Dynamic NAT

Dynamic NAT

According to the definitions outlined in the NAT Terminology article, a Dynamic NAT implies a translation of just the IP address, where the post-translation attributes are selected by the router.

In a Dynamic NAT, a multitude of hosts with private IP addresses can share an equal or fewer amount of public IP addresses.

It may seem very similar to a Dynamic PAT, but the major difference is this is a *NAT* – the port number is not changing, only the IP address. Which means a single public IP address cannot be shared among multiple internal Hosts at the same time (as occurs with a Dynamic PAT).

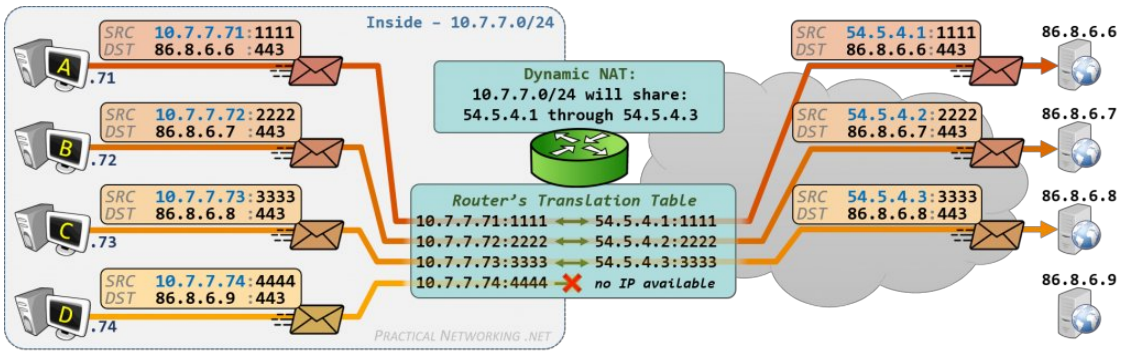
It is best explained with an illustration.

This article is a part of a series on Network Address Translation (**NAT**). Use the navigation boxes to view the rest of the articles.

Network Address Translation

- Why NAT?
- NAT Terminology
- Static NAT
- Static PAT
- Dynamic PAT
- **Dynamic NAT**
- Policy NAT and Twice NAT
- NAT Terminology Disambiguation

Dynamic NAT Illustration



In the image we have a Router with an Inside network (**`10.7.7.0/24`**) with four hosts (**`.71`**, **`.72`**, **`.73`**, **`.74`**). The Router is configured with a Dynamic NAT which states the hosts on the Inside network can share three public IP addresses: **`54.5.4.1`**, **`54.5.4.2`**, and **`54.5.4.3`**.

Host A (**`10.7.7.71`**) initiates a connection to **`86.8.6.6`**, and the Router assigns Host A the public IP **`54.5.4.1`**.

Host B (**`10.7.7.72`**) initiates a connection to **`86.8.6.7`**, and the Router assigns Host B the public IP **`54.5.4.2`**.

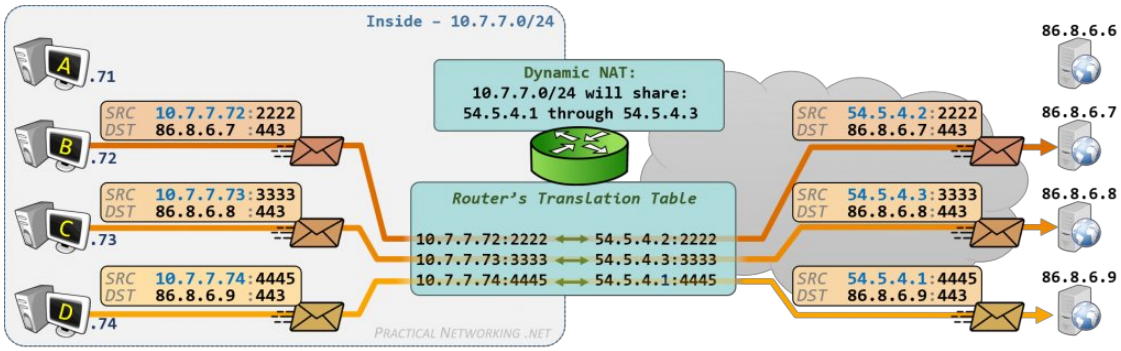
Host C (**`10.7.7.73`**) initiates a connection to **`86.8.6.8`**, and the Router assigns Host C the public IP **`54.5.4.3`**.

