NAT (Network Address Translation)

Overview

- Primarily NAT was introduced to the world of IT and networking due to the lack of IP addresses, or looking at it from another view, due to the vast amount of growing IT technology relying on IP addresses.
- To add to this, NAT adds a layer of security, by hiding computers, servers and other IT equipment from the outside world.

How NAT works

- When computers and servers within a network communicate, they need to be identified to each other by a unique address, in which resulted in the creation of a 32 bit number, and the combinations of these 32 bits would accommodate for over 4 billion unique addresses, known as IP address.
- This was named IPv4, and although over 4 billion addresses sounds a lot, it really is not considering how fast the world of computers and the internet has grown.

How NAT works

- To circumvent this problem, a temporary solution was produced known as NAT.
- NAT resulted in two types of IP addresses, public and private.
- A range of private addresses were introduced, which anyone could use, as long as these were kept private within the network and not routed on the internet.

How NAT works

- The range of private addresses known as RFC 1918 are;
  - Class A 10.0.0.0 - 10.255.255.255
  - Class B 172.16.0.0 - 172.31.255.255
  - Class C 192.168.0.0 - 192.168.255.255

- NAT allows you to use these private IP address on the internal network.

How NAT works

- When a host on the internal network with an internal IP address does need to communicate outside it's private network, it would use the public IP address on the network's gateway to identify itself to the rest of the world, and this translation of converting a private IP address to public is done by NAT.

How NAT works

- A computer on an internal address of 192.168.1.10 wanted to communicate with a web server somewhere on the internet.
- NAT would translate the address 192.168.1.10 to the company's public address, lets call this 1.1.1.1 for example.
- So that the internal address is identified as the public address when communicating with the outside world.

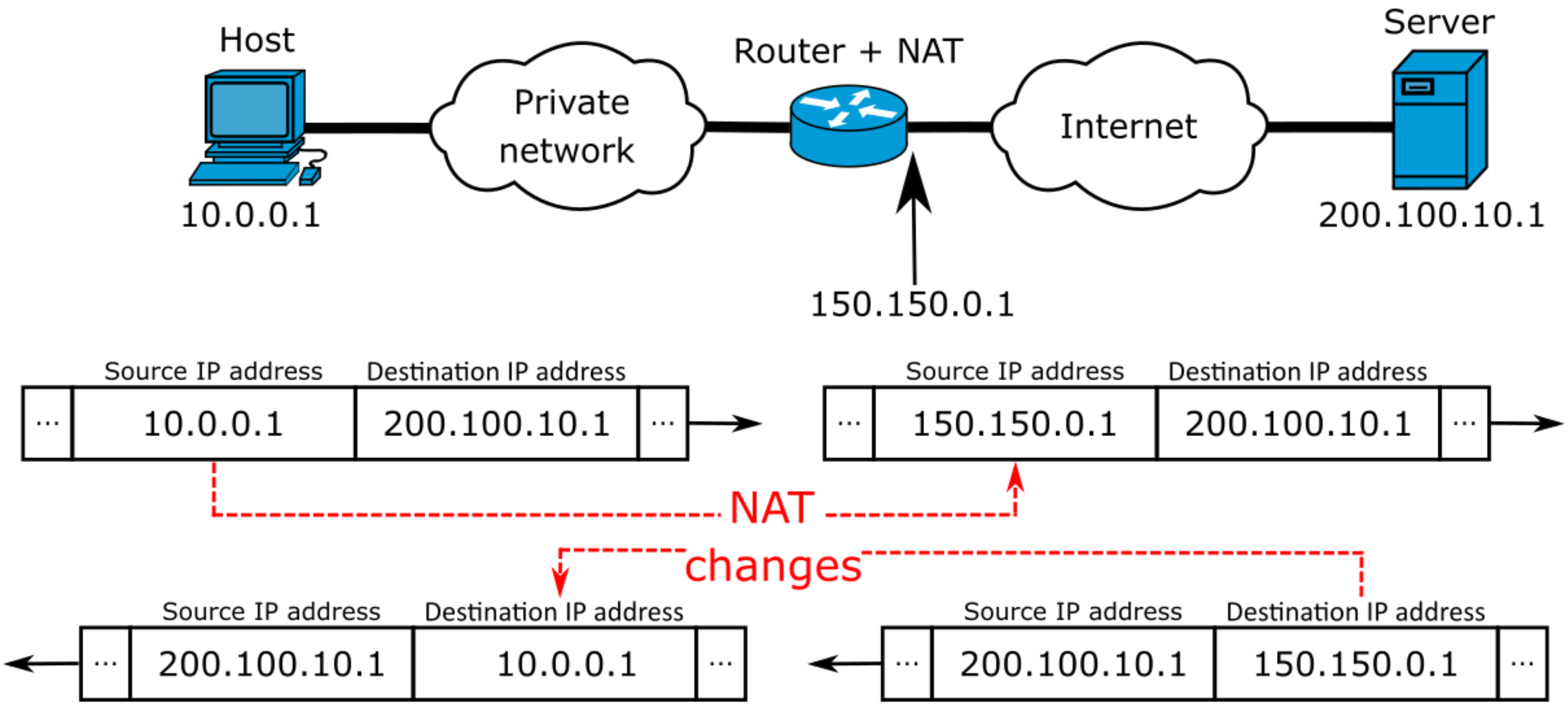
How NAT works

- This has to be done because when the web server somewhere on the internet was to reply to this internal computer, it needs to send this to a unique and routable address on the internet, the public address.
- It can not use the original address of 192.168.1.10, as this is private, none routable and hidden from the outside world.
- This address, of 1.1.1.1 would be the address of the public address for that company and can be seen by everyone.

