu prompting the user if they wish to un-route for that port (2) click ok to un-route, once this is done the link will appear in red and will be displayed in the ‘Un-Route’ table in the ‘To Perform’ menu (3). Click ‘Apply’ in the ‘To Perform’ menu to apply changes (4).



1 - Port 1
Inputs :
1-Core 1

Un-Route
Un-Route all routes for Output 1

CORE	WAN
1	1

Figure 4-24 : WebEASY® - Link Aggregation\Directed View\Removing Links in Directed

4.7.3. Link Aggregation - Tiled

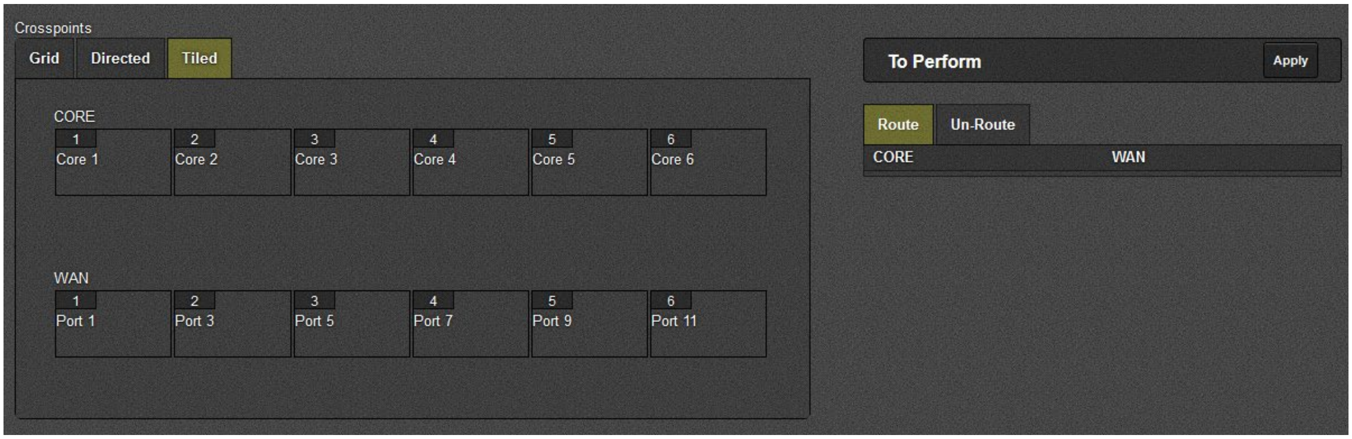
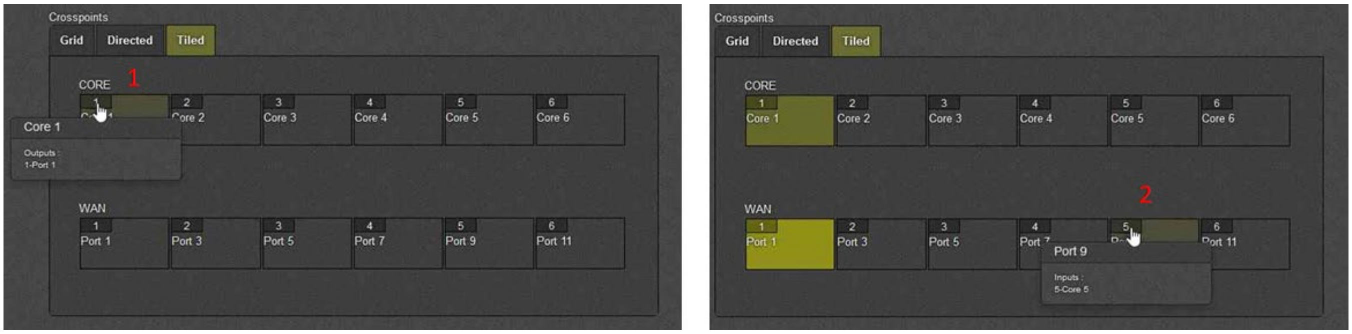


Figure 4-25 : WebEASY® - Link Aggregation\Tiled View

The tiled view allows users to set routes by selecting a tile for a core and matching it to a tile for a port. To create a route, select a core (1) and then select the port you’d like to link it to (2), shown below in Figure 4-26.

