VegaStream Information Note
NAT handling

Voice over IP protocols do not naturally operate through NAT devices; when two VoIP endpoints, which are situated on different sides of a NAT, wish to communicate there are changes to the contents of the VoIP messages that must be made.

The changes to the VoIP message contents can be configured within the Vega.

This document explains the problems of NAT on VoIP protocols, and also how to configure the Vega and NAT device to allow correct transmission of VoIP messages.

Introduction

This document defines the operation of NAT, explains why this is a problem for VoIP, and then identifies a number of solutions. Some solutions are external to the Vega and thus do not need any special configuration in the Vega. This document focuses on a solution where the external IP address of the NAT device is statically configured in the Vega so that when the Vega makes calls across the NAT it provides the correct IP information in the VoIP messages.

If you are configuring a Vega to sit in the DMZ of a NAT firewall where all the private IP ports are mapped 1:1 to a public IP address on the outside of the NAT firewall, and you do not want to read all the background, please jump directly to ‘Annex 2 – Configuring NAT traversal in a Vega placed in a NAT DMZ’

NAT operation

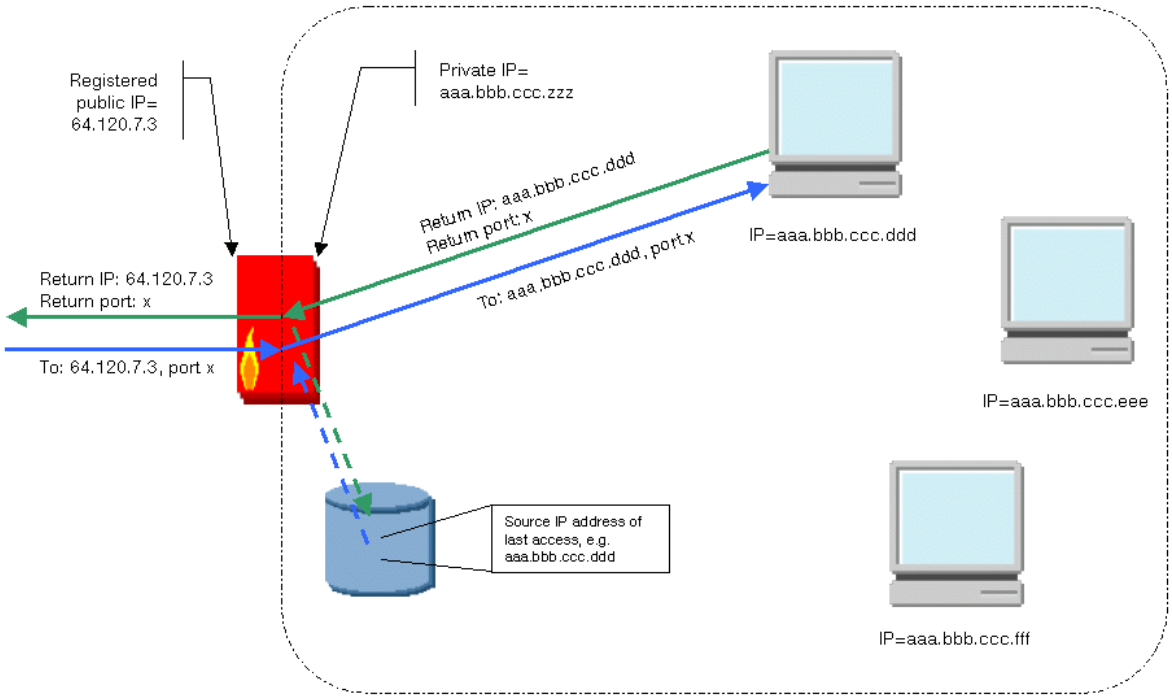
NAT, Network Address Translation is a facility that allows multiple IP addresses to be used within a private network without having to register each IP address with IANA, the IP address registration service. This is useful as it allows the private network to be expanded without using up more “public”

IP addresses. Also, the limited use of public IP addresses is important as the number of public IP addresses is finite.

At a minimum, NAT translation performs IP address translation so that when any access is made to the public internet by a device with a private IP address, to devices in or across the internet, the access appears to have come from a registered public IP address. This is necessary because router devices within the internet only route IP packets to registered IP addresses; they cannot route calls to private IP addresses.

The following diagram shows a device with a private IP address aaa.bbb.ccc.ddd making an access through the NAT router. The NAT router logs the source IP address of the outbound IP packet then changes the Return IP address to its own registered public IP address.

When a response is made to the NAT router, it looks up the IP address it stored earlier, and routes the response to the appropriate private address.

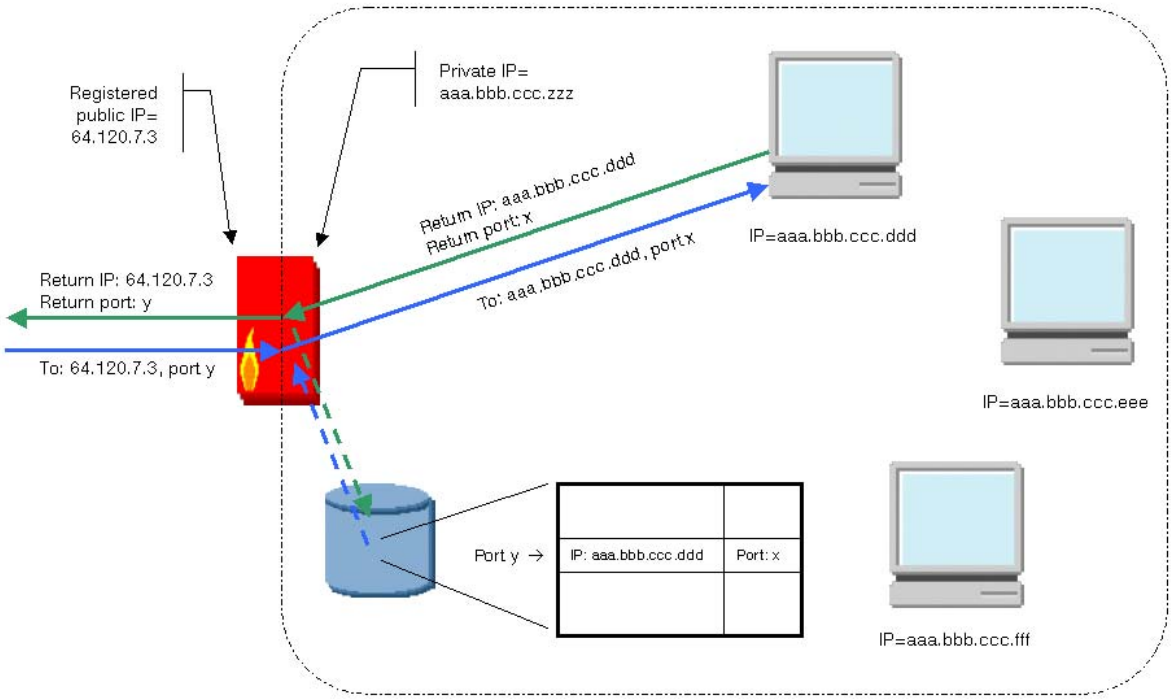


IP address translating NAT router

This form of NAT translation is limited in that only 1 private device at a time can have access to the public internet, if multiple internal devices were to try to get access then replies may get forwarded to the wrong recipient.

