University of Glasgow

School of Computing Science

60 YEARS OF COMPUTING AT GLASGOW

Network Address Translation

Networked Systems (H)

Lecture 16

Lecture Outline

- What is Network Address Translation (NAT)?
- Implications for transport protocols
  - TCP
  - UDP
- NAT traversal

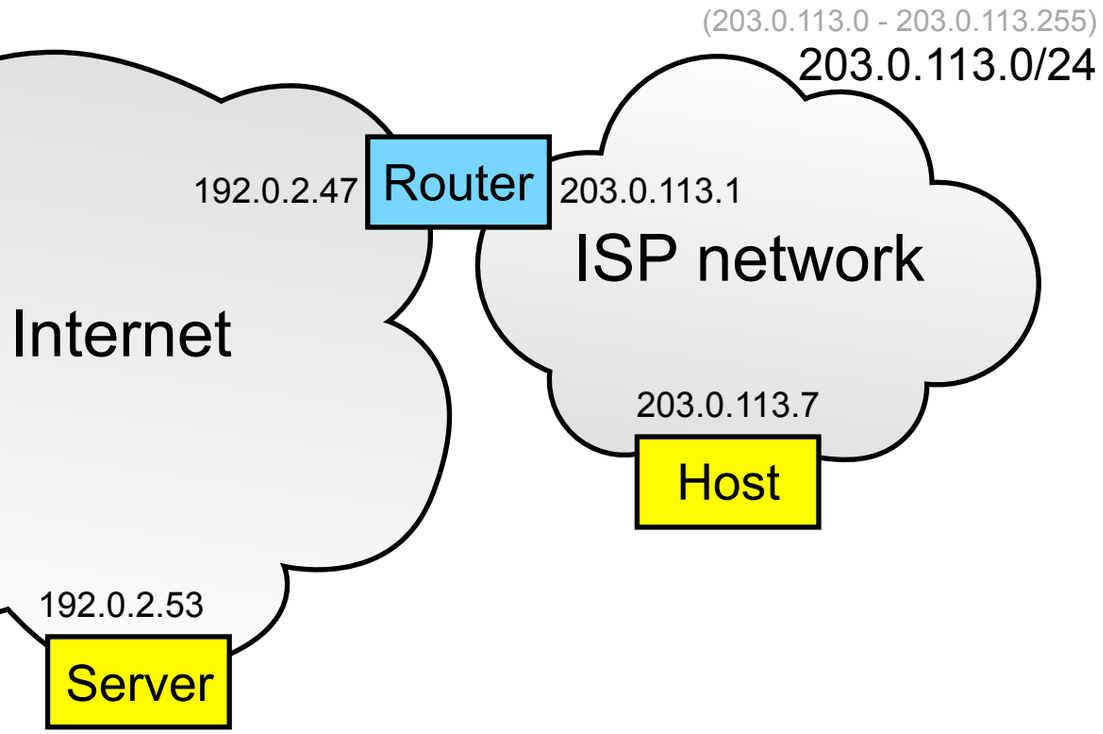
Network Address Translation

- IPv4 address space is exhausted
- IPv6 is the long-term solution

- There is a widely deployed work-around: NAT (network address translation)

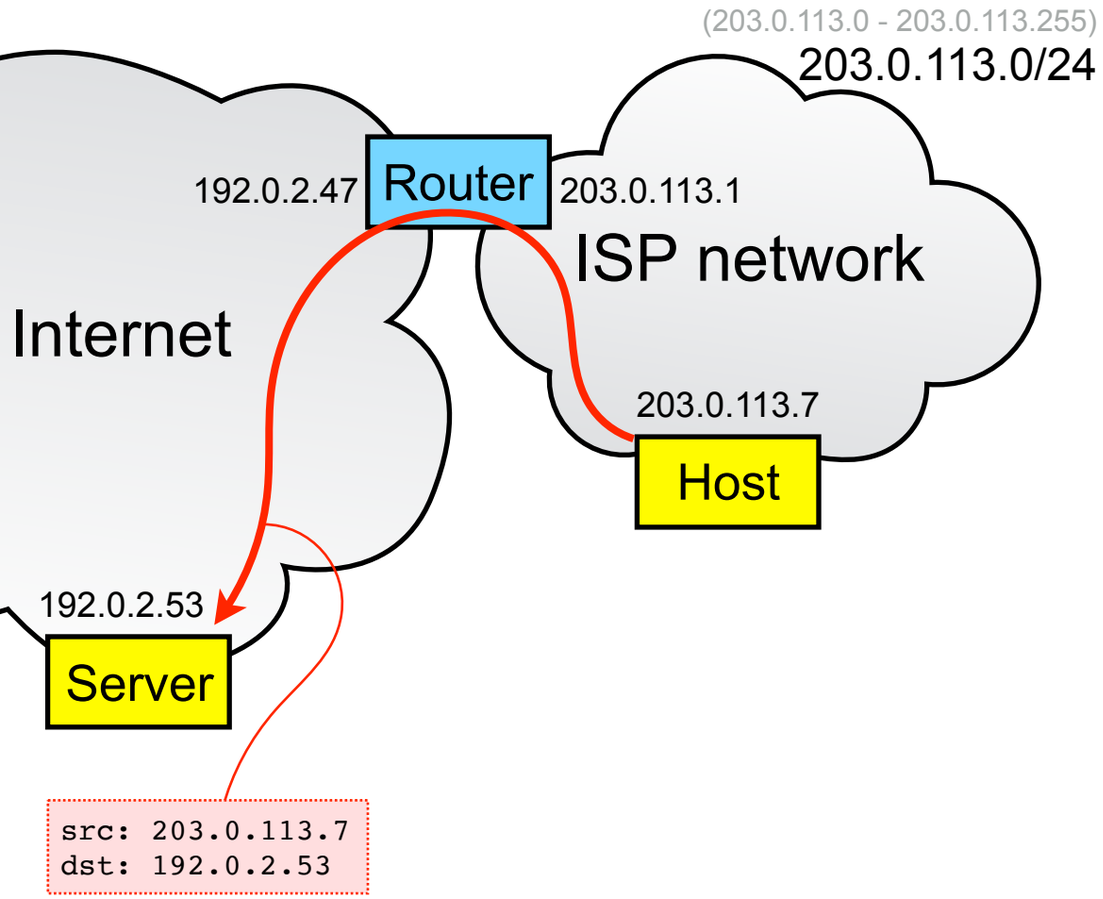
- However, this has serious consequences for the transport layer