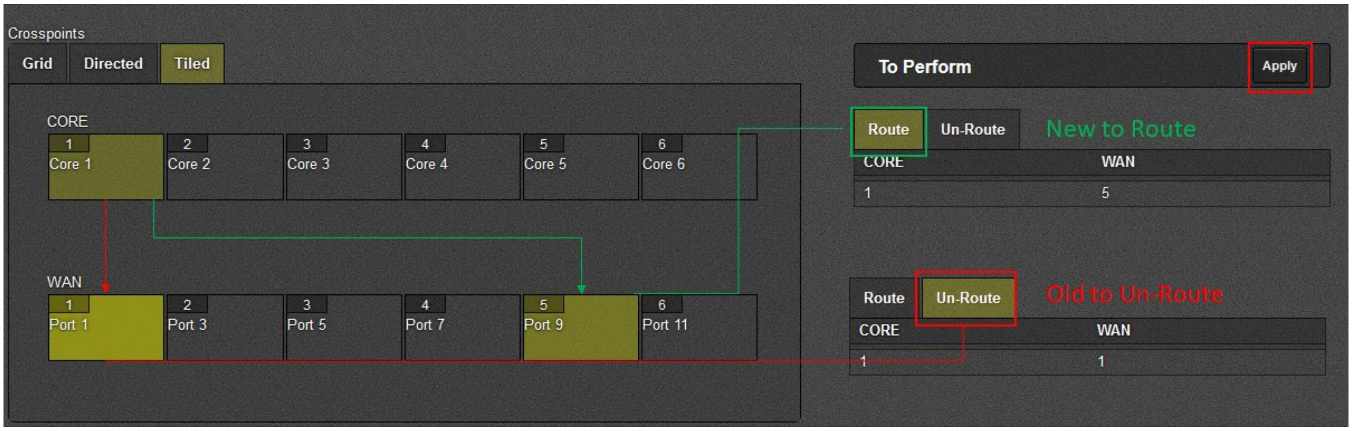


Core 1
Outputs :
1-Port 1

Port 9
Inputs :
5-Core 5

Figure 4-26 : WebEASY® - Link Aggregation\Tiled View\Linking in Tiled

Once you’ve selected a route (shown below in Figure 4-27), both the old route and new route WAN or LAN tile will appear as highlighted along with the highlighted tile for the core being assigned. The changes to the route will appear in the ‘Route’ and ‘Un-route’ (if this new route will undo an old one) tables in the ‘To Perform’ menu. To apply this new route, select ‘Apply’ in the ‘To Perform’ menu.



Route

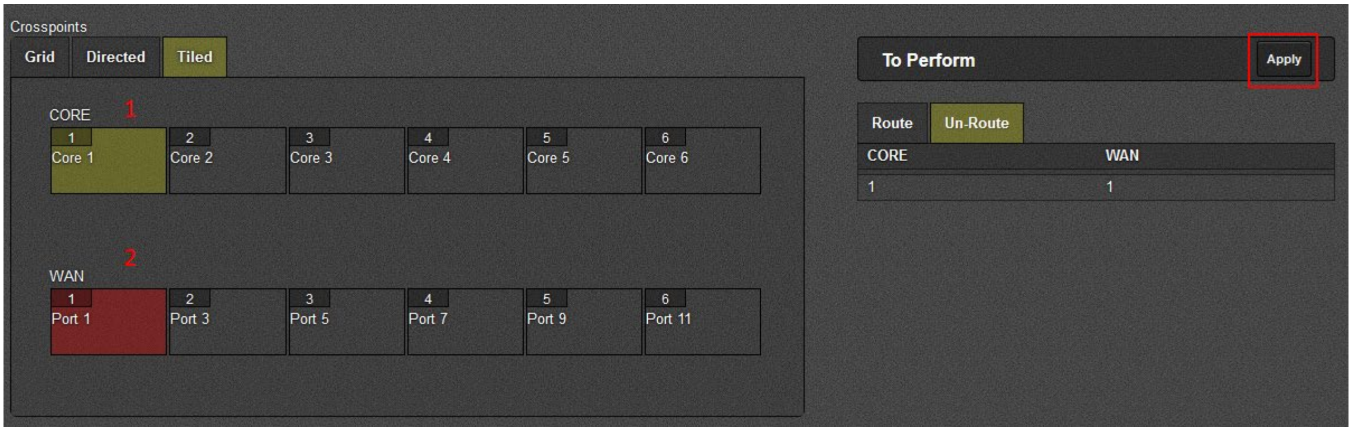
CORE	WAN
1	5

Un-Route

CORE	WAN
1	1

Figure 4-27 : WebEASY® - Link Aggregation\Tiled View\Linking in Tiled

To unlink a port from a core, as shown below in Figure 4-28, select the tile for the respective core, the port currently linked to that core will become highlighted in beige green (the same color the core is highlighted). Next, with the core tile selected, select the highlighted port tile. If it is qued to be un-routed, it will appear red (2) and appear in the ‘Un-Route’ table in the ‘To Perform’ menu.



