

GNAT

A Gateway Network Address Translator



GNAT is a high performance network address translator (NAT) designed for use in an embedded environment. Its core engine maps internal IP addresses to external ones using port translation (NAPT) based on pre-defined mapping rules. With support for bidirectional NAT, static and dynamic rule mappings, and reference Application Level Gateways ALGs such as FTP, GNAT can be used as a tiny, yet flexible functional component in embedded networking devices seeking to isolate a private network from a public one and increase the private IP address space available while using a single or few public IP addresses. It also finds use in separating traffic between an in-system network (e.g. one based on an ethernet backplane) from an external one. **GNAT's** small footprint, low latency and robustness make it the NAT of choice in embedded networking applications.

GNAT's network address translation engine allows IP datagrams to be transparently mapped from one address realm to another. This translation is useful in situations where an internal network's IP addresses are to be kept private or are invalid for use in an external network, as is common in enterprise or home gateway

applications. Further, in an embedded devices that have multiple line cards or blades with unique IP addresses, **GNAT** allows for the system to be treated as a single network node with a single recognizable external IP address having its various service ports redirected to the service provided by its internal units.

GNAT modifies IP packet addresses and rewrites the address headers for packets that are passed through it, according to network specific address translation rules. The packets are then routed according to the newly written header information.

GNAT can be configured for outbound mappings that are created manually or on-the-fly using a dynamic firewall such as FireFly, which provides some measure of added security, by allowing only connections that originate in the internal network. This means that the hosts in the internal network can connect to an outside address, but connections from the outside will not be possible.

GNAT also allows inbound mappings that may be configured when situations demand it, such as when internal servers are to be made available to the outside world. This allows certain TCP or UDP ports to be mapped to specific internal IP addresses making services such as HTTP or HTTPS running on an internal network node externally available.

GNAT supports both static mappings which translate IP addresses on an one-on-one basis and require an equal number of internal and external IP addresses, as well as dynamic mappings through port translation allowing for a single or fewer external IP addresses to be used for IP

Features

- ❖ Many-to-one address translation.
- ❖ Conserves IP addresses.
- ❖ Supports bi-directional translation.
- ❖ Includes static and dynamic NAT with port translation (NAPT).
- ❖ Includes reference ALG implementation for FTP.
- ❖ Supports ICMP ID mapping.
- ❖ Integrates with firewalls for dynamic firewalling.
- ❖ Extremely small footprint.
- ❖ Low network latency.
- ❖ Easily controlled by web server through string based CLI.
- ❖ Supports rule numbering.
- ❖ Validated on big & little endian architectures including PowerPC, MIPS, ARM, XScale, and X86.
- ❖ Royalty-free full-source distribution.

address conservation on a large internal network.

GNAT has been extensively validated on a variety of CPU architectures, and this minimizes development and integration efforts. **GNAT** transparently works with the native OS network stack or with **TeamF1's NetF1** high-performance stack as well as other third-party stacks. **GNAT's** small footprint and robustness have been specifically designed for use in an embedded environment. **GNAT's** unprecedented flexibility and easy customization make it the NAT of choice in embedded networking applications.

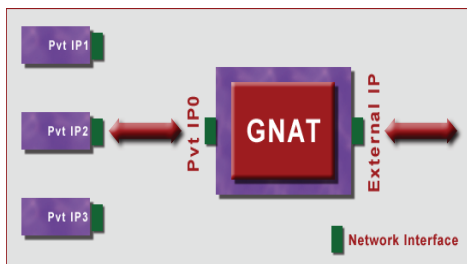


Fig 1: Network Address Translation

Special Features

- ❖ Supports static and dynamic NAT
- ❖ Supports inbound and outbound mappings (bidirectional NAT)
- ❖ Dynamic firewall interface to optionally open NAT mappings for internally initiated connections
- ❖ Supports port redirection on incoming side (servers on internal nodes) and outgoing side (e.g. DNS proxy)
- ❖ Ultra-small memory footprint and minimal dynamic memory usage
- ❖ Very low network latency

GNAT Operation

GNAT typically operates on a gateway or router between an internal and external network and helps to conserve IP addresses. It does this by creating "local" networks, which are connected to the Internet using a single routable (public) IP address. **GNAT** maintains an address translation table containing active mappings of internal/external IP addresses and port numbers. These mappings are

created dynamically based on rule-matching when a packet makes its way through **GNAT**. Based on the mappings, each IP datagram sent out with an internal IP source address has the source address field replaced by the appropriate external IP address and is re-injected into the packet stream. This process is reversed when a packet is received, since the mappings allow **GNAT** to determine the original requestor to which the packet should be forwarded. This makes possible a many-to-one address mapping, since many internal IP addresses can be mapped to one external IP address. Mappings are automatically deleted after a pre-configured inactivity time period.