Connecting a Single Host



- An Internet service provider owns an IP address prefix
- They assign a customer a single address for a single host

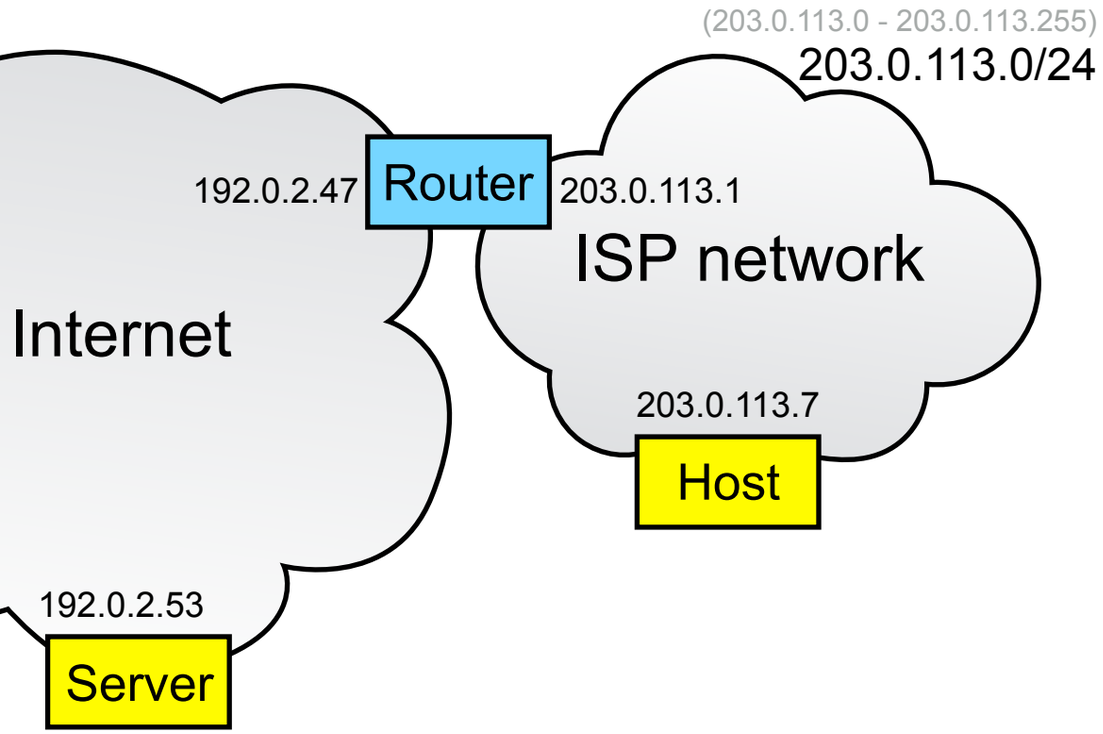
Connecting a Single Host



- An Internet service provider owns an IP address prefix
- They assign a customer a single address for a single host

