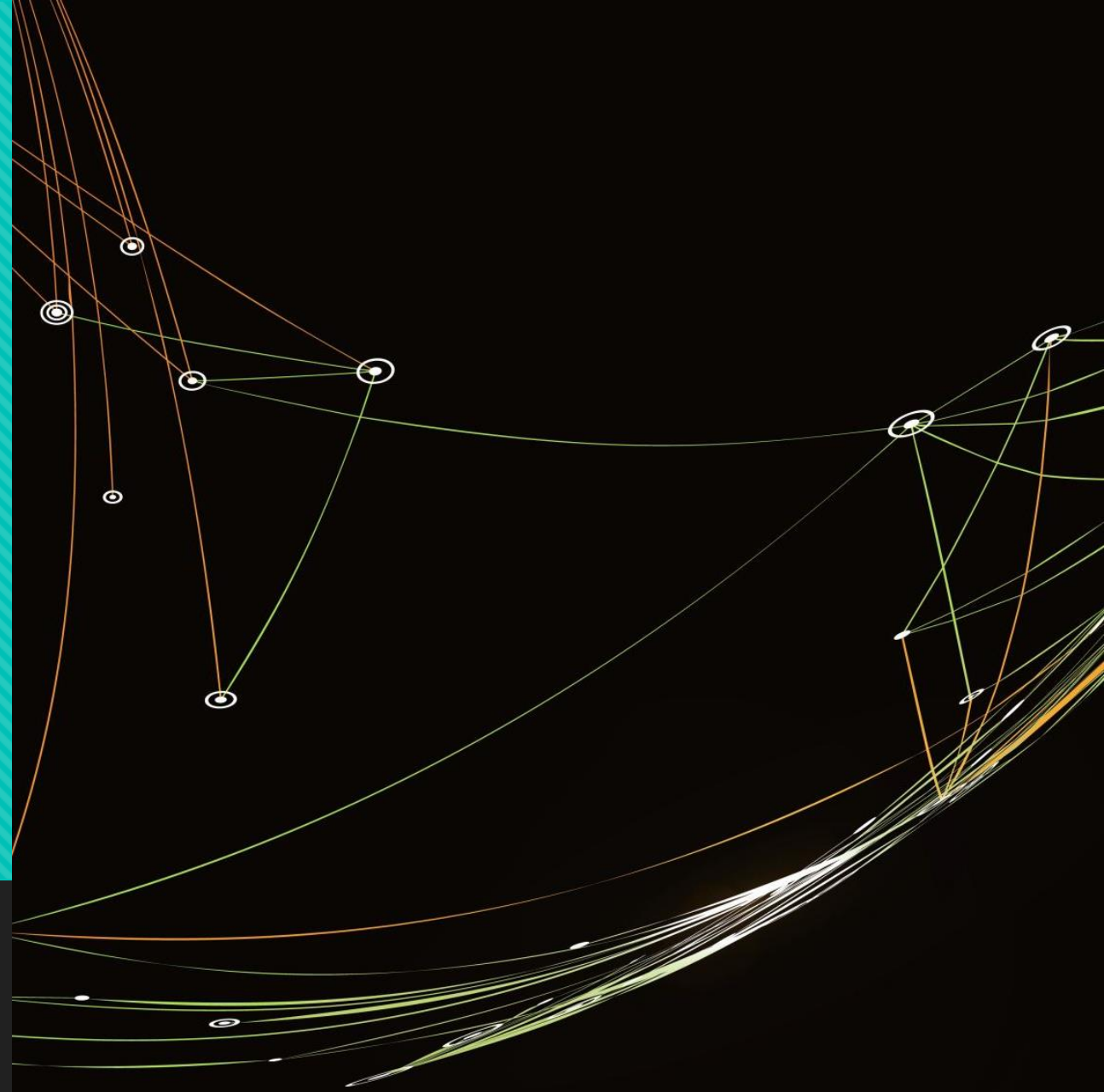


IP Address Depletion, NAT, and PAT

CO1507 Introduction to Networking
Jonathan Edwards 2024



IPv4

- What most people generally think of as IP addresses are not the only type of IP address

