



[Home](#) > Network Address Translation NAT Tutorial

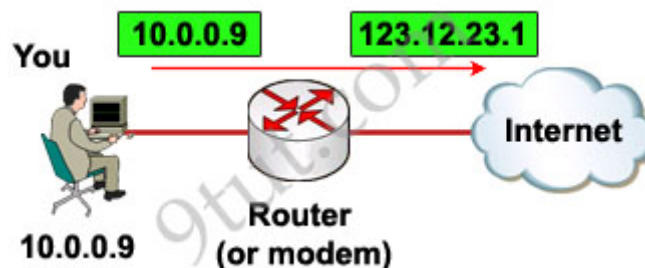
Network Address Translation NAT Tutorial

May 22nd, 2011 [Go to comments](#)

To go to the Internet we need to get an public IP address and it is unique all over the world. If each host in the world required a unique public IP address, we would have run out of IP address years ago. But by using Network Address Translation (NAT) we can save tons of IP addresses for later uses. We can understand NAT like this:

“NAT allows a host that does not have a valid registered IP address to communicate with other hosts through the Internet”

For example your computer is assigned a private IP address of 10.0.0.9 and of course this address can not be routed on the internet but you can still access the internet. This is because your router (or modem) translates this address into a public IP address, 123.12.23.1 for example, before routing your data into the internet.



Of course when your router receives a reply packet destined for 123.12.23.1 it will convert back to your private IP 10.0.0.9 before sending that packet to you.

Maybe you will ask “hey, I don’t see any difference of using NAT to save tons of IP addresses because you still need a public IP address for each host to access the Internet and it doesn’t save you anything, why you need to use NAT?”

Ok, you are right :), in the above example we don’t see its usefulness but you now understand the fundamental of NAT!

Let’s take another example!

Suppose your company has 500 employees but your Internet Service Provider (ISP) only gives you 50 public IP addresses. It means that you can only allow 50 hosts to access the internet at the same time. Here NAT comes to save your life!

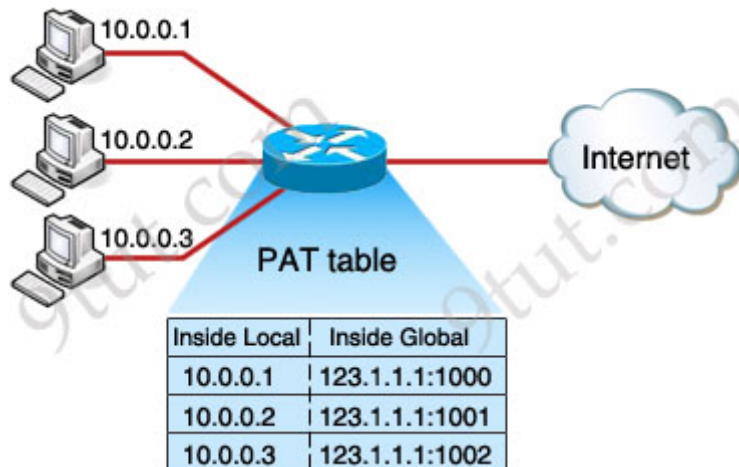
One thing you should notice that in real life, not all of your employees uses internet at the same time. Say, maybe 50 of them use internet to read newspaper at the morning; 50 others use internet at noon for checking mail... By using NAT you can dynamically assign these 50 public IP addresses to those who really need them at that time. This is called **dynamic NAT**.

But the above NAT solution does not solve our problem completely because in some days there can be more than 50 people surfing web at the morning. In this case, only the first 50 people can access internet, others must wait to their turns.

Another problem is, in fact, your ISP only gives you much lesser IP addresses than the number 50 because each public IP is very precious now.

To solve the two problems above, another feature of NAT can be used: **NAT Overload** or sometimes called **Port Address Translation (PAT)**

PAT permits multiple devices on a local area network (LAN) to be mapped to a single public IP address with different port numbers. Therefore, it's also known as port address translation (PAT). When using PAT, the router maintains unique source port numbers on the **inside global** IP address to distinguish between translations. In the below example, each host is assigned to the same public IP address 123.1.1.1 but with different port numbers (from 1000 to 1002).



