Why NAT?

Why NAT?

Before we can discuss how NAT works, we must discuss the purpose of NAT and answer the question, "*Why NAT*?"

In the original plan for the Internet, every host was meant to have its own unique IP address. This means if you had a network which had 30 hosts, you would need 30 unique IP addresses for each host to *access the Internet*, or *to be accessed from the Internet*.

IP addresses are a finite resource – 32 bits allows for roughly 4.2 billion possible IP address combinations.

As the Internet grew in popularity, the industry realized there would one day be more hosts on the Internet than there were IP addresses available.

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

The long term, permanent solution was to create a larger address range, and IPv6 was born which is an addressing scheme that uses 128 bits. However, transitioning to IPv6 would prove to be a complicated and slow process, so a short term solution had to also be implemented: RFC 1918 was created to reduce the rate of IPv4 address utilization and delay the inevitable exhaustion of addresses.

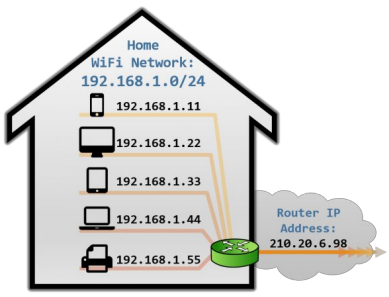
RFC 1918

RFC 1918 designated three different address sets that were considered free to use and reuse by any organization:

- **10.0.0.0 /8** – any IP address in the range of **10 . # . # . #**
- **172.16.0.0 /12** – any IP address in the range of **172 .[16-31]. # . #**
- **192.168.0.0 /16** – any IP address in the range of **192 . 168 . # . #**

These addresses were labeled as **Private** addresses, and were deemed unroutable on the Internet. All the remaining addresses remained **Public** addresses, and able to be routed on the Internet.

With RFC 1918, if you had 30 hosts on your network, all 30 of them would use 30 unique *Private* IP addresses, but for Internet facing traffic, all 30 could share a **single** *Public* address. Allowing you to conserve 29 Public addresses.

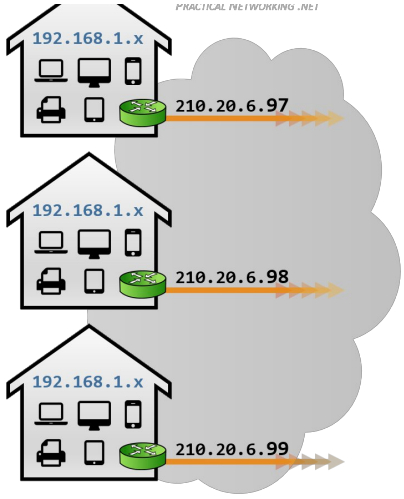


This is exactly what happens on WiFi networks. Whether it is a home WiFi network, or a coffee shop, or airport, each device on the network has a private IP address from one of the private ranges above. When these devices speak to the Internet, they all share the IP address assigned to the WiFi Router.

These Private addresses can be reused with each deployment without fear of duplicate addresses on the Internet. So long as the Public address(es) they are sharing are unique.

For example, a lot of home

WiFi networks use the common range of `192.168.1.0/24` for each of their internal address ranges. The home Wifi router then translates each independent set of *Private* `192.168.1.0/24` addresses into unique *Public* addresses.