Un-Route

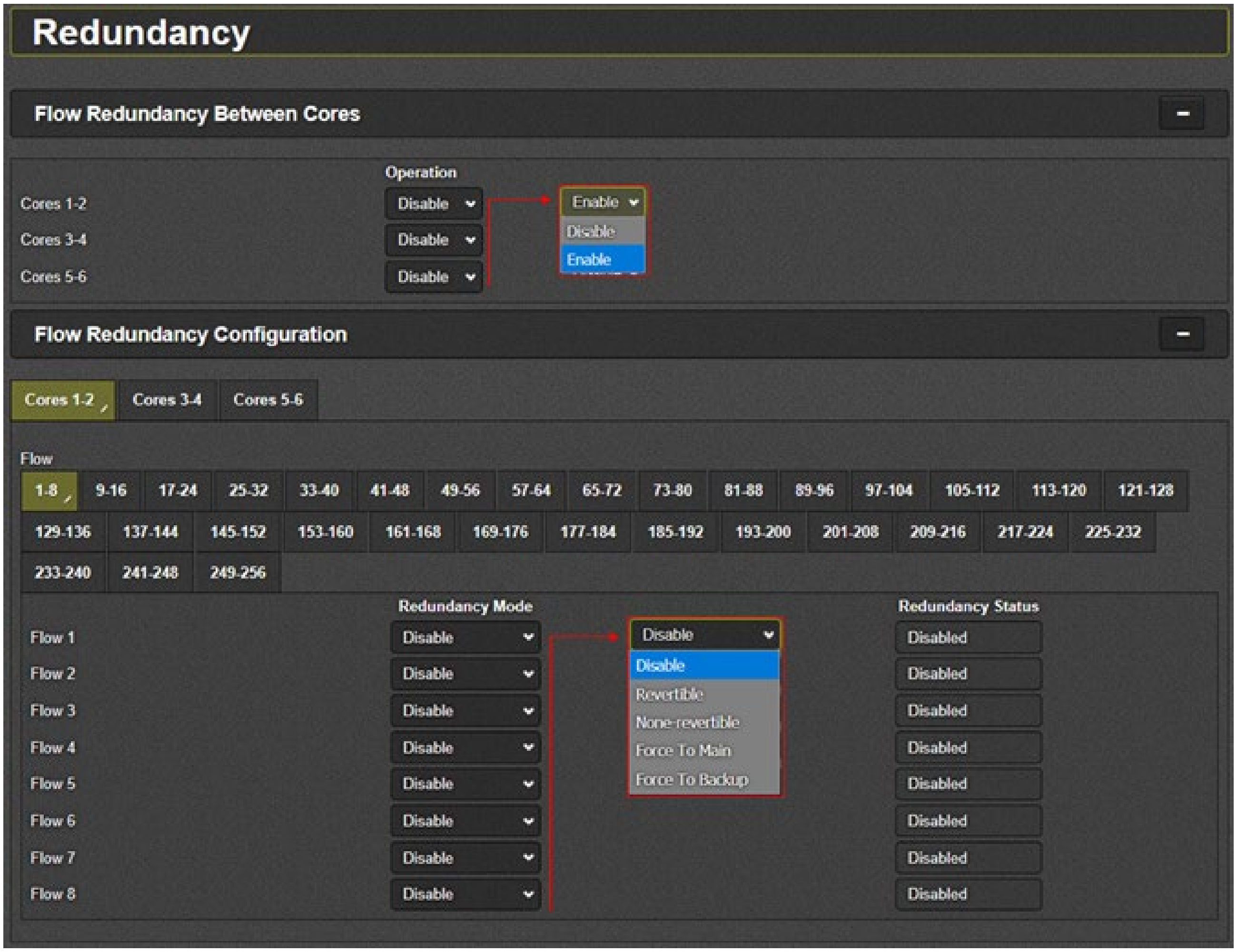
CORE	WAN
1	1

Figure 4-28 : WebEASY® - Link Aggregation\Directed View\Removing Links in Tiled

This feature allows multiple processing cores to aggregate their Tx traffic to a single WAN Port. Correspondingly, Rx traffic from that WAN port is distributed to all contributing processing cores. In the figure above, Cores 1 & 6 are configured to aggregate their traffic to WAN Port 1.

4.8. REDUNDANCY

Redundancy allows for traffic to be re-routed to a backup core upon failure. For redundancy, cores are paired as 1-2, 3-4, 5-6. Behavior of a data flow upon failure can be assigned separately for each individual flow separate from each other flow on that core. Note that flow redundancy must be enabled for the core in order for it to be enabled on the flow within that core.



Redundancy

Flow Redundancy Between Cores

	Operation
Cores 1-2	Disable
Cores 3-4	Disable
Cores 5-6	Disable

Flow Redundancy Configuration

Flow	Redundancy Mode	Redundancy Status
Flow 1	Disable	Disabled
Flow 2	Disable	Disabled
Flow 3	Disable	Disabled
Flow 4	Disable	Disabled
Flow 5	Disable	Disabled
Flow 6	Disable	Disabled
Flow 7	Disable	Disabled
Flow 8	Disable	Disabled

Figure 4-29 : WebEASY® - Redundancy

4.8.1. Flow Redundancy Between Cores

Cores act as backup for for eachother in pairs 1-2, 3-4, and 5-6. Redundancy is enabled for each set of pairs. Flow redundancy between cores must be enabled here to enable flow redundancy for individual flows on the core.