A common extension of NAT translation is to translate the local IP address and port combination into a public IP address / port combination. This translation, though generically still referred to as NAT is more properly known as PAT (Port Address Translation). In this scenario the PAT router receives a request from a private IP device and it converts the IP address and the IP port number, making sure that the outgoing (public) IP address, IP port number combination is unique. When a reply is sent to this unique IP address and IP port combination the PAT router is then able to look up the correct device (private IP address and port) to send it to.

This means that simultaneous accesses from multiple private IP devices may be made through the PAT router, as it is able to keep a table indexed by outgoing port number to keep return IP address and port number information.

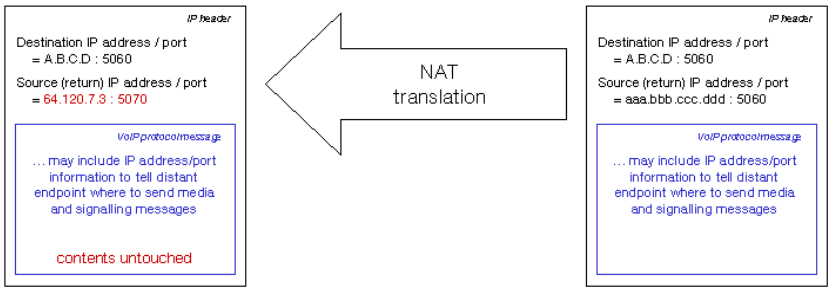


IP address translating PAT router

In order to handle unsolicited data packets arriving on the public side of the PAT router, e.g. for incoming VoIP calls, the NAT/PAT router must be configured with static entries in the table, identifying where to send IP packets if they arrive on specific IP address / port numbers.

Problems of VoIP protocols

Although NAT/PAT routers translate the Return IP address and port and route the packets appropriately, unfortunately both SIP and H.323 protocols send IP addresses and port numbers within the protocol, to for example, tell the far end where to send the media and signalling information. Standard NAT/PAT routers, those that are not VoIP aware, can only modify the VoIP header and so pass these values through without change. When the far end device tries to send, for example, some media packets it will try to send them to the private IP address that will not be known, and will not be route-able within the Public Internet.



Non VoIP-aware NAT/PAT translation

VoIP aware NAT/PAT routers / firewalls solve the NAT problem

There are a number of NAT/PAT routers / firewalls that are VoIP aware. These will not only translate the IP address and port information in the IP headers, but also have enough knowledge of the VoIP protocols to be able to look at the contents of the various messages and apply IP address and port number translation to these where required. Where the Vega is situated behind a VoIP aware NAT/PAT router / firewall, the Vega needs no special configuration to operate correctly.

VPN traversal of NAT solves the NAT problem

VPN tunnels can be created by some firewalls between specific points in a Network. These VPN tunnels, although communicating from private address ranges across the public IP network to destination private IP address ranges hide that traversal from the IP endpoints in the private IP network. Endpoints on different sites can 'see' the far end network as part of its own network. Where the Vega is communicating across a VPN, the Vega needs no special configuration to operate correctly.

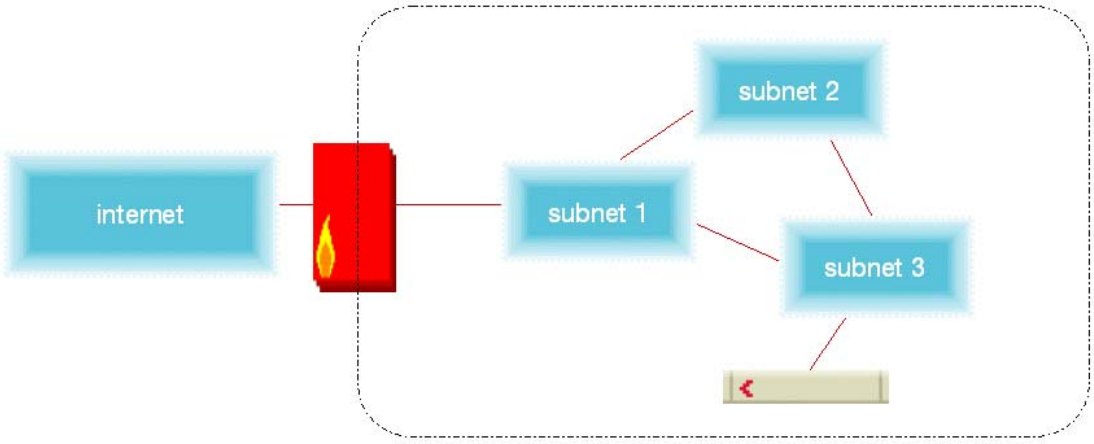
Session Border Controller traversal of NAT solves the NAT problem

A SBC (Session Border Controller) is a device that has a public IP address and is used to proxy VoIP communications. Because it has a public IP address it sees the messaging coming from the outside IP address of the NAT device through which the Vega is communicating. This allows it to intelligently correct private IP addresses presented in the VoIP messaging with the public IP address of the NAT device. Where a SBC is used in conjunction with the Vega, the Vega needs no special configuration to operate correctly.

Configuring the Vega to work with NAT/PAT devices that are not VoIP aware

Local versus public

The first thing that the Vega needs to know is which IP addresses are on the local network (on the private side of the NAT/PAT device, the same side as the Vega itself), and which IP addresses are on the far side of the NAT/PAT device. When communicating with devices on the local Network the Vega will not need to apply any special handling to the IP messages, but when communicating with those on the far side of the NAT/PAT, the Vega will have to apply the IP address and port translation.



Which subnets are on this side of the NAT/PAT device?

IP port ranges and mappings

The second configuration required is to identify which UDP/IP port ranges and which TCP/IP port ranges are to be used by the Vega and what corresponding port ranges will be used when these are translated by the NAT/PAT device.

For instance, if there are two Vegas within the private network, both trying to communicate through the same NAT/PAT device, non intersecting ranges of translated values will be used so that the NAT/PAT device will be able to uniquely identify which Vega to send which data streams to, based on the incoming port number.

Enable NAT/PAT handling

By default the Vega has NAT/PAT handling disabled. If NAT/PAT handling is required it must be enabled.

Configuring a Vega and NAT/PAT device

For example, lets assume a Vega and NAT/PAT configuration as follows:

	protocol	Vega port ranges	NAT/PAT translated ranges
Rtp data, signalling data, web browser data etc. range 1	udp	10,000 to 12,999	20,000 to 22,999
Rtp data, signalling data, web browser data etc. range 2	udp	15,000 to 19,999	25,000 to 29,999
TCP T.38	tcp	10,000 to 19,999	20,000 to 29,999
Web browser	tcp	80	115
SIP signalling (UDP)	udp	5060	5070
SIP signalling (TCP)	tcp	5060	5070
H.323 signalling	tcp	1718 to 1720	1728 to 1730

(No special NAT/PAT translations need to be set up in the Vega for Telnet, tftp, ftp, SNMP, or Radius)

Configuring the NAT/PAT device

In the NAT/PAT device static translations must be set up:

Type	Configuration
Rtp data, signalling data, web browser data etc. range 1	udp: 64.120.7.3 port 20,000 maps to aaa.bbb.ccc.ddd port 10,000 udp: 64.120.7.3 port 20,001 maps to aaa.bbb.ccc.ddd port 10,001 … udp: 64.120.7.3 port 22,999 maps to aaa.bbb.ccc.ddd port 12,999
Rtp data, signalling data, web browser data etc. range 2	udp: 64.120.7.3 port 25,000 maps to aaa.bbb.ccc.ddd port 15,000 udp: 64.120.7.3 port 25,001 maps to aaa.bbb.ccc.ddd port 15,001 … udp 64.120.7.3 port 29,999 maps to aaa.bbb.ccc.ddd port 19,999
TCP T.38	tcp: 64.120.7.3 port 20,000 maps to aaa.bbb.ccc.ddd port 10,000 tcp: 64.120.7.3 port 20,001 maps to aaa.bbb.ccc.ddd port 10,001 … tcp: 64.120.7.3 port 29,999 maps to aaa.bbb.ccc.ddd port 19,999
Web browser	tcp: 64.120.7.3 port 115 maps to aaa.bbb.ccc.ddd port 80
SIP signalling (UDP)	udp: 64.120.7.3 port 5070 maps to aaa.bbb.ccc.ddd port 5060
SIP signalling (TCP)	tcp: 64.120.7.3 port 5070 maps to aaa.bbb.ccc.ddd port 5060
H.323 signalling	tcp: 64.120.7.3 port 1728 maps to aaa.bbb.ccc.ddd port 1718 tcp: 64.120.7.3 port 1729 maps to aaa.bbb.ccc.ddd port 1719 tcp: 64.120.7.3 port 1730 maps to aaa.bbb.ccc.ddd port 1720

Detailed Vega configuration (by Command Line Interface)

Local versus public

To identify which IP addresses are local IP addresses to the Vega, and which IP addresses are only accessible via the NAT/PAT, in the Vega parameters specify the subnets which are local to the Vega. IP addresses not in this list will be treated as only accessible via the NAT/PAT.

```
[lan.private_subnet.1]
 ip=base_ip_address_of_local_subnet_1, e.g. 136.170.209.1
 subnet=subnet_mask_of_local_subnet_1, e.g. 255.255.255.0
 name=textual_name … for self documentation purposes only
[lan.private_subnet.2]
 ip=base_ip_address_of_local_subnet_2
 subnet=subnet_mask_of_local_subnet_2
 name=textual_name … for self documentation purposes only
```

… etc.

For flexibility, it is possible to set up more local subnets than are actually in use; the `private_subnet_list` parameters allow specific or all subnets to be included as currently active subnets.

```
[lan.private_subnet_list.1]
 list=all    … set to "all" or a comma separated list of local subnet definitions
 name=textual_name … for self documentation purposes only
```

Enable this as the subnet list to use, e.g.:

```
[lan.if.x.nat]
 private_subnet_list_index=1 … index into private_subnet_list
```

IP port ranges and mappings

To configure the Vega to use the following values:

	protocol	Vega port ranges	NAT/PAT translated ranges
Rtp data, signalling data, web browser data etc. range 1	udp	10,000 to 12,999	20,000 to 22,999
Rtp data, signalling data, web browser data etc. range 2	udp	15,000 to 19,999	25,000 to 29,999
TCP T.38	tcp	10,000 to 19,999	20,000 to 29,999
Web browser	tcp	80	115
SIP signalling (UDP)	udp	5060	5070
SIP signalling (TCP)	tcp	5060	5070
H.323 signalling	tcp	1718 to 1720	1728 to 1730

Start by configuring the port ranges that the Vega will use:

```
[_advanced.lan.port_range.1]
  min=10000
  max=12999
  protocol=udp
  name=textual_name … for self doc purposes only e.g. rtp_etc_data_1
[_advanced.lan.port_range.2]
  min=15000
  max=19999
  protocol=udp
  name=textual_name … for self doc purposes only e.g. rtp_etc_data_2
 [_advanced.lan.port_range.3]
  min=10000
  max=19999
  protocol=tcp
  name=textual_name … for self doc purposes only e.g. t38_tcp
[_advanced.lan.port_range.4]
  min=80
  max=80
  protocol=tcp
  name=textual_name … for self doc purposes only e.g. web_browser
[_advanced.lan.port_range.5]
  min=5060
  max=5060
  protocol=udp
  name=textual_name … for self doc purposes only e.g. sip_sig_udp
[_advanced.lan.port_range.6]
  min=5060
  max=5060
  protocol=tcp
  name=textual_name … for self doc purposes only e.g. sip_sig_tcp
[_advanced.lan.port_range.7]
  min=1718
  max=1720
  protocol=tcp
  name=textual_name … for self doc purposes only e.g. h323_sig
```

Configure a port range list to group all media (rtp and t.38) port ranges, e.g.:

```
[_advanced.lan.port_range_list.1]
  list=1,2,3
  name=textual_name … for self doc purposes only e.g. rtp_ports
```

Then tell the Vega to use this port range list for media:

```
[_advanced.media]
  rtp_port_range_list=1
```

Now specify the association with the NAT/PAT translated port ranges, e.g.:

```
[lan.nat.port_entry.1]
  internal_port_range_index=1 … pointer into _advanced.lan.port_range.n
  external_port_min=20000
  name=textual_name … for self doc purposes only e.g. rtp_etc_data_1
[lan.nat.port_entry.2]
  internal_port_range_index=2 … pointer into _advanced.lan.port_range.n
  external_port_min=25000
  name=textual_name … for self doc purposes only e.g. rtp_etc_data_2
 [lan.nat.port_entry.3]
  internal_port_range_index=3 … pointer into _advanced.lan.port_range.n
  external_port_min=20000
  name=textual_name … for self doc purposes only e.g. t38_tcp
[lan.nat.port_entry.4]
  internal_port_range_index=4 … pointer into _advanced.lan.port_range.n
  external_port_min=115
  name=textual_name … for self doc purposes only e.g. web_browser
[lan.nat.port_entry.5]
  internal_port_range_index=5 … pointer into _advanced.lan.port_range.n
  external_port_min=5070
  name=textual_name … for self doc purposes only e.g. sip_sig_udp
[lan.nat.port_entry.6]
  internal_port_range_index=6 … pointer into _advanced.lan.port_range.n
  external_port_min=5070
  name=textual_name … for self doc purposes only e.g. sip_sig_tcp
[lan.nat.port_entry.7]
  internal_port_range_index=7 … pointer into _advanced.lan.port_range.n
  external_port_min=1728
  name=textual_name … for self doc purposes only e.g. h323_sig
```

Now group these port_entry definitions into groups that have a single NAT/PAT IP address, e.g.:

```
[lan.nat.port_list.1]
  list=all    … "all" or a comma separated list of lan.nat.port_entry entries
  name=textual_name … for self doc purposes only e.g. all_IP_ports
```

Now associate the NAT/PAT IP address with this set of ports, e.g.:

```
[lan.if.x.nat.profile.1]
  external_ip=64.120.7.3
  port_list_index=1 … index into lan.nat.port_list
```

Enable NAT/PAT handling

The overall NAT/PAT IP address and port number translation is enabled on the Vega with the parameter:

```
[lan.if.x.nat]
  enable=1
```

Activate these changes

To activate these changes type:

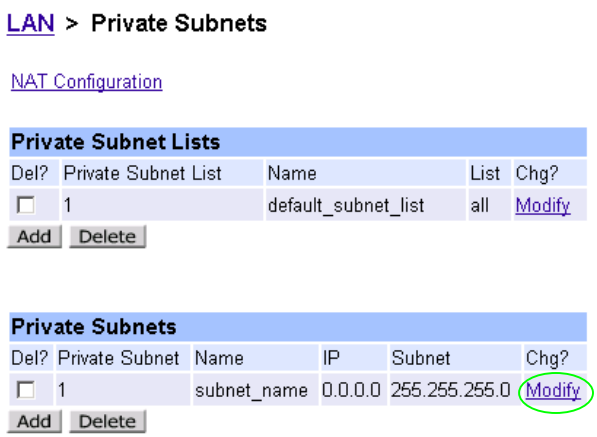
- `save`
- `apply`

Detailed Vega configuration (by Web Browser Interface)

