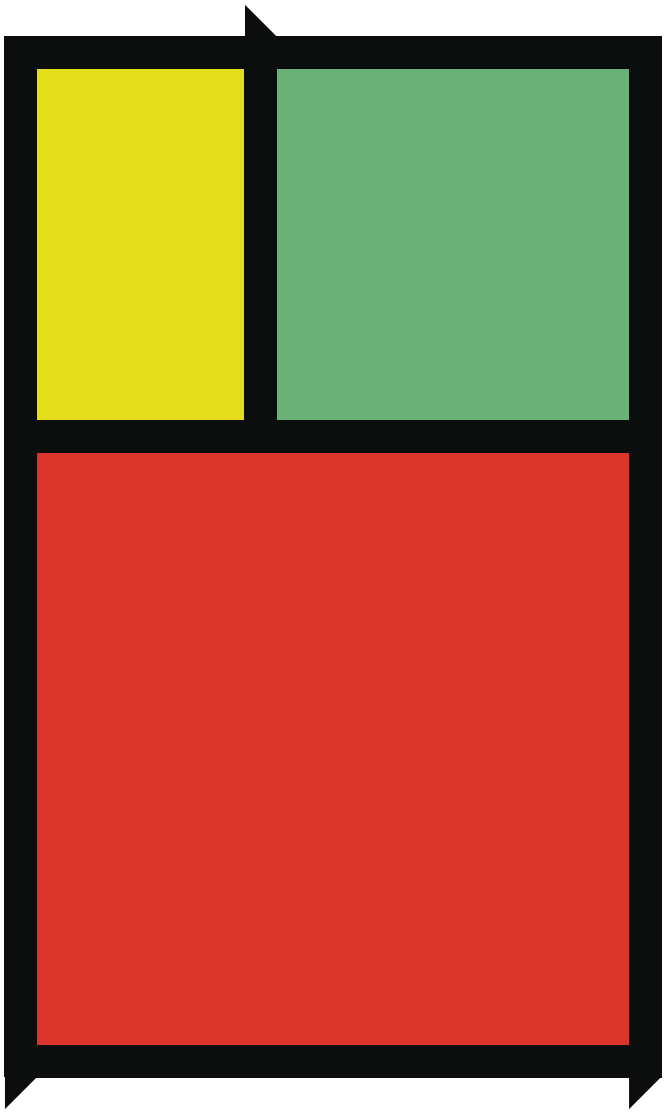


NAT

Network Address Translation

interpeak

Network Address Translation

As millions of devices have been connected to the Internet, lack of Internet addresses has become an increasingly demanding challenge. Using Interpeak NAT significantly reduces this problem, and also improves security by hiding Intranet topology to the public Internet.

The number of devices connected to the Internet has grown rapidly over the past few years. Network managers today have to face problems the original designers probably never considered when they first developed the TCP/IP protocol.

One of the emerging problems is the lack of unique IP addresses. The Internet protocol in its current version theoretically limits the number of connected hosts to 4 billion, but the practical limit is much less. In fact, shortage in the Internet address space was one of the reasons to why a complete redesign of the protocol was started, known as IPv6.

Network Address Translation

A different approach to the problem is called Network Address Translation (NAT). NAT does not only reduce the requirement for globally unique IP addresses, but also introduces other advantages such as network management simplification and network security enhancements.

The NAT software reuses publicly assigned IP addresses for datagrams going from an internal network to the Internet or to a public WAN, thereby reducing the requirement for globally unique IP addresses.

Unique Intranet Addresses

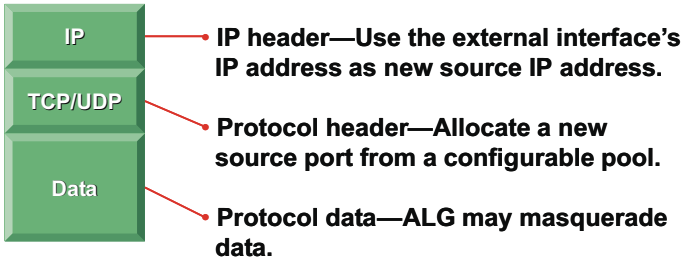
Managing a home or small business network may be a difficult and time consuming task. Using NAT makes that task much simpler since all hosts on the private Intranet can be assigned individual IP addresses, unique only on the Intranet itself. Interpeak NAT supports both statically and dynamically assigned IP addresses on the Intranet.

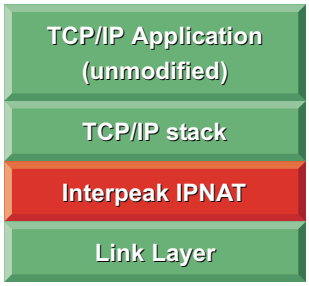
Visible Intranet Addresses

Another shortcoming with globally unique addresses is the fact that these addresses become visible to everyone on the Internet when the host on the private Intranet connects to a server on the Internet. That host's own IP address gets exposed to all routers and hosts the datagram passes on its way to the Internet server. This behaviour introduces a potential security risk to the private Intranet.