4.8.2. Flow Redundancy Configuration

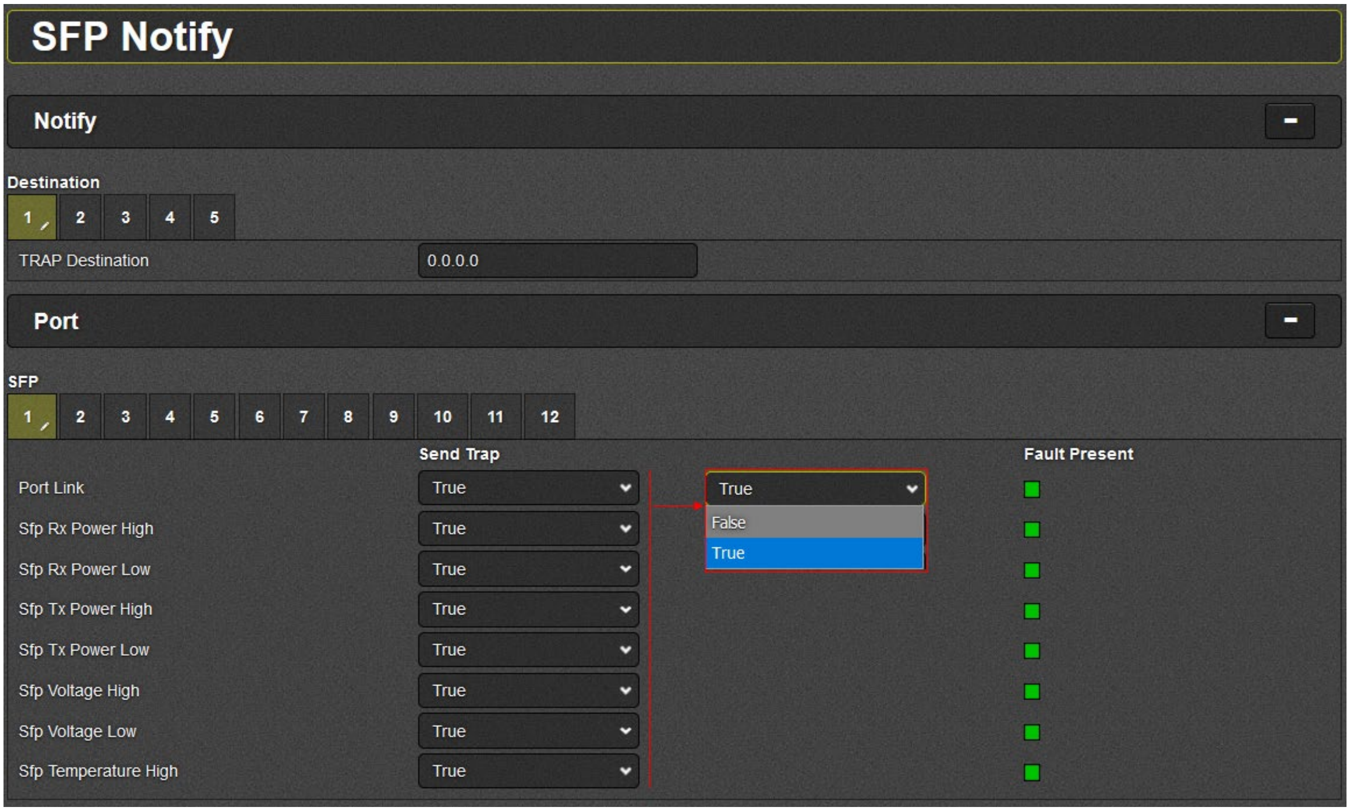
1- **Revertible** - In this mode, when the flow fails over to backup, it will remain on the backup path until the main path heals. When the main path is healed, the output will switch back to main.

2- **None-revertible** – In this mode, when the flow fails over to backup path, it will remain on the backup even when the main path heals. Then when the backup path fails, the unit will switch back to the main path.

3- **Force to Main**- In this mode, when the flow fails over it is forced to main and will remain.

4- **Force to Backup-** In this mode, when the flow fails over it is forced to backup and will remain.

4.9. SFP NOTIFY



TRAP Destination	0.0.0.0

	Send Trap	Fault Present
Port Link	True	🟩
Sfp Rx Power High	True	🟩
Sfp Rx Power Low	True	🟩
Sfp Tx Power High	True	🟩
Sfp Tx Power Low	True	🟩
Sfp Voltage High	True	🟩
Sfp Voltage Low	True	🟩
Sfp Temperature High	True	🟩

Figure 4-30: WebEASY® -SFP Notify

4.9.1. Notify

For Destination 1 to 5

Trap Destination: This control is used to specify the trap address for sending out trap messages for *Link Status* faults and *SFP* faults.

