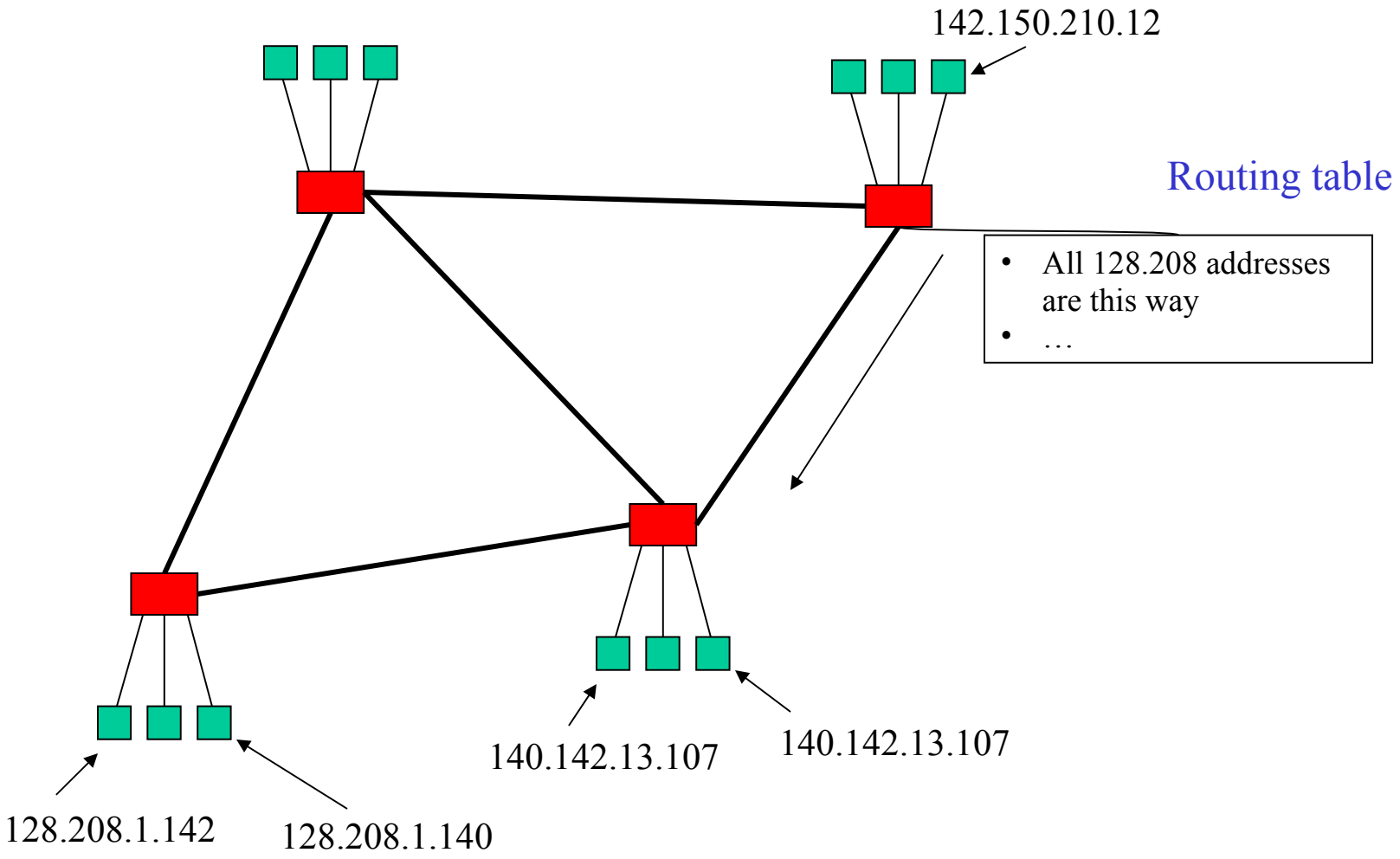
CSE/EE 461: Introduction to Computer Communications Networks Autumn 2010