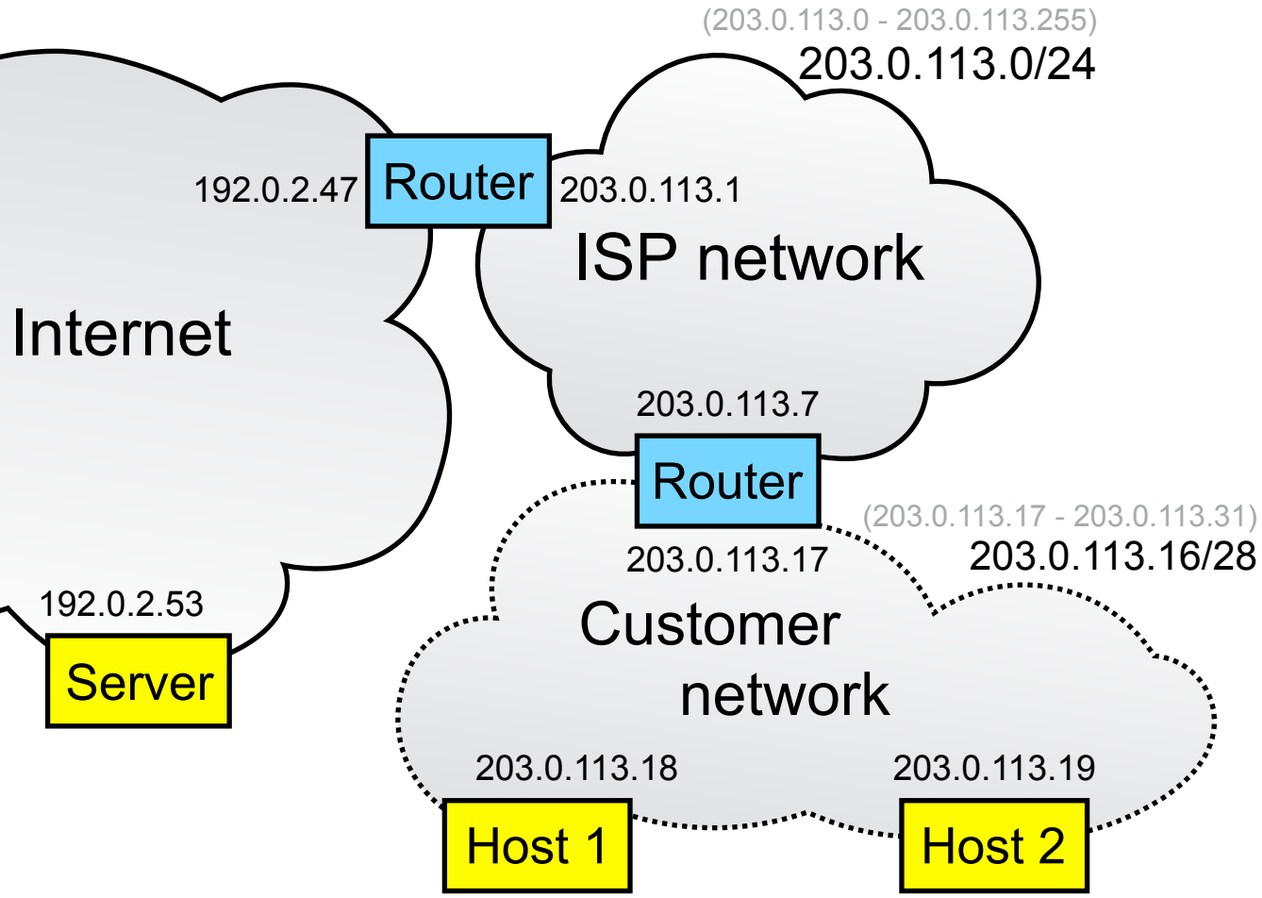
- No address translation

Connecting Multiple Hosts



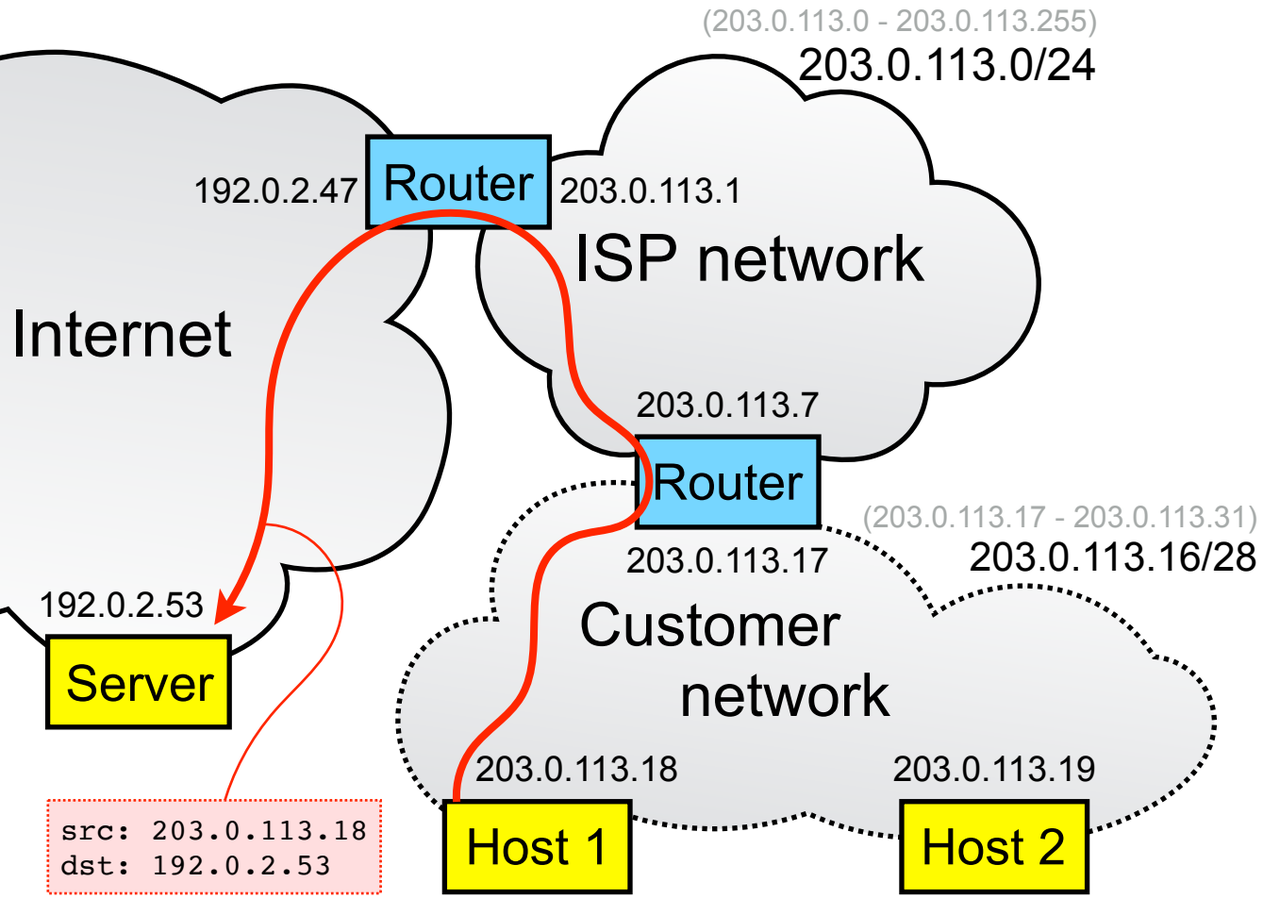
- The customer buys another host
- How does it connect?

