

# Practical Networking



Inside - 10.6.6.0/24

10.6.6.99

Configured  
DNS Server:  
8.8.8.8

Policy Twice NAT:  
If source is 10.6.6.0/24 and destination is 8.8.8.8  
→ Dynamic PAT source to 32.8.2.55  
→ Static NAT destination to 32.9.1.8

Google's  
DNS Servers  
8.8.8.8

Corporate  
DNS Servers  
32.9.1.8

## Policy NAT and Twice NAT

SRC 10.6.6.99:9999  
DST 8.8.8.8:53

SRC 32.8.2.55:5555  
DST 32.9.1.8:53

## Policy NAT and Twice NAT

Every **type of NAT** we have discussed so far have two things in common. The first is that only the source of the packet is used to *make a NAT decision*. The second is that only the *source of the outbound packet* is translated. **Policy NAT** and **Twice NAT** are two ways of performing any type of NAT that expand beyond these two facts.

### Summary of the types of NAT

First, let's quickly recap what we learned in the previous articles:

**NAT vs PAT** – these terms define whether just the IP address portion of the packet, or the IP address *and* Port number are being translated

**Static vs Dynamic** – these terms define whether the post-translation attributes are explicitly defined by the administrator, or ephemerally determined by the router.

When combined, this provides four possible variations of Network Address Translation:

- **Static NAT** – Translation of just the IP address where the administrator explicitly defines the IP address after translation
- **Static PAT** – Translation of the IP address and Port, where the administrator explicitly defines the IP address and Port after translation
- **Dynamic PAT** – Translation of the IP address and Port, where the router determines the new IP address and Port after translation
- **Dynamic NAT** – Translation of just the IP address, where the router determines the new IP address after translation

### Decision Criteria

To configure each type of NAT above, we must define for the router exactly what traffic should be translated, and what it should be translated to.

If we review the configuration applied in the Static NAT or Dynamic PAT articles, we essentially instructed the Router to perform the following translations:

- If the *source IP address* is 10.2.2.33, translate the source IP statically to 73.8.2.33
- If the *source IP address* is 10.6.6.0/24 translate the source IP to 32.8.2.66 and dynamically pick a unique Source port

Notice in both cases we are making a decision to perform address translation based solely upon matching the *source IP address* of the packet – the *destination* address was not considered.

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

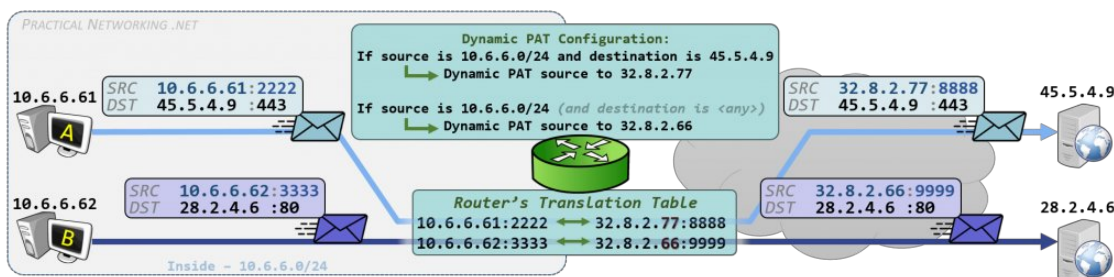
- [Why NAT?](#)
- [NAT Terminology](#)
- [Static NAT](#)
- [Static PAT](#)
- [Dynamic PAT](#)
- [Dynamic NAT](#)
- **Policy NAT and Twice NAT**
- [NAT Terminology Disambiguation](#)

This is fine if you want all traffic from the Inside servers translated the same way for *every* destination they may speak to. However, there are times when you want to translate traffic to a certain destination one way, then translate traffic to a different destination a completely different way.

In such cases, when you need to conditionally translate traffic based upon the destination of the packet, you will need to use what is known as a Policy NAT.

## Policy NAT

The following example is the [same illustration as we used in the Dynamic PAT article](#), except we've added one additional, conditional translation to the configuration:



There are two parts to the Router's configuration. The first part of the configuration produces this behavior:

- If the *source IP address* is **10.6.6.0/24** and the *destination IP address* is **45.5.4.9**, translate the source IP using Dynamic PAT to the address **32.8.2.77**

The additional configuration tells the router to translate a packet based upon the criteria of matching *both* the *Source* and *Destination* of the packet. In the industry, this is referred to as a **Policy NAT**.