At this point, all the shared IP addresses have been used. Because of this, when Host D (**`10.7.7.74`**) attempts to initiate a connection to **`86.8.6.9`**, the packet is dropped because there are no available public IP addresses the router can use to translate Host D's private IP address.

While Host A/B/C have active connections through the Dynamic NAT, communication to those hosts are Bidirectional. Which means any host on the Internet can send packets to **`54.5.4.1`**, **`.2`**, and **`.3`** to reach Host A/B/C, respectively.

We will expand on this in a moment.

When Host A is finished with its connection, the IP address it was assigned (`54.5.4.1`) becomes available again for the next internal host to use:



Here, we see Host D can now initiate a connection through the Dynamic NAT and receives the next available IP address.

In all cases, since this is a Dynamic *NAT*, only the IP address changed – the source port picked by the internal host remains the source port in the packet after translation.

Additionally, a Dynamic NAT has the potential to conserve IP addresses if configured as above where multiple internal hosts are sharing fewer Public IP addresses. However, you'll see in a moment that Dynamic NAT is not always configured in that fashion.

Benefits and Use Cases for Dynamic NAT

The main use case for a Dynamic NAT is that while the translation is active it has the benefit of being bidirectional, just like a Static NAT.

For example, in the images above, Host B (`10.7.7.72`) has an active connection and was assigned the public IP address `54.5.4.2`. So long as the connection is active in the Router's translation able, any host on the Internet can send packets to `54.5.4.2` and they will reach Host B.

In a way, a Dynamic NAT assigns a temporary "dedicated IP" to each internal host (so long as IP addresses are available). Or, said another way, a Dynamic NAT creates a temporary Static NAT.

There are two primary use cases for Dynamic NAT. The first is to allow for protocols which create a secondary, dynamic connection back to the client. The second is if you need a Bidirectional mapping of Private IPs to Public IPs, but don't particularly care about the explicit mapping between the two.

File Transfer Protocol and Dynamic NAT

The initial intent of a Dynamic NAT was to allow for protocols which create a second, dynamic connection back to the client. The main example of which is the File Transfer Protocol, or FTP.

FTP clients initiate outbound connections to FTP servers over destination port `TCP/21`. This connection serves as what FTP considers the *control channel*.

Over the control channel, a FTP client makes a request for a file and provides a random port number to the Server. The FTP Server then *initiates a second connection back to the client* from source port `TCP/20`, to the destination port *provided by the client in the control channel*. It is over this second connection that the file is actually transferred – this second connection is what FTP considers the *data channel*.

The issue is the data channel is a connection initiated from an external host on the Internet, destined to a host behind the Router. In a Dynamic PAT, which only allows connections initiated from the internal hosts, the data channel connection would be dropped.

But with a Dynamic NAT, the inbound data channel connection would be able to pass through the translation and the clients on the Inside server would be able to successfully use FTP to access files on the Internet.

The above describes the classic implementation of FTP known as *Active FTP*. There is a more modern implantation of FTP known as *Passive FTP* which does not require FTP clients to sit behind a Dynamic NAT, and instead allows them to sit behind the much more ubiquitous Dynamic PAT.

Dynamic Bidirectional Mappings

Beyond the case of dynamic protocols described above, one other usage for a Dynamic NAT is if you have an equal number of Public IP addresses as you do Private hosts, and don't particularly care which host get which public IP address, so long as each host gets one.

An example of such a case would be if the Router above could be configured to Dynamic NAT the entire **`10.7.7.0/24`** network into the entire **`54.5.4.0/24`** network. All 256 IP addresses in the Private range would receive an associated IP address on the Public range.

This would be the same effect of creating 256 individual Static NAT entries, except since the Dynamic NAT is *Dynamic*, there wouldn't be an explicit mapping of a Private IP to a Public IP. The Router would be choosing which Private addresses map to which Public addresses.

