

Cisco IOS Network Address Translation

This data sheet provides an overview of the Network Address Translation features available in select Cisco IOS® Software images.

Overview

Network Address Translation (NAT) simplifies and conserves IP addresses. It enables private IP networks to connect to the Internet using unregistered IP addresses (in the private address space specified in RFC 1918). NAT operates on a router, usually connecting two networks together, and is used to translate the private addresses in the internal network into legal routable addresses, before packets are forwarded to another network, because ISPs will not route RFC 1918 addresses. NAT can be configured to advertise only one address for the entire network to the outside world. This provides additional security by effectively hiding the entire internal network behind that one address. This capability is called Port Address Translation (PAT) and is also referred to as “overloading” (Figure 1). NAT offers the dual functions of security and address conservation, and is typically implemented in remote-access environments at the edge of the network where an enterprise connects to its ISP.

Key Benefits

The NAT function available in Cisco IOS Software offers the following benefits:

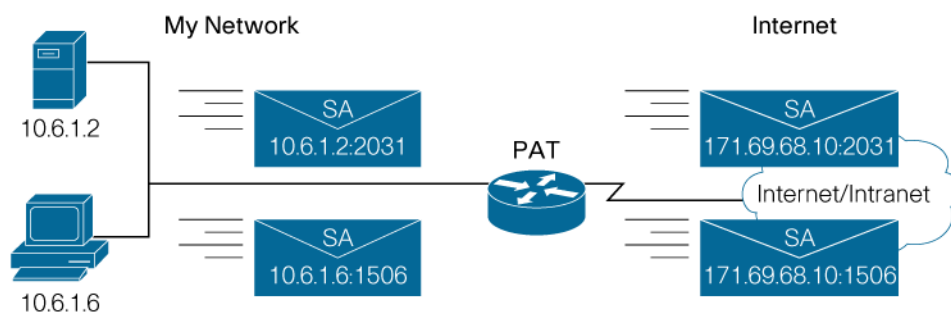
- IP address preservation
- Easy management
- IP address and application privacy

Cisco IOS NAT Features

- **Static address translation:** You can establish one-to-one mapping between local and global addresses. You can also configure static address translations to the port level, and use the remainder of the routable IP address for other translations; this is typically performed in conjunction with PAT.
- **Dynamic address translation:** You can establish dynamic mapping between the local and global addresses. This is done by defining the local addresses to be translated and defining the pool of addresses from which to allocate global addresses, and associating the two.
- **Match host:** This capability allows you to configure NAT to assign the same host portion of an IP address and only translate the network prefix portion of the IP address. This is useful where you are using the host portion as a means to identify or number users uniquely.

Port Address Translation

Figure 1. Basic Concepts of PAT



Port Address Translation (PAT) extends NAT from “one-to-one” to “many-to-one” by associating the source port with each flow

| Pro | Inside Global | Inside Local | Outside Local | Outside Global |
|-----|------------------|----------------|------------------|------------------|
| tcp | 171.69.68.5:1405 | 10.6.15.2:1405 | 204.71.200.69:80 | 204.71.200.69:80 |

PAT (Port Address Translation) includes ports in addition to IP addresses:

- Many-to-one translation
- Maps multiple IP addresses to 1 or a few IP addresses
- Unique source port number identifies each session
- Conserves registered IP addresses
- Also called NAPT in IETF documents

The PAT feature, a subset of NAT functionality, can be used to translate several internal addresses into only one or a few external addresses. PAT uses unique source port numbers on the private global IP address to distinguish between translations. Because the port number is encoded in 16 bits, the total number could theoretically be as high as 65,536 per IP address. PAT will attempt to preserve the original source port number. If this number is already allocated then PAT will attempt to find the first available port number starting from the beginning of the appropriate port group 0–511, 512–1023, or 1024–65535¹. If there is still no port number available from the appropriate group and more than one IP address is configured, PAT will move to the next IP address in the pool and try to allocate the original source port number again. This continues until it runs out of available ports and IP addresses.