Typical address: 192.168.10.33

- It is class C
 - It is PRIVATE (more on this later)
 - It is IPv4
- What you are referring to is an **IPv4** IP address
- IPv4 is the fourth version of the Internet Protocol (IP)
- IPv4 was the first version deployed in 1982
- IPv4 is still used to route most Internet traffic despite the development of its successor

IPv4

- IP versions **1-3** have long since been obsolete dating back as far as **1974**
- There was some speculation that the IPv4 draft originally allowed for addresses of up to 128 bits long
- **IPv4** with an address space of **32 bits** has been in use since **1982** and still widely used as of today
- **IPv5** was used by an experimental streaming protocol that was not adopted
- **IPv6** is the successor to **IPv4** with development dating back to **1995**
- Adoption of IPv6 has been (very) slow

IPv4 Limitations

- We initially used **classful addressing** which was not flexible enough to satisfy today's needs:
- **Class A** – 16,777,216 addresses per network
 - 1.0.0.0 – 127.255.255.255
 - **24-bit** host address space
- **Class B** – 65,536 addresses per network
 - 128.0.0.0 – 191.255.255.255
 - **16-bit** host address space
- **Class C** – 256 addresses per network
 - 192.0.0.0 – 223.255.255.255
 - **8-bit** host address space

IPv4 Limitations

- When requesting IP addresses companies were allocated Class A, B, or C address spaces
- No-one thought they were in short supply, there was 4.3 billions of them after all (2^{32}).
- However, this was when users of the internet were primarily large corporations and academic institutions only
- Today we live in a world of home computers, smartphones, and many other devices ALL with access to the internet
- By the 1990s there were already fears we would run of our IPv4 IP addresses

IPv4 Limitations

- In 1998 the IETF* introduce a draft of the **IPv6**
- ARIN** announce in September 2015 that we've officially run out of the **IPv4** addresses
- **IPv6** is ratified as an internet standard in July 2017
- **IPv6** remains the long-term solution to IP address depletion
- However, as of 2024 **IPv4** is still widely used
- It is thought that only **35%** of Google's traffic is routed using **IPv6**

* Internet Engineering Task Force
** American Registry for Internet Numbers

Solutions

- Short-Term (at this point 'short-term' has been nearly 30 years)
 - Custom Subnetting
 - Private IP address ranges
 - Network Address Translation (NAT)
 - Proxies etc.
- Long-term
 - Adoption of IPv6

Private IP Address Ranges

○ 10.0.0.0 – 10.255.255.255	16, 777, 216 addresses	(10.0.0.0 /8)
○ 172.16.0.0 – 172.31.255.255	1, 048, 576 addresses	(172.16.0.0 /12)
○ 192.168.0.0 – 192.168.255.255	65, 536 addresses	(192.168.0.0 /16) *
○ 224.0.0.0 – 239.255.255.255	268, 435, 456 addresses	(224.0.0.0 /4) **

*192.168.0.0/16 addresses are **commonly** used as /24 utilising just one of 256 subnets.

**multicast – we haven't covered this (and won't be doing)

Private IP Address Ranges

- **Private IP** ranges are reserved for private network use
- They are not traceable because they are not assigned to any organization, and it is not possible to find IP location for these ranges
- **Private IP** addresses will never be part of the internet or routed outside of a local area network
- **Private IP** addresses can be used in every home, public building, and business in the world
- You probably have a 192.168.0.0 /24 Wi-Fi network at home
- However, 192.168.x.x is **NOT** your IP address externally to the wider world when you go online

Network Address Translation (NAT)