Connecting Multiple Hosts



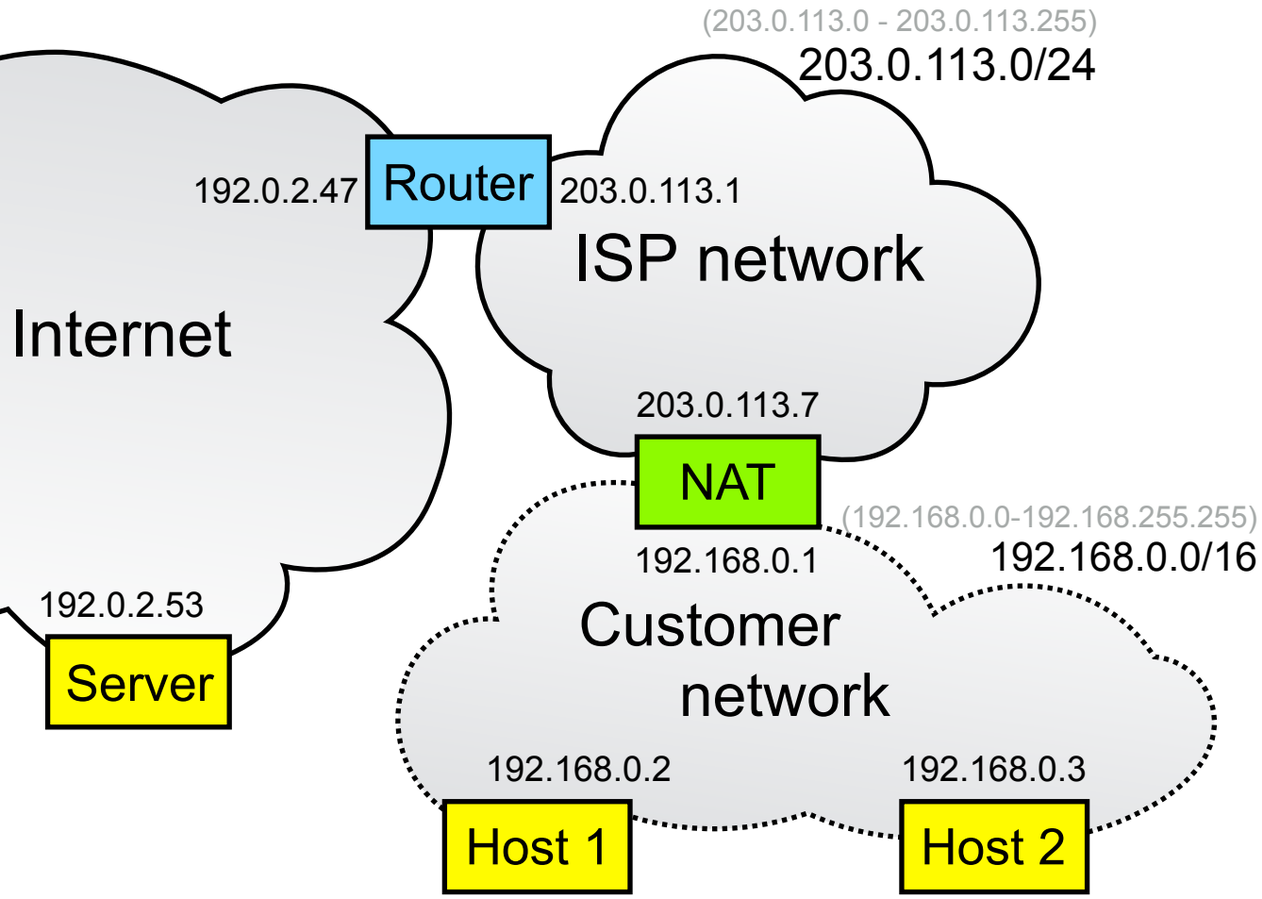
- The customer buys another host
- How does it connect?
- What's supposed to occur:
  - Customer acquires a router, which gets the customer's previous IP address
  - ISP assigns new range of IP addresses to customer (from the ISP's prefix)
  - Customer gives each host an address from that new range

