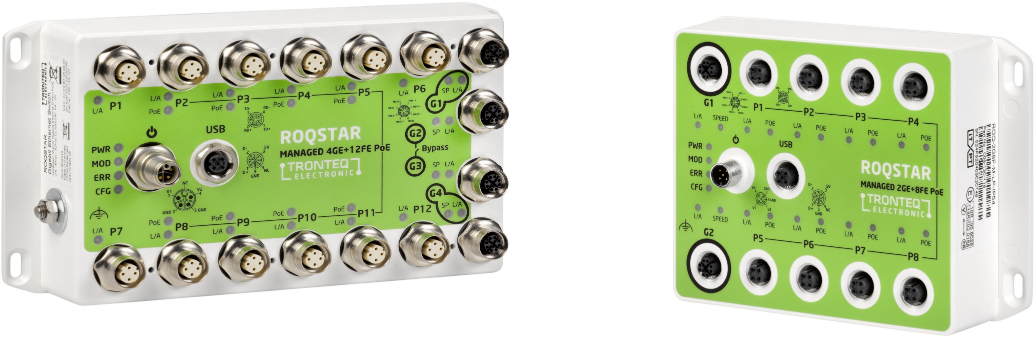
Application Note



Network Address Translation with ROQSTAR Managed Gigabit Ethernet Switches

Introduction

In IP networks with a deliberate network segmentation by VLAN and IP subnets oftentimes there are devices which need to communicate across these borders.

Usually this is the case for internet or backbone connections or with overarching networks that are used to connect multiple local ones.

One common technique used to enable communication from one IP subnet to another is Network Address Translation (NAT), of which there are different variants.

This document describes the NAT functionality offered by ROQSTAR Managed Gigabit Ethernet Switches.

Content

1 Technical description

1.1 Requirements

The Ethernet Switch will need to send and receive Ethernet frames in both subnets between which it shall translate. Therefore the Ethernet Switch needs to have an IP address in each of those subnets.

Since the IP Interfaces run on VLANs and there is one IP Interface per VLAN, NAT will be performed between different IP subnets of different VLANs.

To allow forwarding of IP packets between subnets, those IP Interfaces need to have the ‘IP Forwarding’ setting enabled.

If 1:1 NAT (with or without Masquerading) is used, the switch needs to respond to ARP ping requests to the additional IP addresses. Therefore the IP Interface’s ‘Proxy ARP’ setting needs to be enabled.

To test whether this setting is configured correctly you can send ARP ping requests to the additional address(es) from the matching subnet.

‘Proxy ARP’ is not needed when PAT is used.