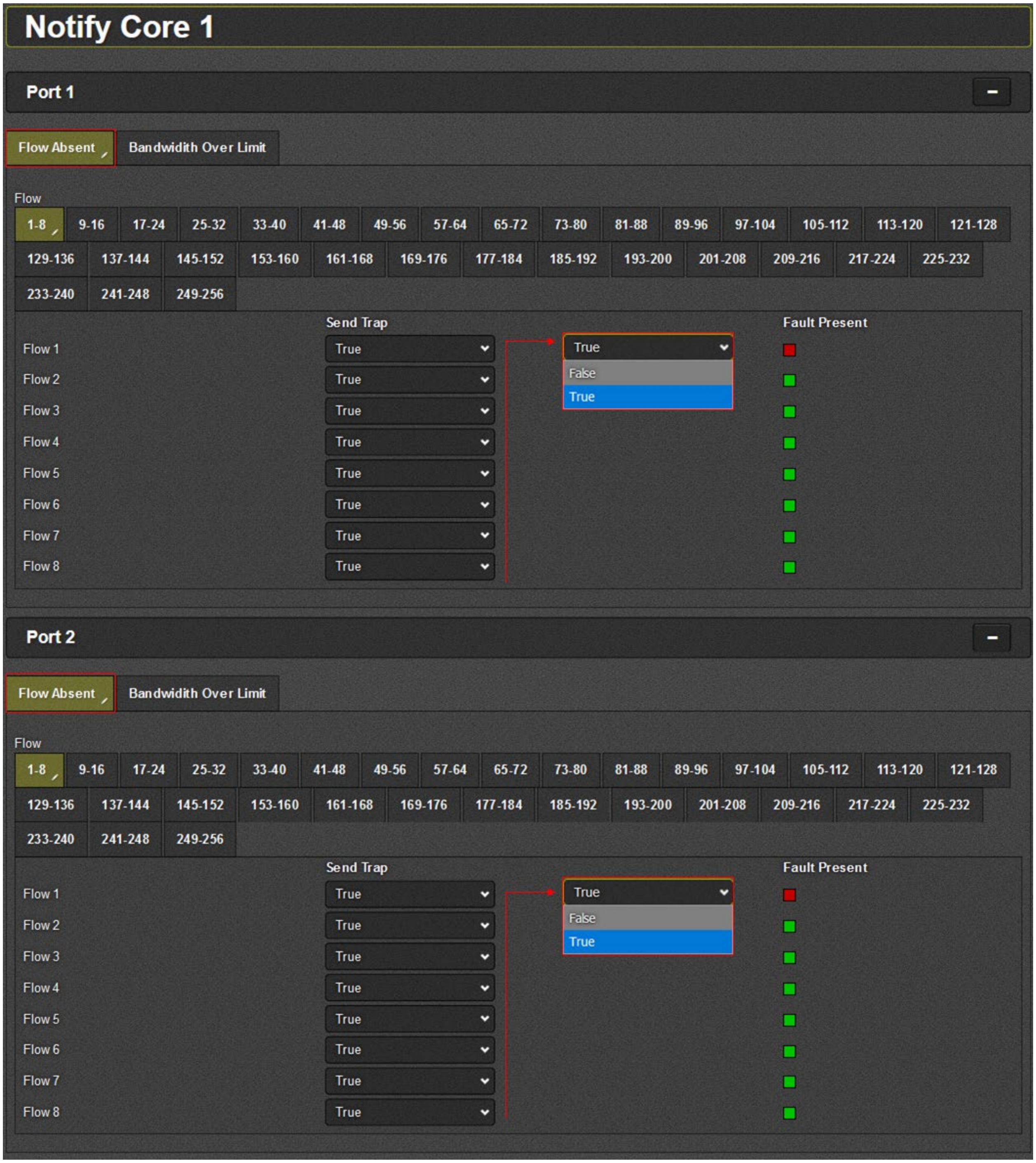
4.9.2. Port

For SFP 1 to 12

Trap alarms can be enabled (True) or disabled (False) for *Port Link*, and SFPs operating outside of a designated range (set in the system menu, see section 4.1.8).

4.10. NOTIFY CORE

A notify core page is available for all 6 cores, each is identical regardless of which NAT configuration the core is using. The Notify Core allows for the user to set traps based on flow absence, and on bandwidth over limit. Traps are set individually for each flow assigned to a core, and are assigned separate on the WAN and LAN ports. Traps are activated by selecting ‘True’ under the ‘Send Trap’ dropdown. The ‘fault present’ monitor will display red if a fault is present on the flow and green if no fault is detected.