Note: Cisco uses the term **inside local** for the private IP addresses and **inside global** for the public IP addresses replaced by the router.

The outside host IP address can also be changed with NAT. The **outside global** address represents the outside host with a public IP address that can be used for routing in the public Internet.

The last term, **outside local** address, is a private address of an external device as it is referred to by devices on its local network. You can understand outside local address as the inside local address of the external device which lies at the other end of the Internet.

Maybe you will ask how many ports can we use for each IP? Well, because the port number field has 16 bits, PAT can support about 2^{16} ports, which is more than 64,000 connections using one public IP address.

Now you have learned all the most useful features of NAT but we should summarize all features of NAT:

There are two types of NAT translation: dynamic and static.

Static NAT: Designed to allow one-to-one mapping between local and global addresses. This flavor requires you to have one real Internet IP address for every host on your network.

Dynamic NAT: Designed to map an unregistered IP address to a registered IP address from a pool of registered IP addresses. You don't have to statically configure your router to map an inside to an outside address as in static NAT, but you do have to have enough real IP addresses for everyone who wants to send packets through the Internet. With dynamic NAT, you can configure the NAT router with more IP addresses in the inside local address list than in the inside global address pool. When being defined in the inside global address pool, the router allocates registered public IP addresses from the pool until all are allocated. If all the public IP addresses are already allocated, the router discards the packet that requires a public IP address.

PAT (NAT Overloading): is also a kind of dynamic NAT that maps multiple private IP addresses to a single public IP address (many-to-one) by using different ports. Static NAT and Dynamic NAT both require a one-to-one mapping from the inside local to the inside global address. By using PAT, you can have thousands of

users connect to the Internet using only one real global IP address. PAT is the technology that helps us not run out of public IP address on the Internet. This is the most popular type of NAT.

Besides NAT gives you the option to advertise only a single address for your entire network to the outside world. Doing this effectively hides the internal network from the public world really well, giving you some additional security for your network.

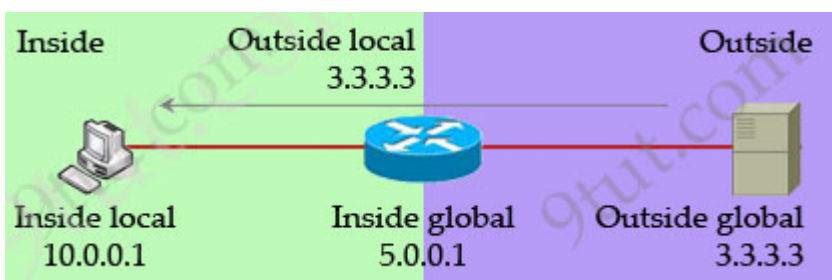
NAT terms:

* **Inside local address** – The IP address assigned to a host on the inside network. The address is usually not an IP address assigned by the Internet Network Information Center (InterNIC) or service provider. This address is likely to be an RFC 1918 private address.

* **Inside global address** – A legitimate IP address assigned by the InterNIC or service provider that represents one or more inside local IP addresses to the outside world.

* **Outside local address** – The IP address of an outside host as it is known to the hosts on the inside network.

* **Outside global address** – The IP address assigned to a host on the outside network. The owner of the host assigns this address.



To learn how to configure NAT please read my [Configure NAT GNS3 Lab tutorial](#)

[Comments \(1\)](#) Comments

1. Anonymous
January 3rd, 2022

thank you

Add a Comment

Name

Submit Comment

[Subscribe to comments feed](#)

[Configure NAT – GNS3 Lab](#) [CCNA – Access List Questions](#)

Premium Member Zone

Welcome [Gurjeet singh!](#)

- [Welcome Premium Member](#)
- [CCNA – New Questions Part 5](#)
- [CCNA – New Questions Part 6](#)
- [CCNA – New Questions Part 7](#)
- [CCNA – New Questions Part 8](#)
- [CCNA – New Questions Part 9](#)
- [Composite Quizzes](#)
- [Logout](#)