Inbound & Outbound Mappings

GNAT includes a redirection command to redirect inbound packets to a specified internal IP address. This allows external devices to initiate connections to internal NAT-ed nodes which may be necessary if the internal nodes are running servers (such as ftp, http, etc.), which require access from the outside. Besides inbound mapping, **GNAT** also supports redirection in the outgoing direction to allow services such as DNS port forwarding from the internal network.

Local Network Security

A useful feature of **GNAT** is its ability to hide private IP addresses on its internal side. The nodes on the internal network may freely establish connections with external nodes. However, connections from the external side may be blocked or made possible with **GNAT** in a controlled manner. **GNAT** can allow just a few connections, or even no connections, to be established in this direction. **GNAT** thus offers security by assigning nodes on the internal network non-routable private IP addresses that

cannot be easily accessed from potential threats on the outside.

Dynamic Firewall Interface

GNAT private IP address hiding complements the perimeter security of IP packet filtering firewalls. A unique feature of **GNAT** allows the association of a NAT mapping with a firewall rule. When the NAT entry is created, it also opens a firewall window. This allows for a convenient way to enable a dynamic firewall rule, allowing activity at specific ports when a connection is initiated from the internal side. The firewall window is closed when the NAT entry expires.

Application Level Gateways

Some TCP/IP protocols embed addressing information in the payload of packets. For example, during an "active" FTP connection, the client informs the server of its IP address & port number and then waits for the server to open a connection to that address. **GNAT** has to monitor these packets and modify them on the fly to replace the client's IP address (which is on the internal network) with the NAT-ed address. This requires defining specialized application level gateway modules (ALGs) for every protocol that uses IP addresses in packet payloads. **GNAT** supplies an implementation of the FTP ALG which can be used as a reference for any other protocols that require a specialized ALG.

Portable Private Networks

GNAT's setup of a "local" network on its internal side, with its own private IP address scheme, allows for maximum address portability since this network can be connected to any external network without any IP address change for the internal nodes. This is particularly useful in

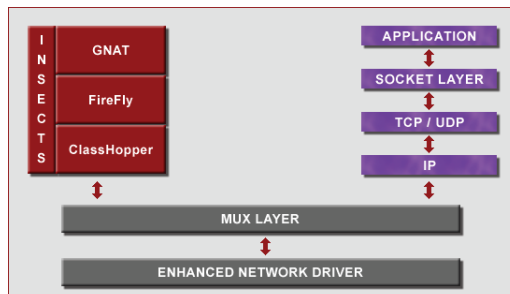


Fig 2: INSECTS "BUMP-ON-THE-STACK" MODEL

Also Available

- ❖ **SSHield**
Secure Shell
- ❖ **SSLimSecure**
Secure Sockets and TLS
- ❖ **ClassHopper**
Alternate Queuing Disciplines

Custom Solutions

GNAT is customizable for your unique application with the help of **TeamF1**'s expert professional services team. Contact us for customized implementations of **GNAT** with support for hardware acceleration using network processors and ASICs.

Customization Flexibility

- ❖ Support for port number ranges.
- ❖ Configurable timeout and NAT table size.
- ❖ Extensible architecture to support Application Level Gateways (ALGs).
- ❖ Support for selectively disabling the incoming or outgoing direction on each interface.
- ❖ Available in full-source format.
- ❖ Customization hooks and callouts.

embedded environments where the "local" network may be part of a single embedded system. **GNAT** allows such applications to refer to the internal addresses without reference to the external IP address in use, which may change based on DHCP assignment, or inclusion of the embedded devices in a customer network.

Management Framework

GNAT supports a customizable management interface presented through a string-based command layer, which can be easily controlled through a web-server or structured data files such as XML or via a CLI. Support for rule numbering provides ease of overriding at any level. Management of nodes on the internal network is also eased, since they can be assigned private IP addresses that do not change even if the external IP address changes based on connection to different external networks.

Email: sales@TeamF1.com
 Web: www.TeamF1.com
 Ph: 510-505-9931 ext. 5
 Fax: (510) 505-9941



© 2011 TeamF1, Inc.