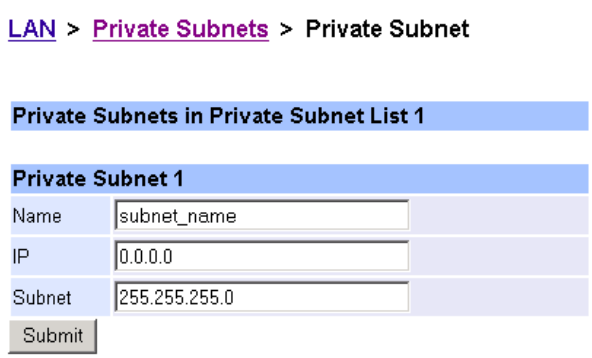
Local versus public

To identify which IP addresses are local IP addresses to the Vega, and which IP addresses are only accessible via the NAT/PAT, in the Vega parameters specify the subnets which are local to the Vega. IP addresses not in this list will be treated as only accessible via the NAT/PAT.

On the LAN>Private Subnets page:



Select Modify in the **Private Subnets** section:



configure:

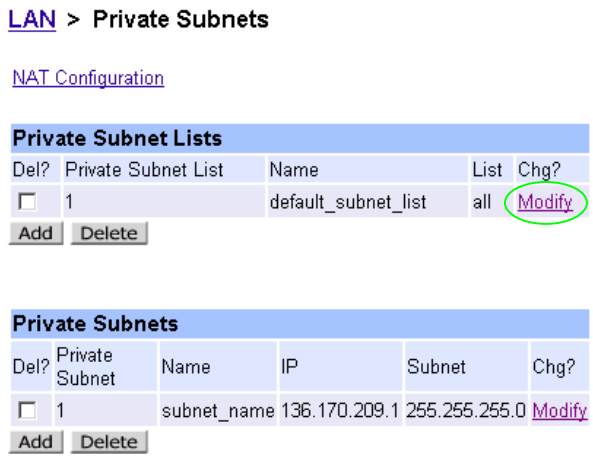
```
name   = textual_name … for self documentation purposes only
ip     = base_ip_address_of_local_subnet_1, e.g. 136.170.209.1
subnet = subnet_mask_of_local_subnet_1, e.g. 255.255.255.0
```

- select Submit and then click "here" to return

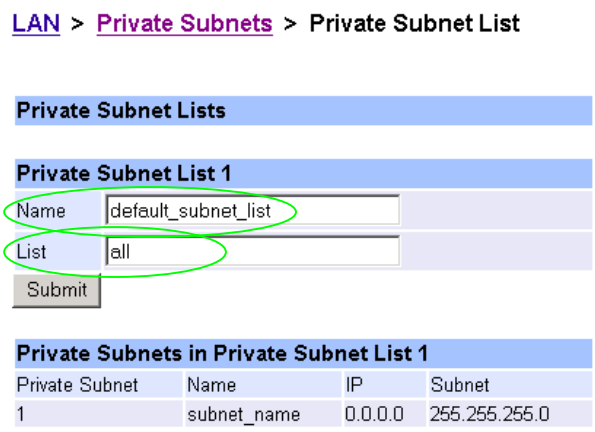
Select Add in the **Private Subnets** section and configure additional entries if there is more than 1 local subnet.

For flexibility, it is possible to set up more local subnets than are actually in use; the **Private Subnet Lists** section allows specific or all subnets to be included as currently active subnets.

From the LAN>Private Subnets page



Select Modify in the **Private Subnet Lists** section:

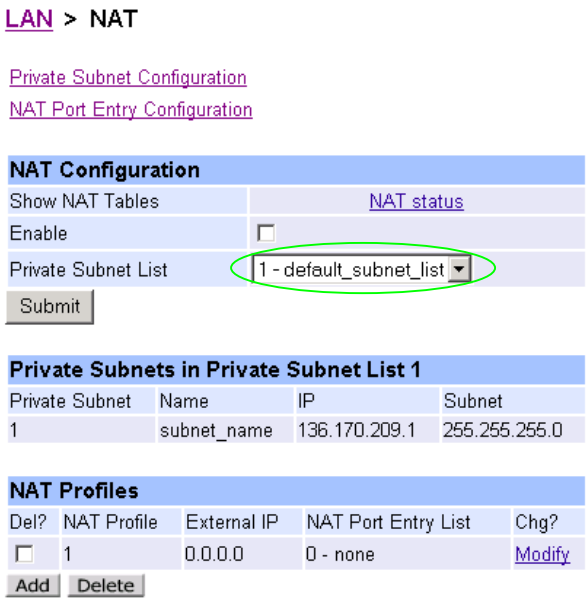


Set

```
list = "all" or a comma separated list of local subnet definitions
name = textual_name … for self documentation purposes only
```

- select Submit and then click "here" to return

Check that this is configured as the subnet list to use. From the LAN>NAT menu:



- select Submit and then click "here" to return

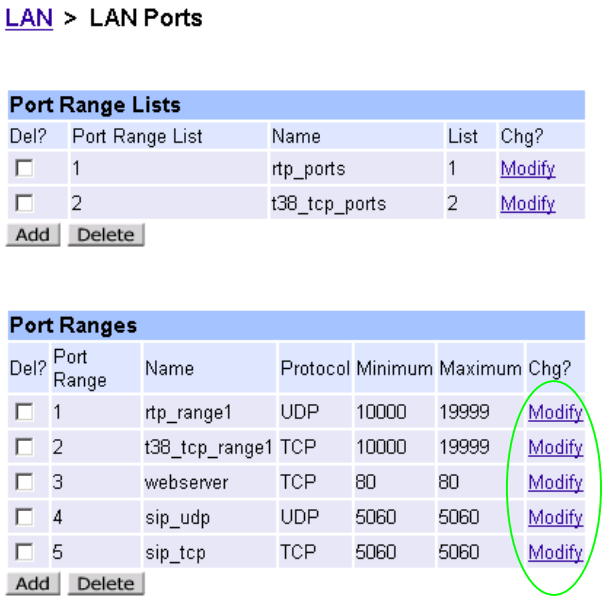
IP port ranges and mappings

IP port ranges are configured on the LAN>LAN Ports page and sub-pages, and NAT mappings are configured on the LAN>NAT page and sub-pages.

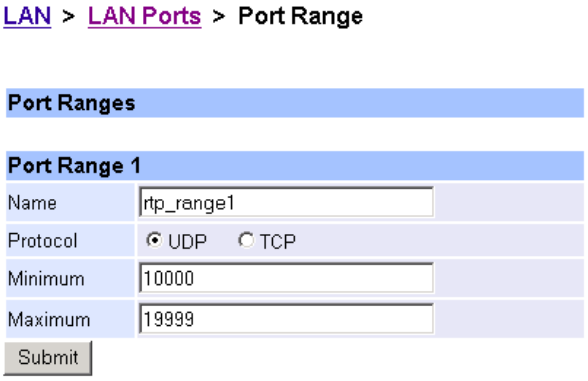
To configure the Vega to use the following values:

	protocol	Vega port ranges	NAT/PAT translated ranges
Rtp data, signalling data, web browser data etc. range 1	udp	10,000 to 12,999	20,000 to 22,999
Rtp data, signalling data, web browser data etc. range 2	udp	15,000 to 19,999	25,000 to 29,999
TCP T.38	tcp	10,000 to 19,999	20,000 to 29,999
Web browser	tcp	80	115
SIP signalling (UDP)	udp	5060	5070
SIP signalling (TCP)	tcp	5060	5070
H.323 signalling	tcp	1718 to 1720	1728 to 1730

Start by configuring the port ranges that the Vega will use. From the LAN>LAN Ports page:



Configure the port ranges by selecting Modify in the **Port Ranges** section:



For Port Range 1, set:

```
name=textual_name … for self doc purposes only e.g. rtp_etc_data_1
protocol=udp
min=10000
max=12999
```

- select Submit and then click "here" to return

To add more entries, select Add at the bottom of the **Port Ranges** section on the LAN > LAN Ports page.