Connecting Multiple Hosts



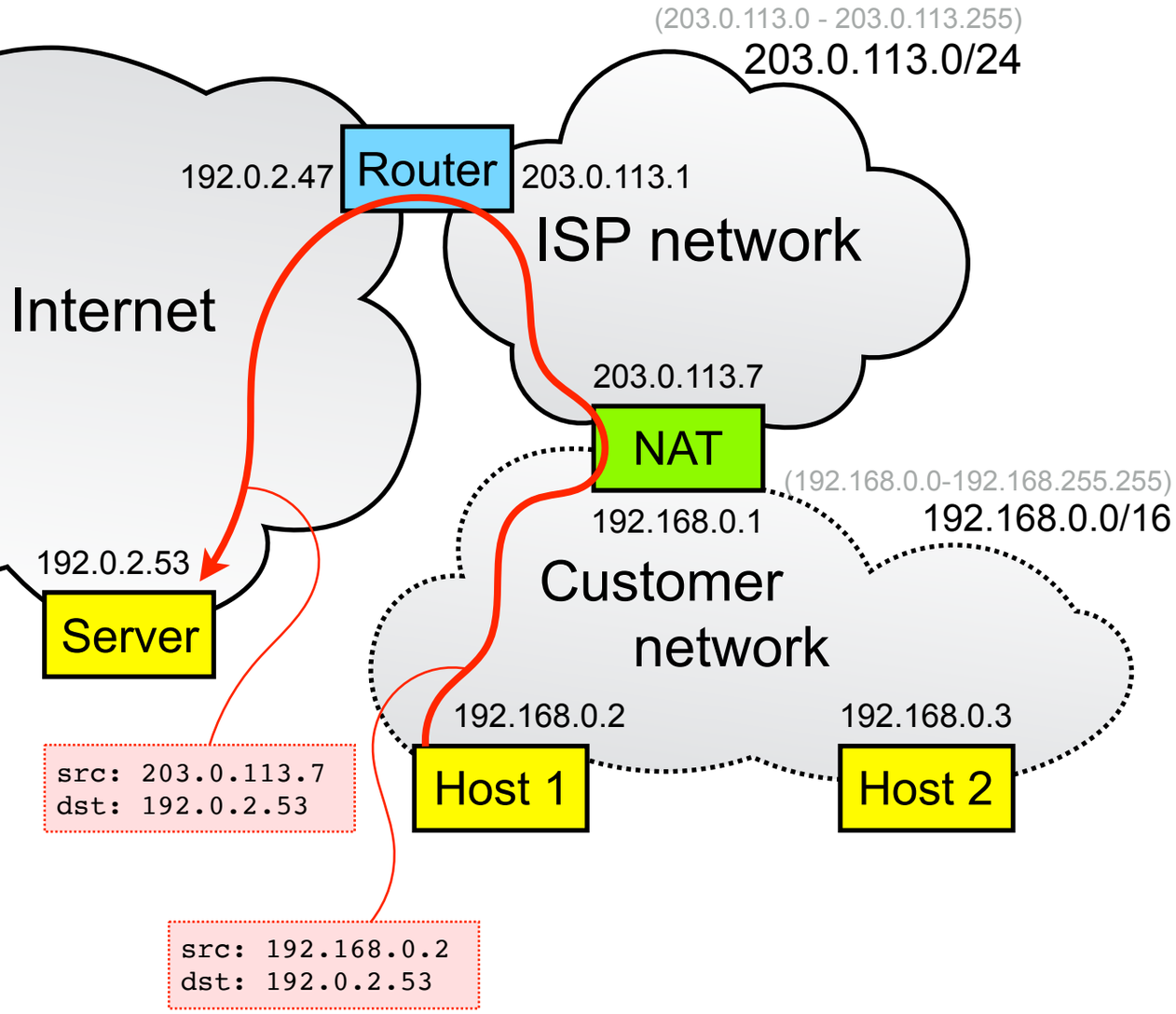
- The customer buys another host
- How does it connect?
- What's supposed to occur:
  - Customer acquires a router, which gets the customer's previous IP address
  - ISP assigns new range of IP addresses to customer (from the ISP's prefix)
  - Customer gives each host an address from that new range
  - No address translation

Network Address Translation



- The customer buys another host
- How does it connect?
- What actually happens:
  - Customer acquires a NAT, which gets the customer's previous IP address
  - Customer gives each host a private address

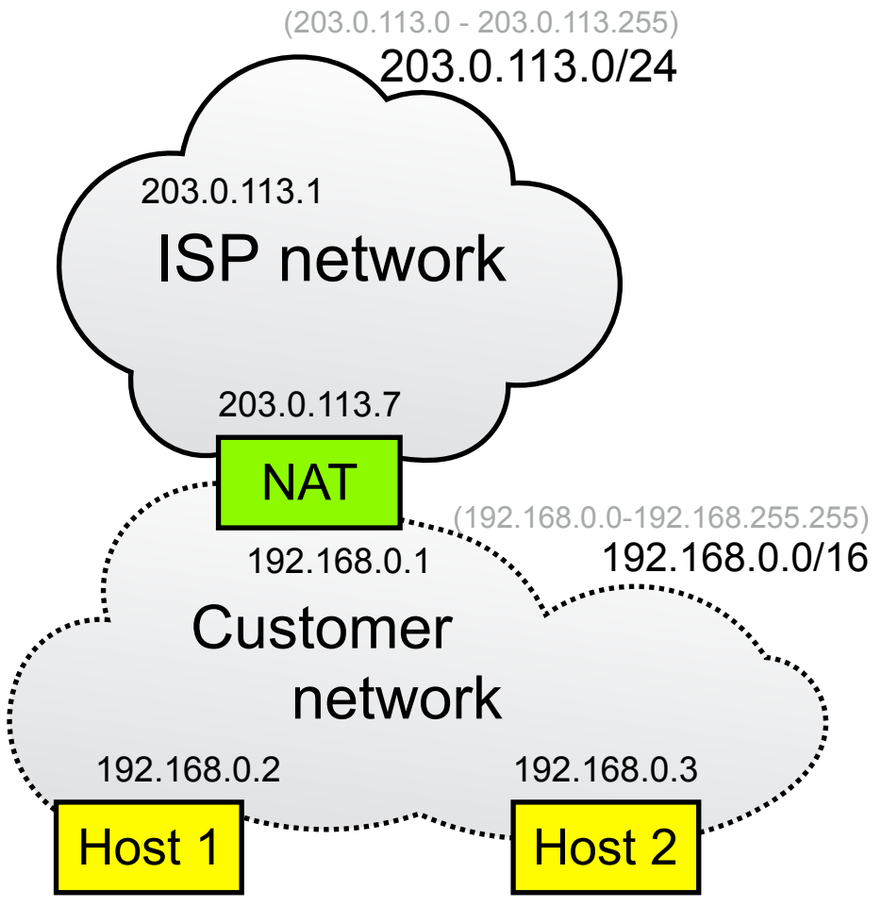
Network Address Translation



- The customer buys another host
- How does it connect?
- What actually happens:
  - Customer acquires a NAT, which gets the customer's previous IP address
  - Customer gives each host a private address
  - NAT performs address translation – rewrites packet headers to match its external IP address

