7880IPG-NAT Series
High Density Network Address Translator
User Manual

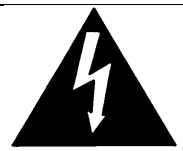
EVERTZ MICROSYSTEMS LTD.
5292 John Lucas Drive
Burlington, Ontario
Canada L7L 5Z9

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 2.1, January 2016

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.

CE

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.

TABLE OF CONTENTS

Figures

Tables

REVISION HISTORY

REVISION	DESCRIPTION	DATE
1.0	First Release	Sep 2015
2.0	Firmware version 1.10 or newer has some major changes and updates. Address Translation feature is available in both LAN-to WAN and WAN-to-LAN directions, for IP-NAT mode. It is available in LAN-to-WAN direction only, for IP-NAT MC-In-MC mode. The direction of the Encap and Decap has changed for the IP-NAT and the IP-NAT MC-In-MC modes. Consistent with VLAN and Port Modes. Port Aggregation and Demux are available in all modes (Previously only in Port Mode).	Nov 2015
2.1	Updated firmware feature set in Figures 4-2, 4-7, 4-10 and 4-12.	Jan 2016

This page left intentionally blank

1. OVERVIEW

The 7880IPG-NAT-6-10GE2 is a high-density, multi-port, multi-flow hardware Network Address Translation (NAT) engine with enhanced features such as Port Aggregation, Tunnelling, Packet Replication and Bandwidth Capping, allowing service providers to seamlessly bridge across networks in multi-tenant environments.

The 7880IPG-NAT-6-10GE is conceptually organized as 6 WAN-side ports + 6 LAN-side ports, with a packet processing core between each WAN-LAN port pair. A given processing core can sustain up to 128 data flows, configurable based on multicasts or VLAN Tags. This gives an exceptional product density of 12 x10GE ports, with 768 multicast/VLAN flows – All in the space-efficient Evertz 7800 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. This WAN-side Port Aggregation feature allows network engineers to achieve functions such as port-based redundancy.

The 7880IPG-NAT-6-10GE is controlled by the industry-leading VistaLINK Pro, and via web interface.

The 12 Ethernet ports can be a mixture of GigE or 10GE, simply by populating the desired SFP, offering full flexibility for LAN & WAN interfacing.

The 7880IPG-NAT-6-10GE2 provides the following four modes of operation:

- The One-to-One or IP-NAT Mode allows multicast IP streams from one network to be translated to different unicast/multicast IP addresses, on a flow-by-flow basis, up to 128 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.

- The Tunnelling (or Encapsulation or MC-in-MC) IP-NAT Mode allows 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.

- 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 128 unique flows can be configured per processing core, with independent encapsulation headers.

- 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

- Four modes of operation,
  - IP NAT mode with optional packet replication
  - MC In MC NAT mode for tunneling flows based on multicast addresses
  - VLAN based NAT for flows based on VLAN tagged datagrams.
  - Port based NAT for encapsulating all traffic on a physical port.
- WAN-side Port Aggregation and Demux, in all modes.
- Point-to-point and multi-point signal distribution/contribution inside the facility.
- Operates over a IP/MPLS/VPLS core network
- In-band Management (Management Traffic transport over Multicast)
- Full integration with VistaLINK PRO and Magnum.
- Flexible SFP Ethernet I/O for 12x1GE or 12 x10GE

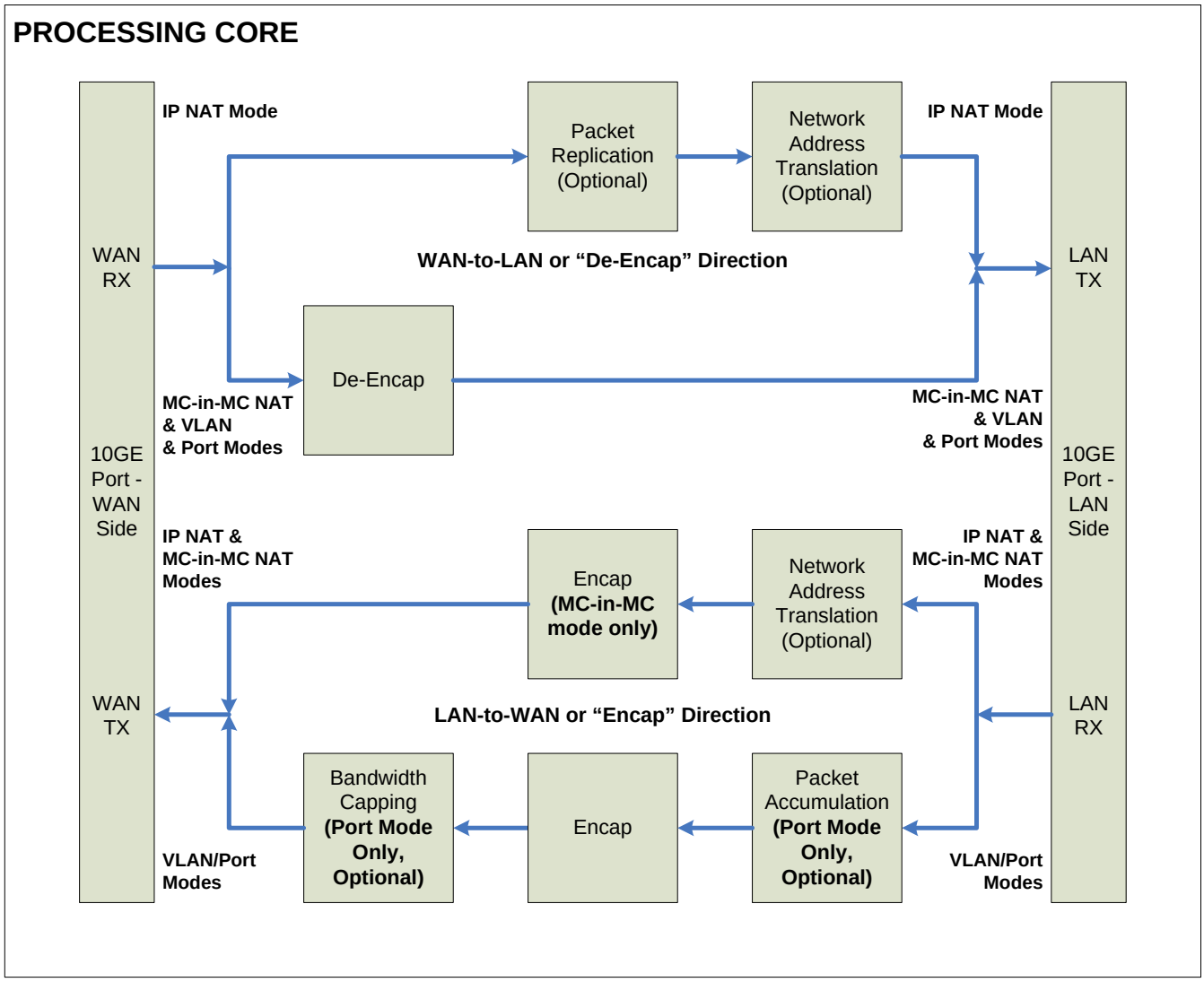


Figure 1-1: Single NAT Core Block Diagram

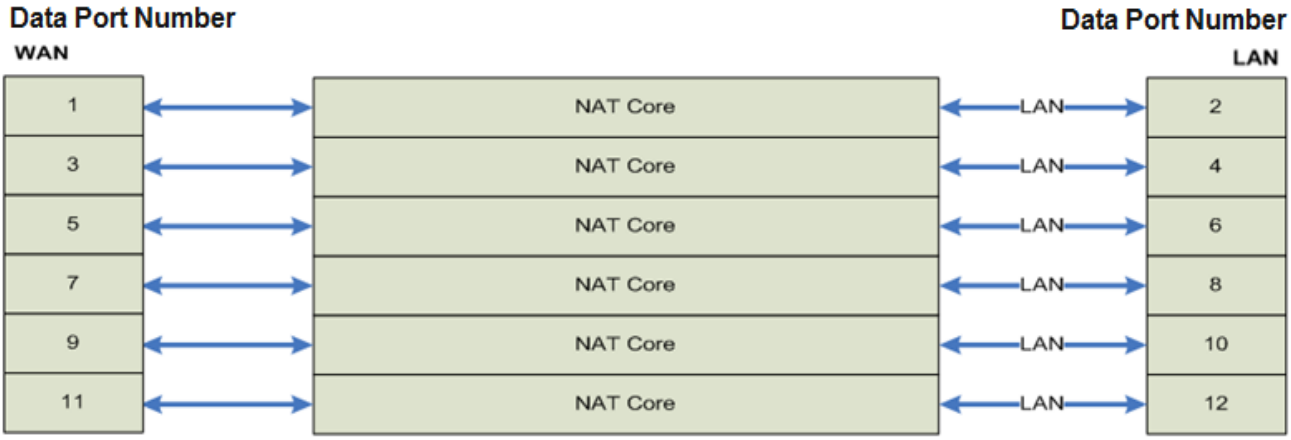


Figure 1-2: 7880IPG-NAT Core Mapping Block Diagram

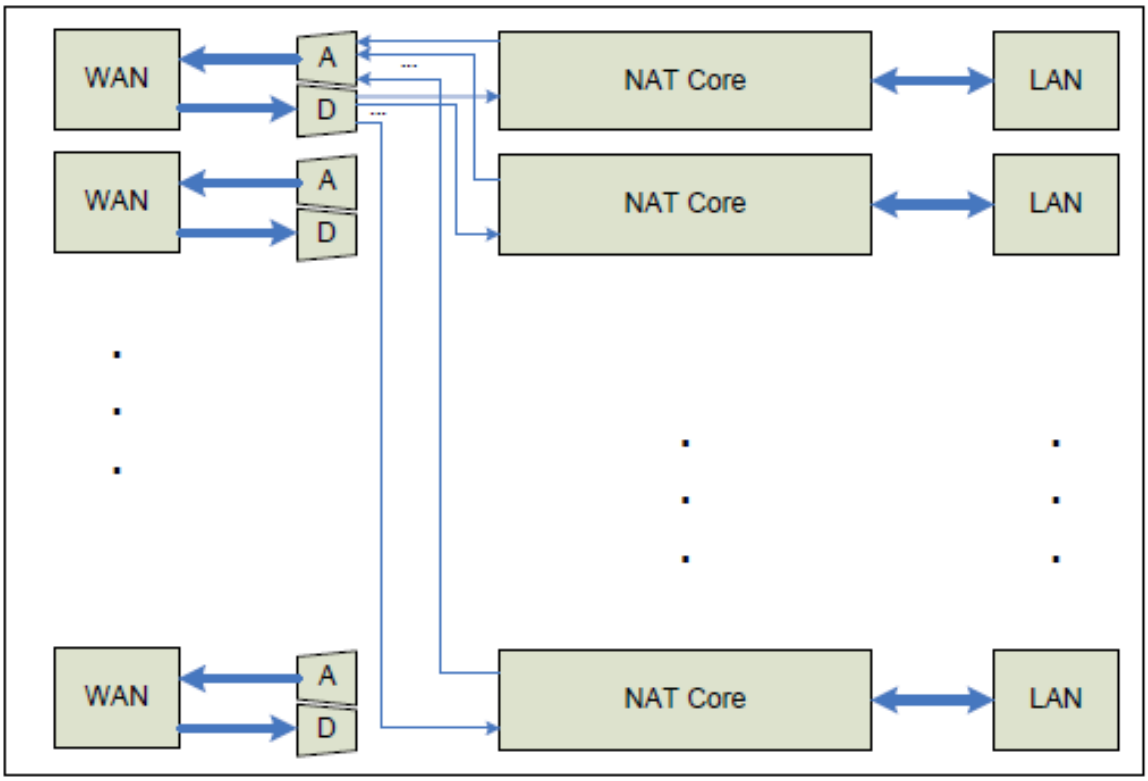


Figure 1-3: WAN-Side Port Aggregation and Demux (available in all modes)

2. GETTING STARTED

2.1. REAR PLATE DESCRIPTION

The 7880IPG-NAT comes standard with a companion rear plate. Figure 2-1 provides an illustration of the 7880IPG-NAT rear plate.