Configure the port ranges until they look as follows:

Port Ranges

Del?	Port Range	Name	Protocol	Minimum	Maximum	Chg?
☐	1	rtp_etc_data_1	UDP	10000	12999	Modify
☐	2	rtp_etc_data_2	UDP	15000	19999	Modify
☐	3	t38_tcp	TCP	10000	19999	Modify
☐	4	web_browser	TCP	80	80	Modify
☐	5	sip_sig_udp	UDP	5060	5060	Modify
☐	6	sip_sig_tcp	TCP	5060	5060	Modify
☐	7	h323_sig	TCP	1718	1720	Modify

Add Delete

Configure a port range list to group all media (rtp and t.38) port ranges:

LAN > LAN Ports > **Port Range List**

Port Ranges in Port Range List 1

Port Range	Name	Protocol	Minimum	Maximum
1	rtp_etc_data_1	UDP	10000	12999

Port Range Lists

Port Range List 1

Name	rtp_ports
List	1

Submit

Set:

```
Name = textual_name … for self doc purposes only e.g. rtp_ports
List = 1,2,3
```

- select Submit and then click "here" to return

This should result in the following configuration:

LAN > LAN Ports

Port Range Lists

Del?	Port Range List	Name	List	Chg?
☐	1	rtp_ports	1,2,3	Modify
☐	2	t38_tcp_ports	2	Modify

Add Delete

Port Ranges

Del?	Port Range	Name	Protocol	Minimum	Maximum	Chg?
☐	1	rtp_etc_data_1	UDP	10000	12999	Modify
☐	2	rtp_etc_data_2	UDP	15000	19999	Modify
☐	3	t38_tcp	TCP	10000	19999	Modify
☐	4	web_browser	TCP	80	80	Modify
☐	5	sip_sig_udp	UDP	5060	5060	Modify
☐	6	sip_sig_tcp	TCP	5060	5060	Modify
☐	7	h323_sig	TCP	1718	1720	Modify

Add Delete

Also set up Port Range List 2 – t38_tcp_ports (in the **Port Range Lists** section) to be the correct entry, i.e. now 3 instead of 2.

Now tell the Vega to use this port range list for media. In the **Advanced Media Parameters** section of the Advanced > Advanced_media page, select entry 1 – rtp_ports:

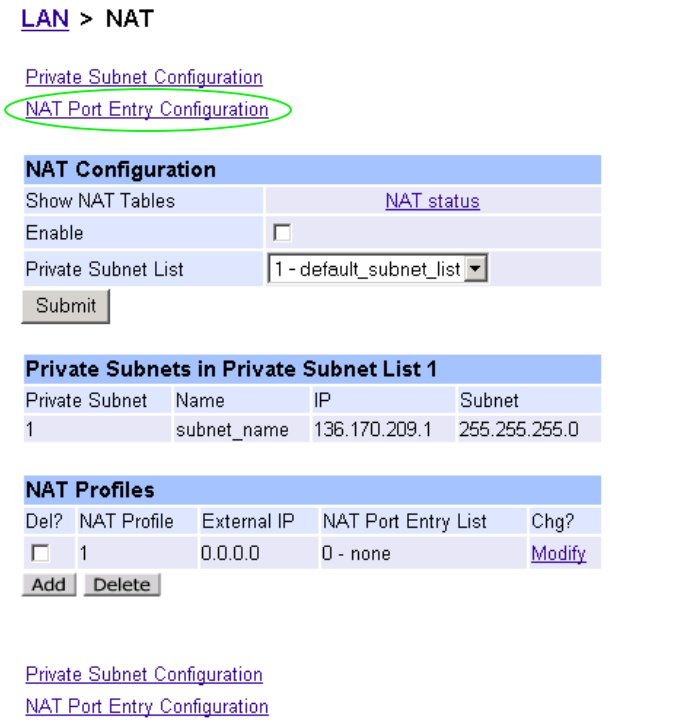
Advanced Media Parameters

Direct TDM Enable	☑
RTP Port Range List	1 - rtp_ports

Submit

1 - rtp_ports
2 - t38_tcp_ports

Now specify the association with the NAT/PAT translated port ranges. From the LAN>NAT page:



LAN > NAT

Private Subnet Configuration
NAT Port Entry Configuration

NAT Configuration

Show NAT Tables	NAT status
Enable	☐
Private Subnet List	1 - default_subnet_list

Submit

Private Subnets in Private Subnet List 1

Private Subnet	Name	IP	Subnet
1	subnet_name	136.170.209.1	255.255.255.0

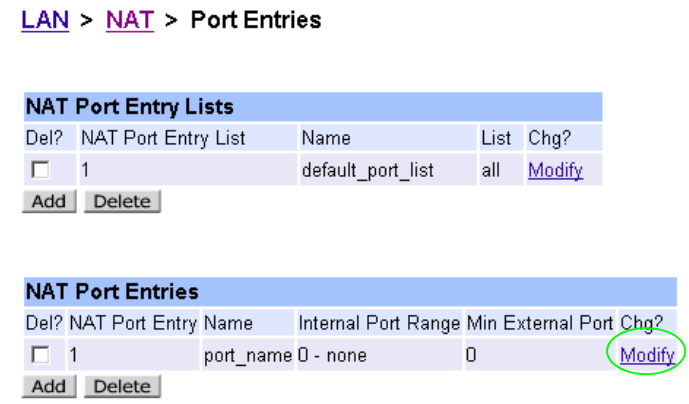
NAT Profiles

Del?	NAT Profile	External IP	NAT Port Entry List	Chg?
☐	1	0.0.0.0	0 - none	Modify

Add Delete

Private Subnet Configuration
NAT Port Entry Configuration

Select NAT_Port_Entry_Configuration:



LAN > NAT > Port Entries

NAT Port Entry Lists

Del?	NAT Port Entry List	Name	List	Chg?
☐	1	default_port_list	all	Modify

Add Delete

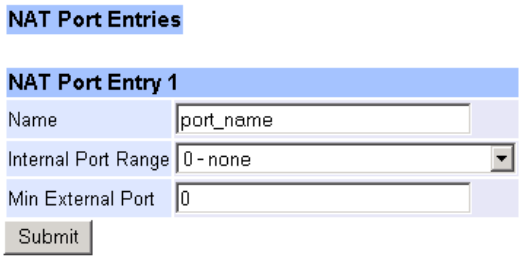
NAT Port Entries

Del?	NAT Port Entry	Name	Internal Port Range	Min External Port	Chg?
☐	1	port_name	0 - none	0	Modify

Add Delete

Select Modify in the **NAT Port Entries** section:

LAN > NAT > Port Entries > Port Entry



For NAT Port Entry 1, set:

```
Name = textual_name … for self doc purposes only e.g. rtp_etc_data_1
Internal Port Range = 1 – rtp_etc_data_range_1 … pointer into the LAN
   Port Range entries
Min External Port = 20000
```

- select Submit and then click "here" to return

To add more entries, select Add at the bottom of the **NAT Port Entries** section on the LAN > NAT > Port Entries page.