CCNA 200-301

- [Basic Questions](#)
- [Topology Architecture Questions](#)
- [Cloud & Virtualization Questions](#)
- [CDP & LLDP Questions](#)
- [Switch Questions](#)
- [VLAN & Trunking Questions](#)
- [VLAN & Trunking Questions 2](#)
- [STP & VTP Questions](#)
- [EtherChannel Questions](#)
- [TCP & UDP Questions](#)
- [IP Address & Subnetting Questions](#)
- [IP Routing Questions](#)
- [IP Routing Questions 2](#)
- [OSPF Questions](#)
- [OSPF Questions 2](#)
- [EIGRP Questions](#)
- [NAT Questions](#)
- [NTP Questions](#)
- [Syslog Questions](#)
- [HSRP Questions](#)
- [Access-list Questions](#)
- [AAA Questions](#)
- [Security Questions](#)
- [Security Questions 2](#)
- [DAI Questions](#)
- [IPv6 Questions](#)
- [DNS Questions](#)
- [QoS Questions](#)
- [Port Security Questions](#)
- [Wireless Questions](#)
- [Wireless Questions 2](#)
- [SDN Questions](#)
- [DNA Center Questions](#)
- [Drag Drop Questions](#)
- [Drag Drop Questions 2](#)
- [Drag Drop Questions 3](#)
- [VPN Questions](#)
- [DHCP Questions](#)
- [Automation Questions](#)
- [Miscellaneous Questions](#)
- [CCNA FAQs & Tips](#)
- [Share your new CCNA Experience](#)

CCNA Self-Study

- [Practice CCNA GNS3 Labs](#)
- [CCNA Knowledge](#)
- [CCNA Lab Challenges](#)
- [Puppet Tutorial](#)
- [Chef Tutorial](#)
- [Ansible Tutorial](#)
- [JSON Tutorial](#)
- [Layer 2 Threats and Security Features](#)
- [AAA TACACS+ and RADIUS Tutorial](#)
- [STP Root Port Election Tutorial](#)
- [GRE Tunnel Tutorial](#)
- [Basic MPLS Tutorial](#)
- [TCP and UDP Tutorial](#)
- [Border Gateway Protocol BGP Tutorial](#)
- [Point to Point Protocol \(PPP\) Tutorial](#)
- [WAN Tutorial](#)
- [DHCP Tutorial](#)
- [Simple Network Management Protocol SNMP Tutorial](#)
- [Syslog Tutorial](#)
- [Gateway Load Balancing Protocol GLBP Tutorial](#)
- [EtherChannel Tutorial](#)
- [Hot Standby Router Protocol HSRP Tutorial](#)
- [InterVLAN Routing Tutorial](#)
- [Cisco Command Line Interface CLI](#)
- [Cisco Router Boot Sequence Tutorial](#)
- [OSI Model Tutorial](#)
- [Subnetting Tutorial – Subnetting Made Easy](#)
- [Frame Relay Tutorial](#)
- [Wireless Tutorial](#)
- [Virtual Local Area Network VLAN Tutorial](#)
- [VLAN Trunking Protocol VTP Tutorial](#)
- [IPv6 Tutorial](#)
- [Rapid Spanning Tree Protocol RSTP Tutorial](#)
- [Spanning Tree Protocol STP Tutorial](#)
- [Network Address Translation NAT Tutorial](#)
- [Access List Tutorial](#)
- [RIP Tutorial](#)
- [EIGRP Tutorial](#)
- [OSPF Tutorial](#)

Network Resources

- [Free Router Simulators](#)
 - [CCNA Website](#)
 - [ENCOR Website](#)
 - [ENSDWI Website](#)
 - [ENARSI Website](#)
 - [DevNet Website](#)
 - [CCIE R&S Website](#)
 - [Security Website](#)
 - [Wireless Website](#)
 - [Design Website](#)
 - [Data Center Website](#)
 - [Service Provider Website](#)
 - [Collaboration Website](#)

[Top](#)



Copyright © 2021 CCNA Training

[Site Privacy Policy](#). Valid XHTML 1.1 and CSS 3.H