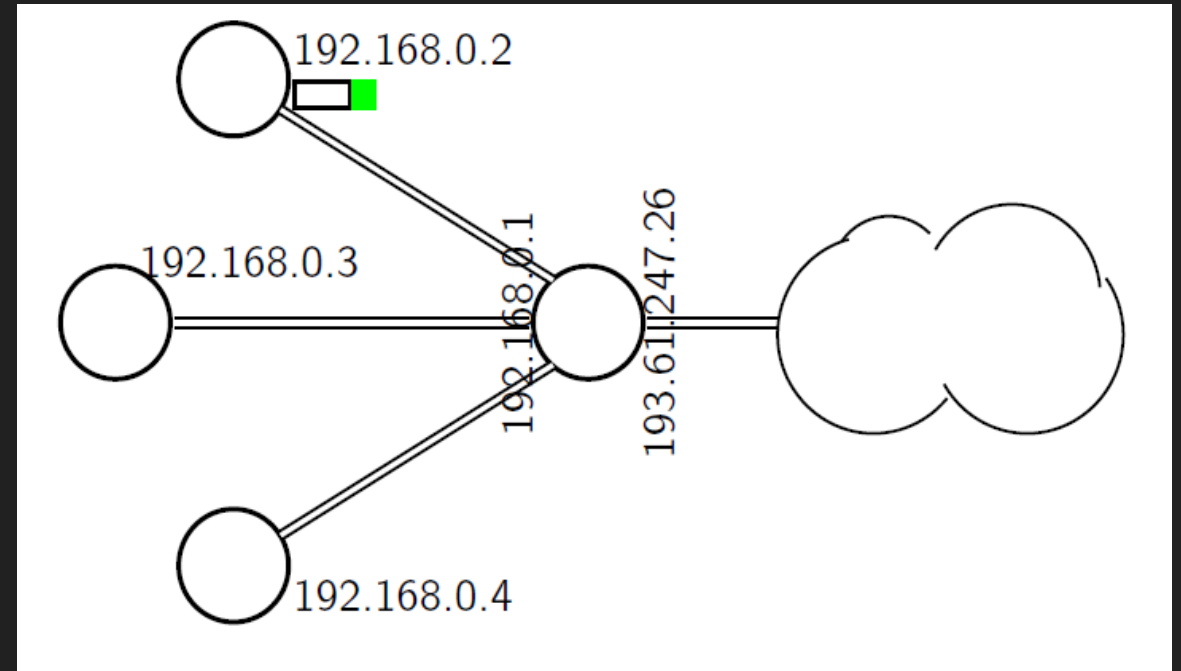
- **Network address translation (NAT)** is a way to conserve IP addresses
- It can be used to hide multiple hosts behind a single IP address
- **NAT** is a router function where IP addresses (and possibly port numbers) of IP datagrams are replaced at the boundary of a private network
- **NAT** is a method that enables hosts on **private networks** to communicate with hosts on the **internet**
- **NAT** is run on routers that connect private networks to the public Internet to replace the IP address and port pair of a **packet** with another IP address and port pair

Types of Network Address Translation

- **S**tatic **N**etwork **A**ddress **T**ranslation (SNAT)
- **D**ynamic **N**etwork **A**ddress **T**ranslation (DNAT)
- **P**ort **A**ddress **T**ranslation (**PAT**) a.k.a. 'NAT overload'