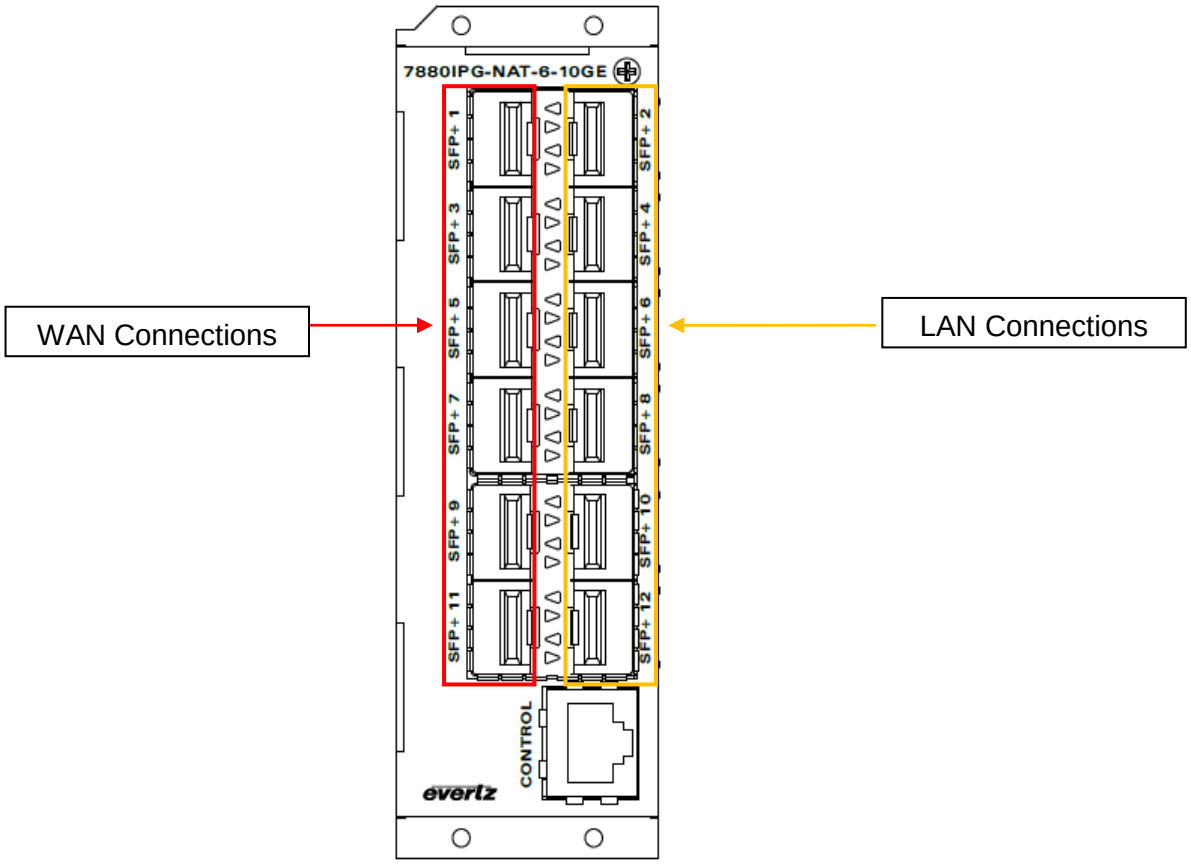


Figure 2-1: 7880IPG-NAT-6-10GE Rear Plate

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

CTRL: There is one RJ45 Connector used for communications with a web browser using WebEASY.

2.1.1. Ethernet Connection Control

The 7880IPG-NAT is designed to be used with either 10Base-T (10 Mbps), 100Base-TX (100 Mbps) also known as *Fast Ethernet* cabling systems. When connecting for 10Base-T systems, category 3, 4, or 5 UTP (unshielded twisted pair) cable as well as EIA/TIA – 568 100Ω STP (shielded twisted pair) cable may be used. When connecting for 100Base-TX systems, category 5 UTP cable or better is required. When connecting for 1000Base-T system, category 5, 5e, 6, or 7 UTP cable is required. The cable must be "straight-through" with a RJ-45 connector at each end. Make the network connection by plugging one end of the cable into the RJ-45 receptacle of the 7880IPG-NAT and the other end into a port of the supporting switch or directly to a computer.

The straight-through RJ-45 cable can be purchased or can be constructed using the pin out information in Table 2-1 or Table 2-2 for the current RJ-45 standards (AT&T 258A, EIA/TIA 568A or EIA/TIA 568B - colour coding listed). Also refer to the notes following the table for additional wiring guide information.

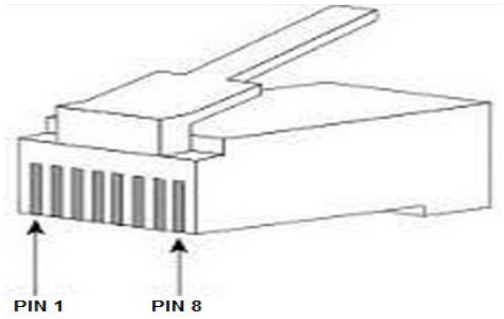
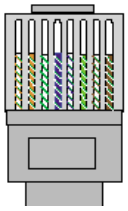


Figure 2-2: RJ-45 Connector Pin-Out Locations

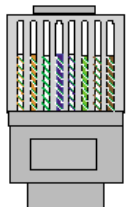


Pin #	Signal	EIA/TIA 568A	AT&T 258A or EIA/TIA 568B	10BaseT or 100BaseT
1	Transmit +	White/Green	White/Orange	X
2	Transmit –	Green/White or White	Orange/White or Orange	X
3	Receive +	White/Orange	White/Green	X
4	N/A	Blue/White or Blue	Blue/White or Blue	Not used (required)
5	N/A	White/Blue	White/Blue	Not used (required)
6	Receive –	Orange/White or Orange	Green/White or Green	X
7	N/A	White/Brown	White/Brown	Not used (required)
8	N/A	Brown/White or Brown	Brown/White or Brown	Not used (required)

Table 2-1: 10BaseT and 100BaseT Straight Through Wiring Connections

Note the following cabling information for this wiring guide:

- On 10Base-T and 100Base-T, only two pairs of wires are used in the 8-pin RJ-45 connector to carry Ethernet signals. Even though pins 4, 5, 7 and 8 are not used, it is mandatory that they be present in the cable
- Pairs may be solid colours and not have a stripe
- Category 5 cable must use Category 5 rated connectors



Pin #	Signal	EIA/TIA 568A	AT&T 258A or EIA/TIA 568B
1	DA +	White/Green	White/Orange
2	DA -	Green/White or White	Orange/White or Orange
3	DB +	White/Orange	White/Green
4	DC +	Blue/White or Blue	Blue/White or Blue
5	DC -	White/Blue	White/Blue
6	DB -	Orange/White or Orange	Green/White or Green
7	DD +	White/Brown	White/Brown
8	DD -	Brown/White or Brown	Brown/White or Brown

Table 2-2: 1000BaseT Straight Through Wiring Connections

The maximum cable run between the 7880IPG-NAT and the supporting switch is 328 ft (**100 m**). The maximum combined cable run between any two end points (i.e. 7880IPG-NAT and PC/laptop via network switch) is 675 feet (205 m).

Devices on the Ethernet network continually monitor the receive data path for activity as a means of checking that the link is working correctly. When the network is idle, the devices also send a link test signal to one another to verify link integrity.

LN/ACT: This dual purpose Green LED indicates that the card has established a valid linkage to its switch, and whether the module is sending or receiving data. This LED will be ON when the module has established a good link to its supporting switch. This gives you a good indication that the segment is wired correctly. The LED will BLINK when the module is sending or receiving data. The LED will be OFF if there is no valid connection.

2.2. CARE AND HANDLING OF OPTICAL FIBER

2.2.1. Handling and Connecting Fibers

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. HARDWARE INSTALLATION

The 7880IPG-NAT is designed to operate with its own control port using a web browser such as Chrome or Fire Fox.

To successfully install the 7880IPG-NAT, you will require the following:

1. Unused IP address on the network
2. Evertz serial cable

Before handling the card it is important to minimize the potential effects of static electricity. It is therefore recommended that an ESD strap be worn.

Locate on the chassis two adjacent vacant slots. Unpack the 7880IPG-NAT and separate the rear panel from the main card. Locate on the rear of the rack the two slots and remove the blanking panels. Insert the rear panel into the back of the chassis and secure using the four screws provided.

Before inserting the front card, connect the serial cable to the board using the rainbow coloured serial cable provided. Now insert the 7880IPG-NAT card into the corresponding front slots ensuring the card lines up with the slot runners on the bottom and the top of the chassis. Push the card **firmly** into the slot ensuring that when it mates with the rear card it has been firmly pushed into a seated position. Do not connect any cables to the rear plate (failure to do this could cause unwanted network issues) until the initial configuration has been completed.

Ensure that the device is powered up and the top green LED is on (LED 1) at the front of the card. Connect the device via the COM port.