PAT offers the following capabilities:

- Provides many-to-one address translation
- Maps multiple IP addresses to one or a few IP addresses
- Identifies a unique source port number in each session
- Conserves registered IP addresses

¹ Group starts at 0 for ICMP, but 1 for all other applications. As of DDTs CSCdm05636, the number of port groups changed from four to three. As of DDTs CSCed93887 Cisco IOS Software Releases 12.3(09.10) Mainline and 12.3(09.10)T, each PAT IP address can accommodate all 64,000 ports for IPsec sessions using the NAT-T UDP wrapper. The new CLI command required is “ip nat service full range udp port 500”. With this new feature, PAT can allocate a maximum of 65536 ports.

Destination Address Rotary Translation

A dynamic form of destination translation can be configured for some outside-to-inside traffic. After a mapping is set up, a destination address matching one of those on an access control list (ACL) will be replaced with an address from a rotary pool. Allocation is done on a round-robin basis, performed only when a new connection is opened from the outside to the inside. All non-TCP traffic is passed untranslated (unless other translations are in effect). This feature was designed to provide protocol-translation load distribution. It is not designed nor intended to be used as a substitute technology for the Cisco® LocalDirector appliance and software. Destination-address rotary translation should not be used to provide Web service load balancing because, like basic Domain Name System (DNS), it knows nothing about service availability. As a result, if a Web server were to go offline, the destination-address rotary translation feature would continue to send requests to the unavailable server. For more information, please visit <http://www.cisco.com/warp/public/732/Tech/ipservices/natalgs.pdf>.

Platform Support

Cisco NAT is available in Advanced Security, Advanced Enterprise, and Advanced IP Services software images for all currently supported Cisco access router platforms, Cisco 7200 Series Routers, and the Cisco 7301 Router (Table 1). The default Security Router Bundle includes the appropriate Cisco IOS Software image, along with enough memory and storage to support NAT features and other threat-defense capabilities.

Table 1. Feature Availability

| Product Series | Platforms Supported |
|-------------------|--|
| Cisco 800 Series | Cisco 831, 836, 837, 851, 857, 871, 876, 877, 878 |
| Cisco 1700 Series | Cisco 1701, 1702, 1711, 1712, 1721, 1751, 1751-V, 1760 |
| Cisco 1800 Series | Cisco 1801, 1802, 1803, 1811, 1812, 1841 |
| Cisco 2600 Series | Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, 2691 |
| Cisco 2800 Series | Cisco 2801, 2811, 2821, 2851 |
| Cisco 3600 Series | Cisco 3660 |
| Cisco 3700 Series | Cisco 3725, 3745 |
| Cisco 3800 Series | Cisco 3825, 3845 |
| Cisco 7200 Series | Cisco 7204VXR, 7206VXR |
| Cisco 7300 Series | Cisco 7301 |

Additional Resources

- Cisco NAT: <http://www.cisco.com/go/nat>
- Router security: <http://www.cisco.com/go/routersecurity/>

For More Information

For more information about Cisco NAT, visit <http://www.cisco.com/go/nat> or contact your local Cisco account representative.



Americas Headquarters
 Cisco Systems, Inc.
 170 West Tasman Drive
 San Jose, CA 95134-1706
 USA
www.cisco.com
 Tel: 408 526-4000
 800 553-NETS (6387)
 Fax: 408 527-0689

Asia Pacific Headquarters
 Cisco Systems, Inc.
 155 Robinson Road
 #29-01 Capital Tower
 Singapore 068912
www.cisco.com
 Tel: +65 6317 7777
 Fax: +65 6317 7799

Europe Headquarters
 Cisco Systems International BV
 Heerlenbergpark
 Heerlenbergweg 13-19
 1101 CH Amsterdam
 The Netherlands
www.europe.cisco.com
 Tel: +31 0 20 620 0791
 Fax: +31 0 20 657 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, AirNet, BPK, Catalyst, CCD, CCO, CCIE, CCR, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fax, Step, Follow Me Browsing, FormShare, Go to Drive, HomeLink, Internet Quotient, IOS, iPhone, IPTV, IQ Expertise, the IQ logo, IQ Notepad, Scorecard, QuickStudy, SignStream, iInlays, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, SsookWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (9705R)