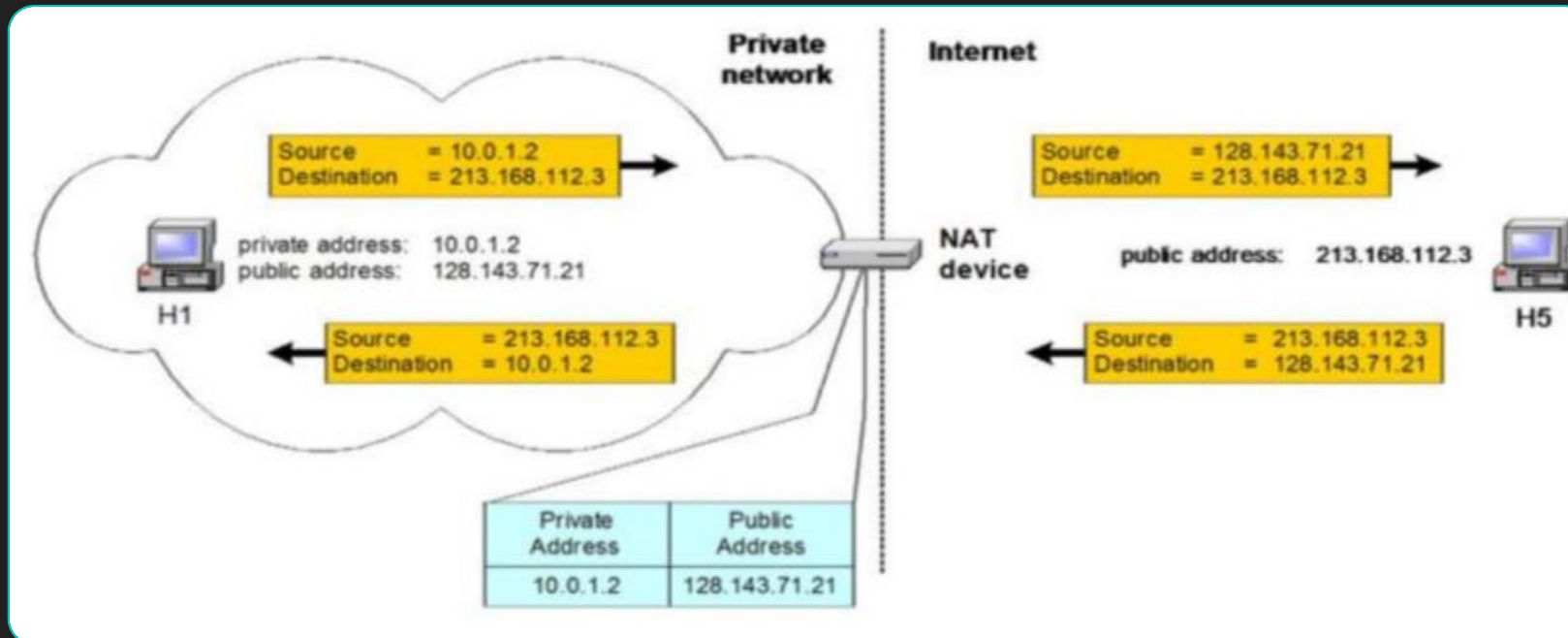
Network Address Translation

- A single IP address acts for all computers on the network
- Typically, a local network uses private address range
 - 192.168.1.0 /24 or similar is common in homes
 - UCLan network uses 10.x.x.x /24 addresses
- The internet side uses a public IP address provided by an ISP



Static NAT (SNAT)

- A NAT enabled device (such as router) has address translation table
- With static NAT one-to-one address translation is used
- Therefore you need to have 1 public IP address for every 1 private IP address



Pooling of IP Addresses

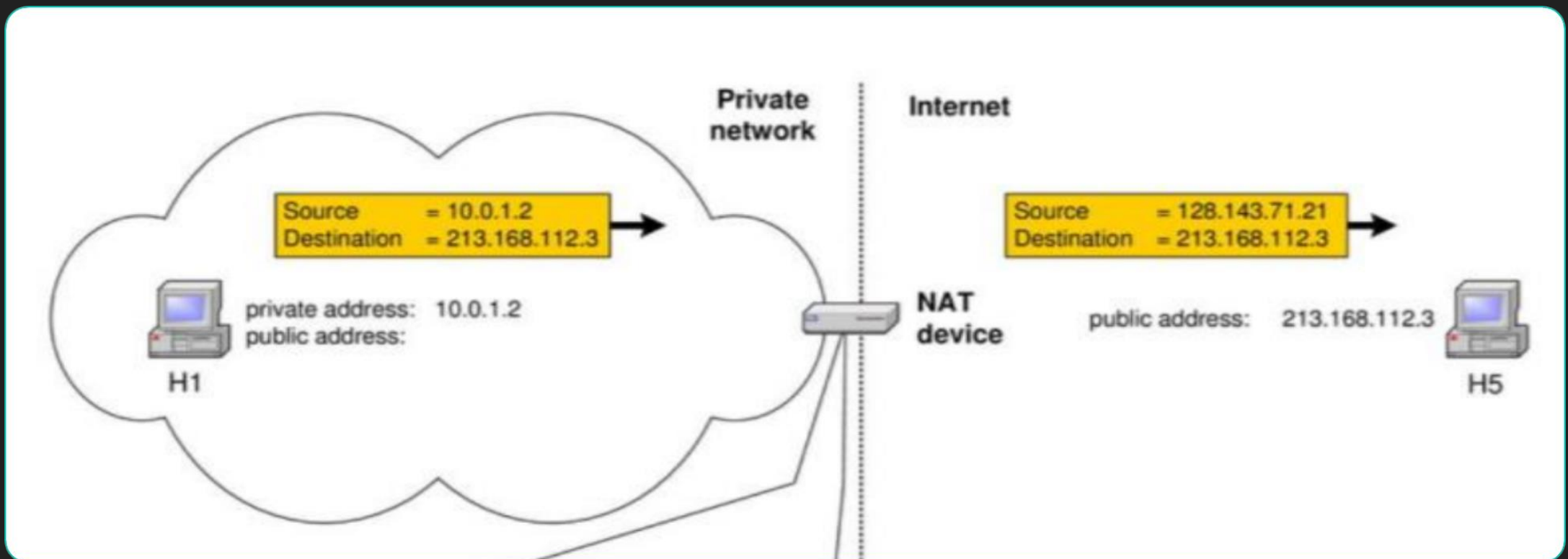
Scenario: A corporate network has **many hosts** but only a **small number** of **public IP addresses***