Notify Core 1

Port 1

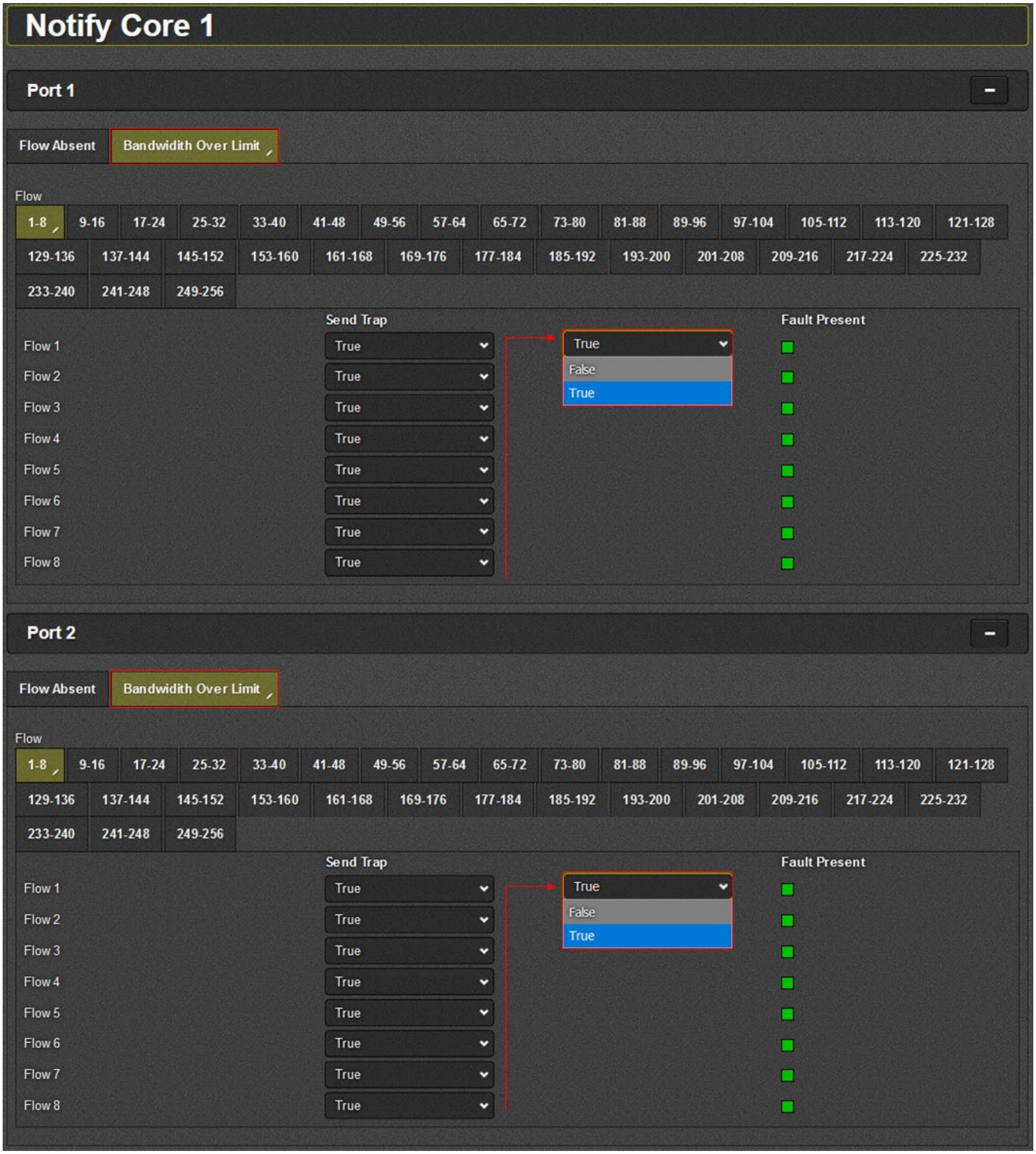
	Send Trap	Fault Present
Flow 1	True	🟥
Flow 2	True	🟩
Flow 3	True	🟩
Flow 4	True	🟩
Flow 5	True	🟩
Flow 6	True	🟩
Flow 7	True	🟩
Flow 8	True	🟩

Port 2

	Send Trap	Fault Present
Flow 1	True	🟥
Flow 2	True	🟩
Flow 3	True	🟩
Flow 4	True	🟩
Flow 5	True	🟩
Flow 6	True	🟩
Flow 7	True	🟩
Flow 8	True	🟩

Figure 4-31 : WebEASY® - Notify Core (1) \ Flow Absent

Like the ‘Flow Absent’ notify menu (shown above in **Figure 4-31**), the ‘Bandwidth Over Limit’ menu (shown beloe in **Figure 4-32**)



Port 1

	Send Trap	Fault Present
Flow 1	True	🟩
Flow 2	True	🟩
Flow 3	True	🟩
Flow 4	True	🟩
Flow 5	True	🟩
Flow 6	True	🟩
Flow 7	True	🟩
Flow 8	True	🟩