Open TeraTerm (if using Windows XP or older open Hyper Terminal) to make the required changes to the IP address on the card. Set the TeraTerm serial port settings to following:

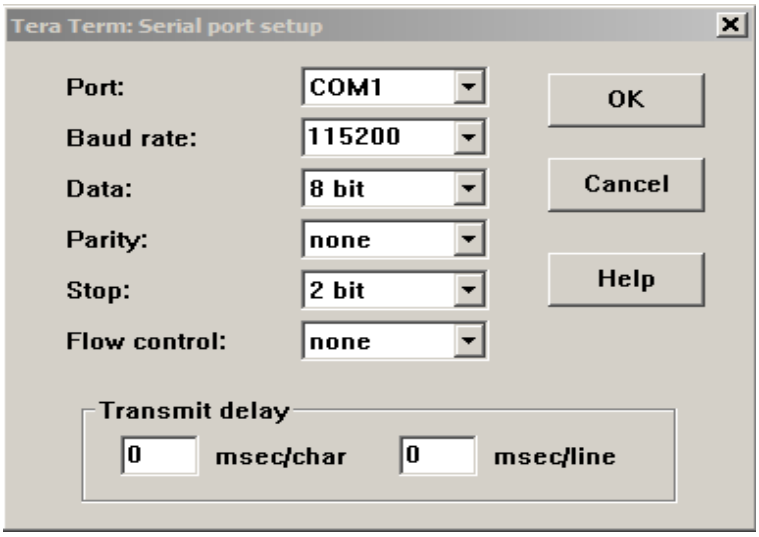


Figure 2-3: COM Port – Serial Port Settings

Click OK to apply these settings and press return. The session should respond with the 7880IPG-NAT Main Menu as shown in Figure 2-4. A prompt will ask for a login name and password. Enter "***customer***" for both prompts.

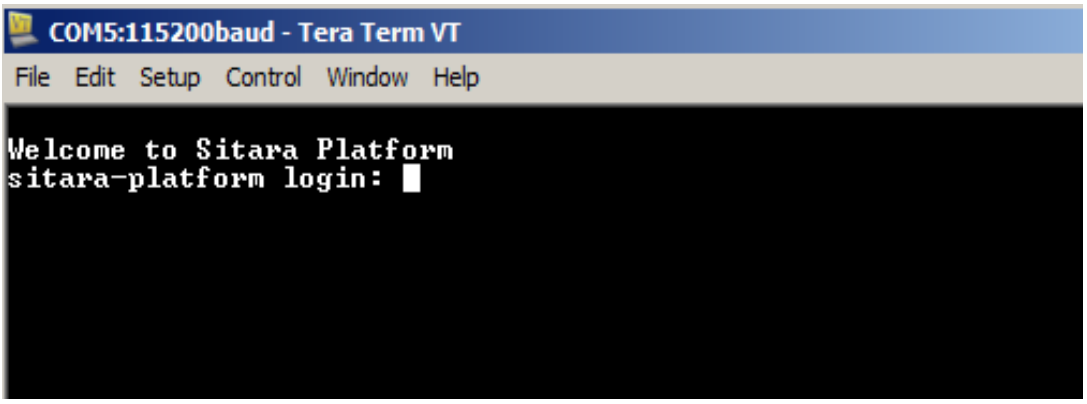


Figure 2-4: COM Port – Login Menu

Note: Enter "**customer**" for both login and password prompts.

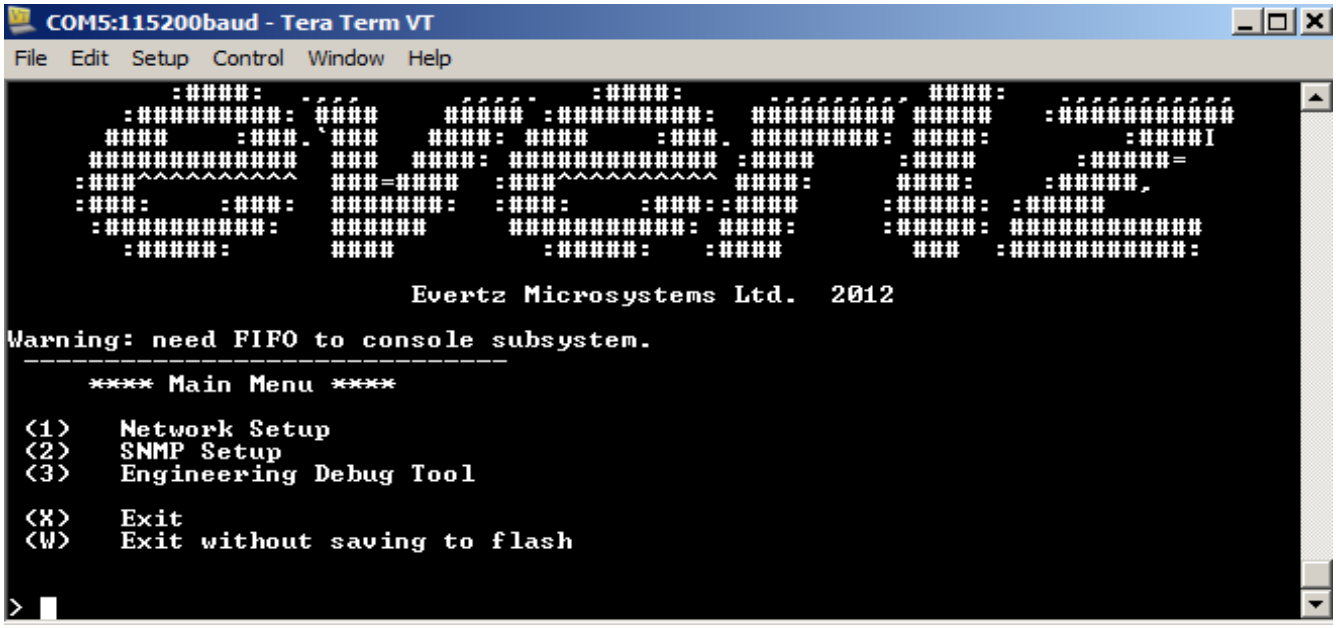


Figure 2-5: COM Port - 7880IPG-NAT Main Menu

1) **Network Setup**
   This sub-menu enables the user to configure the control network settings for the card. Configuring this sub-menu allows the user to access the card through the User Interface.

2) **SNMP Setup**
   This sub-menu enables the user to configure the Simple Network Management Protocol settings. In this menu you can set or remove the SNMP trap IP address and the SNMP Read and Set community strings.

3) **Engineering Debug Tool**
   This menu is for Evertz technical support staff only. You may be requested to access and execute options within this menu when seeking technical support from Evertz. Guidance will be given should this be required.

2.4. CONFIGURING THE BASIC NETWORK SETTINGS FOR THE CONTROL PORT

Now select option (1) *Network Setup*, the Network Configuration menu will be displayed as shown in **Error! Reference source not found.**.**Error! Reference source not found.**

1. Select option (1) *Set IP Address* and configure the IP address for the 7880IPG-NAT ensuring that the IP address is not already in use on the network.

2. Now select option (2) *Set Netmask* and configure the correct subnet mask for your network.

3. If required also configure option (3) *Set Gateway* and (4) *Set Broadcast Address.*

4. Enter *(X) to go one level up*.

5. From the main menu in Figure 2-5, enter *(X)* to save and apply settings.

Power Cycle the 7880IPG-NAT to ensure all changes are applied and saved to the card. Connect an RJ45 cable to the Control Port of the device. Verify the network connectivity by opening the command window and try to ping the 7880IPG-NAT using the IP address that was set. Make sure your computer is on the same subnet before trying to ping.

If you are not configuring SNMP settings, you have now completed the minimum necessary network configuration and can connect the cables to the rear card when ready.

2.5. CONFIGURING SNMP SETTINGS

From the Main Menu, select option (2) *SNMP Setup*.

Figure 2-6: SNMP Setup Menu

2.5.1. SNMP Setup

In the *SNMP Setup* menu, there are four submenus to choose from:

SNMP Version Setup	This menu item identifies which of the two version of SNMP will be used to communicate to the device.
SNMP V1 Setup	This menu item contains setup information for SNMP version 1 related configurations.
SNMP V3 Setup	This menu item contains setup information for SNMP version 3 related configurations.
Trap Setup	This menu item allows the user add or remove trap destinations.

2.5.1.1. SNMP V1 Setup

In the *SNMP V1 Setup* menu, three parameters are configured:

Read Community String	Factory default “public” (No changes required. However, if these settings are changed, the manager must have the identical settings. Otherwise no communication will occur between the 7880IPG-NAT and the manager.)
Read/Write Community String	Factory default “private” (No changes required. However, if these settings are changed, the manager must have the identical settings. Otherwise no communication will occur between the 7880IPG-NAT and the manager.)

Once the *SNMP V1 Setup* parameters have been configured, exit *SNMP V1 Setup* by pressing X then <Enter>.

2.5.1.1.1. SNMP V3 User Setup

The *SNMP V3 User Setup* menu defines basic access rules for the SNMP V3 protocol, controlling the ability to read ("GET") or read/write ("SET") parameters. It also provides the password key for authentication as well as AES or DES encryption. A maximum of ten different users can be entered.

Add New User	*Add New User* and *Edit User* will provide the same interface. **User Name** — This is mandatory. **User Type** — Default is READONLY, Options are READONLY, READWRITE. This defines the access mode for the specific user. **Authentication** — Default is NONE. Options are NONE, MD5, or SHA-1. Authentication to check integrity of the incoming messages. **Authentication Password** — If Authentication is not set to NONE then this field is mandatory, otherwise, Authentication will be automatically set back to NONE. The password must be at least 8 characters long. **Use Privacy** — Default is NONE. Options are NONE, AES, or DES. Use Privacy will encrypt incoming and outgoing messages. **Encryption Password** — If Use Privacy is not set to NONE then this field is mandatory, otherwise, Use Privacy will be automatically set back to NONE. The password must be at least 8 characters long. **Included OID 1** — These options are optional. They define the OID tree that the user is restricted to access. The user can not access any other OID that is not listed or included in the OID tree specified.
Edit User	
Remove User	Removes previously entered users. This will affect the SNMP V3 Trap setup as well. Please refer to next section for details.
Show All SnmpV3 User	Lists all entered users. It will show username, access type, authentication type and password, privacy type and password as well as included OIDs.

Once the *SNMP V3 User Setup* parameters have been configured, exit *SNMP V3 User Setup* by pressing X then <Enter>.

2.5.1.2. Trap Setup

"Trap Setup" allows the user to define IP addresses of the trap listeners for when the asynchronous fault messages are sent. A maximum of eight IP addresses can be stored in the 7880IPG-NAT. After selecting "Add…" or "Remove…" IP addresses are entered one at a time.

Add Trap Destinations	Add a SNMP **trap server** IP address to the TRAP distribution list.
Remove Trap Destinations	Remove a SNMP **trap server** IP address from the TRAP distribution list. For example, selecting this option reveals the list of IP addresses with the prompt to remove one from the list: Trap #1: 192.168.1.76 Trap #2: 192.168.8.140 Remove trap # > 2
Show All Trap Destinations	Displays a list of all entered SNMP **trap server** IP addresses. For example: Trap #1: 192.168.1.76 Trap #2: 192.168.8.140 Trap #3: 192.168.8.112

Once the *SNMP V1 Setup* parameters have been configured, exit the *SNMP Setup* by pressing X then <Enter>.

From the main menu in Figure 2-5, enter ***(X)*** to save and apply settings. Power Cycle the 7880IPG-NAT to ensure all changes are applied and saved to the card. Verify the network connectivity by opening the command window and try to ping the 7880IPG-NAT using the IP address that was set.