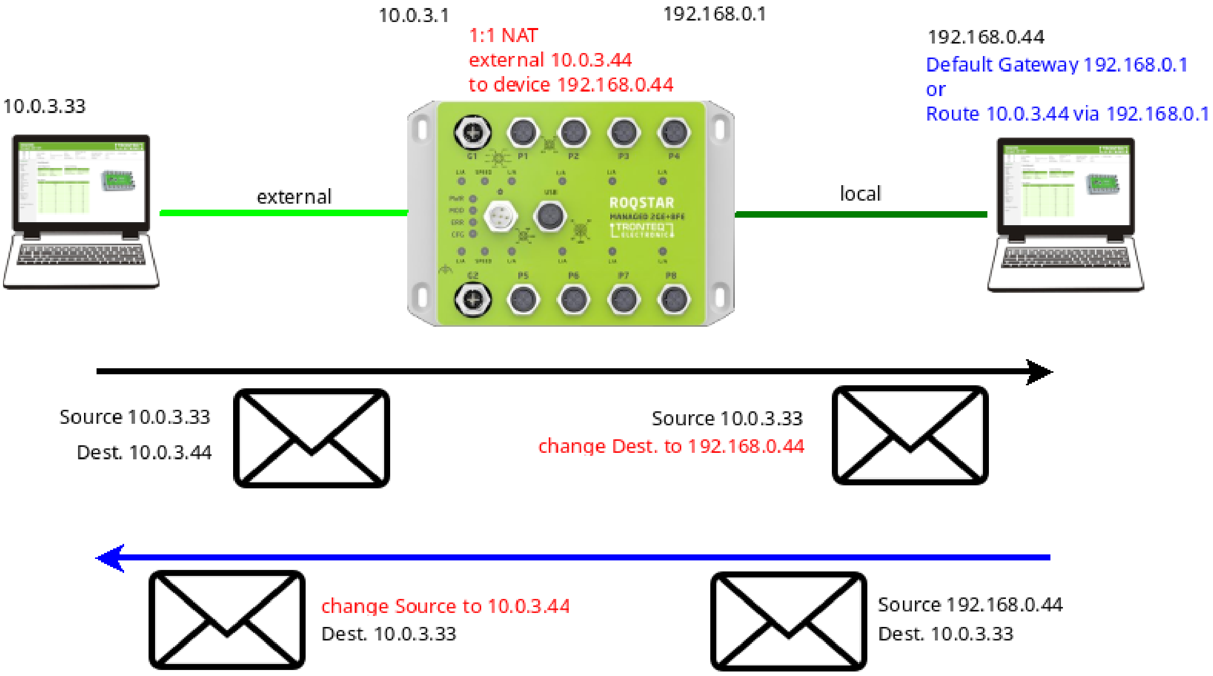
1.2 Supported variants

There is support for two different variants of NAT, each with and without Masquerading option.

1.2.1 1:1 NAT

Adding a 1:1 NAT rule will create an additional IP address internally in the switch. They will not be used by the switch's own IP communication (e.g. web interface or SNMP), but only used for the NAT communication.

This additional IP address is in the subnet of the 'external' side of the communication. This is typically the overarching network or facing the internet connection. There will be one such IP for each 'internal' ('local') end device that will be exposed to the 'external' network. The 1:1 mapping means that all (unicast) protocols and ports of the 'internal' device will be exposed 'externally', so that all services offered by the device will be available 'externally'.

