

Q: What is NAT?

A: NAT stands for Network Address Translation.

To understand what this is, how it functions and why it is needed, we must first cover how the Internet handles communications between computers.

WARNING: Some of the following discussion is simplified and glosses over some of the nit-picking details on how the Internet actually works. For the purpose of this FAQ, the level of detail used is adequate and any statements that are not 100% accurate are intended to avoid needing to go into extraneous detail.

Every computer using the Internet needs an address of the form X.X.X.X (where each X is a number from 0 to 255). Due to the limited number of such addresses, there can be a need for Private Networks with large numbers of computers/devices to have addresses that do not conflict with the Internet Addresses. To fill this need there are certain addresses (10.X.X.X and 192.168.X.X) that have been designated for use on these Private Networks that are not part of the Internet. No computer on the Internet is allowed to have these addresses. When such a network wants to communicate with the Internet it does it through a NAT Gateway (which can often also act as a Firewall) All I will say here about Firewalls is that they are used to control what types of sessions are allowed to cross the Gateway.

When a computer wants to talk to another computer on the Internet it starts a Session with that other computer. For a computer to be contacted to create such a session, it must "listen" for the attempt to start a session. The listening is done via Port-Numbers (ie: Listen for an attempt to start a session to my "Port Number X"). There is a list of "Well Know Ports" that tell what Port Number to use to start different types of sessions. For example if you are Web Surfing, you connect to the Web Site and ask for Port Number 80. To send Email, you'd ask for Port Number 25.

The contacting Computer also needs a Port Number so that it can receive the responses. This Port Number comes from a range that is allocated for stating sessions and is unique for the life of that session. IOW, if you are Web Surfing and have more than one session open, each session has its own unique Port Number (this allows the browser to know which window to display the incoming information in). The Session is defined by its two endpoints. Thus if you have a Web Session it would be X.X.X.X:5788<->Y.Y.Y.Y:80. If you open another Web Window and go to that same site, the session might be X.X.X.X:5789<->Y.Y.Y.Y:80.

The forgoing is what happens when the computers are both on the Internet. What happens if one of the computers (let us for simplicity say the one who is doing the Web Surfing) is on one of the aforementioned Private networks and has an address of 192.168.1.50? When it tries to go to the Web Site, it will try to start a session 192.168.1.50:5789<->Y.Y.Y.Y:80. The messages destined for Y.Y.Y.Y will be sent to a computer that is acting as a Gateway (this is a computer that can talk to both the Private Network and the Internet and does NAT). On the Private Network this Computer is known as 192.168.1.1 while on the Internet it is known as Z.Z.Z.Z. When the message gets to it, it will alter the reference in the message that says "I am from 192.168.1.50" to say "I am from Z.Z.Z.Z". It will also assign its own Port Number from the stating sessions range (let us say 7777). Thus it starts its own session of Z.Z.Z.Z:7777<->Y.Y.Y.Y:80 with the Web Site. It also adds to a table the fact that its Port 7777 is really 192.168.1.50:5789. This is the reason for NOT keeping the real computer's Port Number. It must be able to tell who it is acting as and using the real computer's Port Number can cause problems if another computer (such as 192.168.1.99) wants to start a session as 192.168.1.99:5789 (IOW: using the same Port Number as 192.168.1.50 is using). By assigning a Port number of 7778 to 192.168.1.99's request the two attempts to use Port Number 5789 are kept separate.

To the Internet, the two sessions LOOK like they are the same computer (which in reality they are since they are being sent to/from the Gateway Computer). As each message comes in from the Internet the Gateway Computer uses the Port Number in the incoming message to determine who to send it to on the Private Network and it sends the message to the Private Network with the correct 192.168.1.X address and Port Number). Internet directed messages get the same treatment in the other direction (use the table to get the Internet side address and port and send it on its way).

It is all very elegant. The Internet sees the whole Private Network as being the Gateway Computer (and is not even aware of the Private Network) while the computers on the Private Network see the Gateway as the Internet.

NATting is the extended version of Proxyserver. Using proxy server one can not do telnet/ftp/ssh/sftp other internet machines.

NATting is of two types:

1. Dynamic NATting: Several machines use one internet IP address.
Purpose: To allow a person to do telnet/ftp/ssh/sftp other internet machines (One Way access).
2. Static Natting: Machine will have one local IP, which will be mapped to one unique internet IP.
Purpose: Same as dynamic NATting plus it will allow other internet systems to access this system. For example one person is running a local web site, which he wants to make visible on internet also. Also from other internet system one can do telnet/ftp/ssh/sftp etc. to the local machine (Two way access).