This page left intentionally blank

3. TECHNICAL SPECIFICATIONS

3.1. SFP MODULES

- 12 x 10GbE optical
- 12 x 1GbE optical or RJ45

3.2. IP NAT AND MC IN MC NAT MODES

- 768x Static IP flows capacity per direction.

3.3. VLAN BASED NAT

- 768x VLAN ID flows capacity per direction.

3.4. PORT BASED NAT

- 6x Physical flows capacity.

3.5. ELECTRICAL

- Power: 40W
- Voltage: 12VDC
- EMI/RFI: Complies with FCC Part 15, Class
- AEU EMC directive

3.6. COMPLIANCE

- Electrical Safety: Power supply UL listed complies with CE Low Voltage Directive
- EMI/RFI: Complies with FCC Part 15, Class A EU EMC directive

3.7. PHYSICAL (NUMBER OF SLOTS) AND ENCLOSURES

350FR: 2
7800FR: 2

This page left intentionally blank

4. WEB INTERFACE

The 7880IPG-NAT provides a built-in web interface, WebEASY®, which allows a user to interact with using a standard Internet web browser. The 7880IPG-NAT web interface can be accessed by entering the IP address of the control port of the 7880IPG-NAT into the address bar of an Internet web browser. Refer to section 2.4 for setting the network configurations.

When first visiting the 7880IPG-NAT 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.

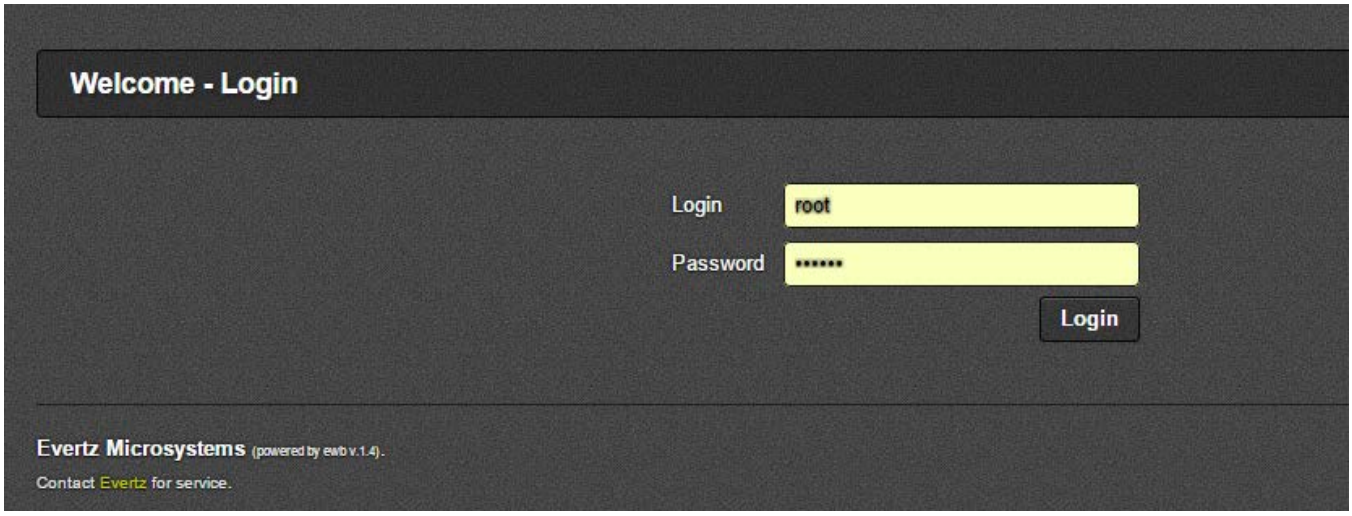


Figure 4-1: WebEASY® - Login Screen

4.1. SYSTEM TAB

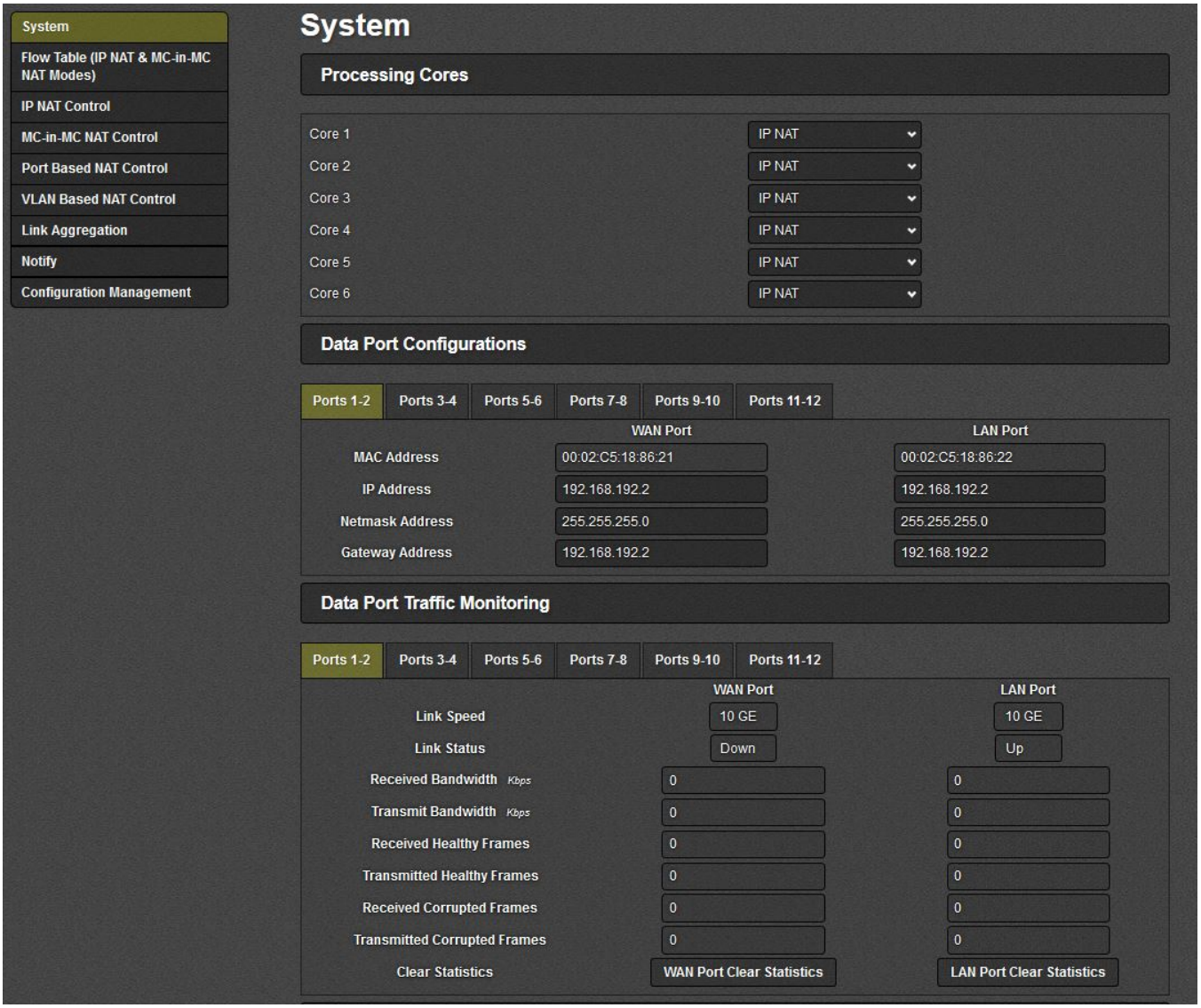


Figure 4-2: WebEASY® - System Tab – Part 1

Processing Cores

Configurations for Core 1 to Core 6

Mode of Operation: Within this drop down menu the user can configure the desired mode of operation for the 7880IPG-NAT.

The NAT can be set to:

- *IP NAT* mode
- *MC-In-MC NAT + IP NAT* mode
- *Port Based NAT* mode
- *VLAN Based NAT* mode

Note: The Flow Table tab only applies to the flows for IP NAT and MC-In-MC NAT Modes.

Data Port Configurations
Data Ports 1-2 are physically connected to Core 1 and Data Ports 3-4 are physically connected to Core 2 and so on respectively. Also note, WAN ports are odd numbered ports while LAN ports are even number ports.

For each of 12 Data ports, the following controls are configurable.

MAC Address: This field displays the MAC Address of the corresponding Ethernet port.

IP Address: This control allows the user to set the IP Address of the corresponding Ethernet port; a reboot is required after modifying this field.

Netmask Address: This control allows the user to set the Netmask Address of the corresponding Ethernet port; a reboot is required after modifying this field.

Gateway Address: This control allows the user to set the Gateway Address of the corresponding Ethernet port, a reboot is required after modifying this field.

Data Port Traffic Monitoring
For each of the 12 Data ports the following parameters can be monitored.

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.