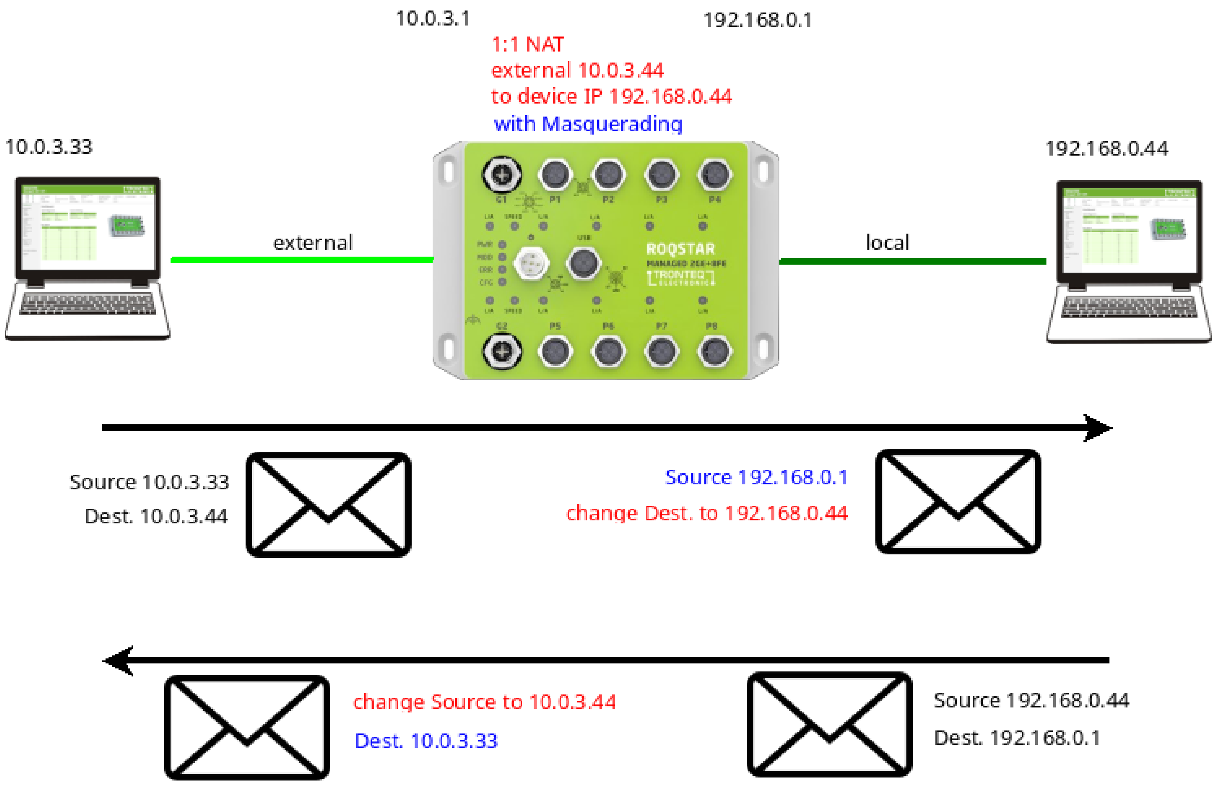


1.2.2 1:1 NAT with Masquerading

1:1 NAT is a special case of Source NAT (SNAT). If Masquerading is used, there will also be Destination NAT (DNAT) to replace the source address of the IP packet in the destination network (before it leaves the switch). Therefore the destination end device will not know that this packet originated in another IP subnet; it looks like it was sent by the switch using the switch's local IP address.

Thus any response the end device sends will be addressed to the switch, which must then know to modify the packet and transmit it to the other subnet. This behaviour of the switch for the return path is configured automatically when the NAT rule was added, so there is no need for a 'reverse' rule.

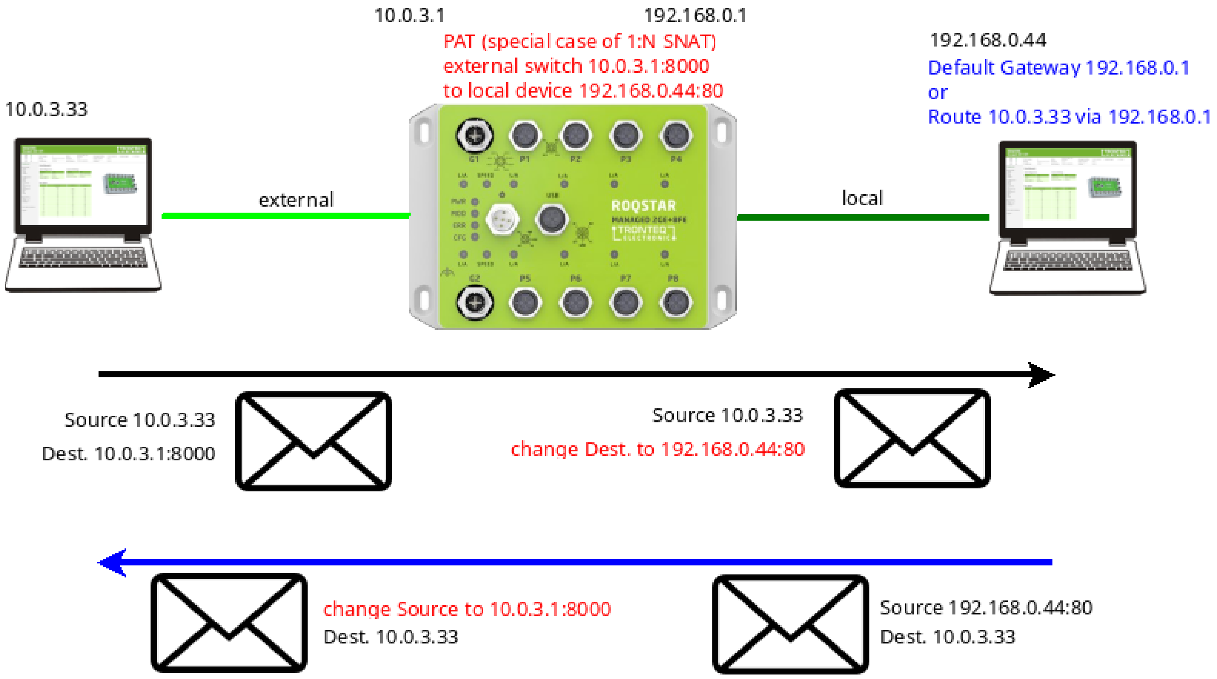
The switch is using 'connection tracking' in order to facilitate this. This means that both end devices can open the communication between each other.