No Restrictions on Intranet Addresses

When the private Intranet is managed, the hosts are typically assigned class A (10.X.X.X) or class C (192.168.X.X) network addresses. However NAT does not restrict the use to predefined address ranges. Any Internet address may be translated by NAT which increases flexibility and enables NAT to be used in other gateway applications.





Interpeak NAT inserted in a TCP/IP stack to perform address translation.

Hide Intranet Topology

When the NAT software is installed in a gateway or router, all datagrams being forwarded through the router gets a new source Internet address. Hence, it seems as if the datagram was sent from the gateway or router itself. This functionality hides the network topology of the private Intranet. The number of hosts and their IP addresses are not revealed to the outside world.

Two-Way NAT

Interpeak NAT can also be configured to pass incoming requests to hosts on the private network. This enables servers to reside on the private network and still be accessible from hosts on the Internet. Any port can be opened for incoming requests which means that you can set up for example WEB, FTP, or TELNET servers on any host on your private network.

This functionality called two-way NAT runs in parallel with the regular NAT operation.

Interpeak NAT Features

The Interpeak NAT product is ideally located in the protocol stack between the link layer and the TCP/IP stack. It will therefore not introduce any requirements on existing TCP/IP applications. The customer can run standard and custom TCP/IP applications unmodified and need not spend time redesigning host application software.

Configurable

Applications that requires special handling are dealt with using ALGs (Application Level Gateways). Such applications are those that include source IP address or source port in the payload data, for example FTP. The Interpeak NAT design very much simplifies integration of new ALGs to support customer specific applications.

Interpeak NAT supports multi-interface products. Each interface can be configured to act as an inner or an outer interface. Address translation is performed on datagrams going from an inner to an outer interface. When there are multiple outer interfaces, NAT uses the IP address of the interface the datagram is sent on when it performs address translation. Therefore, the NAT software need not know the routing tables of its host which reduces processing time.

- Servers can be added to your private network by configuring the NAT gateway to handle incoming requests to server ports and forward them to the right server.
- The customer can configure which ports to use for port translation.
- The customer can configure how many hosts that are supported on the private Intranet.

Fast

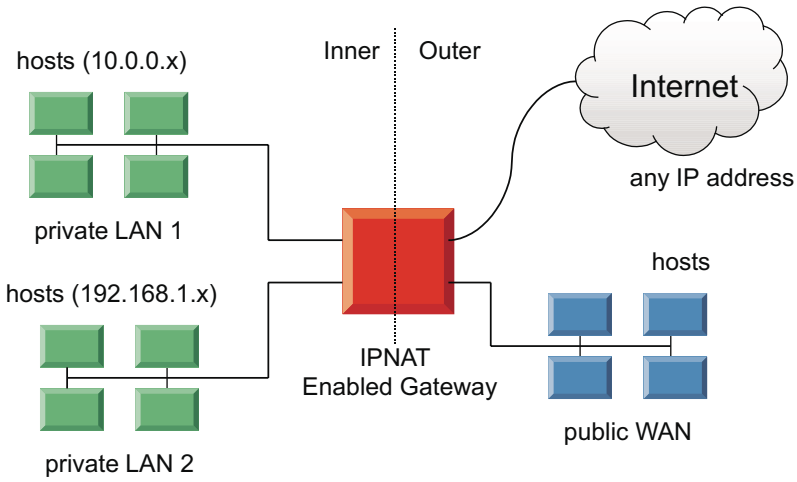
Since the NAT software operates on link layer frames and does not intervene with the TCP/IP stack software, the burden on the host processor is minimal and performance is increased.

- **The IP Network Address Translator (NAT) [RFC-1631]**
- **IP Network Address Translator (NAT) Terminology and Considerations [RFC-2663]**
- **Supports Traditional (Outbound) NAT**
- **Supports Network Address Port Translation (NAPT)**
- **Supports Two-Way NAT**
- **Supports multiple internal and external interfaces**
- **High performance**
- **Delivered in ANSI compliant "C" source code.**
- **Complete ready-to-run RTOS integration with examples, makefiles etc.**

Interpeak NAT features.

Defacto Standard

NAT is either included directly in many operating systems or available as applications. NAT is available for Solaris, Linux, Windows and BSD. Many companies such as Sun, Microsoft, Cisco and other telecom and datacom equipment vendors make use of NAT. NAT is also very likely included in products from router and firewall makers.



The picture above describes a typical network configuration and use for the NAT gateway. There are four interfaces on the gateway, two inner and two outer. The inner interfaces connects to two private Intranets which use the 10.0.0.X and 192.168.1.X series of IP addresses respectively. The outer interfaces connects to the Internet and a public Wide Area Network of some kind. The dotted line draws the border between the inner and outer world.

Address translation is performed on datagrams going from one of the inner interfaces to one of the outer interfaces. The hosts on the inner side of the gateway needs to be configured with a default route pointing to the NAT enabled gateway.

Interpeak Secure Networking Software

Interpeak provides state-of-the-art networking solutions specifically designed for embedded systems. The company´s embedded networking and security software is currently used in thousands of applications across the globe.

Headquartered in Stockholm, Sweden, Interpeak operates through a global network of distribution channels and has its own sales and field application force dispersed in strategic locations worldwide, including the USA, Europe, and Asia. For additional information, please visit our homepage *www.interpeak.com*.