A **Policy NAT** is simply any of the [four NAT types we discussed prior in this article series](#), except the **NAT decision** requires matching both the *Source* and *Destination* of a packet.

By contrast, every example of address translation thus far made a NAT decision based upon only the *source* of the packet.

The specific illustration immediately above was an example of a **Policy Dynamic PAT** – A translation decision based upon matching the source and destination of the packet (**Policy**), with the router determining the attributes after translation (**Dynamic**), which translated the source IP address and port (**PAT**).

The second part of the configuration produces this behavior:

- If the *source IP address* is **10.6.6.0/24**, and the *destination IP address* is **<anything>**, translate the source IP using Dynamic PAT to the address **32.8.2.66**

The second configuration item in the illustration above is simply a regular, **Dynamic PAT**.

Every traditional Dynamic PAT implies matching for *any* destination. Whereas the **Policy Dynamic PAT** in the [first example](#) would only match for *specific* destinations.

## Twice NAT

In each example of the traditional [four types of NAT](#) we've discussed in this article series, only one "side" of the packet was being modified: the Source of the outbound packet or the Destination of the inbound packet.

Moreover, in the prior section we discussed Policy NAT: making a NAT *decision* based upon matching both the source and destination of traffic. However, even in a Policy NAT, once the decision was made, only one side of the packet was being modified.

If you refer back to the [Policy Dynamic PAT example](#), when Host A (**10.6.6.61**) was speaking to the Server, we translated **10.6.6.61** using a Dynamic PAT into **32.8.2.77**. Notice the Server's IP address (**45.5.4.9**) was never

translated, only the client's – only one side of the packet was changed (the source of the outbound packet).

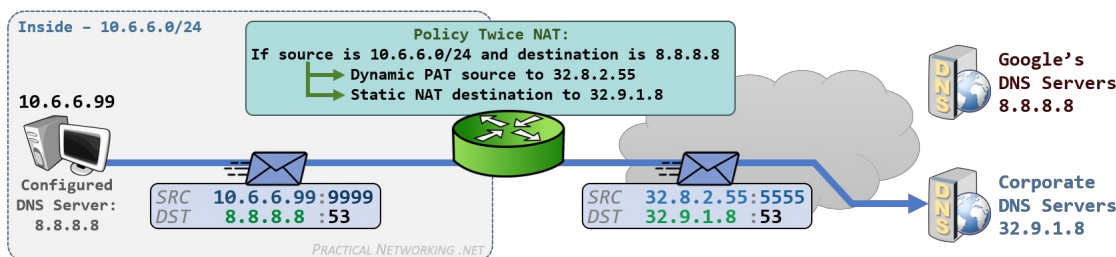
There are occasions where you need to translate *both* sides of the packet – this type of translation is referred to as a **Twice NAT**. The term comes from the fact that you are performing NAT twice: once on the source of the packet and another time on the destination of the packet.

There are many use cases for Twice NAT, we will provide one examples below. Another example will be illustrated in [a separate article](#).

## Changing the Destination with Twice NAT

At the core of it, a **Twice NAT** is a type of NAT where both the Source and Destination of the packet will be translated. Take this scenario as an example.

You are in charge of a Router with hosts on a private network (**10.6.6.0/24**) that have chosen to use Google's Public DNS Resolving Server (**8.8.8.8**). However, company policy states DNS requests must be made using the Corporate DNS server (**32.9.1.8**). One option is to manually verify every user's DNS configuration, but that does not scale. Instead, another option would be to translate any outbound requests to **8.8.8.8** into a request for **32.9.1.8**.



Notice the configuration is making a decision based upon matching a Source of **10.6.6.0/24** and a Destination of **8.8.8.8** – this makes the configuration a **Policy NAT**. Furthermore, the configuration is *translating the source* using a Dynamic PAT, *and the destination* using a Static NAT – this makes the configuration a **Twice NAT**, since we are doing *two instances of address translation*.

The packet sent by the host is sourced from a private IP address and destined to Google's DNS servers. But after crossing the router, the packet is now sourced from a public IP address and destined to the Corporate DNS servers.