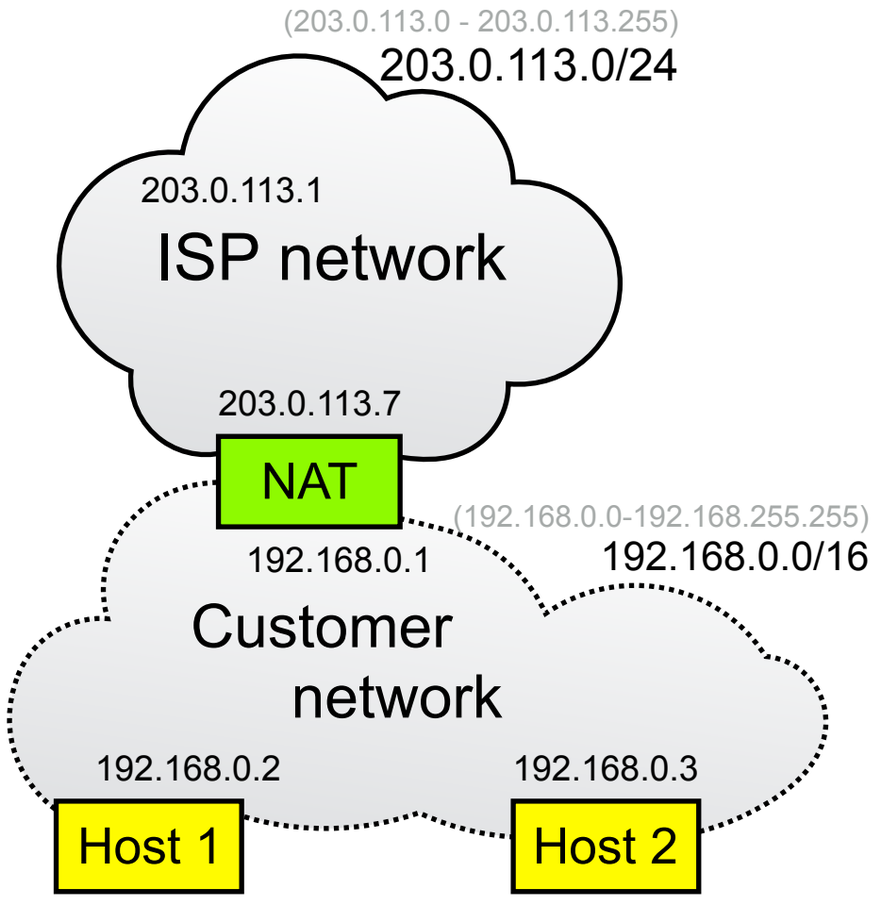
    (likely also rewrites the TCP/UDP port number)

NAT and Private Address Ranges



- The NAT hides a private network behind a single public IP address
- Private IP network addresses:
  - 10.0.0.0/8
  - 176.16.0.0/12
  - 192.168.0.0/16
- Tries to give the illusion of more address space

Problems due to NAT



- Many applications fail with NAT:
  - 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 ICE algorithm needed to connect
- NAT provides no security benefit:
  - Most NATs also include a firewall to provide security, but NAT function gives no security or privacy benefits

Why use NAT? (1)

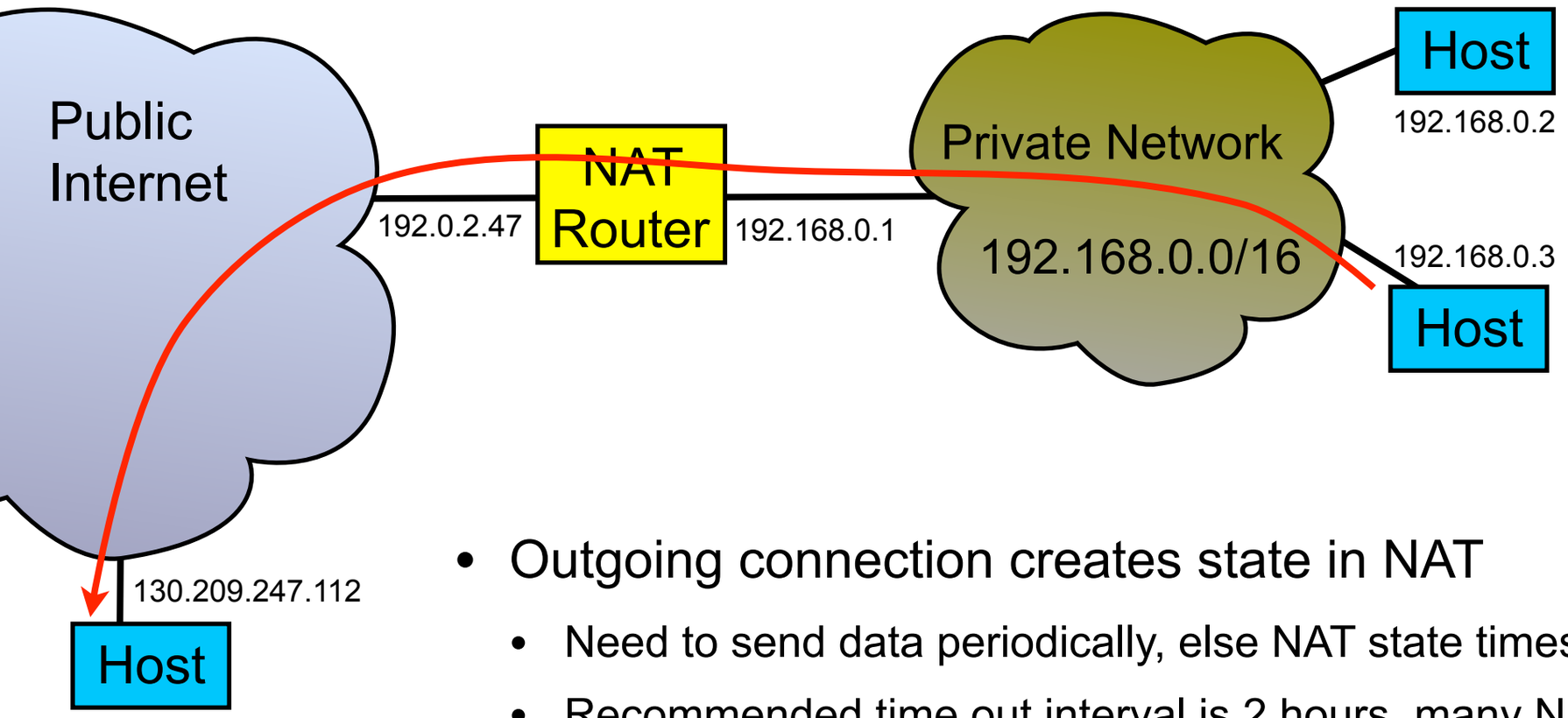
- NAT breaks many applications – so why use it?
  - Many ISPs have insufficient addresses to give customers their own prefix
  - Many customers don't want to pay their ISP more addresses

