Dynamic PAT

According to the definitions outlined in the NAT terminology, a Dynamic PAT implies a translation of the IP address and port, where the post translation attributes are selected by the router.

Dynamic PAT is the most common of the types of adress translation we will discuss in this article series. Dynamic PAT is used any time multiple internal hosts need to share a single public IP address.

On a small scale, this is exactly what your home Wi-Fi router does. You may have 5-25 unique devices on your home network, each of them with their own private IP address. But when any of them try to speak with the Internet, they all share the single, unique public IP address assigned to your router.

The same type of translation happens with the Wi-Fi at coffee shops, or restaurants, or airports. This was the exact same example that was provided in the “Why NAT?” article – the illustrations are examples of a Dynamic PAT.

Of all the types of Network Address Translation, a Dynamic PAT is the most conducive to conserving IP address space. It is not uncommon to have hundreds of internal hosts sharing one public IP address.

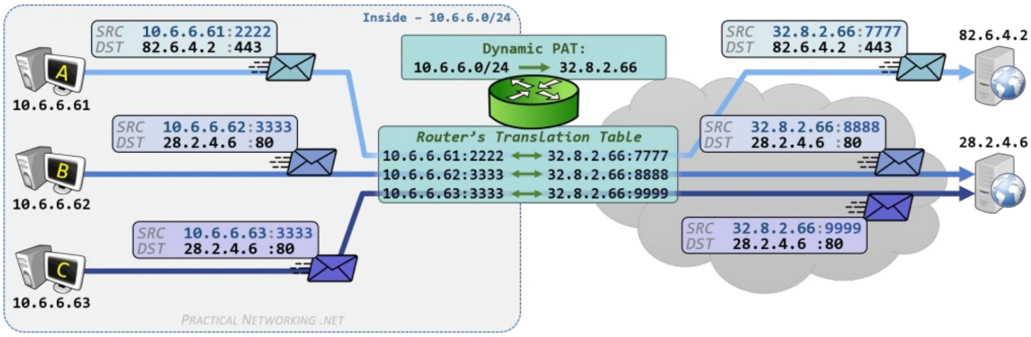
Of all the types of Network Address Translation, a Dynamic PAT is the most conducive to conserving IP address space. It is not uncommon to have hundreds of internal hosts sharing one public IP address.

Dynamic PAT is often referred to as a many-to-one or one-to-many translation, implying the many hosts on the Wi-Fi network are sharing the one Public IP address on the Internet.

Of course, this simple example referred to earlier hasn’t quite shown how ports are translated, or how the Router selected the post-translation attributes. To illustrate those concepts, we will have to look at the packet flow through a Dynamic PAT in more detail.

Packet Flow – Outbound Traffic

The image below illustrates what is occurring at the packet level:



The Router is serving as our translation device, and is configured with a Dynamic PAT which translates any IP address on the Inside network (10.6.6.0/24) to the IP address 32.8.2.66. When packets are translated, the Router makes note of the attributes of the original and translated packet in the Router’s Translation Table.

Hosts A, B, and C each send a packet. They each use their own, unique Private IP address as the Source IP address, and they each randomly select a Source Port.

There are approximately 60,000 port numbers that can be chosen, and it is entirely feasible for two different hosts to randomly select the same source port (as is the case with Host B and Host C above).

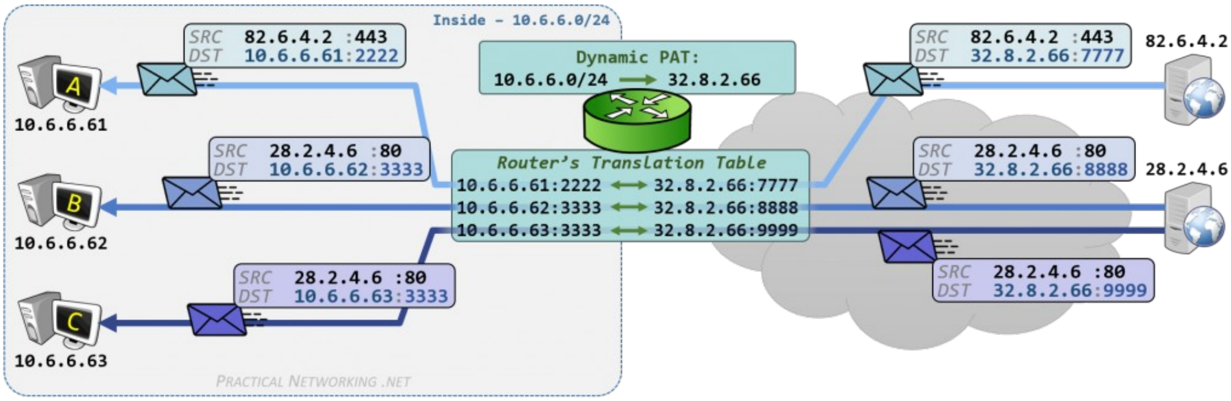
Notice the configuration of the Dynamic PAT does not include specifying a port number.Even though the ports are not explicitly set in the Router's configuration, this translation is still classified as a PAT because the port is dynamically changed by the Router.