1.2.3 PAT

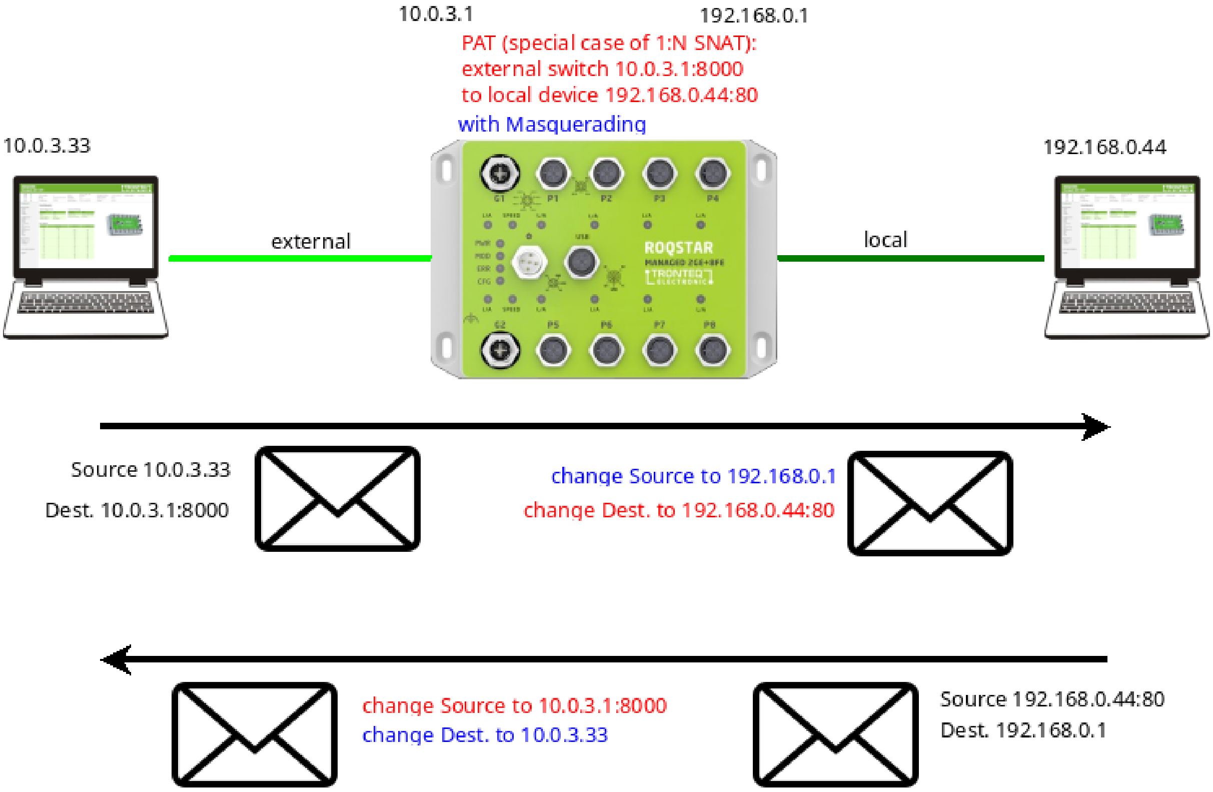
PAT is a form of NAT where only certain TCP or UDP protocol ports are translated and forwarded to another IP address. The communication partner on the ‘external’ side will send the packets to a specific protocol port at the switch’s IP address.

Only the switch’s own IP is exposed; the ‘internal’ device’s IP is hidden.


10.0.3.1
192.168.0.1
PAT (special case of 1:N SNAT)
external switch 10.0.3.1:8000
to local device 192.168.0.44:80
192.168.0.44
Default Gateway 192.168.0.1
or
Route 10.0.3.33 via 192.168.0.1
10.0.3.33
external
local
ROQSTAR
Source 10.0.3.33
Dest. 10.0.3.1:8000
Source 10.0.3.33
change Dest. to 192.168.0.44:80
change Source to 10.0.3.1:8000
Dest. 10.0.3.33
Source 192.168.0.44:80
Dest. 10.0.3.33

1.2.4 PAT with Masquerading

PAT, too, is available with the Masquerading option.


