

Network Address Translation (NAT)

All Mediatrix units

DGW 49.2.2941

2023-08-09

Table of Contents

Basic Concepts	3
Network Address Translation (NAT)	3
Understanding Network Address Translation Rules	3
NAT Rule Order - Important	4
Destination or Source IP Address Format	4
Source or Destination Port Format	5
Interaction of NAT rules with the Firewall Service	5
Basic Tasks	6
Starting/Stopping/Restarting the NAT Service Using the DGW Web Page	6
Enabling IPv4 Forwarding	6
Creating a Source NAT Rule	7
Creating a Destination NAT Rule	7
NAT Rule Examples	9
Creating a Source NAT Rule to Forward the Lan to the Uplink Network Interface	9
Online Help	10
DGW Documentation	11
Copyright Notice	12

Basic Concepts

Network Address Translation (NAT)

Network Address Translation (NAT, also known as network masquerading or IP masquerading) rewrites the source and/or destination addresses/ports of IP packets as they pass through a router or firewall. It is most commonly used to connect multiple computers to the Internet (or any other IP network) by using one IP address. This allows home users and small businesses to cheaply and efficiently connect their network to the Internet.

The basic purpose of NAT is to multiplex traffic from the internal network and present it to the Internet as if it was coming from a single computer having only one IP address. The Mediatrix unit's NAT service allows the dynamic creation and configuration of network address translation rules. Depending on some criteria, the packet matching the rule may see its source or destination address modified.

There are two types of NAT rules:

- Source rules: They are applied on the source address of outgoing packets.
- Destination rules: They are applied on the destination address of incoming packets.

A rule's priority is determined by its index in the Source NAT or Destination NAT tables (Network/NAT). If the NAT service is stopped, this tab is greyed out and the parameters are not displayed.

The maximum number of rules allowed in the configuration is 10 of each Source NAT and Destination NAT.

Note: Adding source or destination NAT rules has an impact on the Mediatrix unit's overall performance as the NAT requires additional processing. The more rules are enabled, the more overall performance is affected. Furthermore, Media5 recommends to use a 30 ms packetization time when the NAT is enabled (instead of a 20 ms ptime, for instance) in order to simultaneously use all the channels available on the unit.

Note: The Mediatrix unit NAT service does not support IPv6

Understanding Network Address Translation Rules

A NAT rule specifies a set of matching conditions for network packets.

Each rule can use one or more of the following criteria:

- Source Address
- Destination Address
- Protocol (All, TCP, UDP or ICMP).

If the protocol is set to TCP or UDP, the following criteria can also be used:

- Source Port
- Destination Port

When all the criteria of a rule match, the NAT will modify the packet to use the **New Address** field, either for the **Source Address** or the **Destination Address**, according to the type of NAT for which the rule is applied.

NAT Rule Order - Important

The NAT rules are applied on a first match basis, in the order they appear in the configuration.

Because the first match is applied, you must ensure that specific rules come before more general rules, or the specific rules might not be applied as desired.

Destination or Source IP Address Format

IP Addresses can take the form of:

- An empty string, meaning that the rule will match any IP address
- An IP address, for example 192.168.0.11
- A network address, for example 192.168.1.0/24, which corresponds to all IP addresses in the range 192.168.1.0 to 192.168.1.255

It is also possible to use the name of a network interface to represent either the current IP address or network of that interface.

- Specifying the interface name without a trailing slash represents the IP address
- The same name with the trailing slash represents the network.

Note: This is case sensitive (the first letter must be uppercase)

For example, if your lan interface is configured as 192.168.0.10/24

- **Lan1** will be replaced by the current IP address of the lan interface, 192.168.0.10
- **Lan1/** will be replaced with the network of the lan interface, /24, meaning the range from 192.168.0.0 to 192.168.0.255.

If the specified interface is disabled or removed, the rule is automatically disabled thus removed from the NAT. When the network interface is enabled or added back, the rule is automatically enabled and applied in the NAT.

Source or Destination Port Format

Ports can take the form of either:

- An empty string, meaning that the rule will match any port
- Single port, for example for a web server: 80
- A range of ports, for example to forward RTP: 5004-5099

Interaction of NAT rules with the Firewall Service

When using the Network Firewall service, it is important to configure it with respect to the Destination NAT rules because:

- Source NAT (SNAT) rules are executed after the routing decision, before the packet leaves the unit.
- Destination NAT (DNAT) rules are executed before the routing decision, as the packet enters the unit.

An example of this would be port forwarding where the DNAT changes the routed address of a packet to a new IP address/port. The Network Firewall must also accept connection to this IP/port in order for the port forwarding to work.

Basic Tasks

Starting/Stopping/Restarting the NAT Service Using the DGW Web Page

Steps

- 1) Go to **System/Services**.
- 2) In the **User Service** table, on the line of the NAT service set the **Startup Type** selection list to **Auto**.
- 3) Then,
 - click  if you wish to start the service, or
 - click  to restart the service.
 - click  to stop the service.

Note: When stopping or restarting a service, some interruptions might occur, such as dropped calls, virtual machine shutdown or loss of network connectivity, depending on the affected services and/or its dependencies.

- 4) Click **Apply**.