Module 9

IP Addressing

John Zahorjan
zahorjan@cs.washington.edu
534 Allen Center

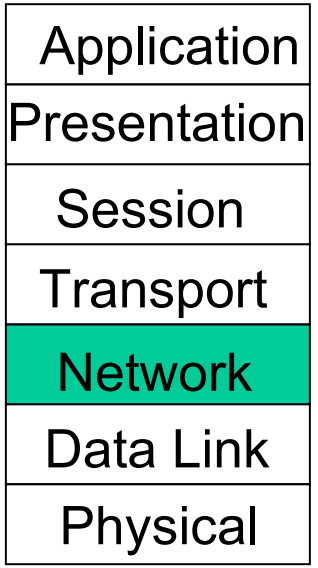
Last Time: Addresses Imply Location



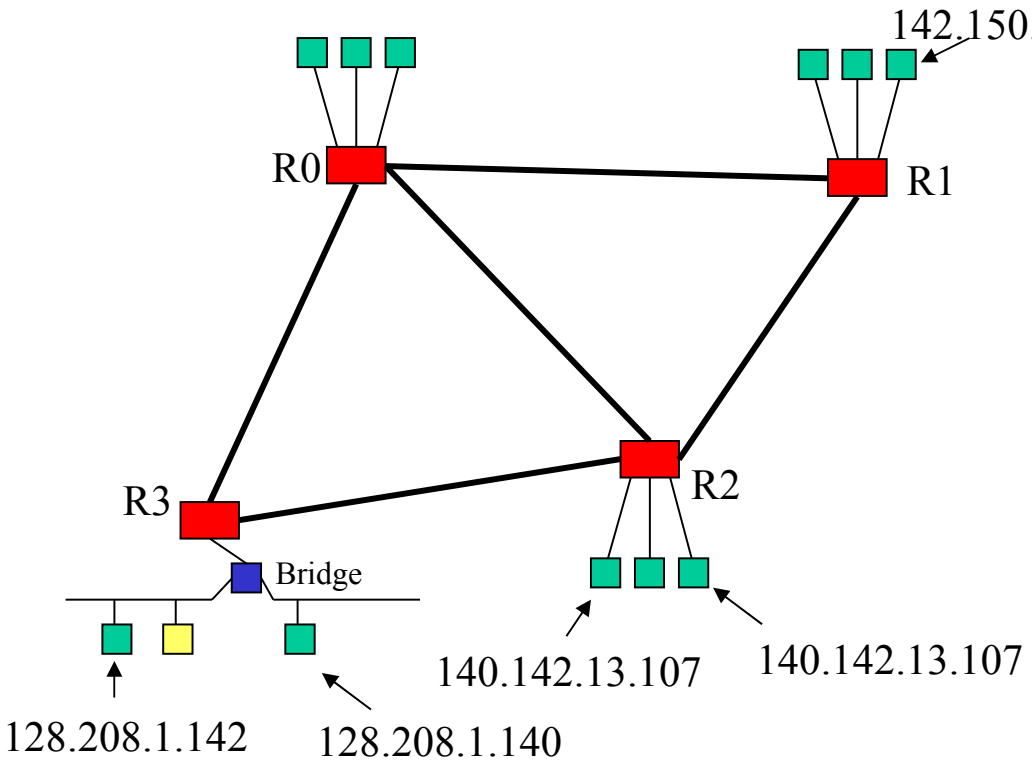
This Lecture

IP Addresses

- Address allocation and discovery
  - DHCP
  - ARP
  - NAT
  - STUN



Address Allocation and Discovery



The yellow node boots. It has a MAC address.

- It needs an IP address.
- It needs to know to use router R3.
- R3 needs to discover the new host's MAC address.

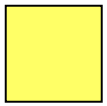
DHCP is used.
ARP is used.

Topic 1: Obtaining an IP address

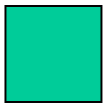
- Old fashioned way: sysadmin configured each machine
  - E.g., a local file contained the IP address to use
  - Imagine deploying 50 new machines in one of the labs…
- Future fashioned way (IPV6): Stateless Autoconfiguration
  - Addresses are wide / plentiful
  - Form IPv6 address by concatenating "network's address" (prefix) with your own MAC address
  - Learn "network address" portion from router
- Current (IPv4) way: Dynamic Host Configuration Protocol (DHCP)
  - Addresses are narrow (32-bits) / scarce
    - Have to hand them out carefully
  - Use a DHCP server that provides bootstrap info to hosts
    - Host's IP address, gateway address, …
  - An immediate problem: how does a host without an IP address communicate with the DHCP server?