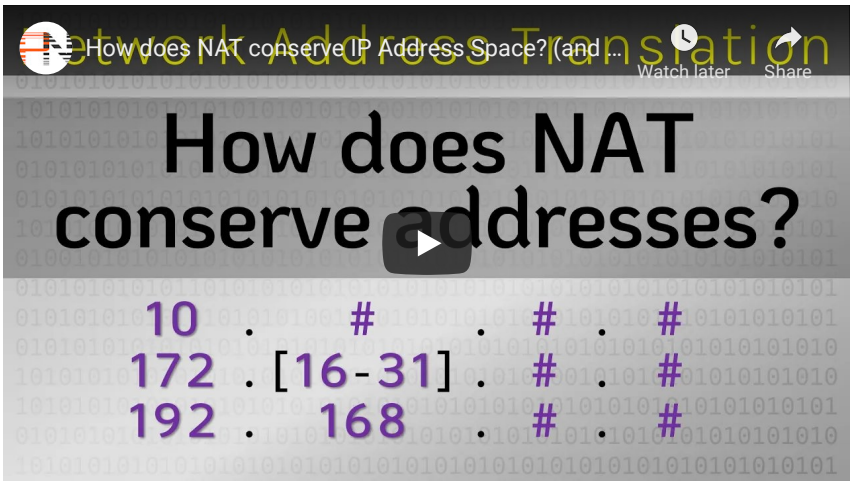
The idea is anyone can use these addresses, or even re-use these addresses, for as many hosts as they like on their internal network. NAT can then translate the multitude of hosts using *Private* addresses into a much smaller set of *Public* addresses – thereby curbing the rate of which IPv4 addresses are being utilized.

Private addresses are theoretically infinite, since they can be reused with each deployment. Public addresses are finite, and tracked by the Internet Authority for Assigned Numbers (IANA) to ensure no organization inadvertently uses duplicate Public addresses.

Consequently, the concept of **Network Address Translation was born to facilitate the translation between Private addresses and Public addresses**.

> Traditionally, NAT exists to translate Private IPv4 addresses into Public IPv4 addresses. For the sake of simplicity, this article series will describe NAT from this perspective. However, in reality, it does not matter whether the IP addresses being translated are public or private. NAT could easily occur from private addresses to other private addresses or from public addresses to other public addresses.

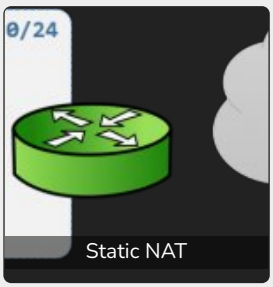
Prefer video content to text? The majority of this article has been recorded and can be viewed on Youtube:

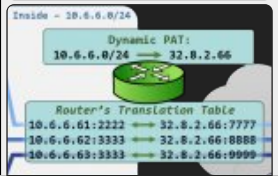


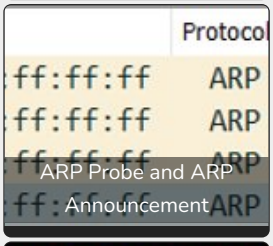
Series Navigation

NAT Terminology >>

Related Posts:







Tags: CCNA NAT

5

Article Rating

Subscribe

9 COMMENTS Oldest

Audrea
4 years ago

Good job Eddie!

0 Reply

Ed Harmoush (@ed) Author
Reply to Audrea 4 years ago

Oh snap! Thanks Audrea =)

0 Reply

Ashish Mishra
4 years ago

Hey Ed,

Your posts are always helpful.
Will there be any post for ospf and certificates ?

Thanku for such wonderful information

0 Reply

Banana-Man
3 years ago

I could never get my head around this until I read your article. Thank you!

0 Reply

JEAN-PIERRE Ernso
3 years ago

Nice

0 Reply

arshad
1 year ago

Hi,
I would like to just know what is pre-translation and post-translation. is there any method to understand that?

0 Reply

> **Ed Harmoush** (@ed) Author
> Reply to arshad 1 year ago
>
> The terms “Pre-Translation” and “Post-Translation” refer to the attributes being translated. This is unpacked in the next article when we discuss the terminology surrounding NAT.
>
> 0 Reply

Mircea
5 months ago

Very good explanation!
Easy to understand. Very helpful.
Many thanks!