10.0.3.1
192.168.0.1
PAT (special case of 1:N SNAT):
external switch 10.0.3.1:8000
to local device 192.168.0.44:80
with Masquerading
10.0.3.33
192.168.0.44
external
local
ROQSTAR
TRONTEQ
Source 10.0.3.33
Dest. 10.0.3.1:8000
change Source to 192.168.0.1
change Dest. to 192.168.0.44:80
change Source to 10.0.3.1:8000
change Dest. to 10.0.3.33
Source 192.168.0.44:80
Dest. 192.168.0.1

1.3 Limitations

1.3.1 Performance

The address translation is done in software using the built-in CPU. Performance is depending on the packet size:

Constant stream of packets of size	Throughput
60 Bytes	approximately 10 Mbit/s
1500 Bytes	approximately 90 Mbit/s

For comparison: A video stream with Full-HD resolution, h.264 compression and 25fps, using RTSP protocol, has an average bit rate of less than 1Mbit/s using large (>1000 Bytes) packets. Performing NAT of one such stream will increase the CPU usage by about 1%.

Running NAT with near-maximum performance will inhibit the performance of other software services of the switch (e.g. the web interface, SNMP, etc.).

1.3.2 Number of NAT Rules

The maximum number of NAT rules per Ethernet switch is 20.

1.3.3 Unicasts

The offered NAT function will translate unicast IPv4 packets. Multicast packets (which have different IPv4 addresses) are not translated.

2 Usage Scenario

2.1 Recommendations

2.1.1 Choosing a variant

These are some general recommendations regarding the choice of NAT variant. The main difference between the two offered variants is that 1:1 NAT is for a single device, whereas PAT is for a single service.

If you prefer to open protocol ports selectively instead of exposing a complete device, this is possible using PAT. PAT is a viable option especially if only one protocol port of a device needs to be translated.

In contrast, if multiple services using multiple protocol ports running on a device shall be made available using NAT, 1:1 NAT may be the better option, since it requires only one rule per device.

In case you would like to avoid using the switch’s IP for communication with the end devices, use 1:1 NAT.

If the ROQSTAR Switch shall handle NAT for multiple devices that are addressed via hostname (DNS), then using PAT means less DNS names in the ‘external’ net are necessary.

2.1.2 Masquerading

Regarding the usage of Masquerading please consider the visibility of the end devices as well as their default gateway / routing settings.

Especially for end devices that are members of only one VLAN oftentimes it is more practical to use Masquerading.

2.1.3 Choosing protocol ports

When defining PAT rules it is recommended to avoid using the protocol ports that are already in use by the switch’s IP services, otherwise they will be blocked. These are for example

Protocol	Port
Web interface, HTTP	80
Web interface, HTTPS	443
SNMP	161, 162
DHCP	67, 68

2.1.4 Mitigation of limitations

To lessen the impact of or work around the beforementioned limitations, especially in larger networks, it is good practice to use NAT on multiple Ethernet switches.

Each switch can be configured to perform NAT for the addresses of the connected devices. That way the NAT load is divided between the switches. This is also good for grouping/localizing dependencies regarding availability.

