Industrial Networking
Tech Note 12 RAM®-6021: Configuring NAT

Abstract:

How to configure the RAM-6021 for Network Address Translation (NAT) – 1 to 1

Products:

RAM-6021

Use Case / Problem Solved: Short Description

Often in factory automation applications, the network will be comprised of cells and/or panels of different networks that have duplicated IP addressing schemes. The RAM-6021 and NAT functionality can be used to isolate these devices from one another and allow remote access to those devices from the network at the same time.

Required Software:

Web Browser

Required Firmware:

4.22 or higher

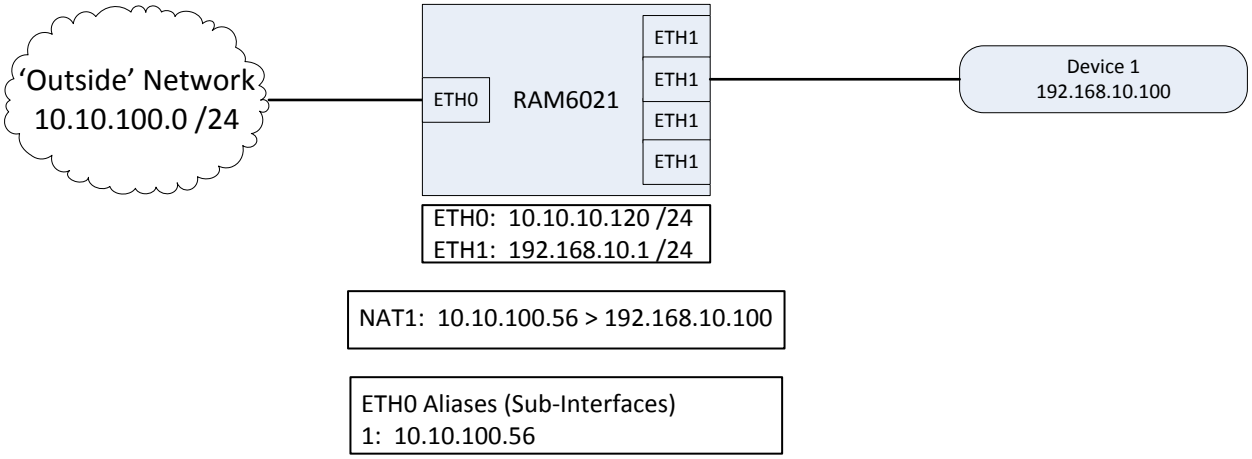
Scenarios

There are two common scenarios when using NAT.

1. The NAT address(es) will be on the same subnet as Eth0.
2. The NAT address(es) will be on a different subnet than both Eth0 and Eth1.

Same Subnet

When the NAT addresses being used are on the same subnet as ETH0 a sub-interface must be defined on ETH0 (called an Alias on the RAM). There will be one Alias address per NAT address (the Alias and NAT address will be the same address).



The 'outside' network (WAN side, corporate network) is 10.10.100.0 with a mask of 255.255.255.0 (24 bit mask).