0 Reply

> **Ed Harmoush** (@ed) Author
> Reply to Mircea 5 months ago
>
> You’re welcome, Mircea.
>
> 0 Reply

Most read articles this week:

Routing Between VLANs
2k views

OSI Model
1.2k views

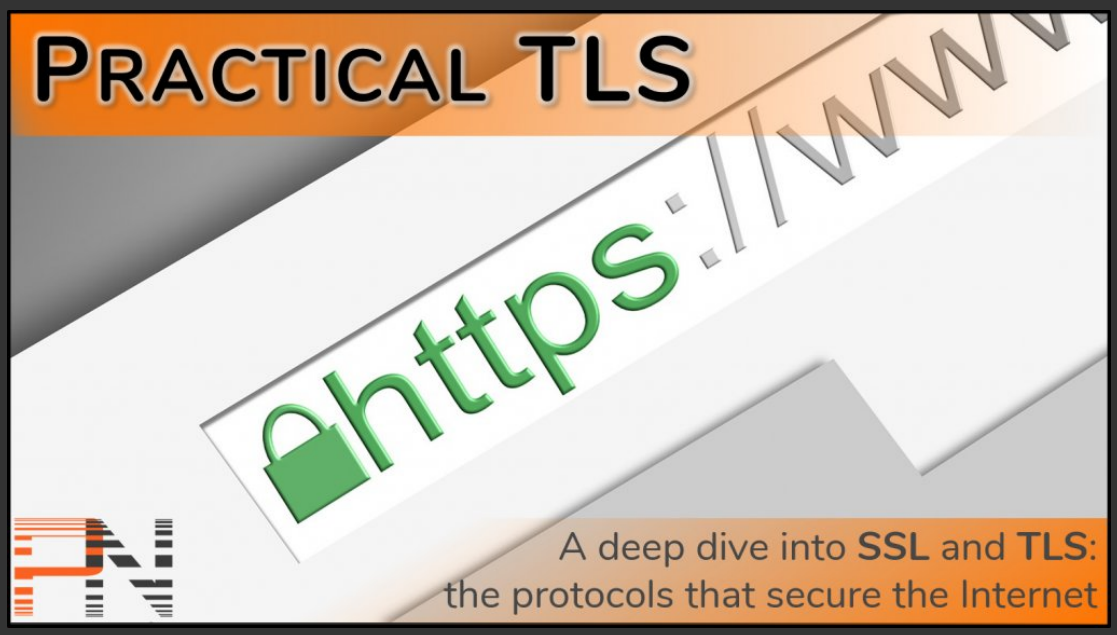
Virtual Local Area Networks (VLANs)
1.1k views

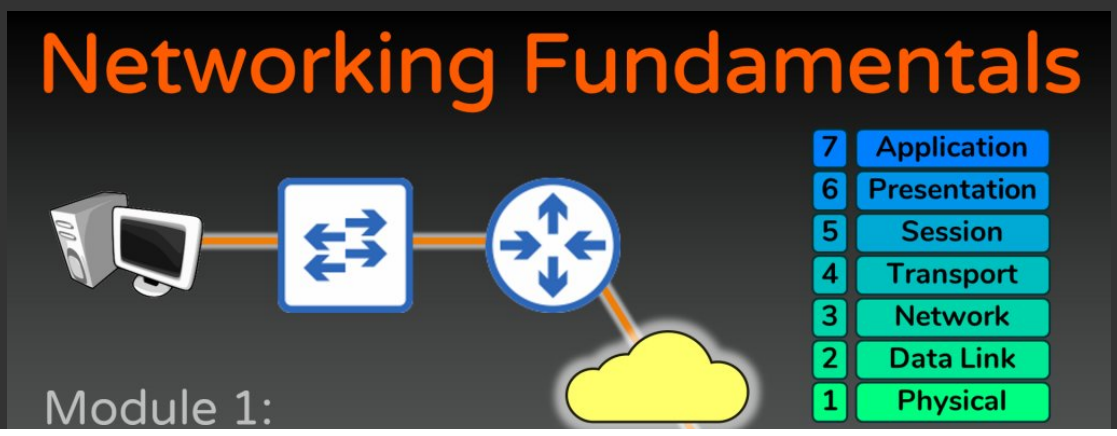
Cisco Firepower & Cisco ASA – NAT Configuration Guide
0.9k views

