

Static PAT

Static PAT

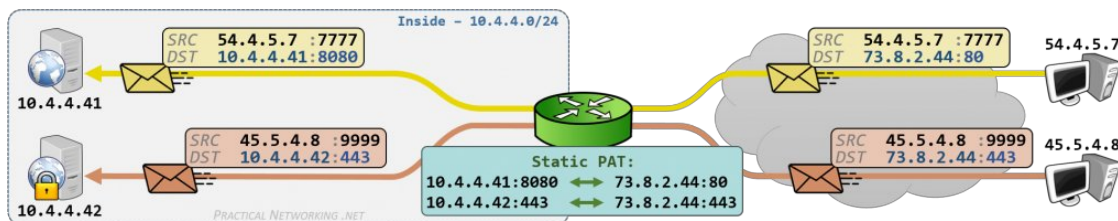
According to the definitions outlined in the [NAT Terminology](#) article, a **Static PAT** implies a translation of the **IP address and Port**, where the **post-translation attributes are explicitly defined**.

There are multiple use cases for a Static PAT, but they all have one thing in common – a need to manually change the TCP or UDP port as a packet moves through a router or firewall.

Multiple Servers using one Public IP Address

One specific use case for Static PAT is to use a *single* Public IP address to host *multiple* services on *different* internal servers. This is in contrast with a **Static NAT** which would only allow you to use a single Public IP address to host *multiple* services on the *same* server.

This illustration will show how Static PAT can enable the single IP address **73.8.2.44** to host two different services (HTTP and HTTPS) using two separate internal servers (**10.4.4.41** and **10.4.4.42**):



The Router is acting as our translation device and is configured with two Static PAT entries. Since these are **static** translations, the mapping is explicitly defined: **73.8.2.44:80** will always be translated to **10.4.4.41:8080** and **73.8.2.44:443** will always be translated to **10.4.4.42:443**.

Two hosts somewhere on the Internet both make a request to the *same* IP address (**73.8.2.44**) – one request using **HTTP** (port **80**), one request using **HTTPS** (port **443**). When their packets arrive on the Router, they get translated and sent to two *different* servers for processing.

The single Public IP address (**73.8.2.44**) is hosting two services (HTTP and HTTPS) served by two different internal servers (**10.4.4.41** and **10.4.4.42**).

If you use a Static PAT in this way (where one public IPv4 address is used to host multiple services on *multiple* servers), then you are conserving IPv4 address space. You could theoretically have 10 (or 50, or 200, or 1000+) different servers, each hosting a different service, all using a single Public IPv4 address.

Non-Standard Ports

The same illustration above also provides yet another use case for Static PAT – the **10.4.4.41** server is hosting HTTP

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](#)

traffic on a non-standard port (**8080**).

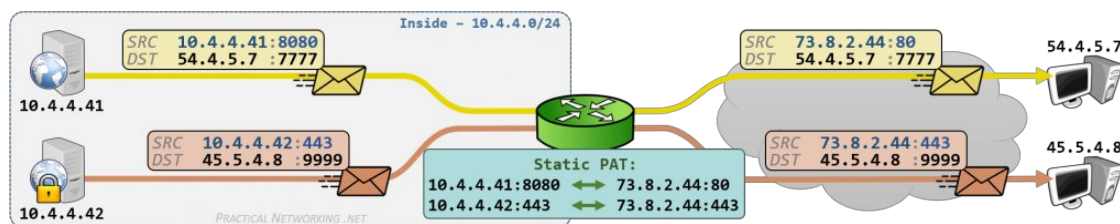
Without the port translation, hosts on the Internet would have to specify the non-standard port in their web browser by visiting “[www.site.com:8080](#)”. Instead, with the Static PAT, the users can just type “[www.site.com](#)” (which implicitly assumes the standard web port of **80**) and the router automatically translates the packet to port **8080** instead.

This could work in reverse as well. Where a non-standard port is used on the outside, but a standard port is used on the inside server.