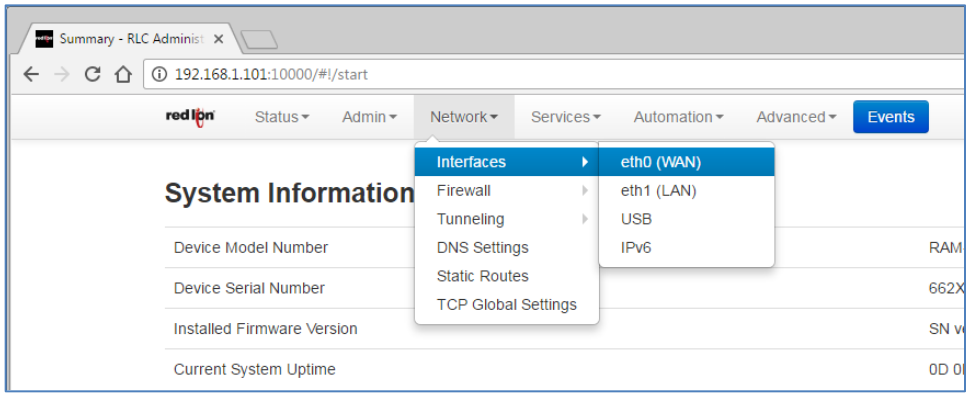
ETH0 = 10.10.100.120 /24

NAT address #1 = 10.10.100.56 /24 (translating to 192.168.10.100 on the Eth1 side)

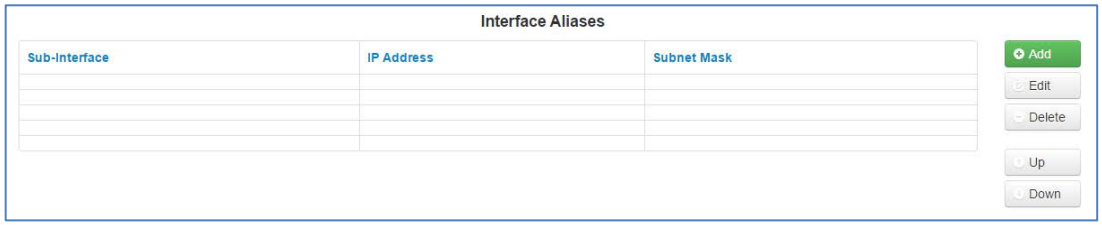
An Alias/Sub-Interface has to be defined under ETH0 with an address of 10.10.100.56 /24.

Define the alias (sub-interface) on Eth0:

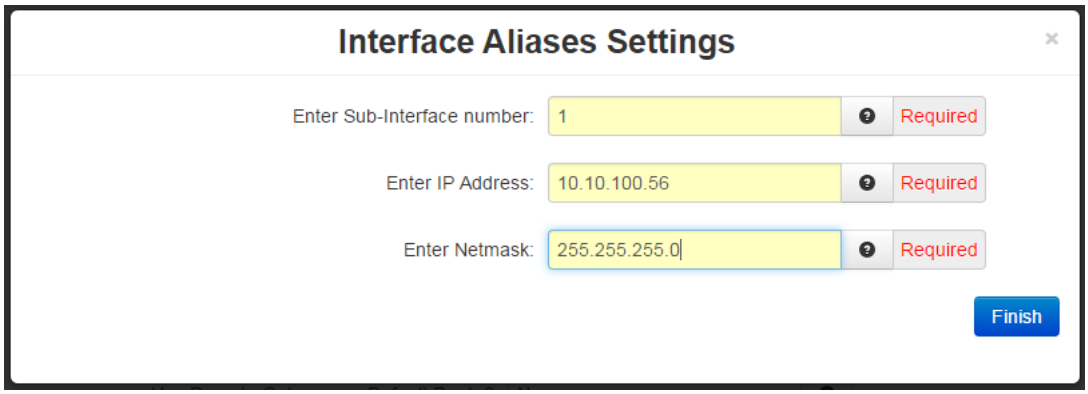
1. Navigate to *Network - Interfaces - Ethernet 0*.