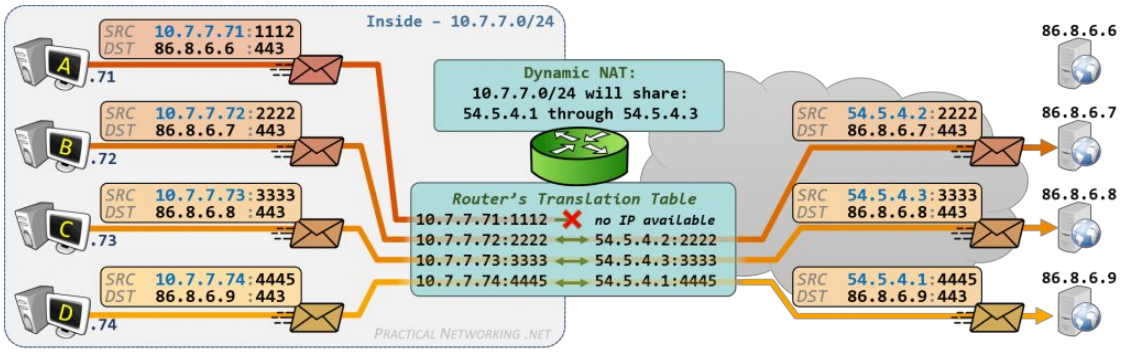
If a particular deployment doesn't necessarily care for a permanent, explicit mapping of private to public IP addresses, then Dynamic NAT could be used as a type of short cut to configuring 256 individual Static NAT entries.

When configured in this manner, a Dynamic NAT does not actually conserve any IP addresses, since it would be necessary to have a public IP address for each private host.

Disadvantages of Dynamic NAT

Despite the potential use cases outlined above, in the grand scheme of things, a Dynamic NAT is the least common type of translation deployed. This is due to the mapping created by a Dynamic NAT being temporary by nature, and therefore inconsistent.

In the first illustration above, Host A/B/C received the IP addresses **`54.5.4.1`**, **`54.5.4.2`**, **`54.5.4.3`** respectively. A moment later, in the second illustration, Host A's connection terminated, and Host D received the IP address **`54.5.4.1`**. If a moment after that, Host A attempted to communicate, there would be no available IP addresses and Host A's packet would be dropped:



From Host A's perspective, there was connectivity one moment, and no connectivity the next. This creates a generally poor experience for the user. And some of the most difficult for the network administrator to troubleshoot, as the connectivity issue is intermittent.

Of course, running out of available addresses and losing connectivity would only occur when there are less public IP addresses available in your translation pool than you have internal hosts – as is the case above with four internal hosts sharing three public IP addresses.

If you had a similar number of internal hosts and external IP addresses, as discussed in our second use-case example, you wouldn't run into the inconsistent connectivity problem. However, you would still run into the issue of inconsistent

IP addresses.

For example, if there were no Host D in our illustration and there were just Hosts A/B/C sharing the IP addresses **`54.5.4.1`**, **`54.5.4.2`**, **`54.5.4.3`**. Host A may get **`54.5.4.1`** for the first connection, **`54.5.4.2`** for the next, and **`54.5.4.3`** for the third. At any given time, Host A would have connectivity, but there is no telling which public IP address Host A would receive at any given time.

Strictly speaking, this isn't intrinsically a bad thing if you are using a Dynamic NAT for the specific case described above where you don't necessarily need an explicit mapping.

But non-deterministic configurations can lead to unexpected and unintended results. So as a general rule in the Network Engineering field, deterministic designs are more favorable than non-deterministic designs.

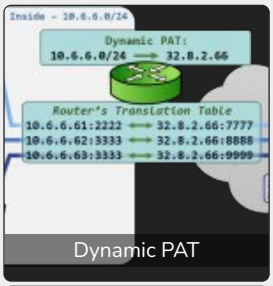
Hence, if you have the public IP addresses available to give each of your private hosts a unique address, it is generally looked at as more favorable to configure multiple Static NAT translations instead of a single Dynamic NAT.

> It should be noted that often when discussing address translation people will use the term *Dynamic NAT* when they actually mean *Dynamic PAT*. For the reasons mentioned above, Dynamic NAT is rarely used in production. If a single IP address is *shared* among many internal users, and if the *port number changes*, than it is indeed a Dynamic ***PAT***.

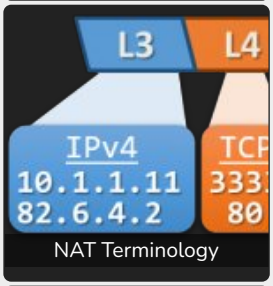
Series Navigation

Dynamic PAT >>Policy NAT and Twice NAT >>

Related Posts:

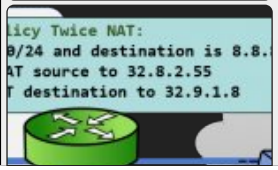


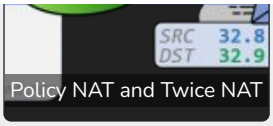
Dynamic PAT



NAT Terminology

Network Address Translation (NAT)





Tags: CCNA NAT

0

Article Rating

Subscribe

7 COMMENTS Oldest

Vishal kumar
4 years ago

In this article, u r talking about active type of FTP which ofcourse would be possible in dynamic nat case but if it is a passive connection then dynamic pat should work i guess.