2.1.5 IP assignment

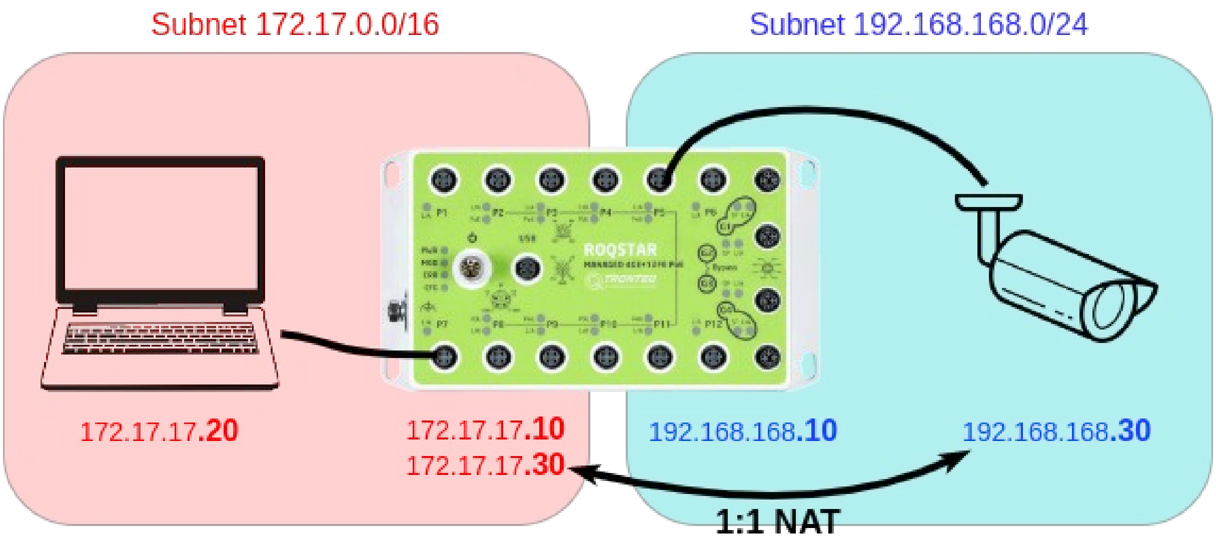
It is recommended to configure the ROQSTAR Ethernet Switch with fixed (static) IP addresses, since the offered IP-based services, including NAT, are based on the switch's IPs.

Devices connected to the switch are free to have fixed IPs or use assignment via port-based DHCP.

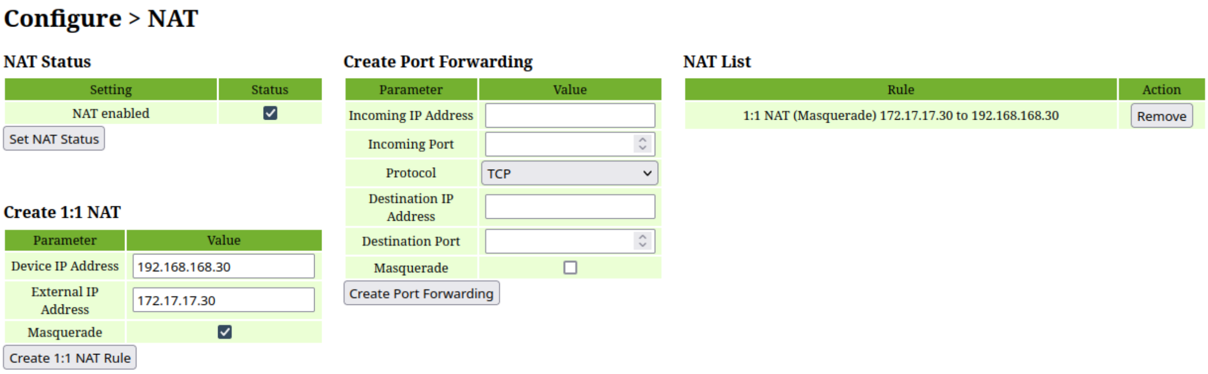
2.2 Examples

2.2.1 1:1 NAT with Masquerading

1:1 NAT for an IP camera. The camera is in the ‘internal’ subnet, the laptop is in the ‘external’ subnet. All protocol ports of the camera are accessible by the laptop: For example both the video stream (RTSP, unicast) as well as the camera’s web interface (HTTP/HTTPS).



Settings in the web interface:



Configure > NAT

NAT Status

Setting	Status
NAT enabled	☑

Create 1:1 NAT

Parameter	Value
Device IP Address	192.168.168.30
External IP Address	172.17.17.30
Masquerade	☑