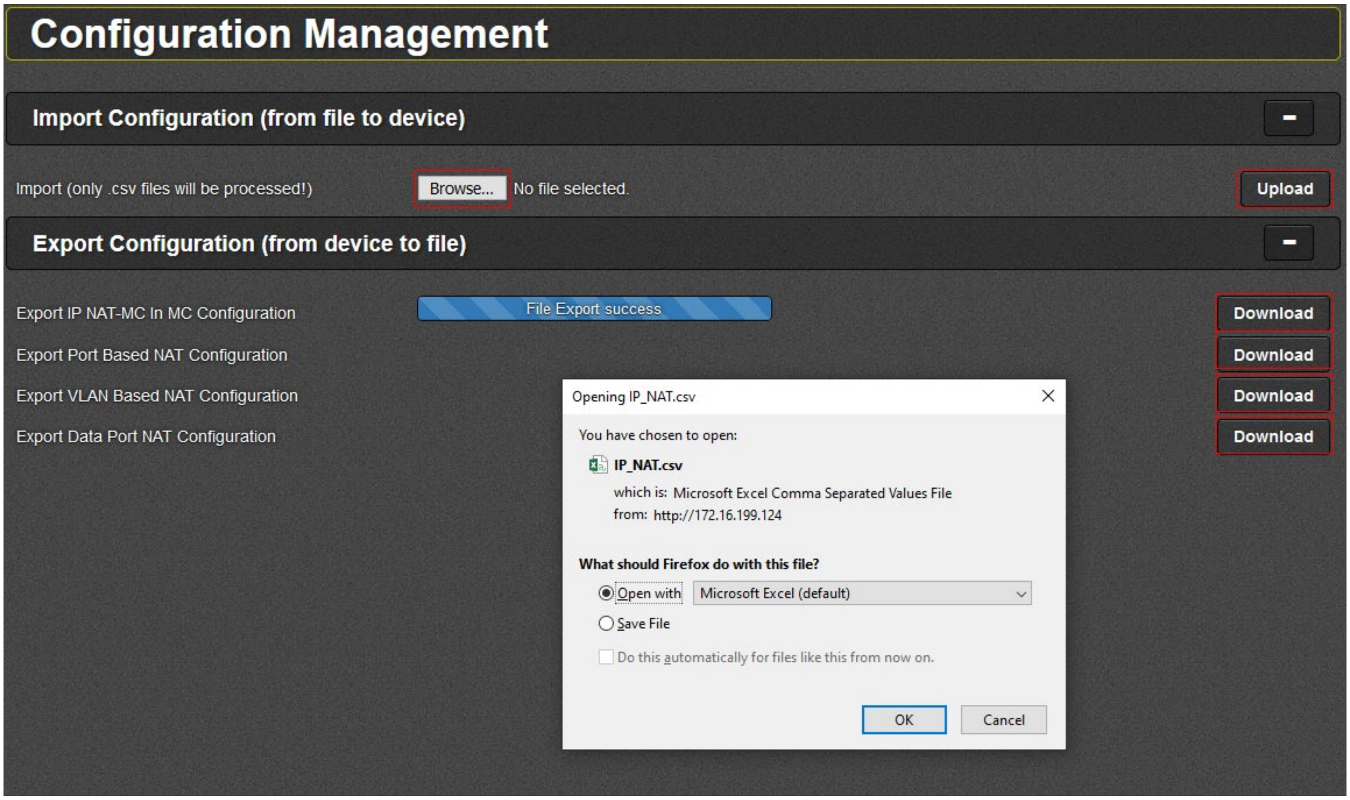
Port 2

	Send Trap	Fault Present
Flow 1	True	🟩
Flow 2	True	🟩
Flow 3	True	🟩
Flow 4	True	🟩
Flow 5	True	🟩
Flow 6	True	🟩
Flow 7	True	🟩
Flow 8	True	🟩

Figure 4-32 : WebEASY® - Notify Core (2) \ Bandwidth Over Limit

4.11. CONFIGURATION MANAGEMENT TAB

The Configuration Management tab allows the user to export, edit and import each mode in a CSV file format. The CSV file is useable in Microsoft Excel and allows for easy editing, saving and uploading file using the ***Browse*** and ***Upload*** buttons.


Configuration Management
Import Configuration (from file to device)
−
Browse...
Upload
Export Configuration (from device to file)
−
Download
Download
Download
Download
OK
Cancel

Import (only .csv files will be processed!) No file selected.

Export IP NAT-MC In MC Configuration — File Export success

Export Port Based NAT Configuration

Export VLAN Based NAT Configuration

Export Data Port NAT Configuration

Opening IP_NAT.csv

You have chosen to open:

IP_NAT.csv

which is: Microsoft Excel Comma Separated Values File

from: http://172.16.199.124

What should Firefox do with this file?

● Open with Microsoft Excel (default)

○ Save File

□ Do this automatically for files like this from now on.

Figure 4-33: WebEASY® - Configuration Management Tab

The current configuration for each currently used NAT type can also be exported from the 570NAT-X19-10G by selecting ***Download*** beside the respective NAT configuration you wish to download. Doing so will load a progress bar that, upon export will read 'File Export Success', at which time your browser's file download window will pop up. From here, users can save file to local disk or open the .csv file (note, this is the browser download window and as such will vary by web browser)

5. UPGRADE PROCEDURE

5.1. WEB INTERFACE - FIRMWARE UPGRADE

Using the Web interface is the fasted and recommended procedure to load the firmware onto the 570NAT-HW-X19.

When first visiting the 570NAT-HW-X19 web interface, the user will be asked to enter a Login and Password. Enter "***root***" for Password and "***evertz***" for Login.

On the top of the web page for the 570NAT-HW-X19, there is a tab labeled **Upgrade**. The **Upgrade** tab is used to check current firmware version and upload the latest firmware.