In our example above, upon reception of each packet, the Router translates the source IP address of each packet to 32.8.2.66 (as explicitly configured), and randomly selects a new, unique source port number for each packet (7777, 8888, and 9999). The Router translated the port (PAT) and the Router selected the new source port (Dynamic).

Each specific mapping is recorded in the Router's Translation Table. This translation table will be used to "un-translate" the response packets when they return from the Internet.

Packet Flow – Response Traffic

When the two webservers respond to the three packets illustrated in the example above, the packet flow will resemble the following:



The response traffic from the web servers simply reverses the source and destination from the initial packet Each web server sends the response traffic to the destination of the shared IP address (32.8.2.66), with the destination port number which the Router had selected in the original outbound traffic.

When the packets arrive on the Router, it matches them against the translation table to know how to "un-translate" the packet to their original attributes to get them to the appropriate host:

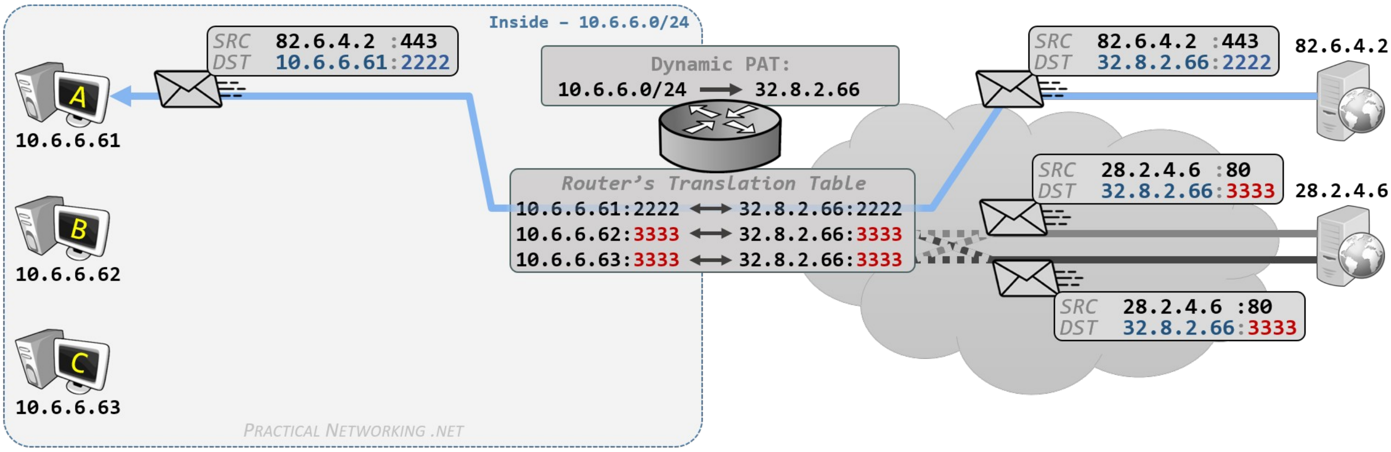
•The response packet sent to 32.8.2.66:7777 is forwarded to Host A (10.6.6.61:2222)
•The response packet sent to 32.8.2.66:8888 is forwarded to Host B (10.6.6.62:3333)
•The response packet sent to 32.8.2.66:9999 is forwarded to Host C (10.6.6.63:3333)

Why was the source port re-randomized?

In the last section, we pointed out that the router selected a new, random source port for the outbound packet. This re-randomizing of the source port is crucial to enabling successful communication through a Dynamic PAT.

Had the router not re-randomized the source port number, the outbound post-translation packets from Host B and Host C would have looked identical – they both would have had a Source IP of 32.8.2.66 and a Source port of 3333.

Which means the response traffic for both packets from the 28.2.4.6 server would have looked identical – the Destination IP would have been 32.8.2.66 and the Destination port would have been 3333.