How NAT works

- Now the web server would reply to that public address, 1.1.1.1.
- NAT would then use its records to translate the packets received from the web server that was destined to 1.1.1.1 back to the internal network address of 192.168.1.10, and though the computer who requested the original info, will receive the requested packets.

How NAT works



Host

10.0.0.1

Private network

Router + NAT

150.150.0.1

Internet

Server

200.100.10.1

	Source IP address	Destination IP address	
…	10.0.0.1	200.100.10.1	…

	Source IP address	Destination IP address	
…	150.150.0.1	200.100.10.1	…

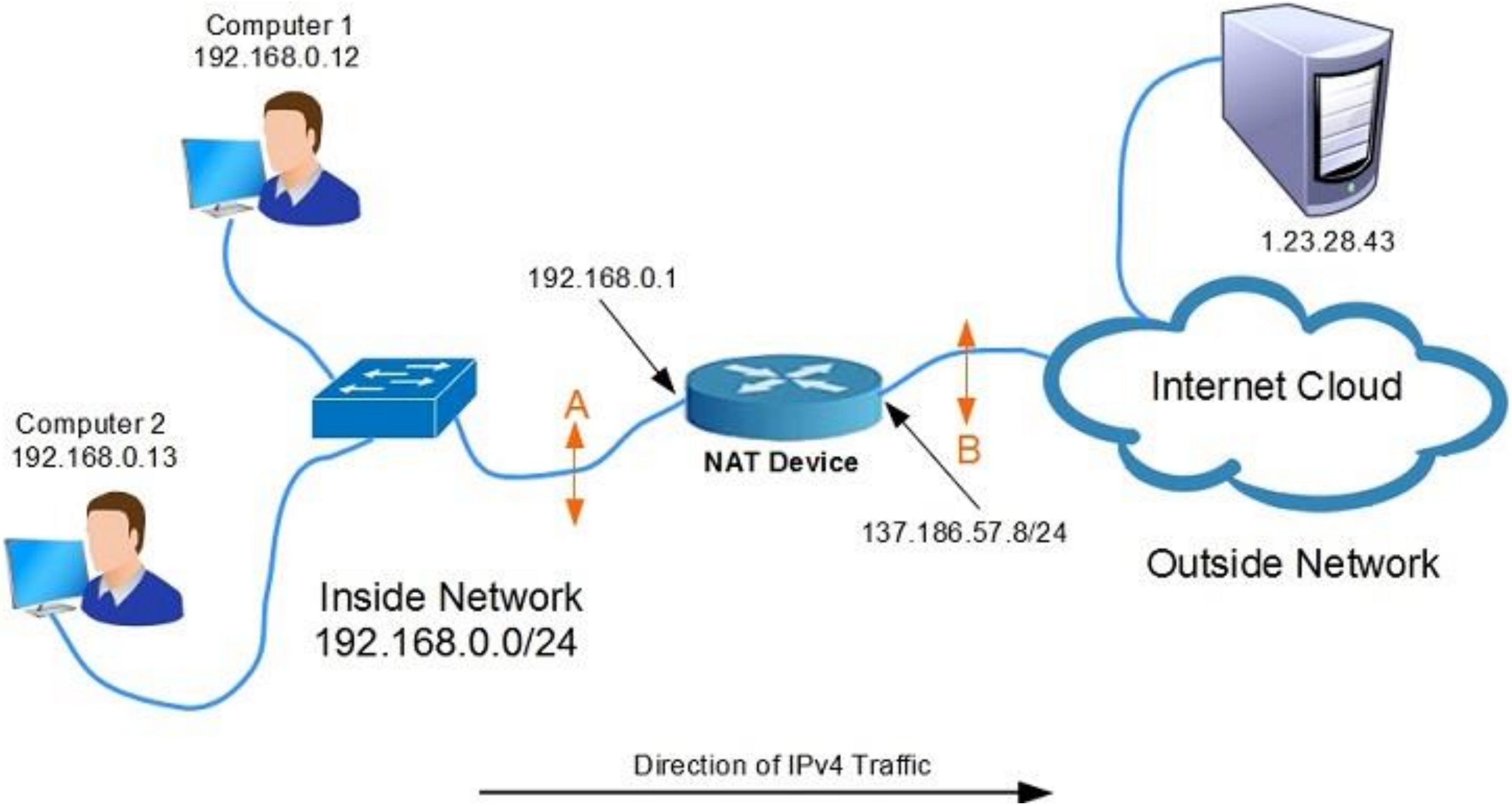
NAT

changes

	Source IP address	Destination IP address	
…	200.100.10.1	10.0.0.1	…

	Source IP address	Destination IP address	
…	200.100.10.1	150.150.0.1	…

How NAT works



NAT Types

1. Static NAT
   - When the local address is converted to a public one, this NAT chooses the same one.
   - This means there will be a consistent public IP address associated with that router or NAT device.
2. Dynamic NAT
   - Instead of choosing the same IP address every time, this NAT goes through a pool of public IP addresses.
   - This results in the router or NAT device getting a different address each time the router translates the local address to a public address.

NAT Types

3. PAT
   - PAT stands for port address translation.
   - It’s a type of dynamic NAT, but it bands several local IP addresses to a singular public one.
   - Organizations that want all their employees’ activity to use a singular IP address use a PAT, often under the supervision of a network administrator.

Advantages of NAT

- NAT conserves legally registered IP addresses .
- It provides privacy as the device IP address, sending and receiving the traffic, will be hidden.

Disadvantage of NAT

- Translation results in switching path delays.
- Certain applications will not function while NAT is enabled.
- Complicates tunneling protocols such as IPsec.
- Also, router being a network layer device, should not tamper with port numbers(transport layer) but it has to do so because of NAT.