Network Address Translation (NAT)

- Clearly Classless Addressing uses less IP addresses than Classful Addressing.
- However, there are more efficiencies that can be derived.
- Consider an ISP with many **residential** customers:
  - Typically an ISP will only allocate each customer **one** IP address.
  - However, customers will likely have multiple devices wishing to connect to the internet.
  - How is it possible for these devices to share a single IP address?
  - It's possible because of a technique called **Network Address Translation** (NAT).

Network Address Translation (NAT)

- NAT makes use of special IP addresses which reside in the **"Private"** IP Address space:

Range			*Total*
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

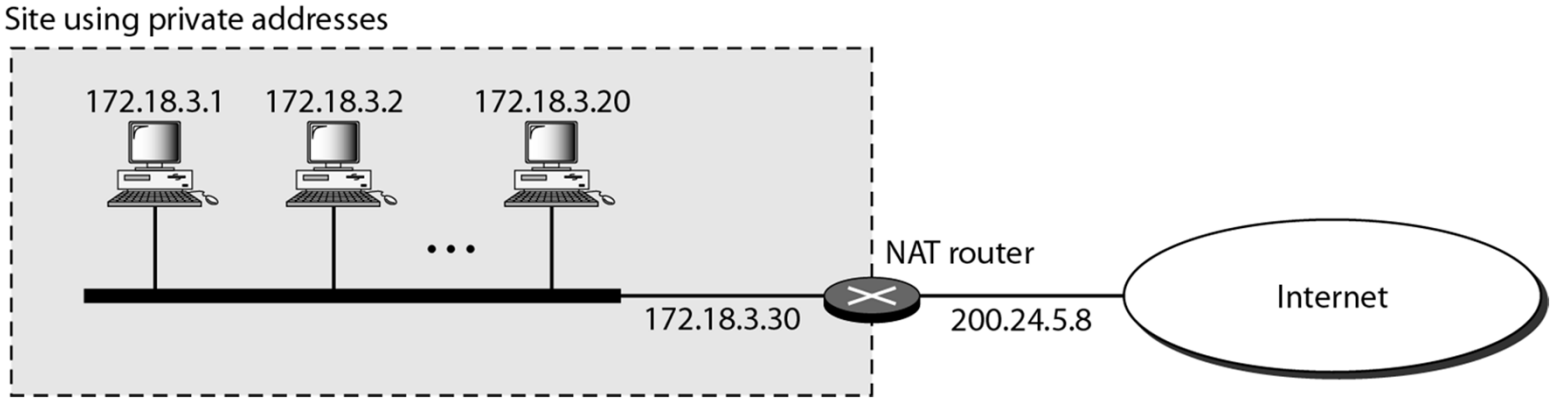
- These IP addresses **cannot** be used on the **Public** Internet:
  - Routers will **not** forward packets with addresses from these ranges.

Network Address Translation (NAT)

- NAT is employed on the customer's router:
  - It requires the use of a **NAT Table,** and,
  - The allocation of **Private** addresses within the customer's network.
- As usual the router is allocated **two** IP addresses:
  - The single IP address supplied by the ISP (the **Public** address),
  - Another address from one of the **Private** address spaces.
- **Each** host machine on the customer's network is also assigned a **Private** address from the same space.