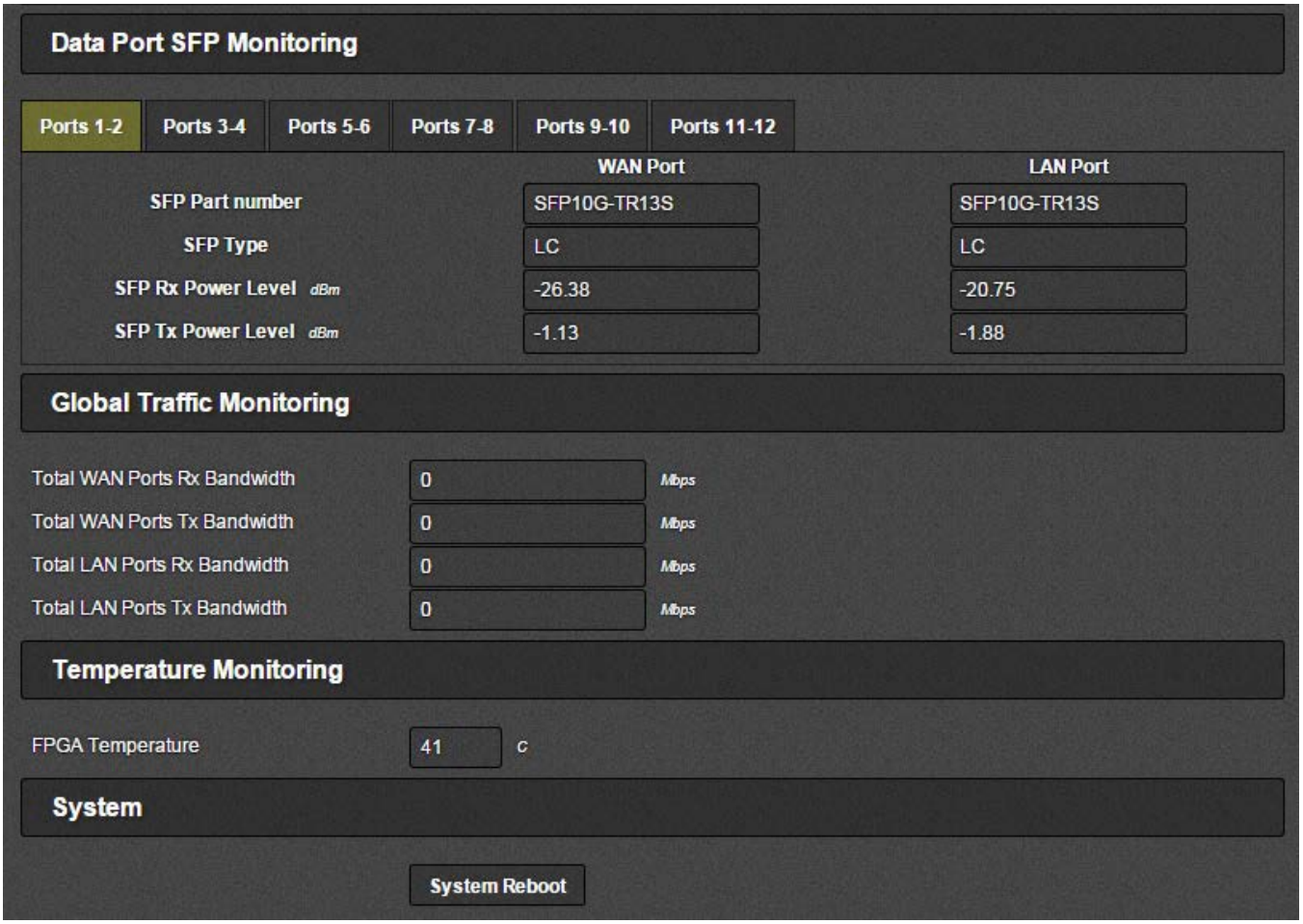


Figure 4-3: WebEASY® - System Tab – Part 2

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

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.

Temperature Monitoring

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

System

System Reboot: This button allows the user to reboot the 7880IPG-NAT module, doing this will result in the connection being lost temporarily.

4.2. FLOW TABLE (IP NAT MODE / MC IN MC NAT MODE)

The Flow Table section only applies to the flows for IP NAT Mode and MC In MC NAT Mode.

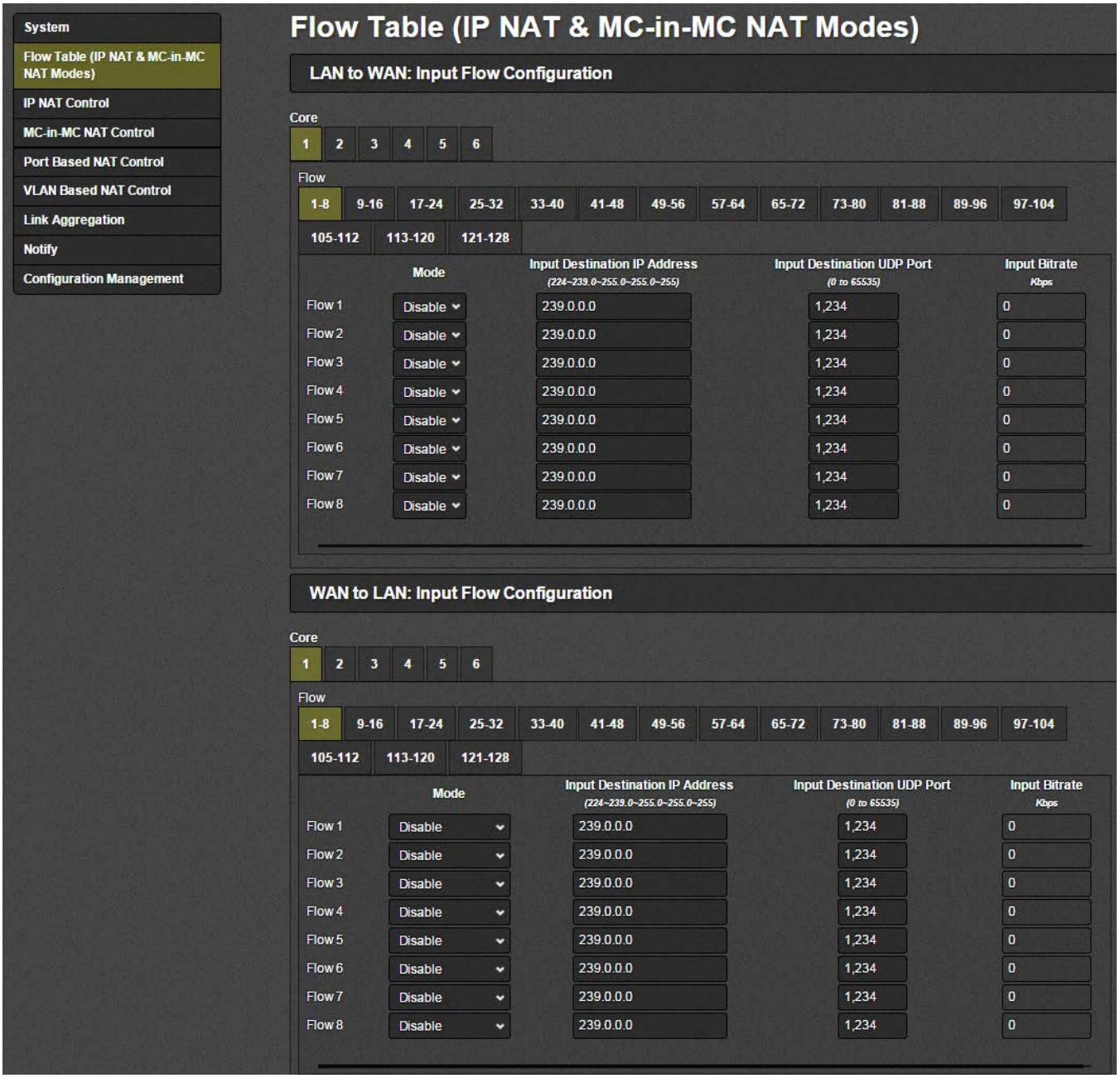


Figure 4-4: WebEASY® - Flow Table (IP NAT & MC-in-MC NAT Modes) Tab

There is up to 128 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 16 flow groups in total.

Note: *Packet Replication* option is generated by specifying the same Input Destination IP address for multiple flows, and is applicable in WAN-to-LAN direction and in IP-NAT mode.

Flow Configurations (IP NAT & MC-in-MC NAT Modes)
LAN to WAN: Input Flow Configuration
NAT Cores (1 to 6)

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.

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

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

WAN to LAN: Input Flow Configuration
NAT Cores (1 to 6)

Mode: This control allows the user to enable *De-Encap/NAT* or disable the input associated with that flow. Only when in MC-in-MC mode, the module will de-encapasulate.

Input Destination IP Address (also used for Packet Replication): This control allows the user to set the Input Destination IP address of the packets to be received. *Packet Replication* option is generated by specifying the same Input Destination IP address for multiple flows.

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

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

4.2.1. IP NAT Mode and MC In MC NAT Mode Block Diagrams

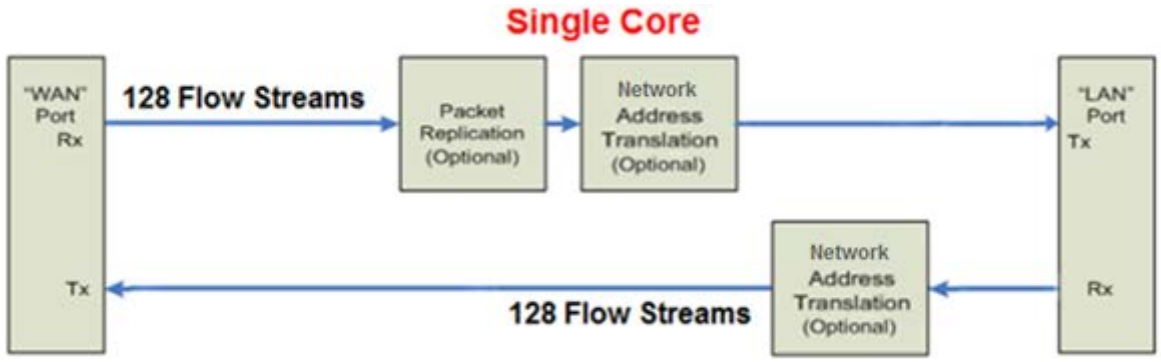


Figure 4-5: IP NAT Mode Block Diagram

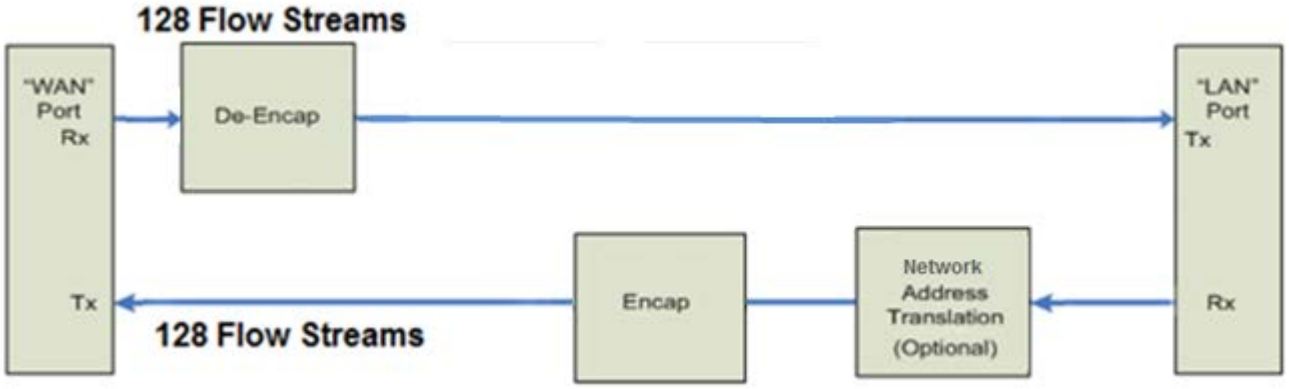


Figure 4-6: MC In MC NAT Mode Block Diagram

4.3. IP NAT CONTROL TAB

The IP NAT Control section applies to IP NAT Mode. The LAN to WAN configuration also applies to MC-in-MC mode, if "Modify" option is chosen.