The DHCP Problem

Host



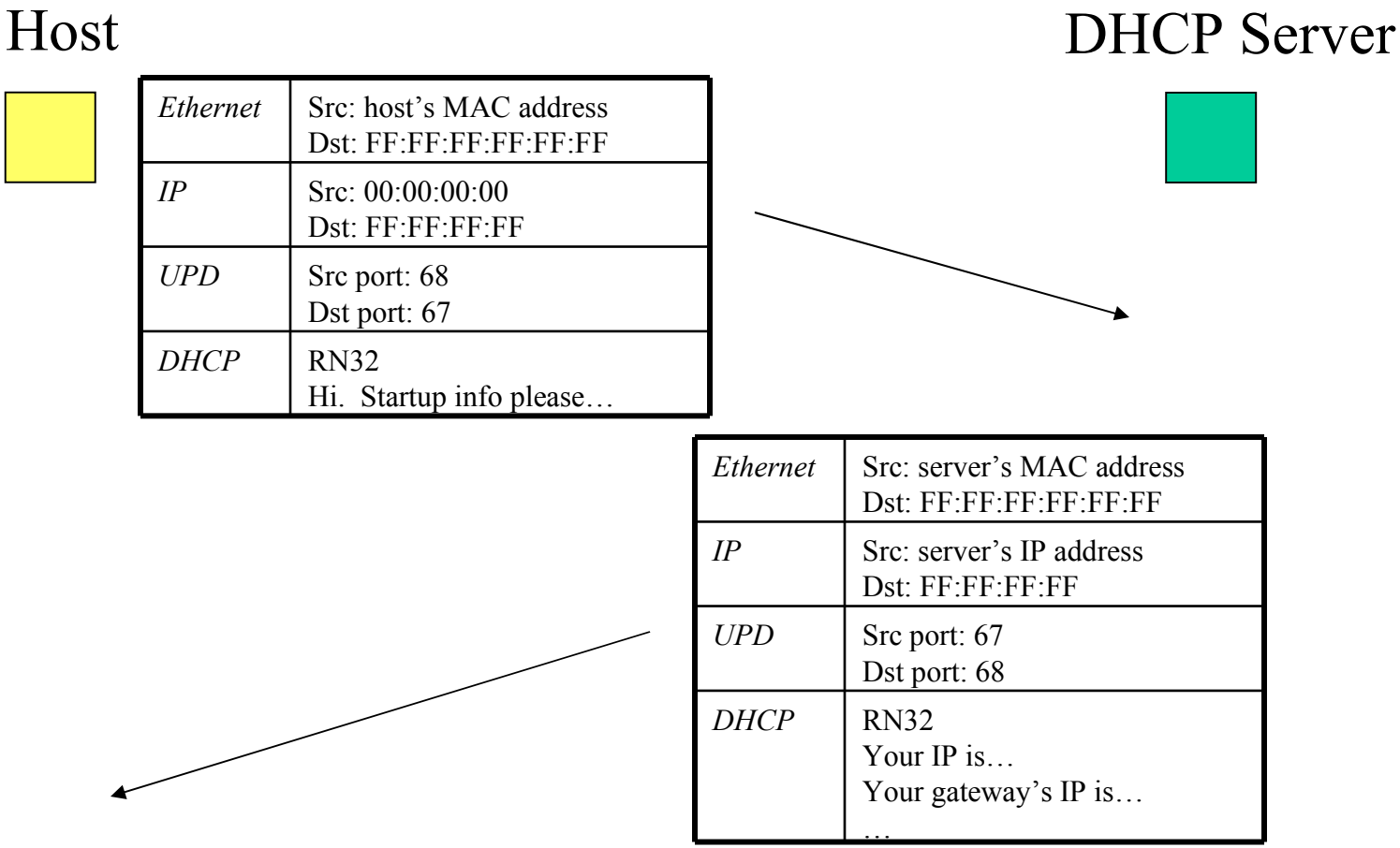
DHCP Server



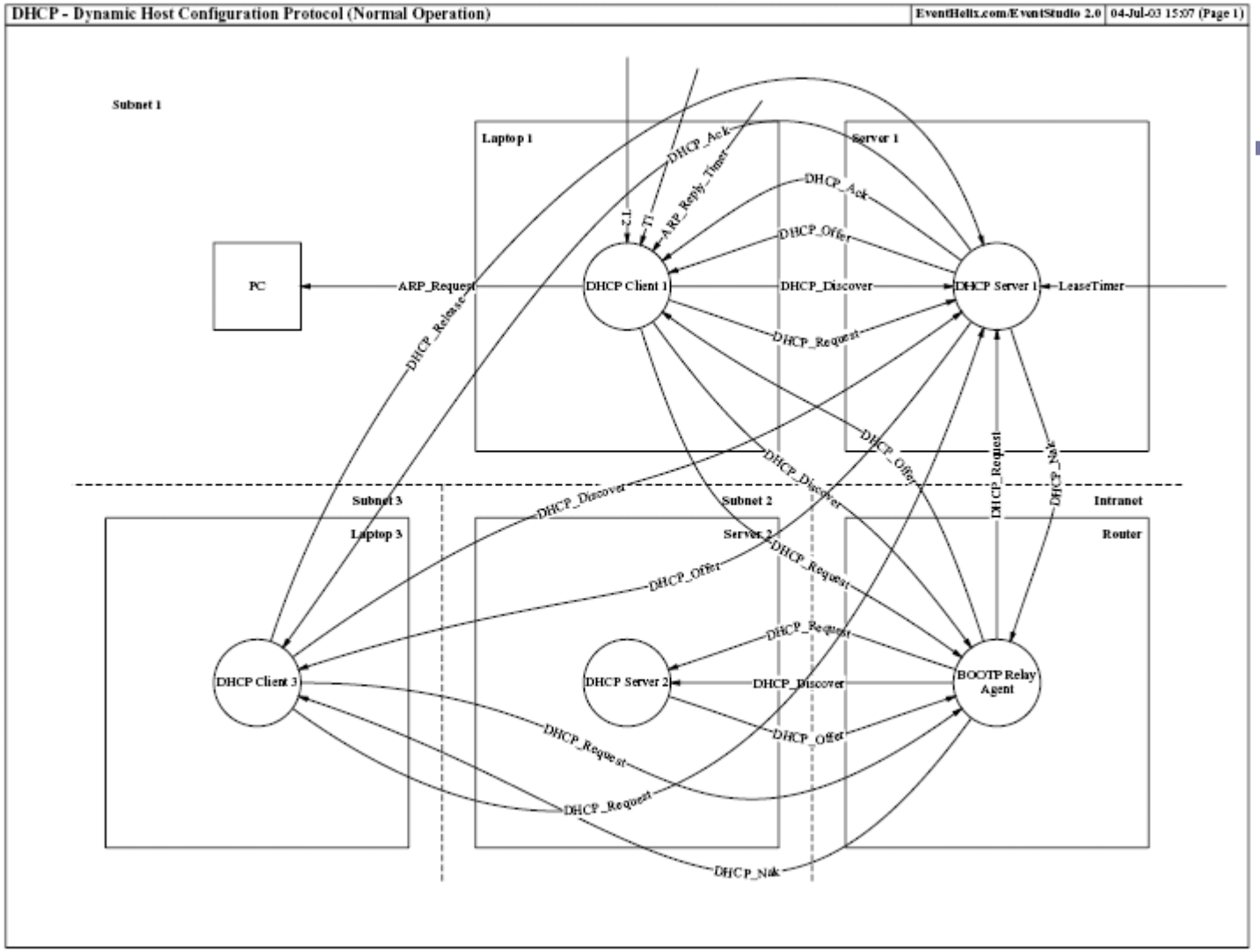
- The host doesn't have an IP address
- The host doesn't know the address of the DHCP server
- The host wants to contact the DHCP server
- We want to use IP packets to talk with the server
  - Why? Why not talk using link layer packets?