For example, the standard port associated with SSH traffic is TCP/22. Malicious users routinely scan the entire IPv4 address space for servers listening on port TCP/22 to look for all SSH servers in hopes of finding some with weak passwords. A common strategy is to host SSH on a non-standard port in an effort to hide your SSH server from this mass scanning that occurs on port 22.

Response Traffic

The response traffic from these hosts would be untranslated by the router. Since this is the outbound traffic, the source of the packet will be translated. Whereas on the inbound packet above, the destination of the packet was translated.



Once again, since the pre-translation IP:Port and post-translation IP:Port in a Static PAT are explicitly defined, the initial packet could have come from either the Internet hosts or the inside hosts. Therefore, a **Static PAT translation is bidirectional**.

Selectively Punching Holes

There is one final use-case for Static PAT, which is possibly the least common of the three. A Static PAT allows you to selectively “punch holes” through a particular Public IP address.

When we looked at a **Static NAT**, only the IP address is translated – the port numbers are left untouched. Which means, every port is explicitly mapped to every port. It's possible that you may want only ports **80** and **443** to get through, but not port **21** or **23** (or any other). A Static NAT does not allow you to choose.

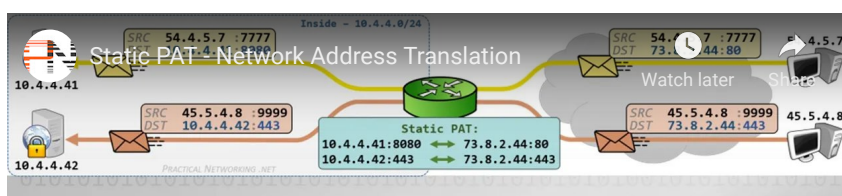
Whereas instead, with a Static PAT, if you only create a translation for port **80** and **443**, only those paths through the router will exist. Protecting your internal servers from unwanted access attempts.

In this context, Static PAT is sometimes referred to as **Port Forwarding**: a specific port on an external address is forwarded to a specific port on an internal address.

Admittedly, the same effect can be attained by creating a Static NAT and applying an access-list or security policy to only allow the desired traffic through. As such, this is a use-case for Static PAT, but by no means is it the only way to attain the same effect.

The most common usage of selectively punching holes is to create a *bidirectional* path through *unidirectional* NAT translation. This will make more sense when we discuss Dynamic PAT in the next article.

Prefer video content to text? The majority of this article has been recorded and can be viewed on Youtube:



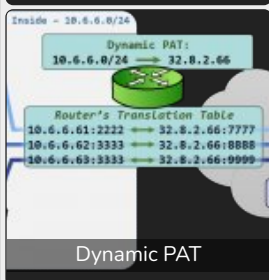
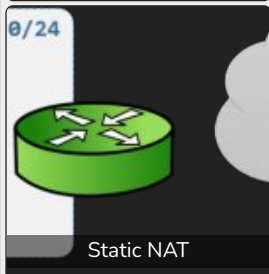
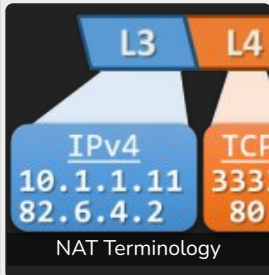
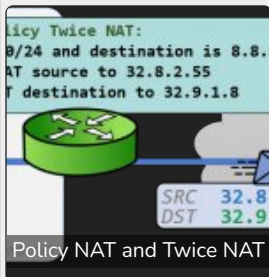
Static PAT

Network Address Translation

Series Navigation

[Static NAT](#) >> [Dynamic PAT](#) >>

Related Posts:



Tags:

CCNA

NAT

0

Article Rating



✉ Subscribe ▼

12 COMMENTS

⚡ 🔥 Oldest ▼

Fereidoun Fatahiany

🕒 4 years ago

This is really good.....

👍 0 ➡ Reply

Sangameshwar

🗨 Reply to Fereidoun Fatahiany 🕒 4 years ago

This is very helpful and important....

As per my understanding in ip nating one to many you can give Data but you can't get back from many because at a time only one connection is possible to give back Data to the internal server.....