- Both problems due to limited IPv4 address space
  - IPv6 is designed to make addresses cheap and plentiful, to avoid these problems

Why use NAT? (2)

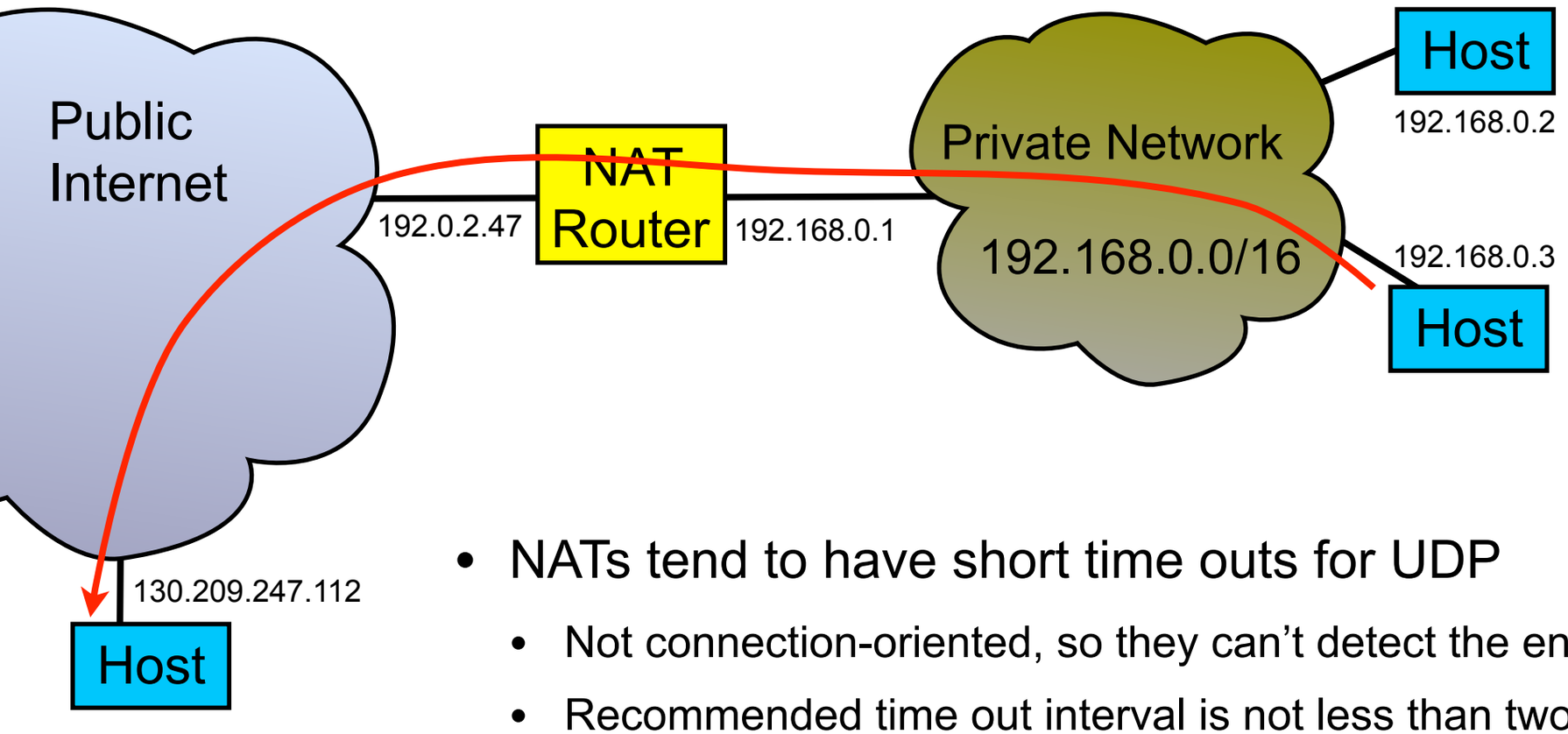
- To avoid re-numbering a network when changing to a new ISP
  - Hard-coding IP addresses, rather than DNS names, in configuration files and application is a bad idea
  - Many people do it anyway – makes changing IP addresses difficult
- IPv6 tries to make renumbering networks easier, by providing better auto-configuration
  - Insufficient experience to know how well this works in practice
  - Some vendors also offer IPv6-to-IPv6 NAT [RFC 6296]