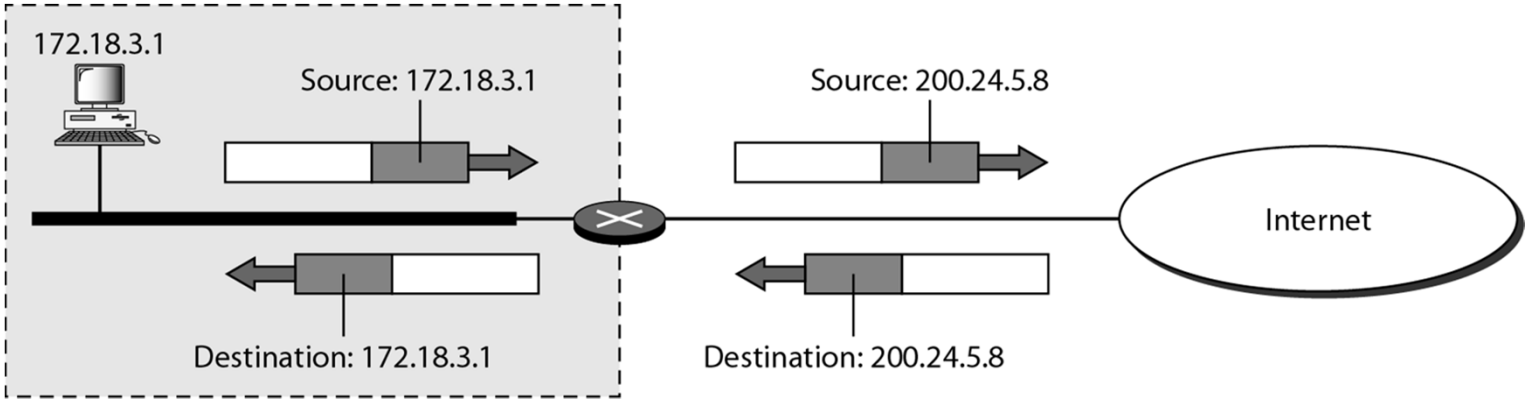
Use of **Public** and **Private** IP addresses.

- In the following example the router has:
  - **Private** address: 172.18.3.30
  - **Public** address: 200.24.5.8
- In effect the internal network on the customer's premises are isolated from the public network by the router.



Traffic between the Private and Public networks.

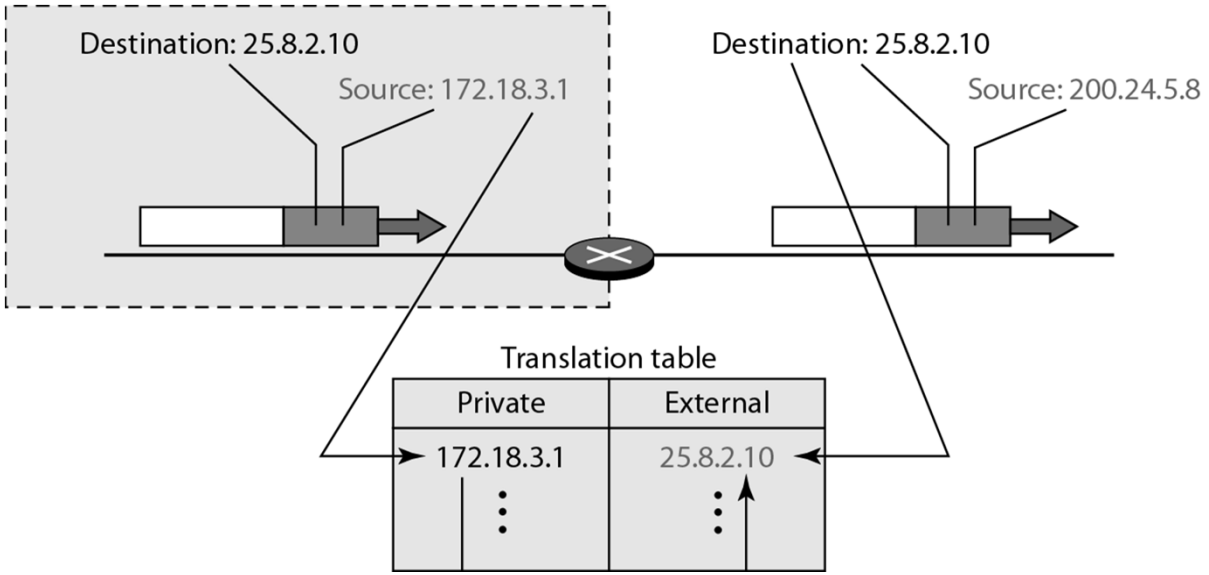
- All datagrams leaving the customer's network can only contain Public IP addresses:
  - Likewise, all datagrams arriving at a host on the customer's network must only contain Private IP addresses in the Destination field.



