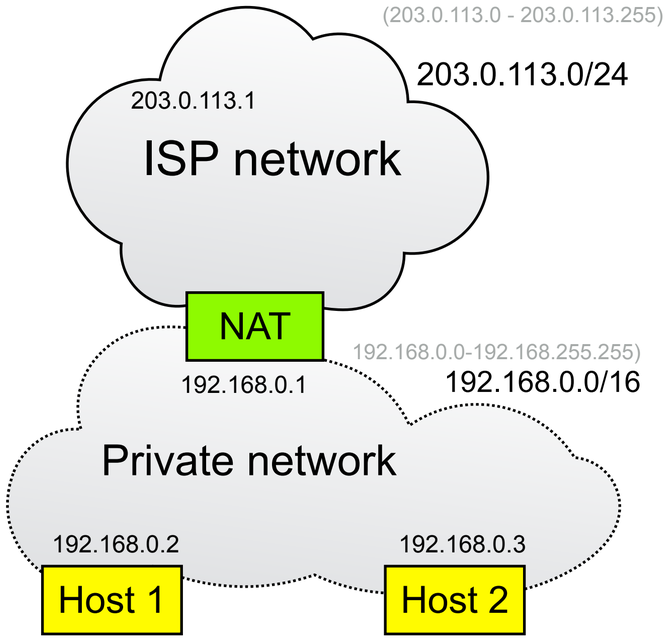
Problems due to Network Address Translation