2. In the Internet Aliases table click *Add*.



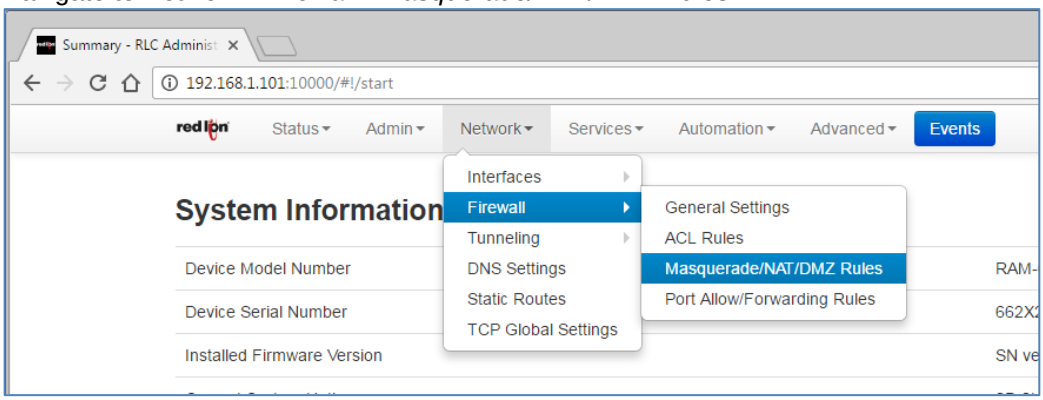
3. Enter the Sub-Interface # (1,2,3....), IP Address (10.10.100.56 in this case) and subnet mask (255.255.255.0 in this case).



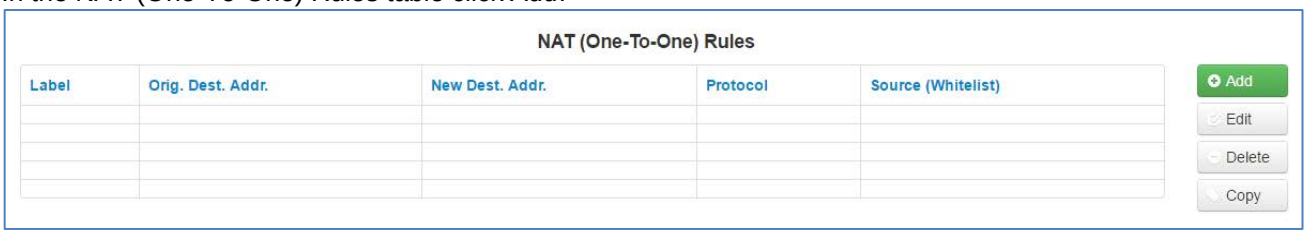
4. Click *Finish*.
5. Click *Apply*.
6. Add additional Sub-Interface (Alias) addresses as needed.

Define the NAT addresses:

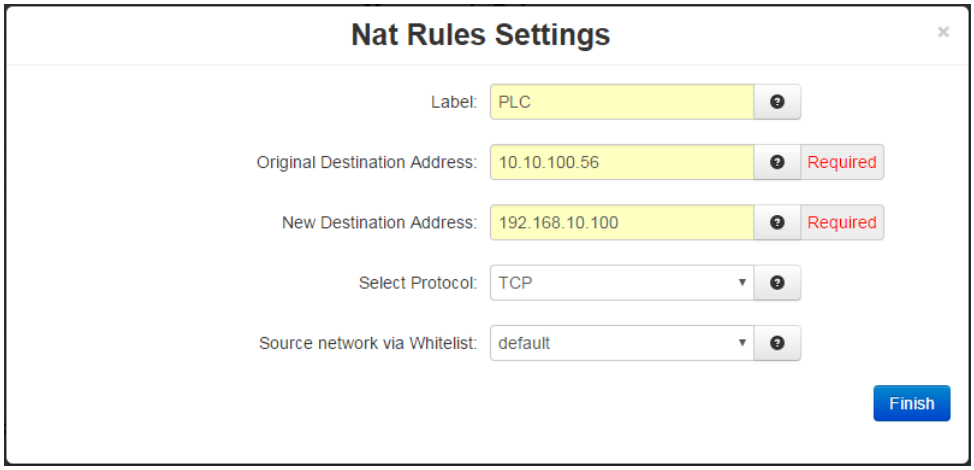
1. Navigate to *Network - Firewall - Masquerade/NAT/DMZ Rules*.