Configure the port ranges until they look as follows:

NAT Port Entries

Del?	NAT Port Entry	Name	Internal Port Range	Min External Port	Chg?
☐	1	rtp_etc_data_1	1 - rtp_etc_data_1:udp,10000-12999	20000	Modify
☐	2	rtp_etc_data_2	2 - rtp_etc_data_2:udp,15000-19999	25000	Modify
☐	3	t38_tcp	3 - t38_tcp:tcp,10000-19999	20000	Modify
☐	4	web_browser	4 - web_browser:tcp,80-80	115	Modify
☐	5	sip_sig_udp	5 - sip_sig_udp:udp,5060-5060	5070	Modify
☐	6	sip_sig_tcp	6 - sip_sig_tcp:tcp,5060-5060	5070	Modify
☐	7	h323_sig	7 - h323_sig:tcp,1718-1720	1728	Modify

Add Delete

Now group these NAT Port Entries into groups that have a single NAT/PAT IP address.

On the LAN > NAT > Port Entries > Port Entry List page. (Select Modify in the **NAT Port Entry Lists** section on the LAN>MNAT>Port Entries page)

LAN > NAT > Port Entries > **Port Entry List**

NAT Port Entry Lists

NAT Port Entry List 1

Name	default_port_list
List	all

Submit

NAT Port Entries in NAT Port Entry List 1

NAT Port Entry	Name	Internal Port Range	Min External Port
1	rtp_etc_data_1	1 - rtp_etc_data_1:udp,10000-12999	20000
2	rtp_etc_data_2	2 - rtp_etc_data_2:udp,15000-19999	25000
3	t38_tcp	3 - t38_tcp:tcp,10000-19999	20000
4	web_browser	4 - web_browser:tcp,80-80	115
5	sip_sig_udp	5 - sip_sig_udp:udp,5060-5060	5070
6	sip_sig_tcp	6 - sip_sig_tcp:tcp,5060-5060	5070
7	h323_sig	7 - h323_sig:tcp,1718-1720	1728

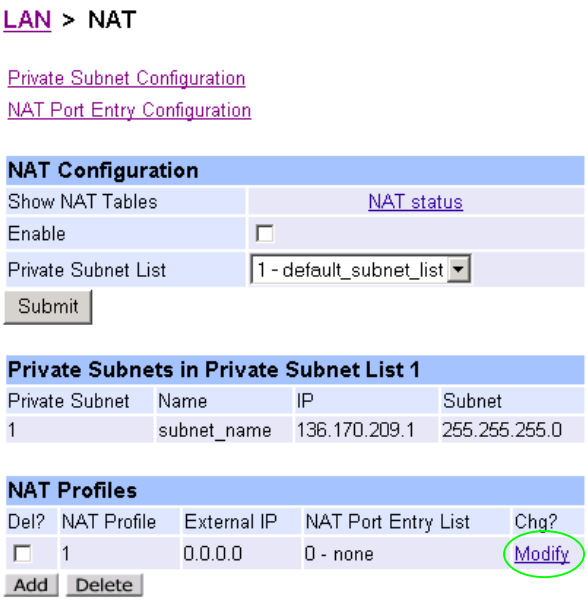
Set

```
List = "all" or a comma separated list of NAT Port Entry IDs
Name = textual_name … for self documentation purposes only e.g.
   all_IP_ports
```

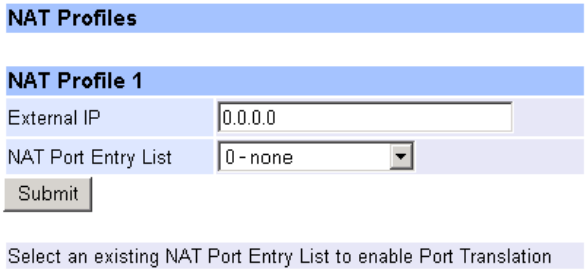
- select Submit and then click "here" to return

Now associate the NAT/PAT IP address with this set of ports:

On the LAN > NAT page:



Select Modify in the **NAT Profiles** section:

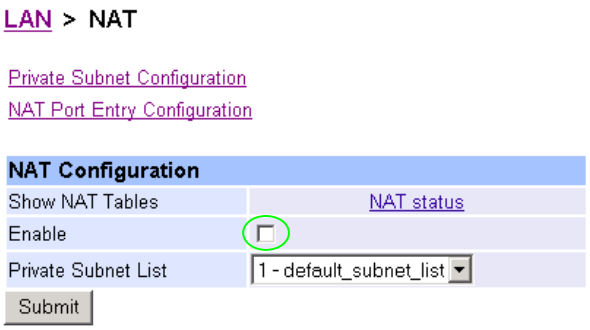


Set:

```
External IP = 64.120.7.3
NAT Port Entry List = 1 - all_IP_ports   … index into NAT Port Entry List
```

Enable NAT/PAT handling

The overall NAT/PAT IP address and port number translation is enabled on the LAN > NAT page by ticking `enable` in the **NAT Configuration** section:



- select Submit and then click "here" to return

Activate these changes

To activate these changes, on the left hand side select:

- Save

then

- Apply Changes

Checking the configuration

To check the configuration of the NAT/PAT related parameters, on the command line interface type:

- `status nat`

or, on the web_browser, on the LAN>NAT page select NAT_status from the **NAT Configuration** section.

`nat status` shows the currently active NAT status, so changes made will only show up in the `nat status` information after an `APPLY` or 

has been executed.

The result will look something like this:

NAT Status

```
LAN NAT enable=1

NAT PROFILE LIST (1 profiles)

  profile 1
    external ip=      64.120.7.3 (40780703)
    PORT ENTRY LIST (7 entries)
      PORT ENTRY 1
        protocol UDP
        internal port range  rtp_etc_data_1
        min internal port       10000
        max internal port       12999
        min external port       20000
        max external port       22999
        external port offset    10000
      PORT ENTRY 2
        protocol UDP
        internal port range  rtp_etc_data_2
        min internal port       15000
        max internal port       19999
        min external port       25000
        max external port       29999
        external port offset    10000
      PORT ENTRY 3
        protocol TCP
        internal port range  t38_tcp
        min internal port       10000
        max internal port       19999
        min external port       20000
        max external port       29999
        external port offset    10000
      PORT ENTRY 4
        protocol TCP
        internal port range  web_browser
```

```
        min internal port          80
        max internal port          80
        min external port         115
        max external port         115
        external port offset       35
      PORT ENTRY 5
        protocol UDP
        internal port range  sip_sig_udp
        min internal port        5060
        max internal port        5060
        min external port        5070
        max external port        5070
        external port offset       10
      PORT ENTRY 6
        protocol TCP
        internal port range  sip_sig_tcp
        min internal port        5060
        max internal port        5060
        min external port        5070
        max external port        5070
        external port offset       10
      PORT ENTRY 7
        protocol UDP
        internal port range  h323_sig
        min internal port        1718
        max internal port        1720
        min external port        1728
        max external port        1730
        external port offset       10

PRIVATE SUBNET LIST (1 subnets)
  subnet 1
    subnet base addr =   136.170.209.0 (88aad100)
    subnet mask      =   255.255.255.0 (ffffff00)
```