0 Reply

Vishal kumar
Reply to Vishal kumar 4 years ago

Sorry i just read the yellow post and u have mentioned it there ..i guess i skiped that part by mistake

0 Reply

Nathan
3 years ago

Ed,
This is a very well written article. Mentioning and recommending the deterministic design patterns as you noted in latter part of your article is a good foundation block for building security. I have a specific question regarding . Is there ever a use case to dynamically NAT an interface to a single ip address. E.G. Nat(inside,outside) dynamic 100.100.100.100 . Is there a difference between that and this – Nat(inside,outside) static 100.100.100.100
I would appreciate your insight

0 Reply

Ed Harmoush (@ed) Author
Reply to Nathan 3 years ago

Hi Nathan,

Glad you enjoyed the article!

The syntax you provided appears to be a Cisco ASA. If so, you might find your answer in this article. The syntax you provided is also a little off, so maybe after reading through that article please feel free to ask again and provide the full syntax of what you are trying to compare. Alternatively, you might want to try in the Network Engineering Stack Exchange or the Networking Sub Reddit.

0 Reply

Matt

2 years ago

Hi Ed,

I have a single public IP – 100.1.1.49 which is already NATted to 192.168.1.36 (Proxy) using a Manual NAT as follows:

ASA#config t
object-group network Proxy-Out-Int
network-object host 192.168.1.36
exit

object-group network Public-Int
network-object host 100.1.1.29
exit

nat (inside,outside) source static Proxy-Out-Int Public-Int

Now I have additional two proxies to deploy to leverage on the existing public IP (100.1.1.29)

Can I create additional two STATIC NAT to achieve this, and will still get the new proxies to work, as shown below ?

ASA#config t
object-group network Proxy-Out-Int2
network-object host 192.168.1.37
exit

ASA#config t
object-group network Proxy-Out-Int3
network-object host 192.168.1.38
Exit

nat (inside,outside) source static Proxy-Out-Int2 Public-Int
nat (inside,outside) source static Proxy-Out-Int3 Public-Int

OR should I just remove the existing MANUAL (STATIC) NAT and put in an entire new config for MANUAL (DYNAMIC) NAT ?, see below

ASA#config t
object-group network Proxy-Out-Int
range 192.168.1.36 192.168.1.38
exit

object-group network Public-Int
network-object host 100.1.1.29
exit

nat (inside,outside) source dynamic Proxy-Out-Int Public-Int

I would appreciate your help on this, thanks.

0 Reply

Binh Thanh Nguyen

2 years ago

Thanks, nice post

0 Reply

Arnold

5 months ago

If a single IP address is shared among many internal users, and if the port number changes, than it is indeed a Dynamic PAT.

Typo: then

Excellent articles; thanks.

0 Reply

Your E-Mail:

Your Name:

Subscribe

Most read articles this week:

Routing Between VLANs
2k views

OSI Model
1.2k views

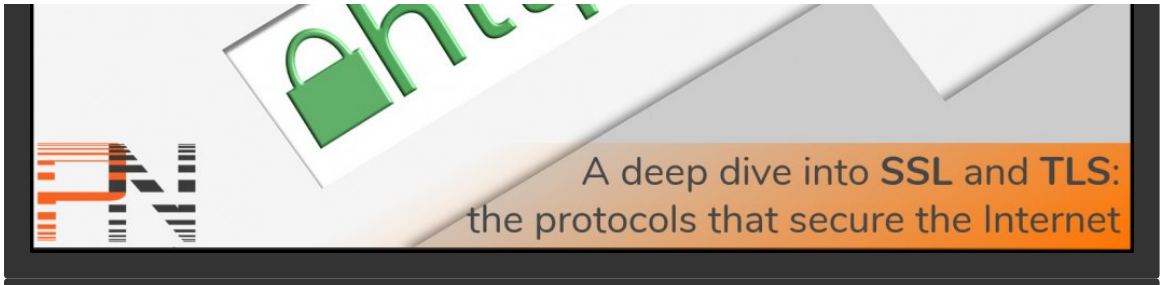
Virtual Local Area Networks (VLANs)
1.1k views