Implications of NAT for TCP Connections



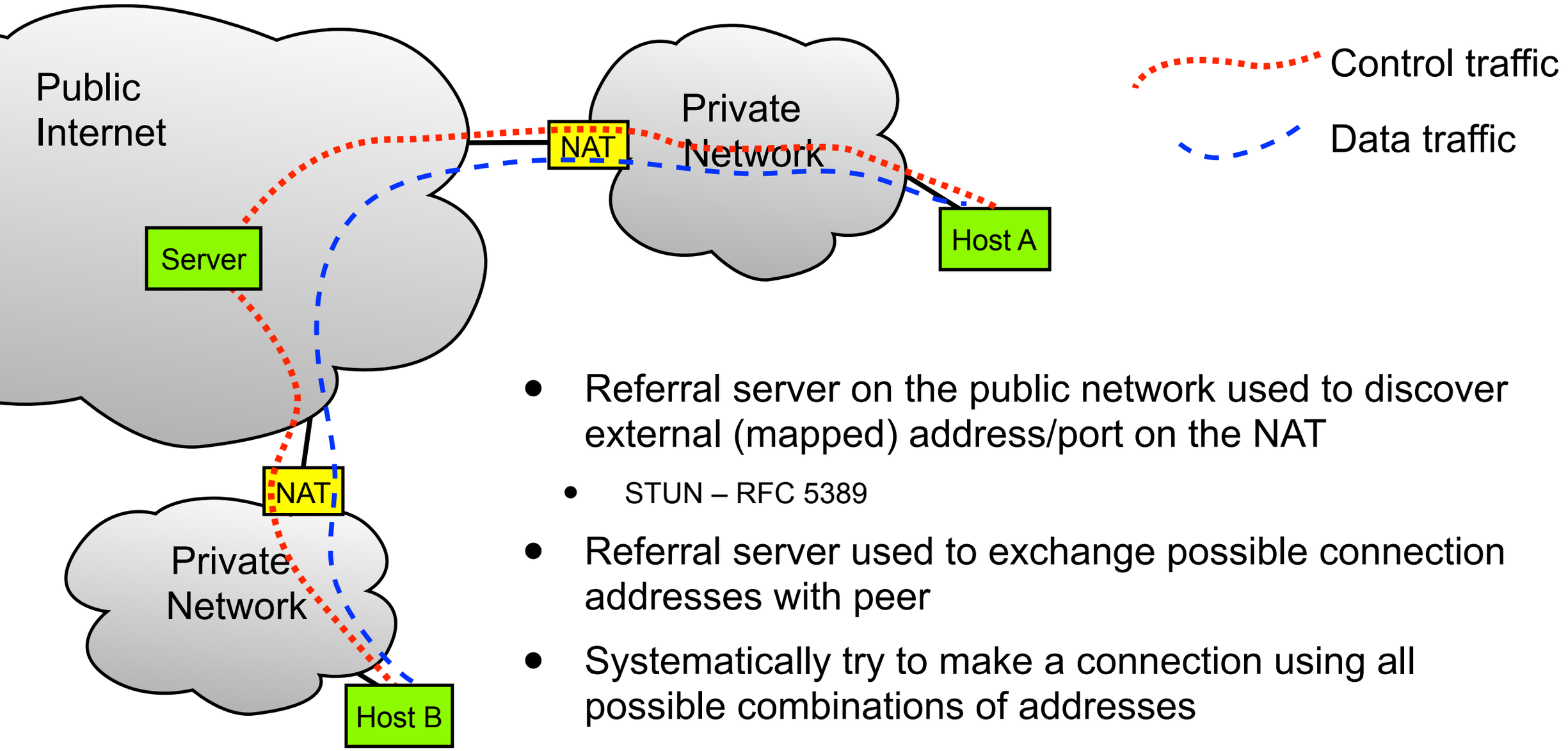
- Outgoing connection creates state in NAT
  - Need to send data periodically, else NAT state times out
  - Recommended time out interval is 2 hours, many NATs use shorter [RFC5382]
- No state for incoming connections
  - NAT can’t know where to forward incoming connections, without manual configuration
  - Affects servers behind a NAT, or peer-to-peer applications

Implications of NAT for UDP Flows



- NATs tend to have short time outs for UDP
  - Not connection-oriented, so they can't detect the end of flows
  - Recommended time out interval is not less than two minutes, but many NATs use shorter intervals – the VoIP NAT traversal standards suggest sending a keep alive message every 15 seconds [RFC4787]
- Peer-to-peer connections easier than TCP
  - UDP NATs often more permissive about allowing incoming packets than TCP NATs; many allow replies from anywhere to an open port

NAT Traversal Concepts



- Referral server on the public network used to discover external (mapped) address/port on the NAT
  - STUN – RFC 5389
- Referral server used to exchange possible connection addresses with peer
- Systematically try to make a connection using all possible combinations of addresses
  - Every possible network interface and protocol, mapped and local
  - Complex and generates significant traffic overhead
  - The ICE algorithm – RFC 5245

Summary

- Network address translation
- Impact on transport protocols
- NAT traversal concepts

- NATs are widely deployed but greatly complicate applications, and hinder evolution of the network