Note: *NAT cores will operate only in the selected NAT Mode under the System tab.*

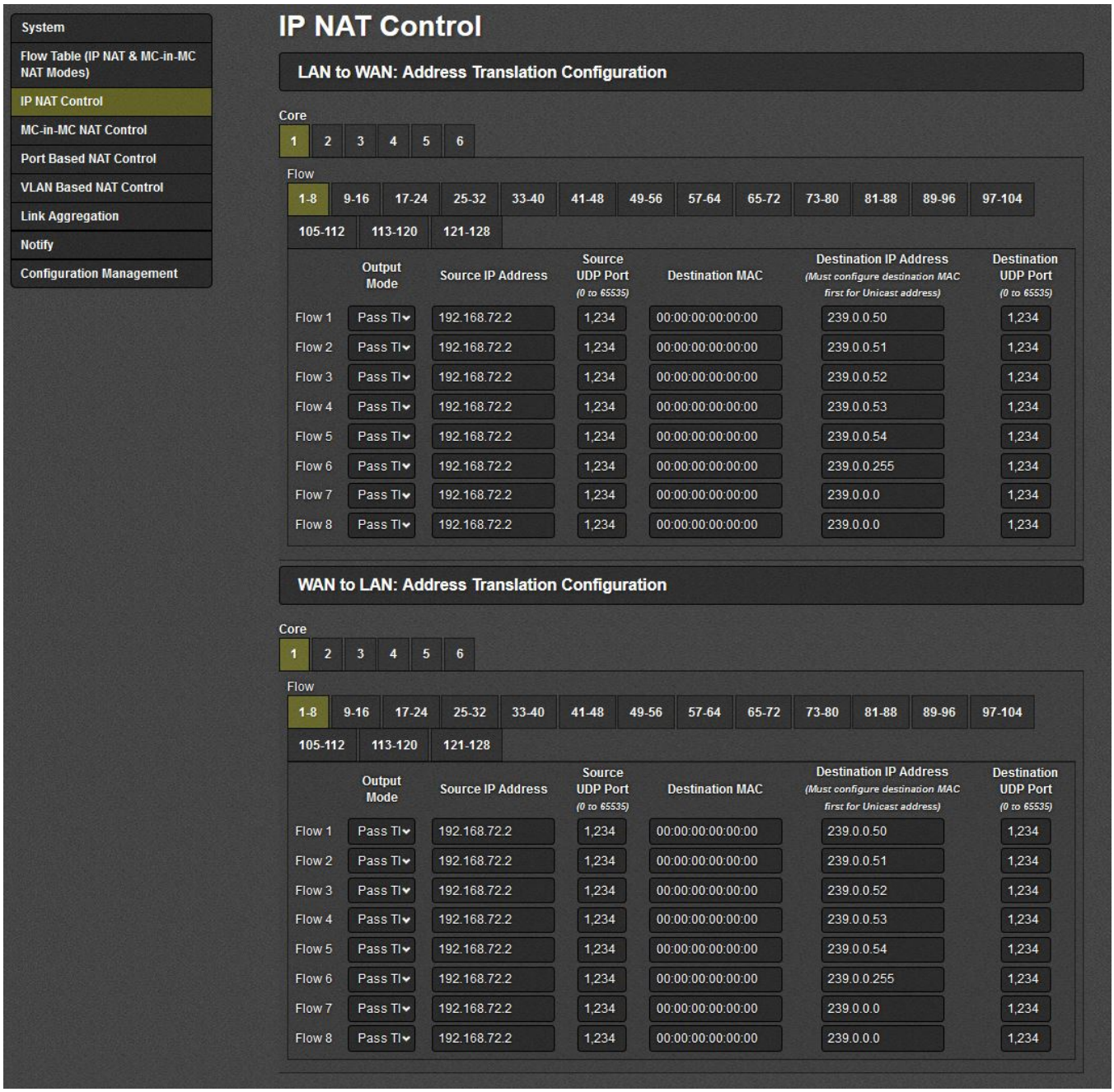


Figure 4-7: WebEASY® - IP NAT Control Tab

LAN to WAN: Address Translation Configuration
and
WAN to LAN: Address Translation Configuration
NAT Cores (1-6) and Flows 1 to 128

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

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

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

4.4. MC IN MC NAT CONTROL TAB

Encapsulation for MC IN MC NAT Control only applies to MC In MC NAT Mode.

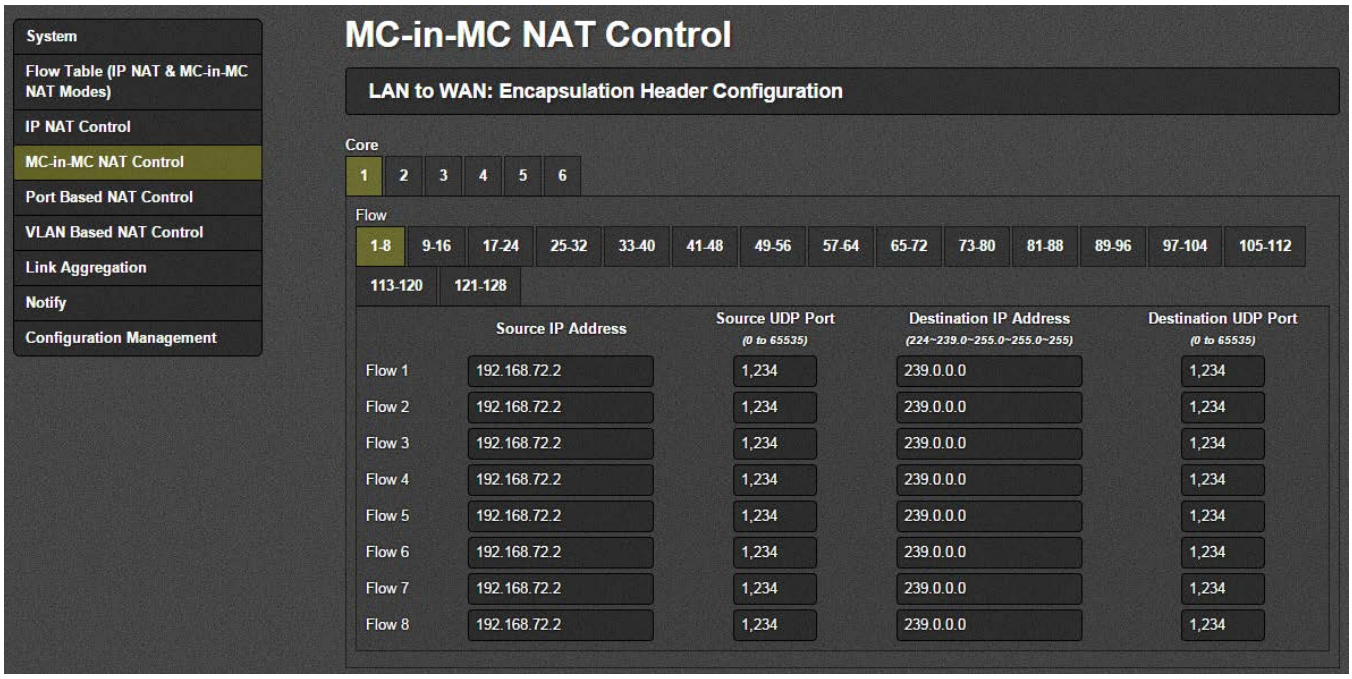


Figure 4-8: WebEASY® - Multicast In Multicast NAT Control

LAN to WAN: Encapsulation Header Configuration
For Cores 1 to 6 and Flows 1 to 128

Source IP Address: This control is used to configure the output header with the desired source IP address when the output is being encapsulated

Source UDP Port: This control is used to configure the output header with the desired source UDP Port when the output is being encapsulated.

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

Destination UDP Port: This control is used to configure the output header with the desired destination UDP Port when the output is being encapsulated.

4.5. PORT BASED NAT CONTROL TAB

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.