Annex 1 – Example Static routing for a Cisco Router

To configure a Cisco router to work with the configuration used in this document, i.e. to set up the following mapping:

Type	Configuration
Rtp data, signalling data, web browser data etc. range 1	udp: 64.120.7.3 port 20,000 maps to aaa.bbb.ccc.ddd port 10,000 udp: 64.120.7.3 port 20,001 maps to aaa.bbb.ccc.ddd port 10,001 … udp: 64.120.7.3 port 22,999 maps to aaa.bbb.ccc.ddd port 12,999
Rtp data, signalling data, web browser data etc. range 2	udp: 64.120.7.3 port 25,000 maps to aaa.bbb.ccc.ddd port 15,000 udp: 64.120.7.3 port 25,001 maps to aaa.bbb.ccc.ddd port 15,001 … udp 64.120.7.3 port 29,999 maps to aaa.bbb.ccc.ddd port 19,999
TCP T.38	tcp: 64.120.7.3 port 20,000 maps to aaa.bbb.ccc.ddd port 10,000 tcp: 64.120.7.3 port 20,001 maps to aaa.bbb.ccc.ddd port 10,001 … tcp: 64.120.7.3 port 29,999 maps to aaa.bbb.ccc.ddd port 19,999
Web browser	tcp: 64.120.7.3 port 115 maps to aaa.bbb.ccc.ddd port 80
SIP signalling (UDP)	udp: 64.120.7.3 port 5070 maps to aaa.bbb.ccc.ddd port 5060
SIP signalling (TCP)	tcp: 64.120.7.3 port 5070 maps to aaa.bbb.ccc.ddd port 5060
H.323 signalling	tcp: 64.120.7.3 port 1728 maps to aaa.bbb.ccc.ddd port 1718 tcp: 64.120.7.3 port 1729 maps to aaa.bbb.ccc.ddd port 1719 tcp: 64.120.7.3 port 1730 maps to aaa.bbb.ccc.ddd port 1720

a Cisco Router can be configured as follows:

Type	Cisco command format:
	ip nat inside source list 50 interface FastEthernet0/1 overload
Rtp data, signalling data, web browser data etc. range 1	ip nat inside source static udp aaa.bbb.ccc.ddd 10000 interface FastEthernet0/1 20000 ip nat inside source static udp aaa.bbb.ccc.ddd 10001 interface FastEthernet0/1 20001 … ip nat inside source static udp aaa.bbb.ccc.ddd 12999 interface FastEthernet0/1 22999
Rtp data, signalling data, web browser data etc. range 2	ip nat inside source static udp aaa.bbb.ccc.ddd 15000 interface FastEthernet0/1 25000 ip nat inside source static udp aaa.bbb.ccc.ddd 15001 interface FastEthernet0/1 25001 … ip nat inside source static udp aaa.bbb.ccc.ddd 19999 interface FastEthernet0/1 29999
TCP T.38	ip nat inside source static tcp aaa.bbb.ccc.ddd 10000 interface FastEthernet0/1 20000 ip nat inside source static tcp aaa.bbb.ccc.ddd 10001 interface FastEthernet0/1 20001 … ip nat inside source static tcp aaa.bbb.ccc.ddd 19999 interface FastEthernet0/1 29999
Web browser	ip nat inside source static tcp aaa.bbb.ccc.ddd 80 interface FastEthernet0/1 115
SIP signalling (UDP)	ip nat inside source static udp aaa.bbb.ccc.ddd 5060 interface FastEthernet0/1 5070
SIP signalling (TCP)	ip nat inside source static tcp aaa.bbb.ccc.ddd 5060 interface FastEthernet0/1 5070
H.323 signalling	ip nat inside source static tcp aaa.bbb.ccc.ddd 1718 interface FastEthernet0/1 1728 ip nat inside source static tcp aaa.bbb.ccc.ddd 1719 interface FastEthernet0/1 1729 ip nat inside source static tcp aaa.bbb.ccc.ddd 1720 interface FastEthernet0/1 1730
Also may want to configure Telnet	ip nat inside source static tcp aaa.bbb.ccc.ddd 23 interface FastEthernet0/1 xxxx where xxxx = port number to be used for telnet traffic to the Vega

Annex 2 – Configuring NAT traversal in a Vega placed in a NAT DMZ

If you have a Vega and you wish to place it in the DMZ of a NAT and all required IP ports are directly mapped from the public side to the DMZ and from the DMZ to the public side, configure the Vega as follows:

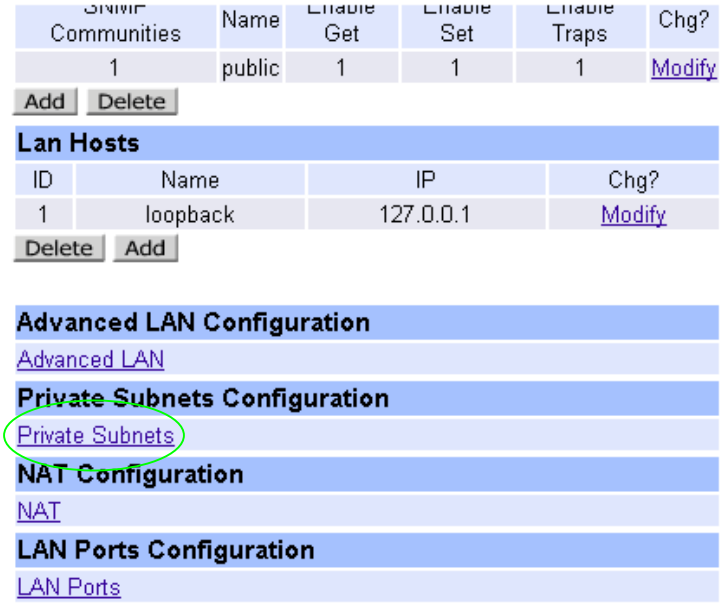
- Ensure that you have the following information:
  - IP address(es) and subnet mask(s) of LAN subnet(s) inside the NAT
  - Public IP address of the NAT device which routes data to the Vega

- Log in to the Vega
- Configure it using the appropriate 'initial configuration guide' from the 'step by step configuration' section of www.VegaAssist.com or the CD-rom supplied with the Vega.

To set up the DMZ NAT traversal:

Start by telling the Vega which subnets are local (and so don't need special NAT traversal handling) and which are outside addresses (and do need special NAT traversal handling).