2. In the NAT (One-To-One) Rules table click *Add*.



   a. In the 'NAT Rules Settings' pop-up menu complete the following:
   b. Label: SimpleText Field – Enter meaningful label
   c. Original Destination Address: NAT address – being seen by remote hosts (external)
      - (10.10.100.56 in this example)
   d. New Destination Address: Actual address of device 'behind the router' (e.g. PLC)
      - (192.168.10.100 in this example)
   e. Protocol and Whitelist can most likely stay as TCP and Default.
   f. Click *Finish*.

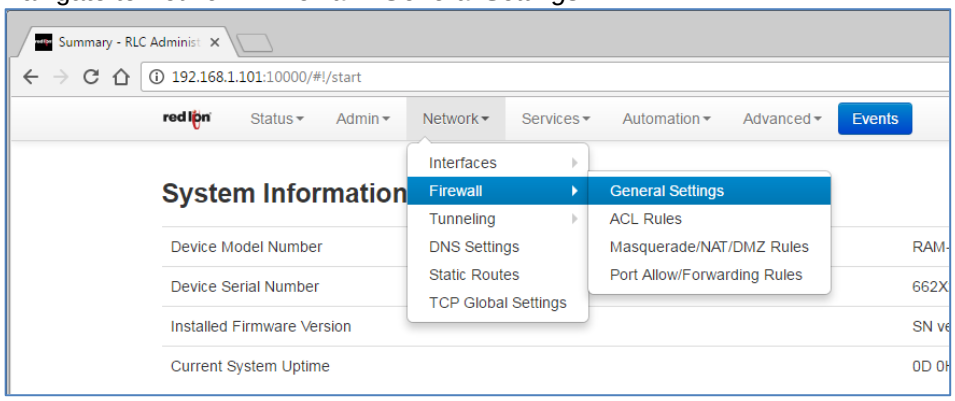


3. Click *Apply*.
4. Add additional NAT address translations as needed.

Define Trusted Interfaces

Eth0 by default is defined as "Untrusted". Eth0 needs to be defined as "Trusted".

1. Navigate to *Network - Firewall - General Settings.*

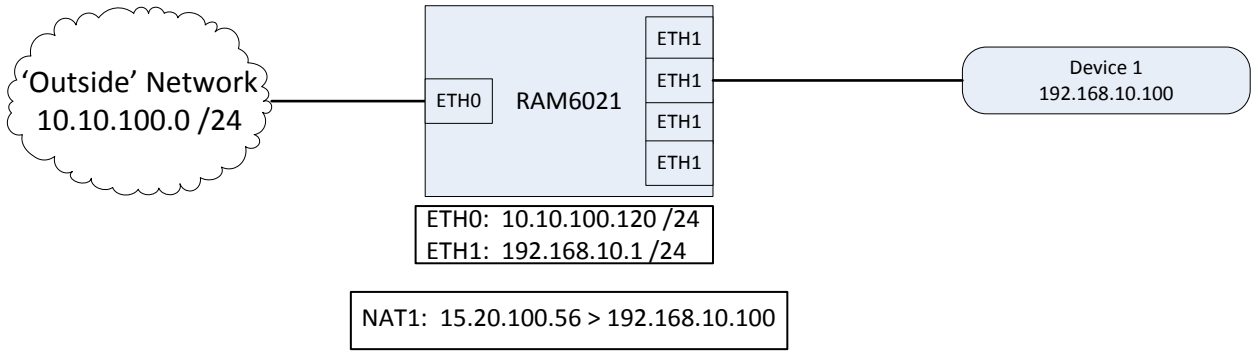


2. Delete Eth0 from the Untrusted Interfaces table.
3. Add Eth0 to the Trusted Interfaces table.

4. Click *Apply*.

Different Subnet:

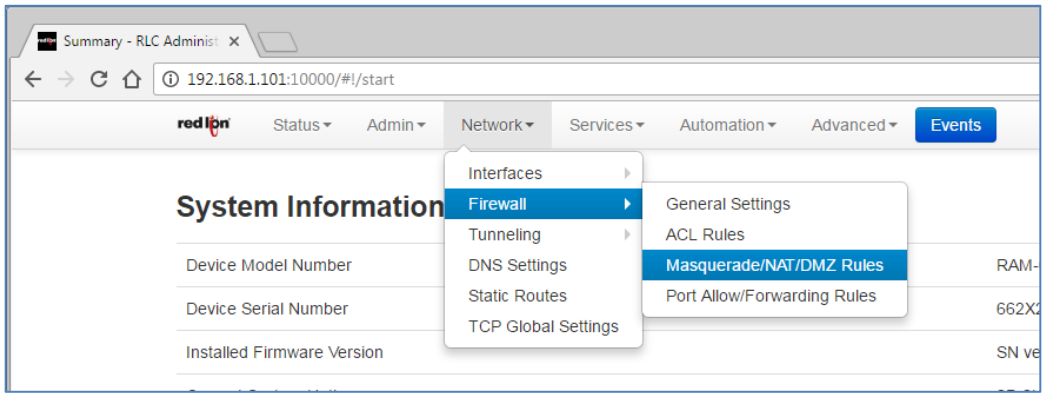
The NAT addresses being used are on a different subnet than ETH0 (and Eth1).



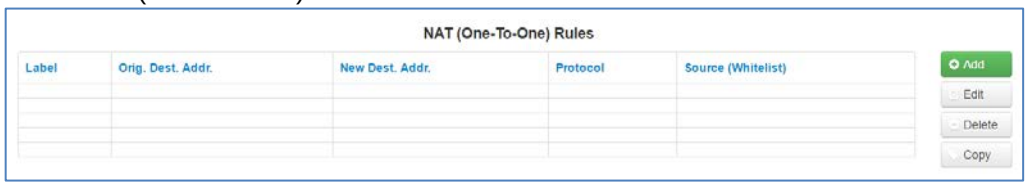
ETH0 = 10.10.100.120 /24
NAT (#1) = 15.20.100.56 /24 (translating to 192.168.10.100 on the Eth1 side)

Define the NAT addresses:

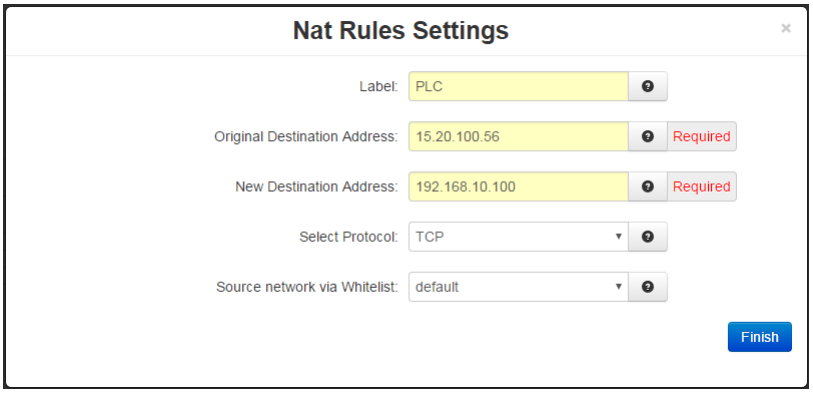
1. Navigate to *Network - Firewall - Masquerade/NAT/DMZ Rules*



2. In the 'NAT Rules Settings' pop-up menu complete the following:
   a. In the NAT (One-To-One) Rules table click *Add*



   b. Label: SimpleText Field – Enter meaningful label
   c. Original Destination Address: NAT address – being seen by remote hosts (external)
      - (15.20.100.56 in this example)
   d. New Destination Address: Actual address of device 'behind the router' (e.g. PLC)
      - (192.168.10.100 in this example)
   e. Protocol and Whitelist can most likely stay as TCP and Default