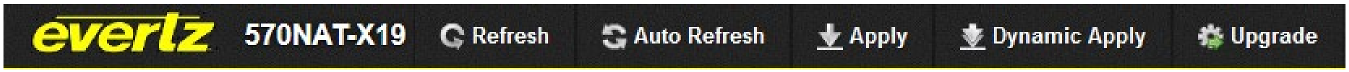
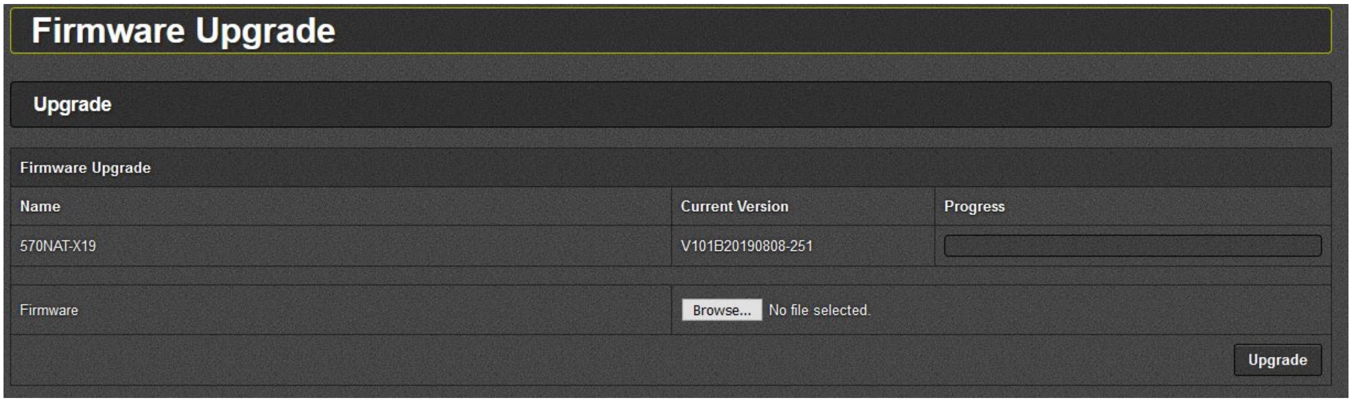


Figure 5-1: WebEASY® - Upgrade Button on Top Menu Bar

Selecting the Upgrade tab, will take you to Figure 5-2 where the current firmware version is shown. Should the firmware version be outdated, you will need to download the firmware image file.

NOTE: Contact Evertz to get the latest firmware image file.



Firmware Upgrade

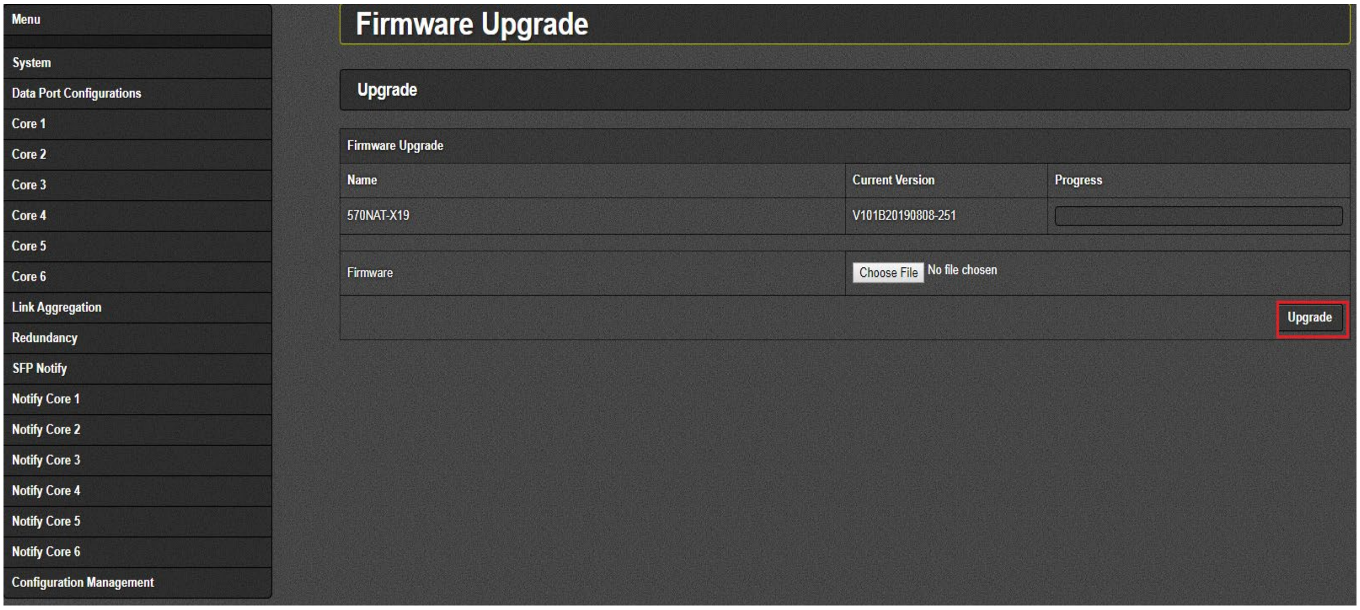
Upgrade

Firmware Upgrade

Name	Current Version	Progress
570NAT-X19	V101B20190808-251	
Firmware	Browse... No file selected.	

Figure 5-2: WebEASY® - Firmware Upgrade Menu

Click ***Choose File*** and browse to locate ***image*** file. Once selected, click ***Open*** to advance to next step. Click ***Upgrade*** and watch progress bar for status. Once completed, the device will automatically restart.



Firmware Upgrade

Name	Current Version	Progress
570NAT-X19	V101B20190808-251	

Firmware: No file chosen

Figure 5-3: WebEASY® - Firmware Upgrade Menu