- Select LAN on the left hand side of the web browser
- Scroll to the bottom of the page



- Select Private Subnets

LAN > Private Subnets

NAT Configuration

Private Subnet Lists

Del?	Private Subnet List	Name	List	Chg?
☐	1	default_subnet_list	all	Modify

Add Delete

Private Subnets

Del?	Private Subnet	Name	IP	Subnet	Chg?
☐	1	subnet_name	0.0.0.0	255.255.255.0	Modify

Add Delete

For each local private subnet, in the **Private Subnets** section,

- Select Add if a new entry is required
- Select Modify to alter an entry

LAN > Private Subnets > Private Subnets

Private Subnets in Private Subnet List 1

Private Subnet 1

Name	subnet_name
IP	0.0.0.0
Subnet	255.255.255.0

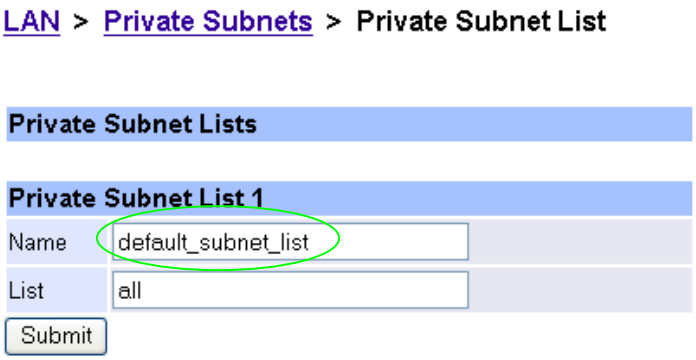
Submit

- Set Name=<name_for_self_documentation>[1] e.g. Local_subnet_192_168_1_0
- Set IP=<IP address of local subnet> e.g. 192.168.1.0
- Set Subnet=<subnet mask of local subnet> e.g. 255.255.255.0
- Select Submit and then click "here" to return

In the **Private Subnets Lists** section

- Select Modify to alter Private Subnet List 1

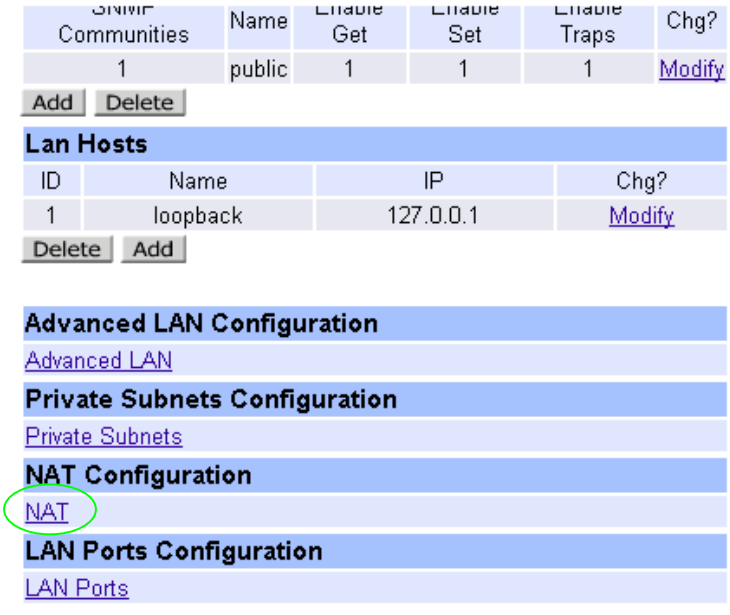
[1] N.B. Vega names must not have spaces; use – (minus) or _ (underscore) in place of spaces.



- Set Name=<name_for_self_documentation>[2] e.g. My_Company_Internal_LAN
- Select Submit and then click "here" to return

Now enable NAT traversal and set up the public IP address that the Vega should use when communicating with devices outside the local subnet(s).

Return to the bottom of the LAN page

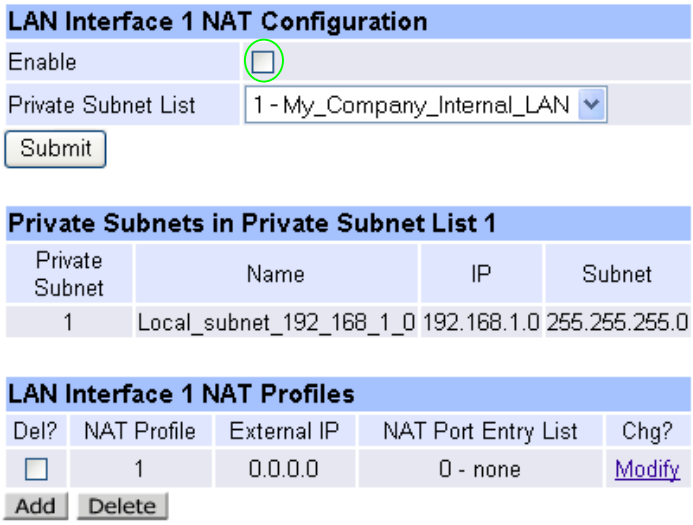


[2] N.B. Vega names must not have spaces; use – (minus) or _ (underscore) in place of spaces.

- Select NAT

For NAT traversal for interface 1 configure the 'LAN Interface 1' sections, For NAT traversal for intrerface 2 configure the 'LAN Interface 2' sections.

e.g. For LAN interface 1:



In the **LAN Interface 1 NAT Configuration** section

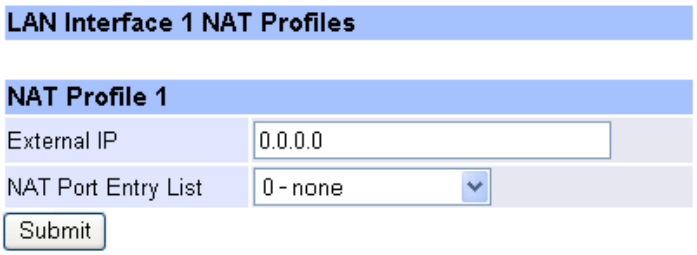
- Tick Enable

Note that the Private Subnet List shows the updated name.

- Select Submit and then click "here" to return

In the **LAN Interface 1 NAT Profiles** section

- Select Modify to alter Private Subnet List 1



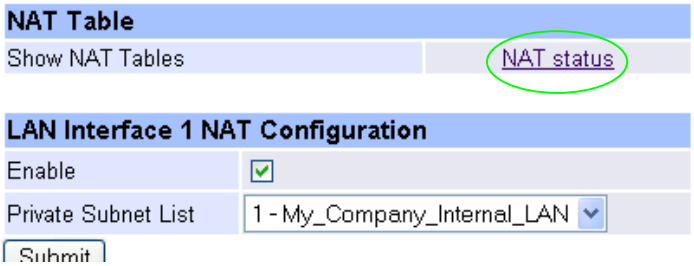
In the **NAT Profile 1** section

- Set External IP=<Public IP address of NAT device that routes data to the Vega>

If there are IP Port mappings as well as the IP address mappings, see the main body of this document to see how to configure those.

- Save and reboot the Vega to activate.

To check the settings, select LAN > NAT and in the **NAT Table** section



- Select NAT status

The output will look similar to:

```
NAT Status

------------------------------------------------------------------------------
LAN Interface 1 NAT Configuration
------------------------------------------------------------------------------
LAN NAT enable=1

NAT PROFILE LIST (1 profiles)

  profile 1
    external ip=  217.205.209.54 (d9cdd136)
    PORT ENTRY LIST (0 entries)

PRIVATE SUBNET LIST (1 subnets)
  subnet 1
    subnet base addr =     192.168.1.0 (c0a80100)
    subnet mask      =   255.255.255.0 (ffffff00)

------------------------------------------------------------------------------
LAN Interface 2 NAT Configuration
------------------------------------------------------------------------------
LAN NAT enable=0

NAT PROFILE LIST (1 profiles)

  profile 1
    external ip=         0.0.0.0 (00000000)
    PORT ENTRY LIST (0 entries)

PRIVATE SUBNET LIST (1 subnets)
  subnet 1
    subnet base addr =     192.168.1.0 (c0a80100)
    subnet mask      =   255.255.255.0 (ffffff00)
```

Contact Details
Email: support@vegastream.com
Web: www.vegastream.com
www.vegaassist.com

EMEA Office
VegaStream Limited
The Western Centre
Western Road
Bracknell
Berks RG12 1RW
UK

+44 (0) 1344 784900

USA Office
VegaStream Inc.
6200 Stoneridge Mall Road
3rd Floor
Pleasanton
California 94588
USA

+1 925 399 6428