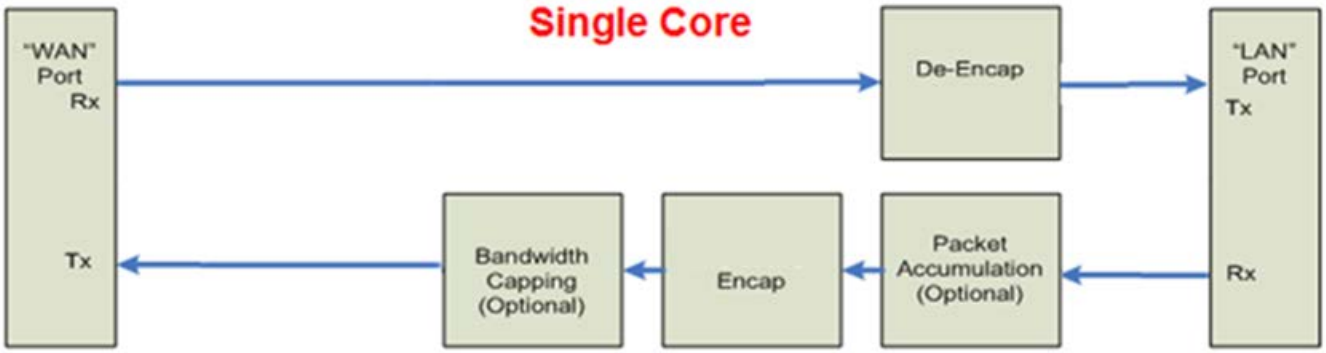


Figure 4-9: Port Based NAT Mode Block Diagram

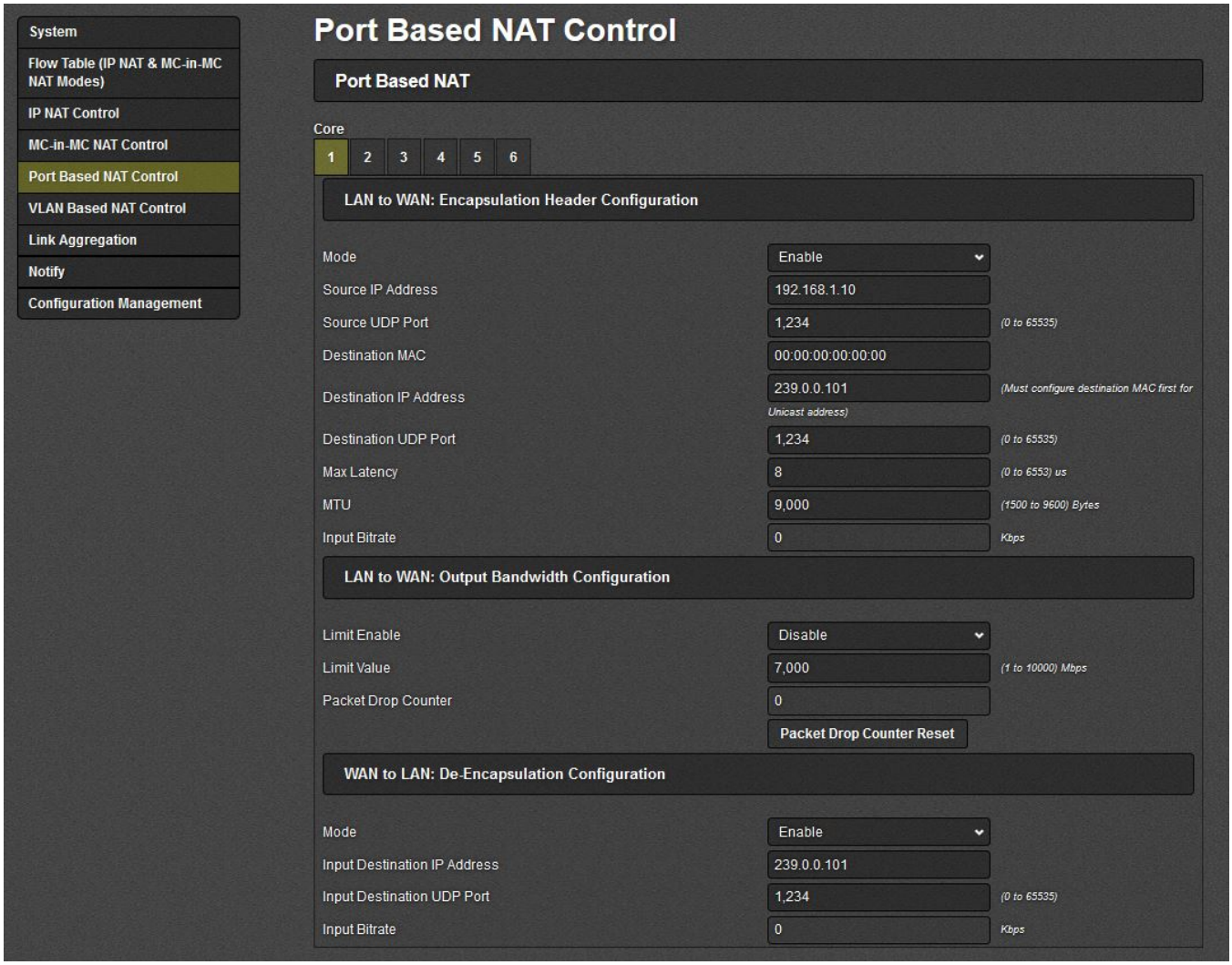


Figure 4-10: WebEASY® - Port Based NAT Control Tab

Port Based NAT
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 MAC: This control is used to configure the output header on the encapsulation with the desired Destination MAC address.

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

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.

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**.**

4.6. VLAN BASED NAT CONTROL

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 128 unique flows can be configured per processing core, with independent encapsulation headers.

Figure 4-11: 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 7880IPG-NAT only supports Ether Type=0x8100 traffic.

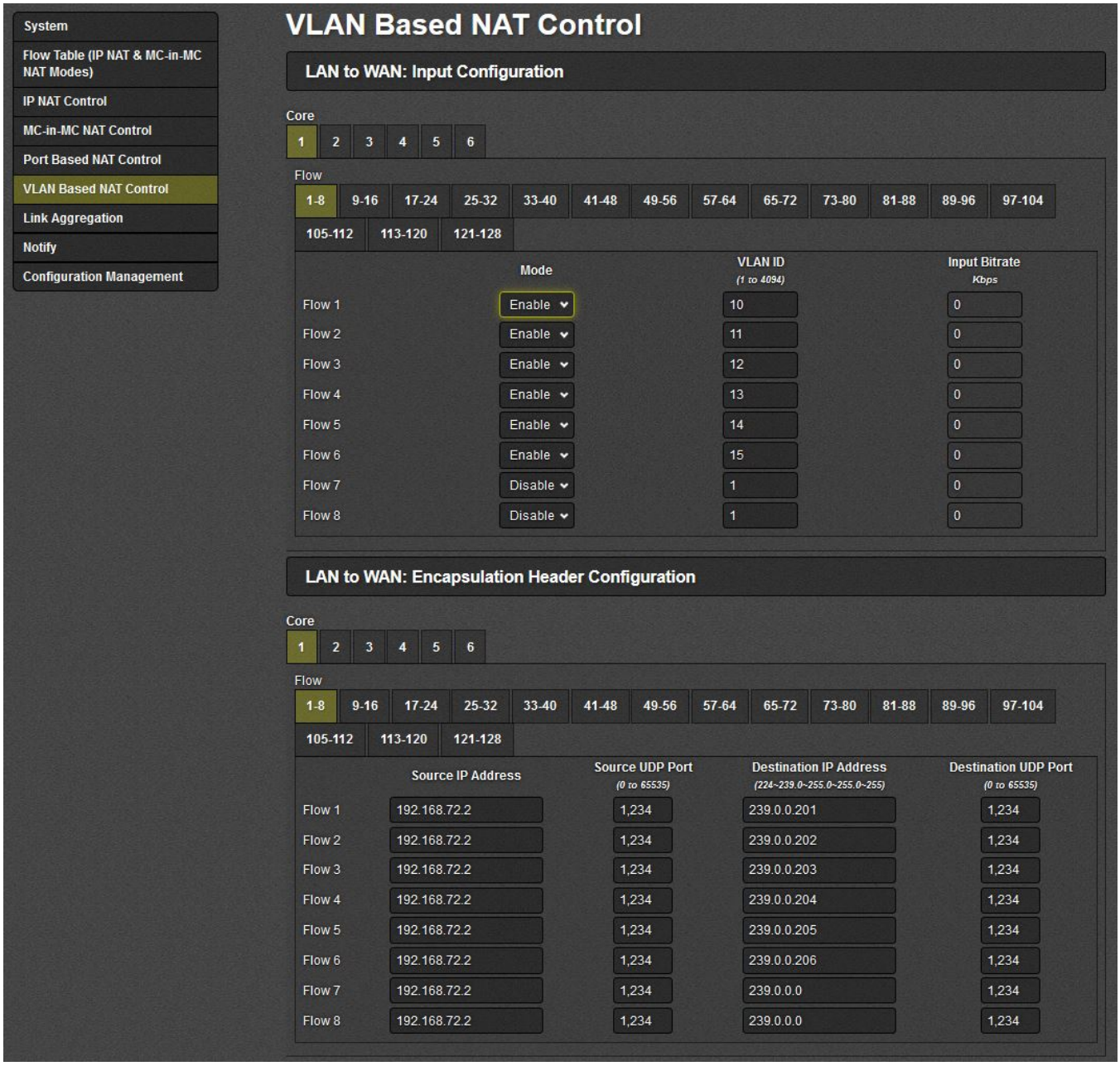


Figure 4-12: WebEASY® - VLAN Based NAT Control Tab

There is up to 128 transport streams that can be specified to configure based on its VLAN ID and is sectioned into flow groups. Each flow group will display 16 flows for configuration. There are eight flow groups in total.

LAN to WAN: Input Configuration

For cores 1 to 6 and flows 1 to 128

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**.**

LAN to WAN: Encapsulation Header Configuration
For cores 1 to 6 and flows 1 to 128

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.

WAN to LAN: De-Encapsulation Configuration
For cores 1 to 6 and flows 1 to 128

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**.**

4.7. LINK AGGREGATION

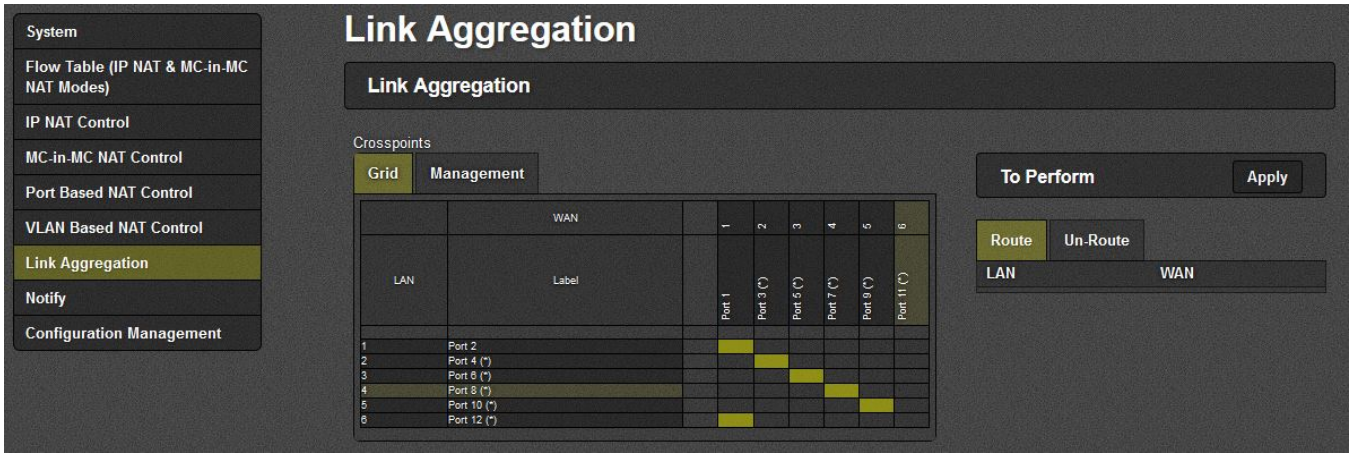
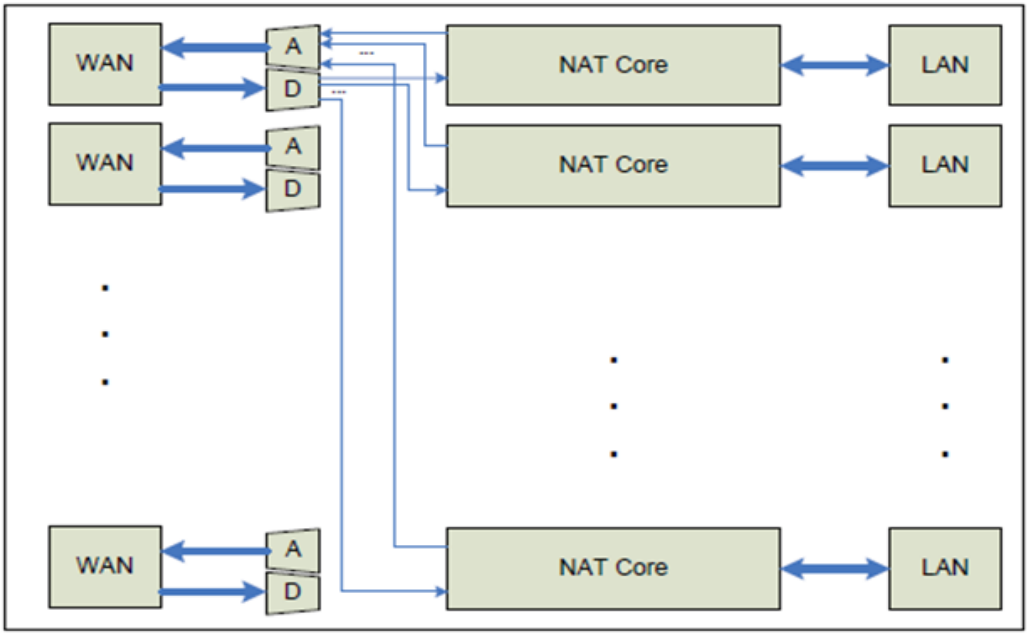


Figure 4-13: WebEASY® - Link Aggregation Tab

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.

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.



4.8. NOTIFY TAB

Figure 4-14: WebEASY® - Notify Tab

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.