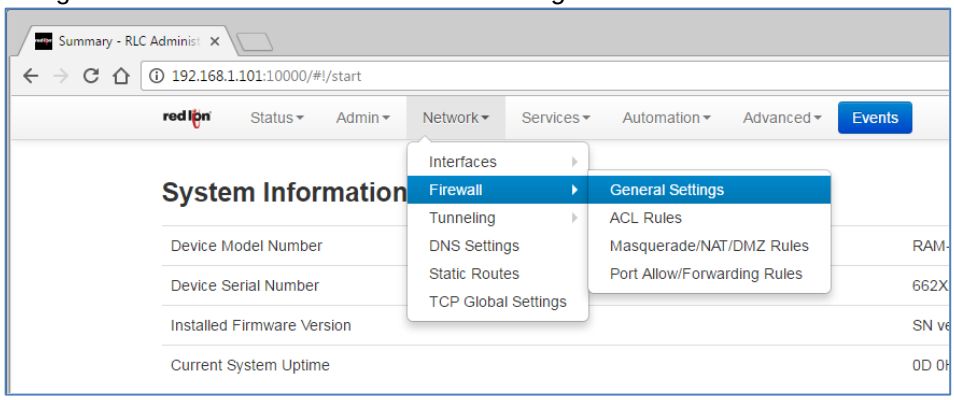


   f. Click *Finish*.
3. Click *Apply*.
4. Add additional NAT address translations as needed.

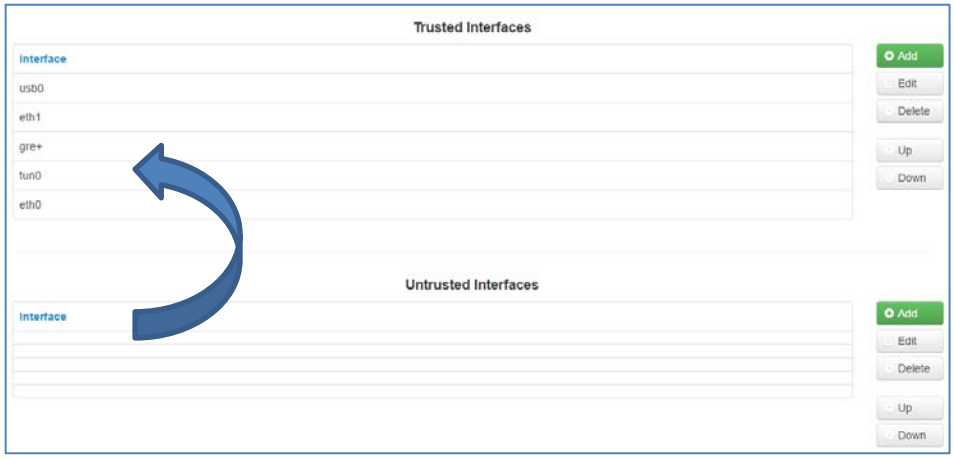
Define Trusted Interfaces

Eth0 by default is defined as “Untrusted”. Eth0 needs to be defined as “Trusted”

1. Navigate to *Network - Firewall - General Settings.*



2. Delete Eth0 from the Untrusted Interfaces table.
3. Add Eth0 to the Trusted Interfaces table.



4. Click Apply.
   NOTE: In this situation the routing has to be in place in the “outside” network to get to the NAT address (in this example 15.20.100.56/24). Meaning, the manager of the network on the Eth0 side of the RAM-6021 needs to add the proper routes to get to the new “made up” NAT addresses.

Disclaimer:

It is the customer's responsibility to review the advice provided herein and its applicability to the system. Red Lion Controls makes no representation about specific knowledge of the customer's system or the specific performance of the system. Red Lion is not responsible for any damage to equipment or connected systems. The use of these documents is at your own risk.

For more information: http://www.redlion.net/support/policies-statements/warranty-statement