The internal host is still configured to use Google's DNS servers, but their traffic is automatically being redirected to the corporate DNS servers. The internal host will not know that anything is different, and unless they go out of their way to validate the DNS responses, they will have no idea that the response is coming from the corporate DNS server and not Google's DNS server.

## Summary of New Terms

In this article, we unpacked and compared the ideas of a **Policy NAT** and a **Twice NAT**. As a quick summary:

- A **Policy NAT** is **any translation** that occurs based upon *matching* both the Source and Destination of traffic.
- A **Twice NAT** is **any translation** that involves *translating* both the Source and Destination of traffic.

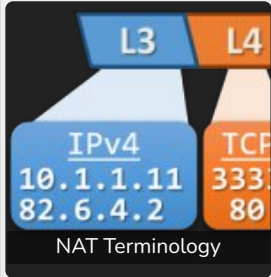
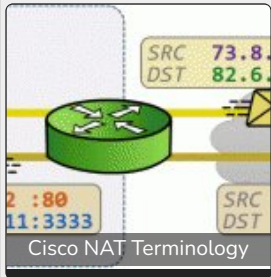
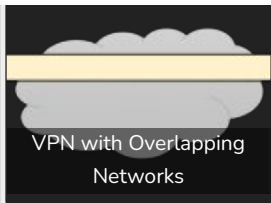
These two terms can be combined, giving us a Policy Twice NAT. Which is a type of NAT which makes a decision based upon the Source and Destination of a packet (**Policy NAT**), and translates both the Source and Destination of a packet (**Twice NAT**).

### Series Navigation

[Dynamic NAT >> NAT Terminology Disambiguation >>](#)

### Related Posts:

PRACTICAL NETWORKING .NET



Tags:

CCNA

NAT

0

Article Rating



Subscribe

21 COMMENTS



Oldest

sen

3 years ago

Thank you Ed for sharing the detail explanation of NAT and PAT concept. If you update the NAT translation same table real output that would be great that will distinguish the outbound and inbound address details.

0

Reply

vibhay kumar

🕒 3 years ago

As it is mentioned the giving DNS to each wont be fesiable but if i change the DNS ip in DHCP pool it wont create much problem, and other example for TWICE NAT, I got the idea of it but require more examples.

👍 0    ➡ Reply

### Poornima Pandey

🕒 3 years ago

Hi Ed,

Thank you for this Article . I was Always confused about NAT and you made it so clear and simple.

Thank you so much .

Can you guide me through the commands used to configure all types of NAT

👍 0    ➡ Reply

#### Ed Harmoush (@ed)

Author

🔗 Reply to Poornima Pandey    🕒 3 years ago

Hi Poornima, glad you enjoyed the article. Here are links to my NAT configuration guides for the [Cisco ASA](#) and [Cisco IOS Router](#). =)

👍 0    ➡ Reply

### Poornima Pandey

🕒 3 years ago

Thank you so much Ed. I have been looking from long time for just one article which has all the information .

Big thanks to you to make concepts so easy to understand .

👍 0    ➡ Reply

### Kumaran

🕒 2 years ago

Hi Ed,

Thanks for the info.

I am confused about source static and source dynamic in twice Nat, what is the different between this two ?

Regards,

Kumaran Sureshan

👍 0    ➡ Reply

#### Ed Harmoush (@ed)

Author

🔗 Reply to Kumaran    🕒 2 years ago

Hi Kumaran, I believe you are referring to Cisco ASA NAT Syntax, in which case I would refer you to [this section of this document](#).

👍 0    ➡ Reply

### kellina

🕒 1 year ago

Valuable info. Lucky me I found your website accidentally, and I'm shocked why this coincidence didn't happened in advance!

I bookmarked it.

👍 0    ➡ Reply

### Lachlan

🕒 1 year ago

You guys are the Masters, cheers.

👍 0    ➡ Reply

## Shraddha Pawar

🕒 9 months ago

Nicely Explained...I was confused in Policy NAT and Twice NAT ...But you explained in easy way...

👍 0   ➡ Reply

### Ed Harmoush (@ed)

Author

🗨 Reply to Shraddha Pawar   🕒 9 months ago

Thank you =). Glad it makes sense now!

👍 0   ➡ Reply

## Tanya

🕒 6 months ago

Great work, thank you!

But I still have one more question.