Link Status

For SFP 1 to 12

Port Link: This monitor will display green when a valid link has been established or red when a link has been disconnected.

4.9. 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.

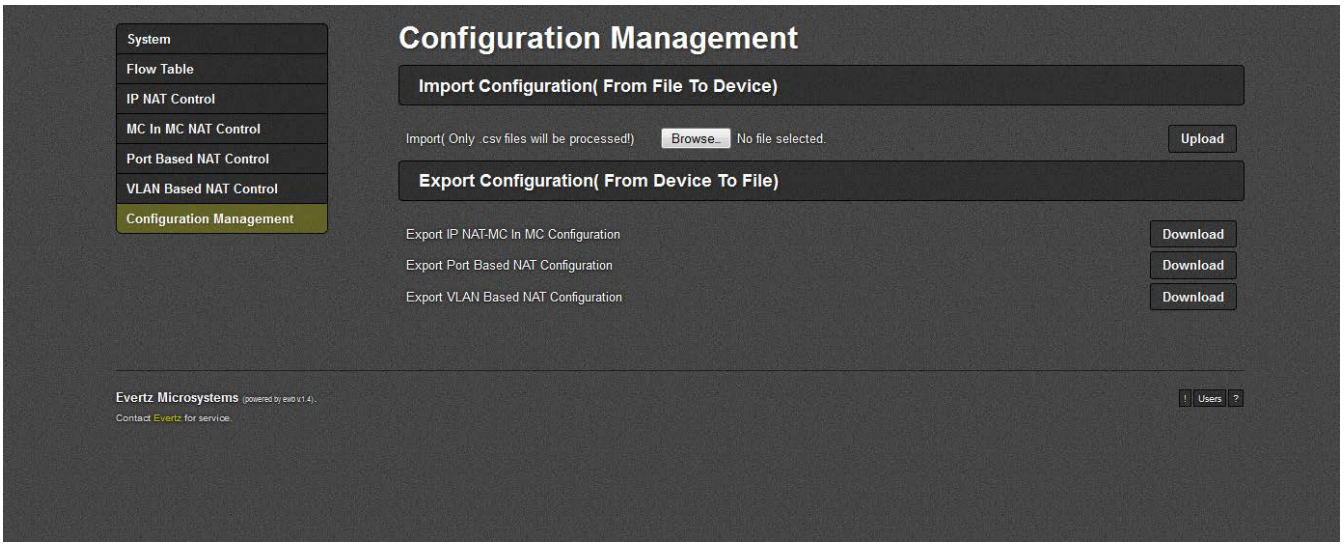


Figure 4-15: WebEASY® - Configuration Management Tab

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 7880IPG-NAT.

When first visiting the 7880IPG-NAT 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 7880IPG-NAT, there is a tab labeled **Upgrade**. The **Upgrade** tab is used to check current firmware version and upload the latest firmware.

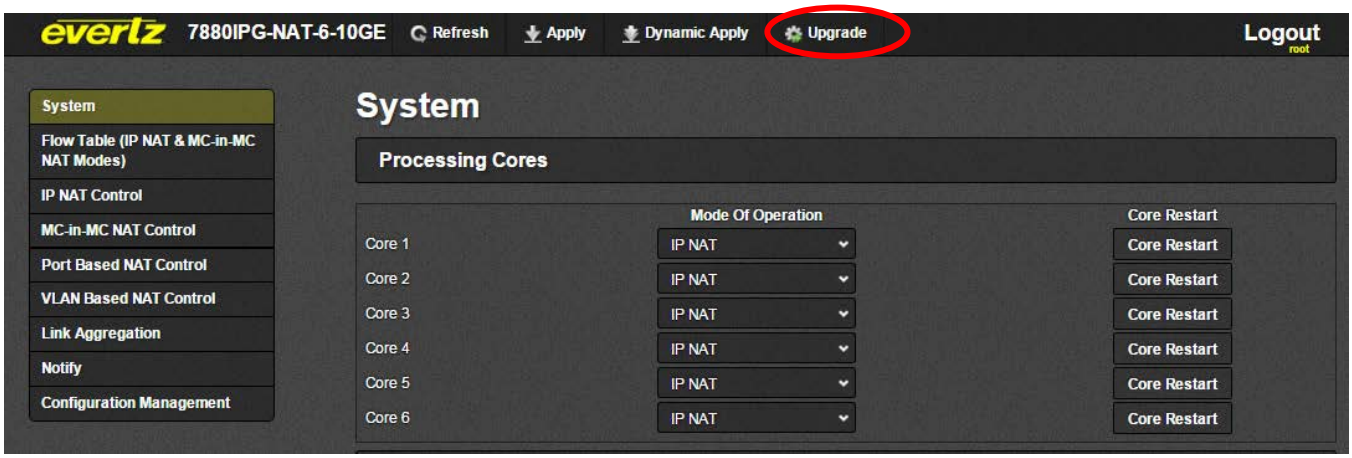


Figure 5-1: WebEASY® - Upgrade Button on Top Menu Bar

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.

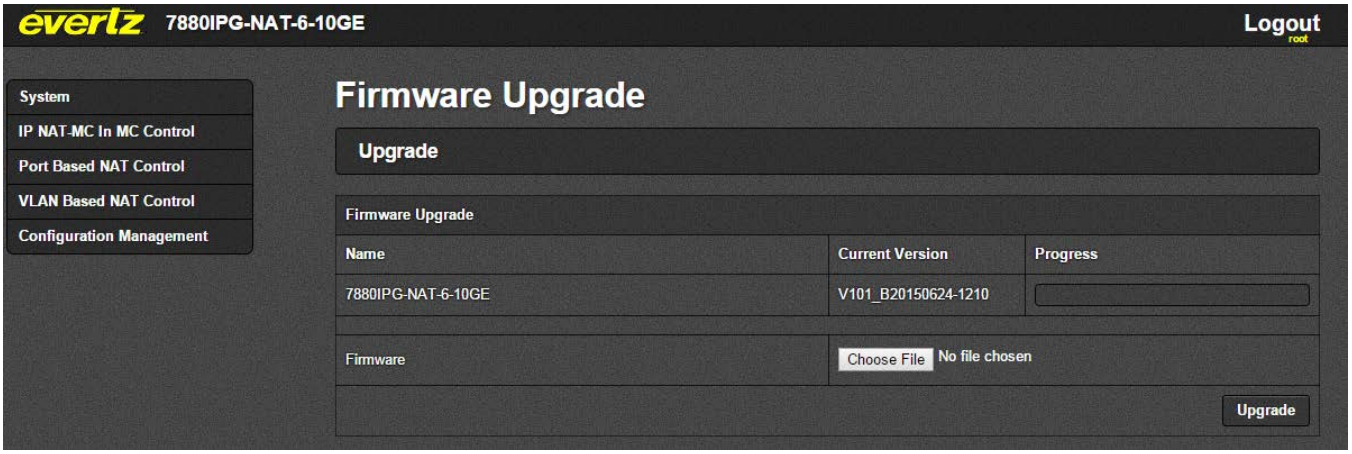


Figure 5-2: WebEASY® - Firmware Upgrade Menu

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.

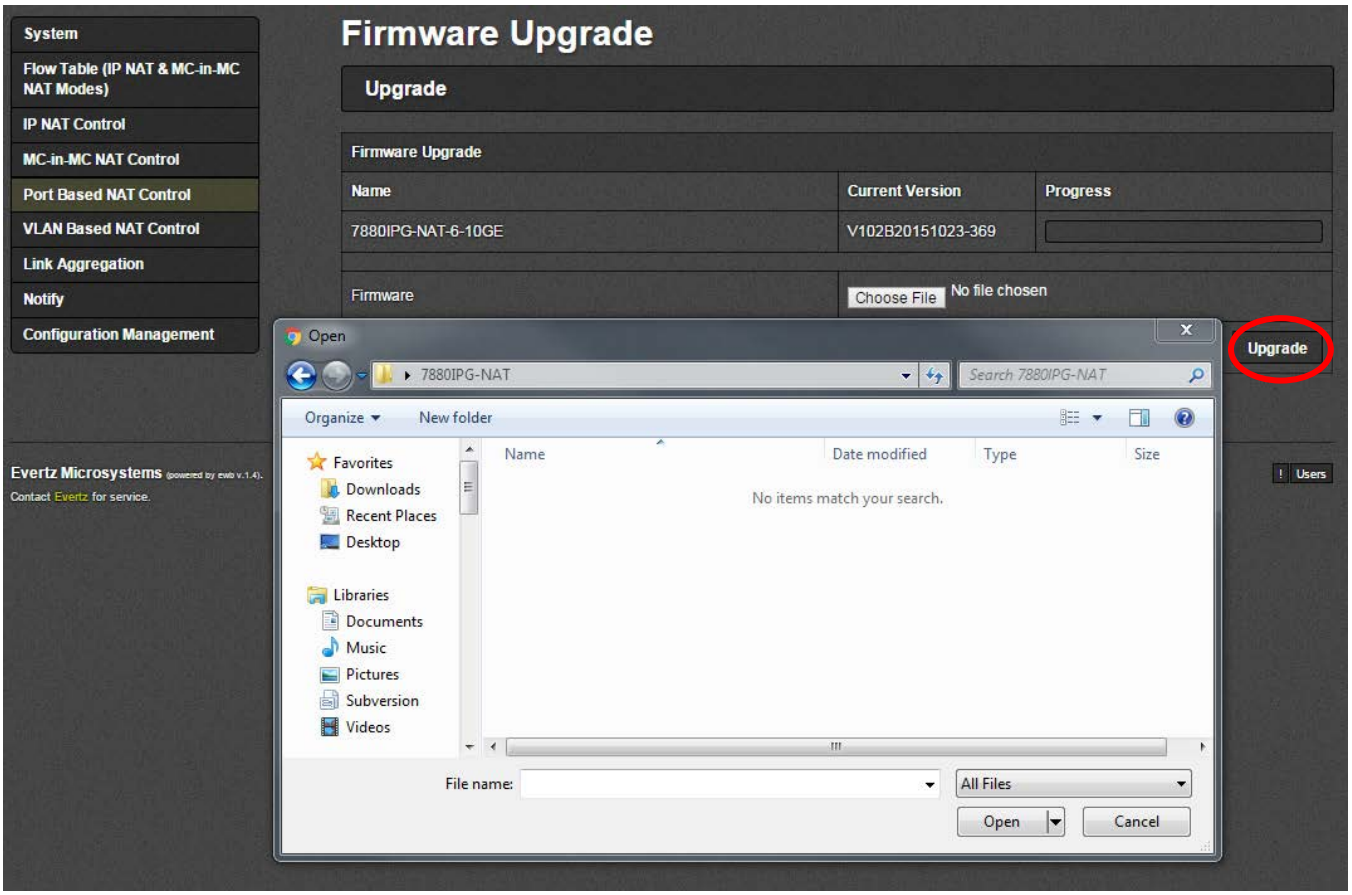


Figure 5-3: WebEASY® - Firmware Upgrade Menu