- Problems due to NAT
- Why use NAT?
- Implications of NAT

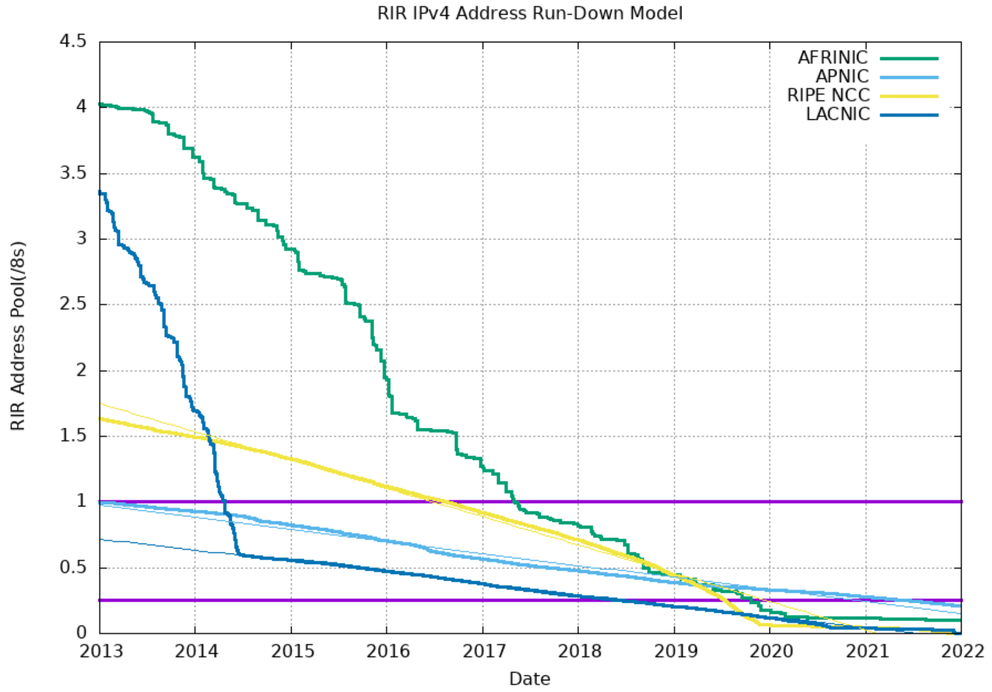
NAT Routers Encourage Centralisation



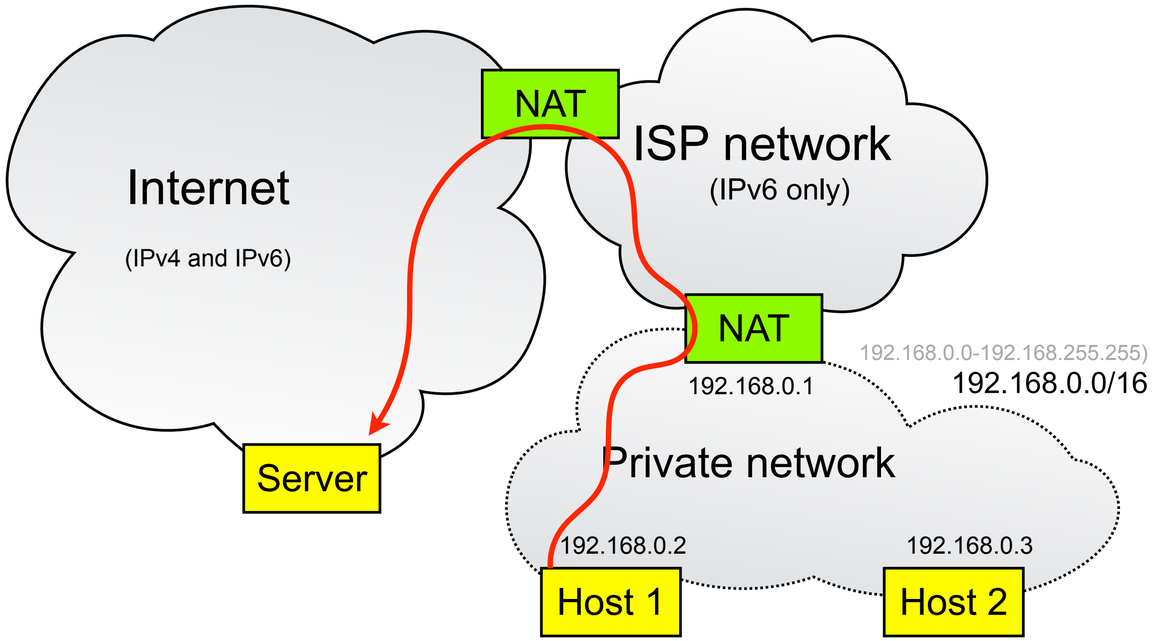
- Client-server applications with client behind NAT work without changes – web and email
- Client-server applications with server behind NAT fail – need explicit port forwarding
- Peer-to-peer applications fail – complex NAT traversal algorithm needed to connect
- Encourages centralisation of services

NAT Breaks Applications – Why Use It? (1/3)

- To work around lack of IPv4 address space:
  - Many ISPs have insufficient IPv4 addresses to give their customers a large enough prefix – each customer given one IPv4 address and a NAT
  - Many customers don't want to pay their ISP for more IPv4 addresses – addresses are scarce, so expensive
  - IPv6 is designed to make addresses cheap and plentiful, to avoid these problems



NAT Breaks Applications – Why Use It? (2/3)



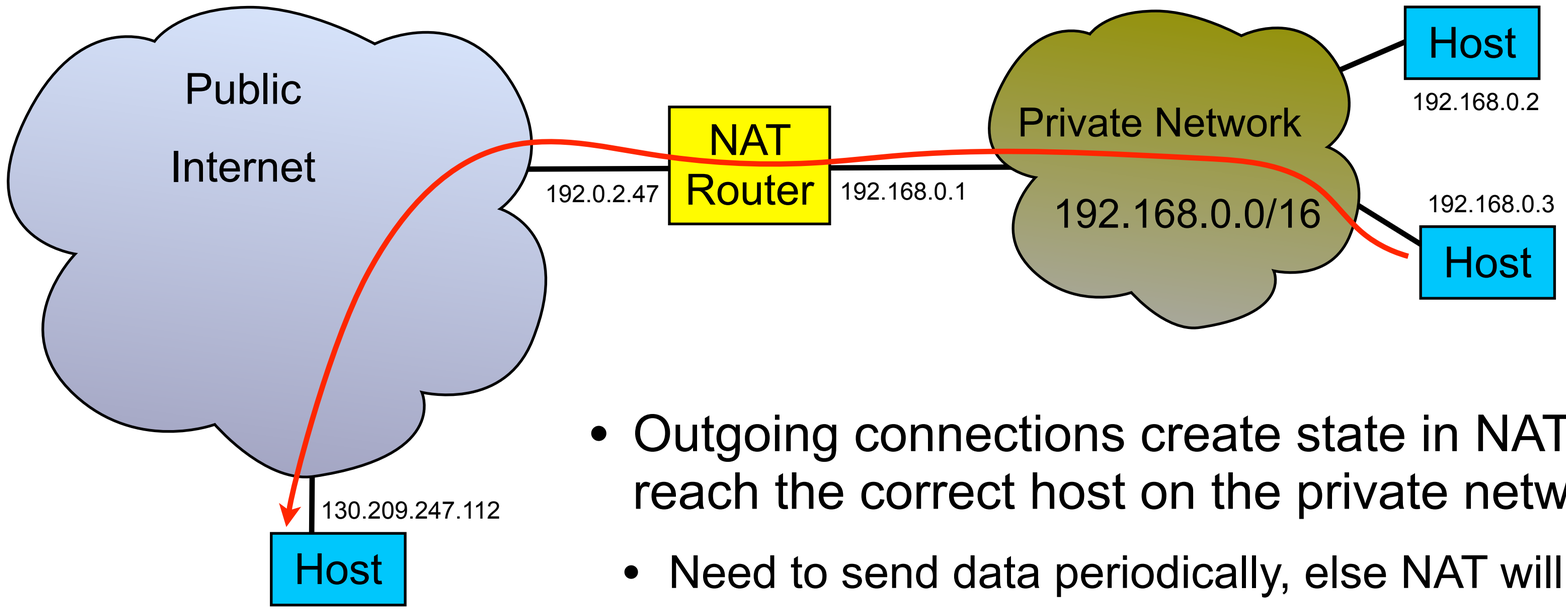
- To translate between IPv4 and IPv6 addresses
  - ISP network runs IPv6 only; customers use public IPv6 addresses
  - Translate IPv4-to-IPv6 as packets leave private network
    - If destined for IPv4 host on the Internet, translate back to IPv4 on leaving ISP network
    - If destined for IPv6 host on the Internet, forward directly
  - May be useful if ISP has more customers than it has IPv4 addresses