- NAT solution:
 - A corporate network is managed within a private IP address space
 - A NAT device, located at the boundary between the corporate network and the public **Internet**, manages a **pool** of **public** IP addresses
 - When a host from the corporate network sends an IP datagram to a host in the public **Internet**, the **NAT** device picks a public IP address from the address **pool**, and binds this address to the private address of the host

*UCLan is a good example of such as institution

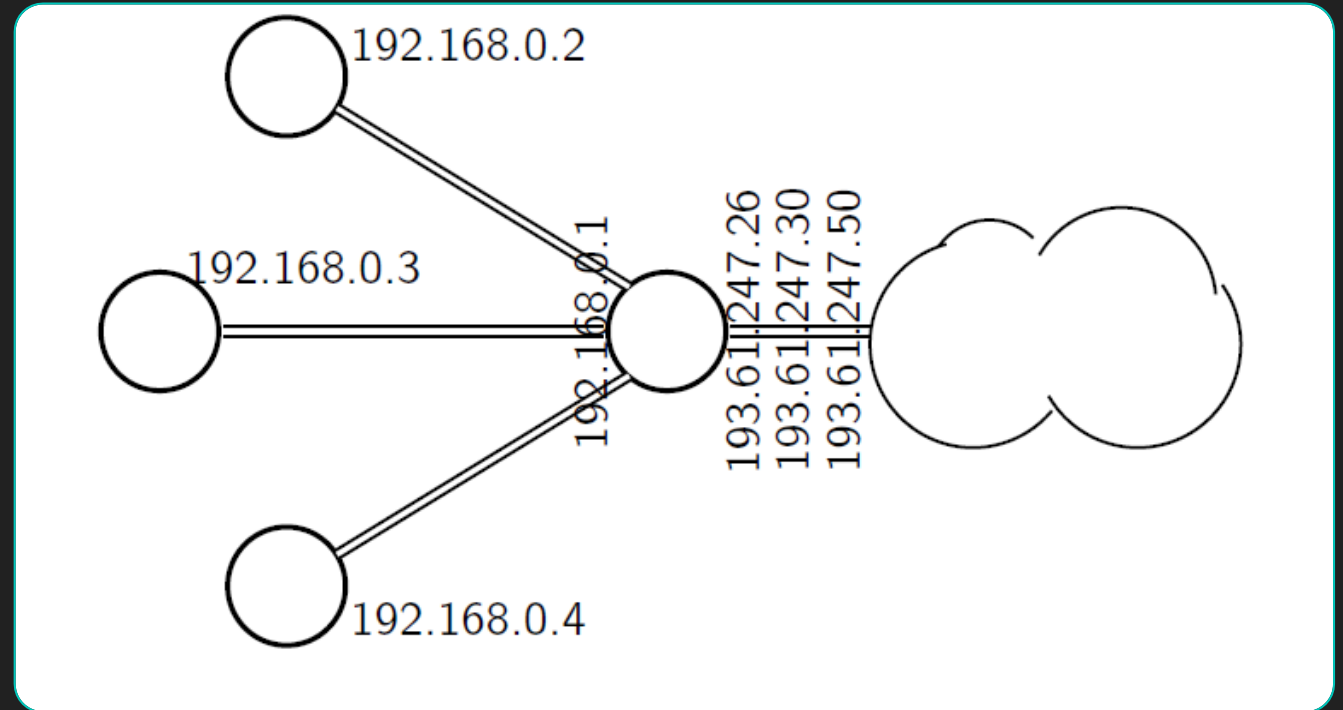
Dynamic NAT (DNAT)

- Dynamic NAT allows the NAT router to pick the public address from a list



Dynamic NAT (DNAT)