Create Port Forwarding

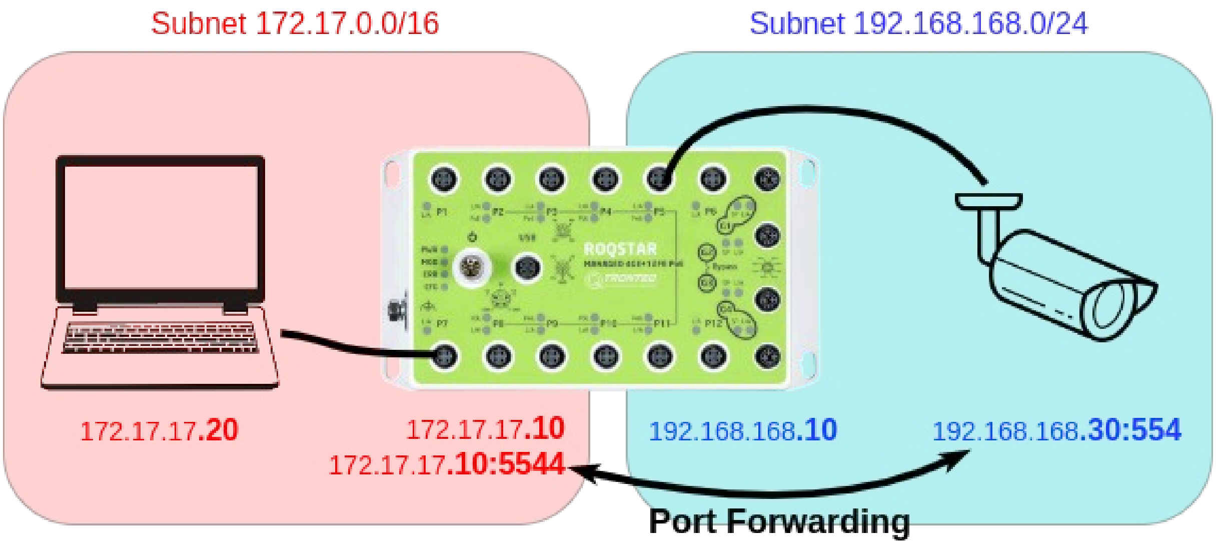
Parameter	Value
Incoming IP Address	
Incoming Port	
Protocol	TCP
Destination IP Address	
Destination Port	
Masquerade	☐

NAT List

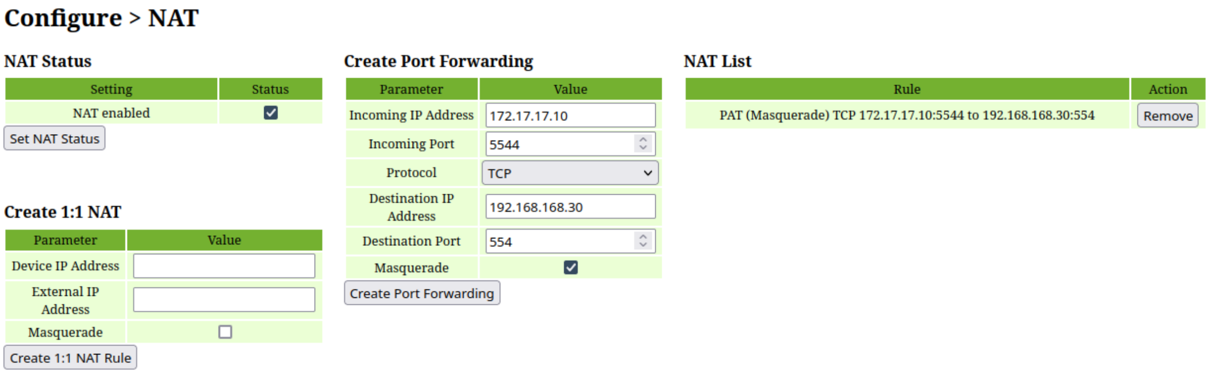
Rule	Action
1:1 NAT (Masquerade) 172.17.17.30 to 192.168.168.30	Remove

2.2.2 PAT with Masquerading

Port Address Translation for a RTSP camera stream (which is using TCP as transport protocol). The camera is in the ‘internal’ subnet, the laptop receiving the stream is in the ‘external’ subnet.



Settings in the web interface:



Configure > NAT

NAT Status

Setting	Status
NAT enabled	☑

Set NAT Status

Create 1:1 NAT

Parameter	Value
Device IP Address	
External IP Address	
Masquerade	☐

Create 1:1 NAT Rule

Create Port Forwarding

Parameter	Value
Incoming IP Address	172.17.17.10
Incoming Port	5544
Protocol	TCP
Destination IP Address	192.168.168.30
Destination Port	554
Masquerade	☑

Create Port Forwarding

NAT List

Rule	Action
PAT (Masquerade) TCP 172.17.17.10:5544 to 192.168.168.30:554	Remove