NAT Breaks Applications – Why Use It? (3/3)

- To avoid re-numbering a network when changing to a new ISP
  - Hard-coding IP addresses, rather than DNS names, in configuration files and application is a bad idea
  - Many people do it anyway – makes changing IP addresses difficult
  - IPv6 tries to make renumbering networks easier, by providing better auto-configuration
    - Insufficient experience to know how well this works in practice
    - Some vendors also offer IPv6-to-IPv6 NAT to ease renumbering

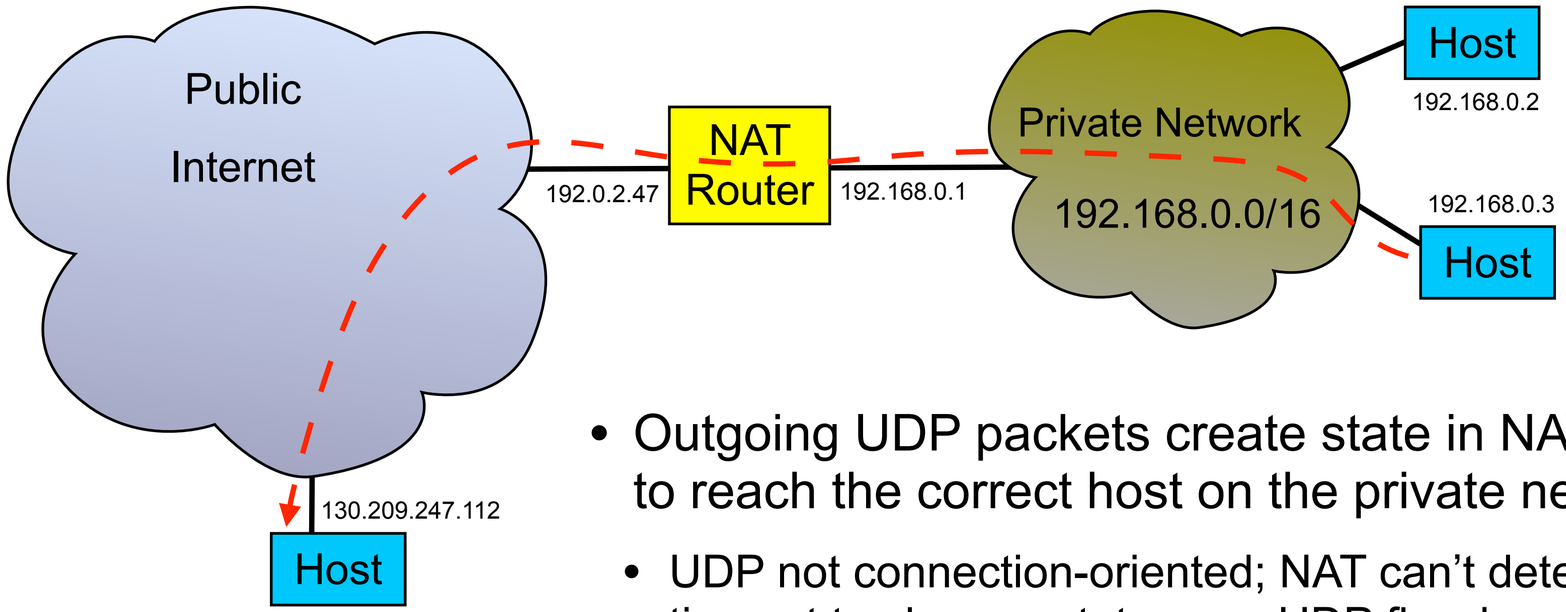
[RFC 6296]

Implications of NAT for TCP Connections



- Outgoing connections create state in NAT, so replies can be translated to reach the correct host on the private network
  - Need to send data periodically, else NAT will assume the connection has failed
  - Recommended time out interval is 2 hours, many NATs use shorter [RFC5382]
- No state for incoming connections
  - NAT can't know where to forward incoming connections, without manual configuration
  - Complicates running a server behind the NAT, or peer-to-peer applications

Implications of NAT for UDP Flows



- Outgoing UDP packets create state in NAT, so replies can be translated to reach the correct host on the private network
  - UDP not connection-oriented; NAT can't detect the end of a flow, so use short timeout to cleanup state once UDP flow has stopped
    - UDP NAT traversal standards suggest sending a keep-alive every 15 seconds [RFC4787]
- No state for incoming connections
  - UDP NATs often more permissive about allowing incoming packets than TCP NATs; many allow replies from anywhere to an open port – simpler for peer-to-peer traffic

Problems due to Network Address Translation

- Problems due to NAT
- Why use NAT?
- Implications of NAT