I really appreciate and wants to understand more on this topic with Configuration details....

👍 0 ➡ Reply

Ed Harmoush (@ed) Author

🗨 Reply to Sangameshwar 🕒 4 years ago

Hi Sangameshwar, Static PAT is still considered a one to one translation. You might be thinking of a Dynamic PAT:

<http://www.practicalnetworking.net/series/nat/dynamic-pat/>

👍 0 ➡ Reply

kushal deshmukh

🕒 4 years ago

Nice explanation. Thanks

👍 0 ➡ Reply

fritz hege

🕒 4 years ago

could you post or send me what the static pat configuration would look like on the router above?

👍 0 ➡ Reply

Ed Harmoush (@ed) Author

🗨 Reply to fritz hege 🕒 4 years ago

Hi Fritz,

Soon, I'll have links for each vendor's actual syntax on the disambiguation page:

<http://www.practicalnetworking.net/series/nat/hat-terminology-disambiguation/>

Feel free to sign up to get updates when it gets published.

👍 0 ➡ Reply

Ed Harmoush (@ed) Author

🗨 Reply to fritz hege 🕒 3 years ago

Hi Fritz, I just finished the [NAT configuration guide on Cisco IOS Routers](#). One of the section describes how to configure a [Static PAT](#).

👍 0 ➡ Reply

hussain

🕒 3 years ago

Great job ... many appreciations ,, my I know what is the program you are using to create these great gif images?

👍 0 ➡ Reply

Ed Harmoush (@ed) Author

🗨 Reply to [hussain](#) 🕒 3 years ago

I use Powerpoint for my animations, export to MP4, then convert to GIF. =)

👍 0 ➡ Reply

varbog

🕒 2 years ago

Good job

👍 0 ➡ Reply

Mircea

🕒 5 months ago

Very good!

👍 0 ➡ Reply

Ed Harmoush (@ed) Author

🗨 Reply to [Mircea](#) 🕒 5 months ago

Thank you again, Mircea =)

👍 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

871 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

PRACTICAL TLS



A deep dive into **SSL and TLS**:
the protocols that secure the Internet

Networking Fundamentals

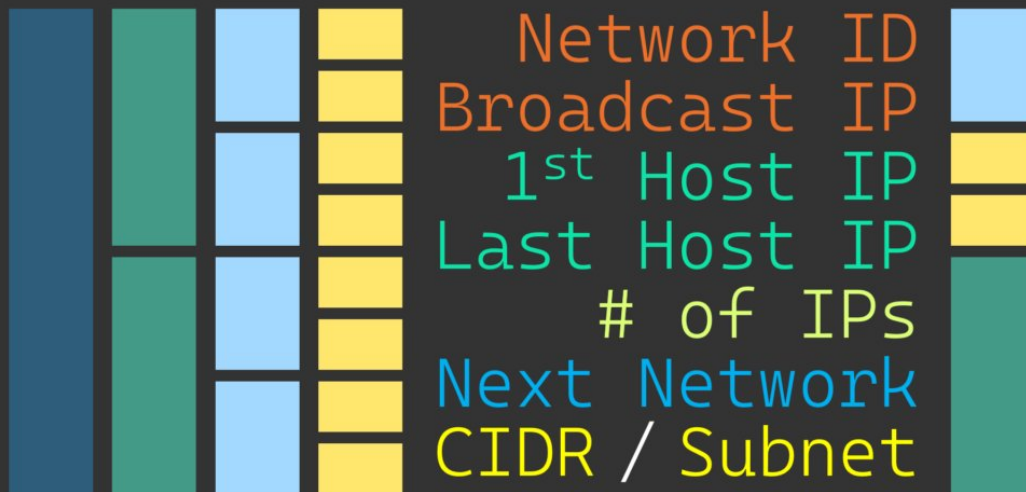


Module 1:

How Data moves
through the Internet

- 7 Application
- 6 Presentation
- 5 Session
- 4 Transport
- 3 Network
- 2 Data Link
- 1 Physical

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