- This requires some form of **address translation.**

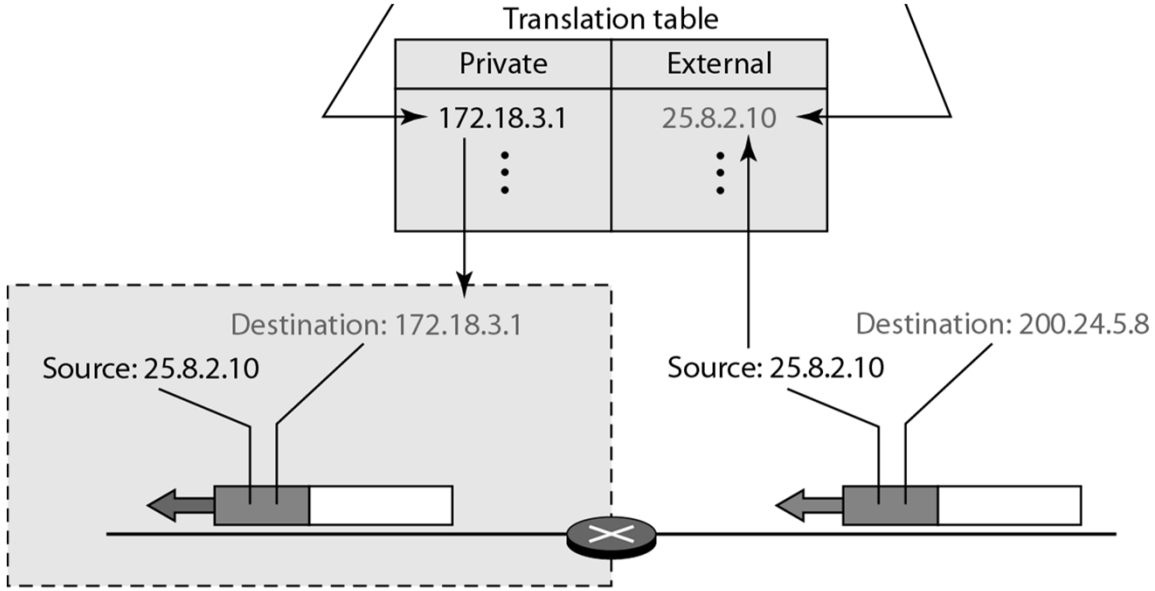
Operation of NAT – Outgoing Datagrams

- For datagrams *leaving* the **Private** network the router performs the following actions:
  - It enters the source (*private* address) and destination (a *public* address) IP addresses into a NAT Table,
  - It changes the source IP address in the datagram to its own *public* address.



Operation of NAT – Incoming Datagrams

- For datagrams *arriving* from the *public* network the router performs the following actions:
  - It uses the source address to query the NAT Table to determine which *private* address it is destined for,
  - It changes the destination address in the datagram to the correct private address.



Restrictions of NAT

- The use of a single *public* address imposes a limit:
  - Two or more host machines on the customer's *private* network cannot communicate with the same public host simultaneously,
  - This is because there would be two entries in the NAT Table associated with the same public address. This would cause queries to the NAT Table to fail.
- To address this restriction the customer could be allocated multiple public addresses (a *pool* of IP addresses):
  - For each additional public address assigned one additional private host can communicate with the same public host.

Restrictions of NAT

- Additional restrictions include:
  - Only one router can be used as there can only be one NAT table.
  - Communications must originate from within the customer's network.
- These restrictions do not suit many business customers
  - Consequently NAT is really only used for residential users.