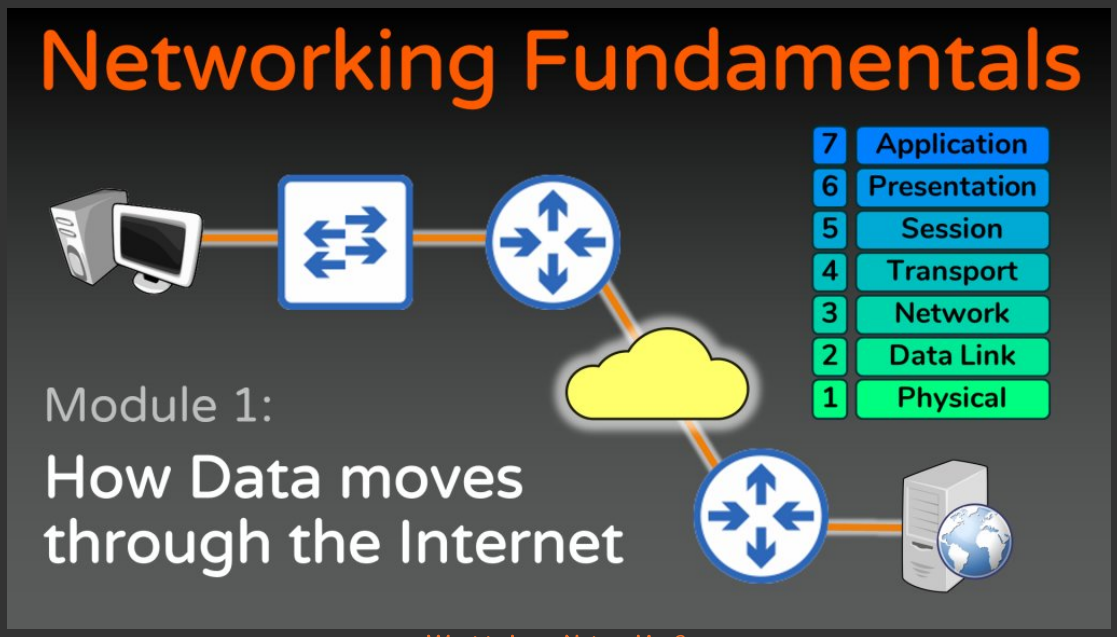
Cisco Firepower & Cisco ASA – NAT Configuration Guide
0.9k views

Gratuitous ARP
870 views

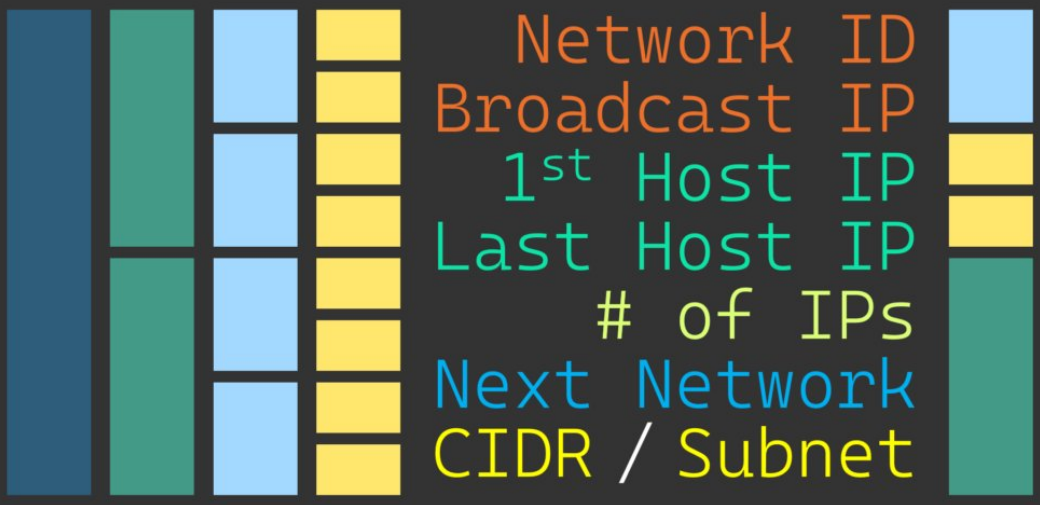
Vote for Practical Networking
in Cisco's IT Blog Awards.

ACL ARP ASA BGP CCNA CCNP CISCO CRYPTOGRAPHY EIGRP ENCRYPTION HASHING
NAT NETWORKING ROUTING SUBNETTING TLS VLANS VPN





Want to learn Networking?
Watch this free video series.



Want to learn Subnetting?
Watch the best Subnetting training videos ever recorded. Then practice Subnetting at: SubnetIPv4.com