- Static NAT has a single public IP
- Dynamic NAT allows the NAT router to pick the public address from a list

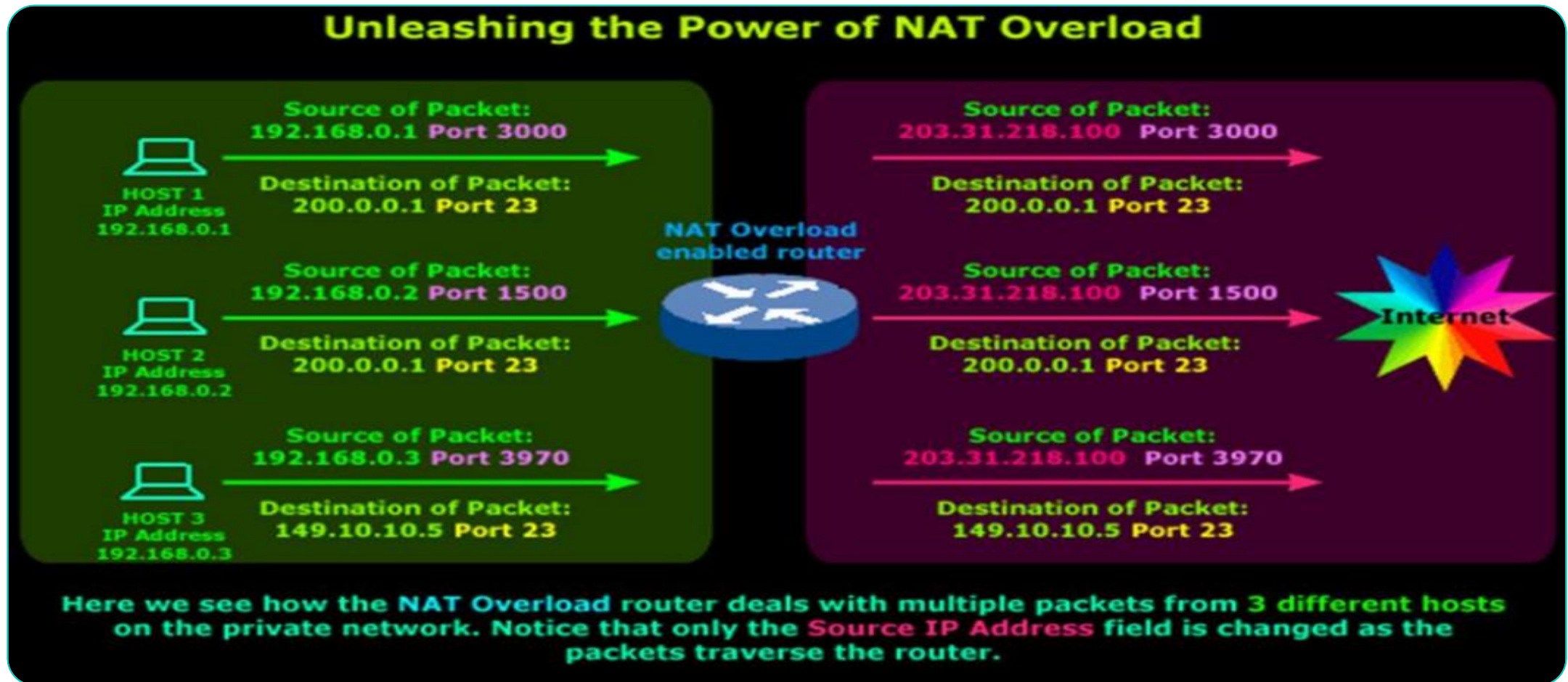


PAT (Port Address Translation)

- Port address translation (**PAT**) is the most common form of **NAT** (also called NAT overload)
- This is when **multiple local** hosts on a private network all want to be translated to a **single public** IP address (Usually used with outgoing traffic).
- Typical example is out to the internet from your home Wi-Fi
- **PAT** allows traffic from multiple local area hosts to be translated to a single public address by adding **SOURCE** port numbers to differentiate the traffic
- These are different from **destination** port numbers such as port **80** for http, port **21** for ftp etc.
- **SOURCE** port numbers are typically much higher numbers e.g. port **2222**

PAT a.k.a. 'NAT overload'

Usually used with outcoming traffic



The End.

Any questions?