Router's Translation Table

10.6.6.61:2222	↔	32.8.2.66:2222
10.6.6.62:3333	↔	32.8.2.66:3333
10.6.6.63:3333	↔	32.8.2.66:3333

When the identical packets arrive, the router would have no way of distinguishing which packet should be untranslated to Host B (10.6.6.62) or which should be translated to Host C (10.6.6.63). The router would have no choice but to drop both packets.

This would cause packets to drop anytime two hosts happen to pick the same source port, which happens often enough that no host would be content with the connectivity (or lack thereof) provided through a Dynamic PAT.

For this reason, it is imperative that the Router ensures every packet sent through a Dynamic PAT uses a unique source port number. This allows the return packets to be distinguishable from one another, and allows the Router to forward the return traffic to the appropriate host.

Some NAT devices assure unique source ports by re-randomizing the source port for all connections when doing a Dynamic PAT translation. Some NAT devices do this by re-randomizing the source port only when duplicate ports are chosen by the inside hosts.

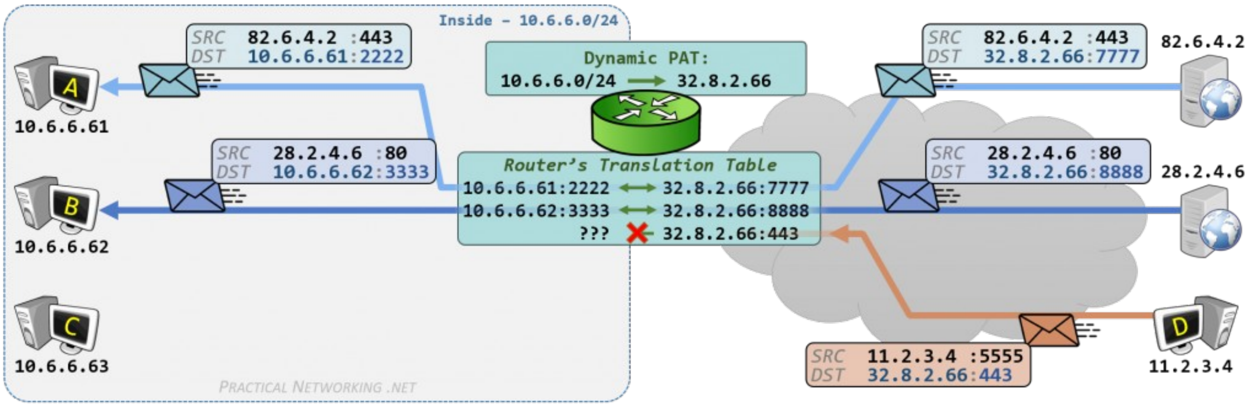
Regardless of the method used, so long as each connection's packets can be identified by both unique IP Address and Port, for both Source and Destination, the response traffic can be successfully un-translated to the appropriate initial host.

Unidirectional

As discussed before, a Dynamic PAT allows many internal hosts to share the same the same public IP address. One of the side effects of multiple hosts sharing a single IP address is the translation only works in one direction.

In the example above, Hosts A, B, and C initiated some traffic to external hosts. When the external hosts responded, the Router had entries in its translation table which allowed it to “un-translate” the packets and send them to the appropriate hosts.

If, however, a new connection was initiated from an external host and destined to the shared IP address, the router will have no way of knowing which internal host was the intended target of the packet.



Not knowing whom to deliver the packet to, the Router has no choice but to drop the packet. As such, a Dynamic PAT only succeeds if the internal host sends the first packet. If the external host sends the first packet, it will be dropped when it reaches the translation device.

This is what is meant by a Dynamic PAT being a unidirectional translation – traffic will flow through a Dynamic PAT only if the internal host initiates the connection.

This is in contrast to static NAT and static PAT, which are both bi-directional – traffic can be translated whether it was initiated by the external host or the internal host.

Keep in mind, this is not a “feature” of Dynamic PAT so much as it is a “side effect” of multiple hosts sharing a single IP address. Since it is possible for hosts to pick identical source ports, the router must change the source port during the translation, which means the packets arriving from the Internet can only make it back through the Dynamic PAT due to the entry in the translation table, which a packet initiated from an external network would not have.

If there is a need for certain ports to be accessible through a shared IP address, this can be achieved by using a Static PAT to selectively punch holes through the shared dress of a Dynamic PAT.

Check on - http://www.practicalnetworking.net/series/nat/dynamic-pat/

https://networkengineering.stackexchange.com/questions/47517/why-does-nat-translate-a-source-port