I have some web resource which is accessible via two local addresses, e.g. 192.168.1.1 and 192.168.1.1. Both addresses use local port 443. Let the external address be 213.180.204.11

Can I make the following configuration:

192.168.1.1:443 → 213.180.204.11:443

192.168.1.2:443 → 213.180.204.11:443

?

It does not matter to the user of the web resource through which internal IP address the connection is made.

Translated with <http://www.DeepL.com/Translator> (free version)

👍 0   ➡ Reply

### Tanya

🗨 Reply to Tanya   🕒 6 months ago

Or this configuration will be useless because only first match will be used?

👍 0   ➡ Reply

### Ed Harmoush (@ed)

Author

🗨 Reply to Tanya   🕒 6 months ago

Correct. On the way in, packets destined to 213.180.204.11:443 will only be translated to *one* of 192.168.1.1:443 or 192.168.1.2:443... not both.

On the way out, depending on the platform you are using, it might work or it might not even let you configure the translation because of the duplicate global attributes (213.180.204.11:443)

👍 0   ➡ Reply

### Tanya

🗨 Reply to Tanya   🕒 6 months ago

>>e.g. 192.168.1.1 and 192.168.1.1

I mean 192.168.1.1 and 192.168.2.1 of course

👍 0   ➡ Reply

## TheSuperHer

o

🕒 6 months ago

Could you please make an article about carrier-grade NAT? it's really confusing and I know your explanation could be easy to understand. Thanks

👍 0   ➡ Reply

### Ed Harmoush (@ed)

Author

🗨 Reply to TheSuperHero   🕒 6 months ago

Hi =). CGN is on the ever growing list of things I'd like to write about some day =).

👍 0   ➡ Reply

### MOHAMMAD AQUIB

🕒 4 months ago

This articles series really helped me to clear all doubts regarding NAT

👍 0   ➡ Reply

**Ed Harmoush** (@ed) Author

🔗 Reply to [MOHAMMAD AQUIB](#) 🕒 4 months ago

Excellent. Glad to hear it =)

👍 0   ➡ Reply

### Sumit Dhotre

🕒 1 month ago

Good article Ed,

I want to know if Dynamic source NAT can be used in twice NAT Policy?

👍 0   ➡ Reply

**Ed Harmoush** (@ed) Author

🔗 Reply to [Sumit Dhotre](#) 🕒 1 month ago

Sure, I don't see why not =).

👍 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](#)



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



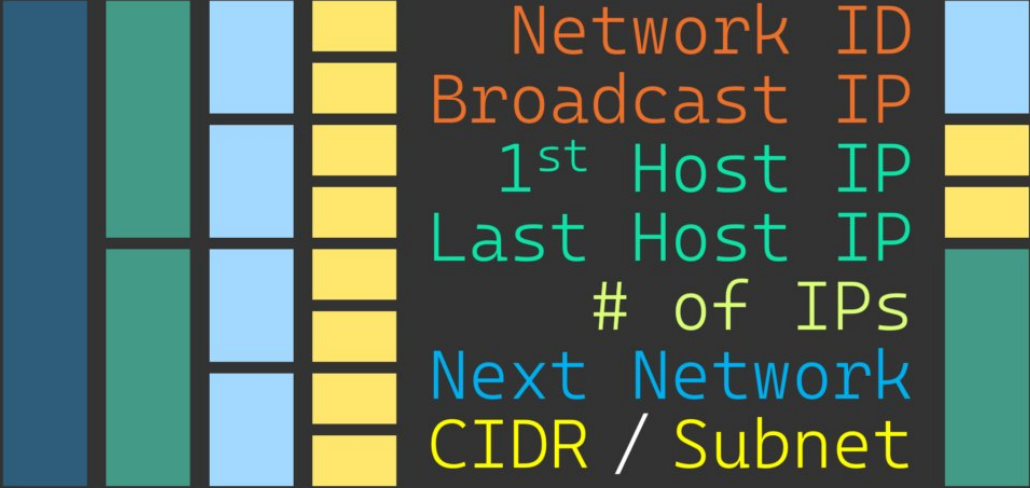
Module 1:

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.





Network ID  
Broadcast IP  
1<sup>st</sup> Host IP  
Last Host IP  
# of IPs  
Next Network  
CIDR / Subnet

Want to learn Subnetting?

Watch the best Subnetting training videos ever recorded. Then practice Subnetting at: [SubnetIPv4.com](https://SubnetIPv4.com)