Result

The status of the service (in the **Status** column) changes following the executed service command.

- If you clicked , the tab from which you can access the service from the Web pages are greyed out
- If you clicked , the tab from which you can access the service from the Web pages are no longer greyed out.

Enabling IPv4 Forwarding

Steps

- 1) Go to **Network/IP Routing**.
- 2) In the **IP Routing configuration** table, select **Enable**.
- 3) Click **Save**.

Result

If IP Forwarding is disabled, the **Advanced IP Routes** table is greyed out.

IP Routing configuration	
IPv4 Forwarding:	Enable 

Creating a Source NAT Rule

Before you start

IPv4 forwarding must be enabled under **Network/IP Routing**.

Steps

- 1) Go to **Network/NAT**.
- 2) In the **Source Network Address Translation Rules**, click 

Note: To add a rule before an existing entry, locate the proper row in the table and click the  button of this row. To add a rule at the end of the existing rows, click the  button at the bottom right of the section.

Note: The yellow Yes in the Config Modified section at the top of the window indicates that the configuration has been modified but not applied (i.e., the Network Address Translation section of the Status page differs from the NAT page).

- 3) Complete the fields as required.
- 4) Click **Apply**.

Result

The applied enabled rules are displayed in the **Network/Status/Network Address Translation** section, which contains the active configuration in the NAT. The yellow Config Modified Yes flag is cleared.

Creating a Destination NAT Rule

Steps

- 1) Go to **Network/NAT**.

- 2) In the **Destination Network Address Translation Rules**, click 

Note: To add a rule before an existing entry, locate the proper row in the table and click the  button of this row. To add a rule at the end of the existing rows, click the  button at the bottom right of the section.

Note: The yellow Yes in the Config Modified section at the top of the window indicates that the configuration has been modified but not applied (i.e., the Network Address Translation section of the Status page differs from the NAT page).

- 3) Complete the fields as required.
4) Click **Apply**.

Result

The applied enabled rules are displayed in the **Network/Status/Network Address Translation** section, which contains the active configuration in the NAT. The yellow Config Modified Yes flag is cleared.

NAT Rule Examples

Creating a Source NAT Rule to Forward the Lan to the Uplink Network Interface

Steps

- 1) Go to **Network/NAT**.
- 2) In the **Source Network Address Translation Rules**, click **+**.
- 3) From the **Activation** selection list, click **Enable**.
- 4) In the **Source Address** field, enter **Lan1/**.
- 5) From the **Protocol** selection list, choose **All**.
- 6) In the **New Address** field, enter **Uplink**.
- 7) Click **Save & Apply**.

Result

Source Network Address Translation Rules							
#	Activation	Source Address	Source Port	Destination Address	Destination Port	Protocol	New Address
1	Enable	Lan1/				All	Uplink
							+

Online Help

If you are not familiar with the meaning of the fields and buttons, click **Show Help**, located at the upper right corner of the Web page. When activated, the fields and buttons that offer online help will change to green and if you hover over them, the description will be displayed.

DGW Documentation

Mediatrix devices are supplied with an exhaustive set of documentation.

Mediatrix user documentation is available on the [Media5 Documentation Portal](#).

Several types of documents were created to clearly present the information you are looking for. Our documentation includes:

- **Release notes:** Generated at each GA release, this document includes the known and solved issues of the software. It also outlines the changes and the new features the release includes.
- **Configuration notes:** These documents are created to facilitate the configuration of a specific use case. They address a configuration aspect we consider that most users will need to perform. However, in some cases, a configuration note is created after receiving a question from a customer. They provide standard step-by-step procedures detailing the values of the parameters to use. They provide a means of validation and present some conceptual information. The configuration notes are specifically created to guide the user through an aspect of the configuration.
- **Technical bulletins:** These documents are created to facilitate the configuration of a specific technical action, such as performing a firmware upgrade.
- **Hardware installation guide:** They provide the detailed procedure on how to safely and adequately install the unit. It provides information on card installation, cable connections, and how to access for the first time the Management interface.
- **User guide:** The user guide explains how to customise to your needs the configuration of the unit. Although this document is task oriented, it provides conceptual information to help the user understand the purpose and impact of each task. The User Guide will provide information such as where and how TR-069 can be configured in the Management Interface, how to set firewalls, or how to use the CLI to configure parameters that are not available in the Management Interface.
- **Reference guide:** This exhaustive document has been created for advanced users. It includes a description of all the parameters used by all the services of the Mediatrix units. You will find, for example, scripts to configure a specific parameter, notification messages sent by a service, or an action description used to create Rulesets. This document includes reference information such as a dictionary, and it does not include any step-by-step procedures.

Copyright Notice

Copyright © 2023 Media5 Corporation.

This document contains information that is proprietary to Media5 Corporation.

Media5 Corporation reserves all rights to this document as well as to the Intellectual Property of the document and the technology and know-how that it includes and represents.

This publication cannot be reproduced, neither in whole nor in part, in any form whatsoever, without written prior approval by Media5 Corporation.

Media5 Corporation reserves the right to revise this publication and make changes at any time and without the obligation to notify any person and/or entity of such revisions and/or changes.



media5corp.com