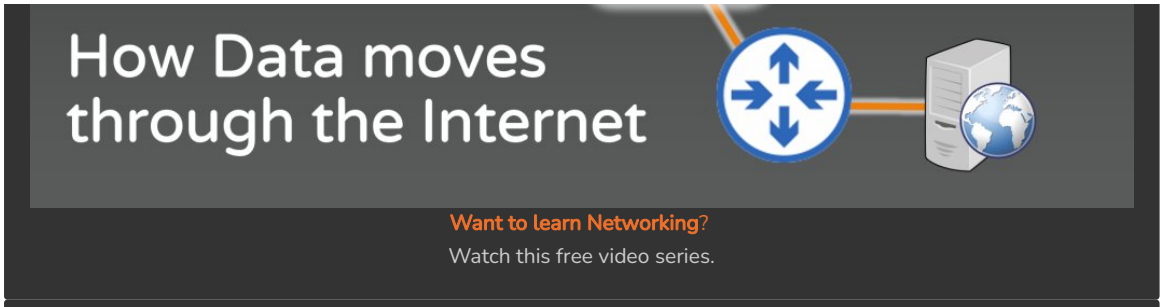
Gratuitous ARP
871 views

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

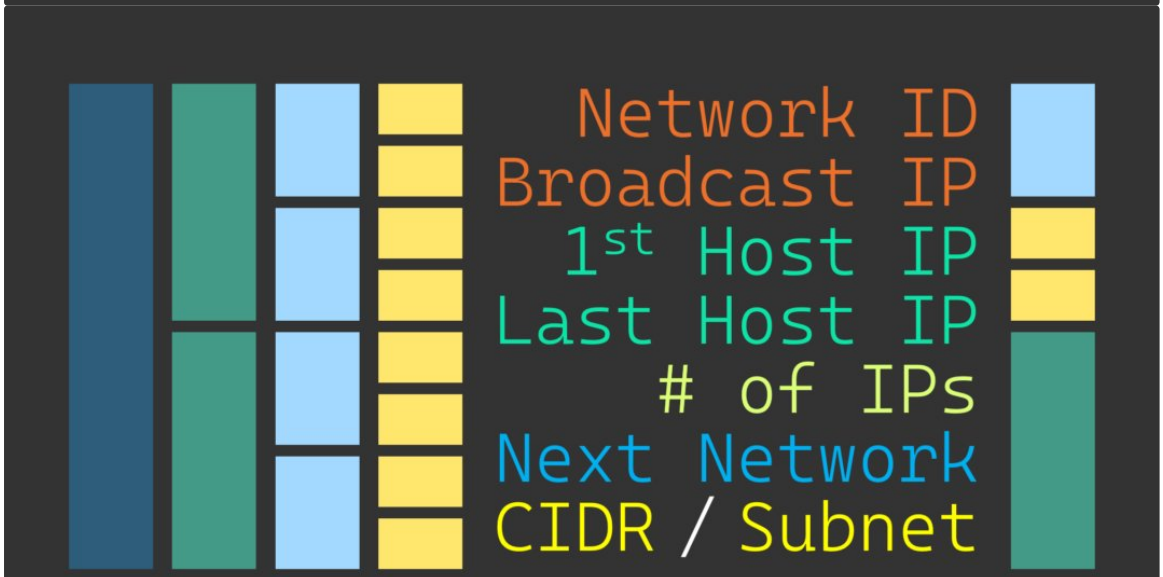






Want to learn Networking?

Watch this free video series.



Want to learn Subnetting?

Watch the best Subnetting training videos ever recorded. Then practice Subnetting at: SubnetIPv4.com