Solution: link and IP layer broadcast

The DHCP Problem Solution



(As always, the actual protocol is richer than what is shown here.)

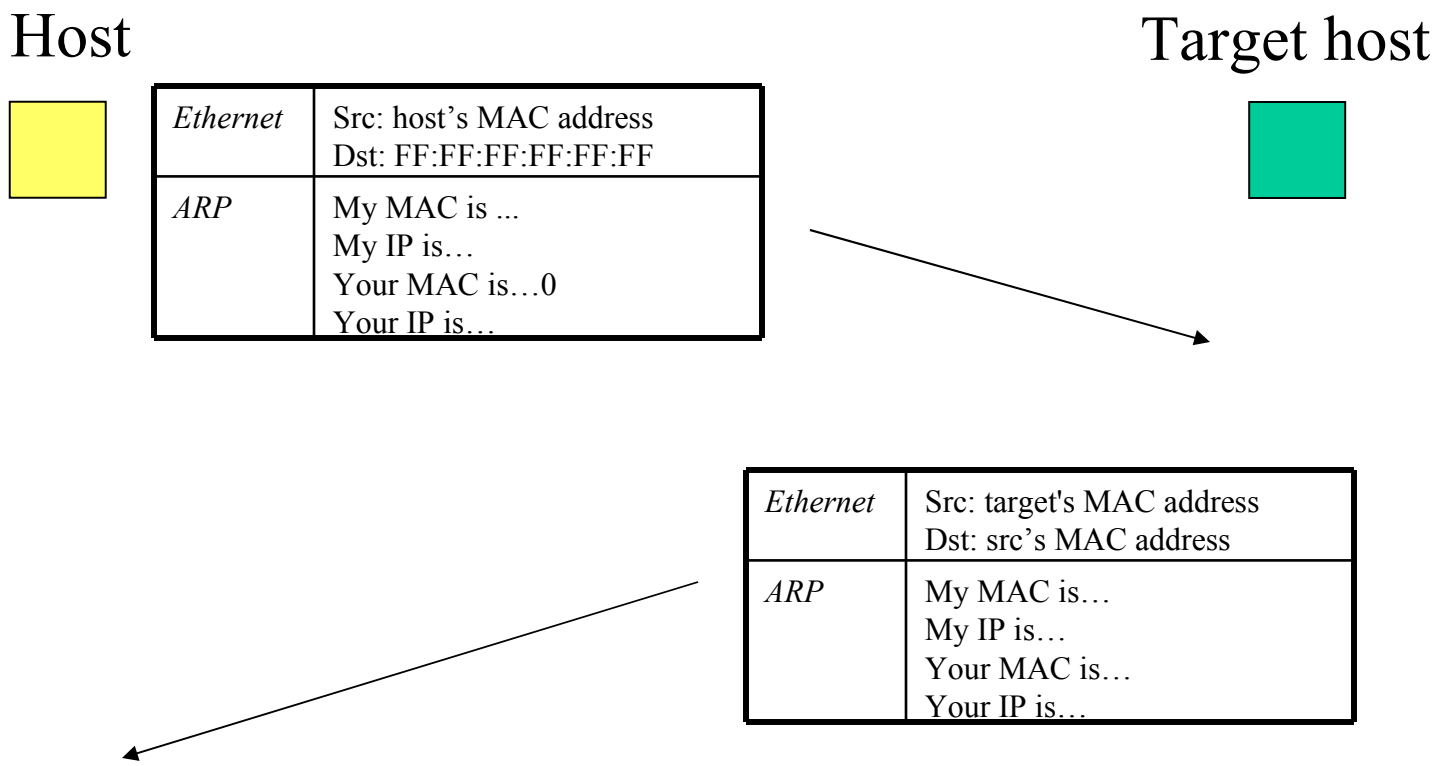


- Client is responsible for all retransmissions. (Why?)
- What dangers are there for losing IP addresses?

Topic 2: Discovering MAC's from IP's

- Host has an IP (e.g., for the gateway). It needs a MAC address to send a frame to it.
- Solution: Address Resolution Protocol (ARP)
- Exploits the physical multicast of Ethernet

The IP->MAC Problem Solution



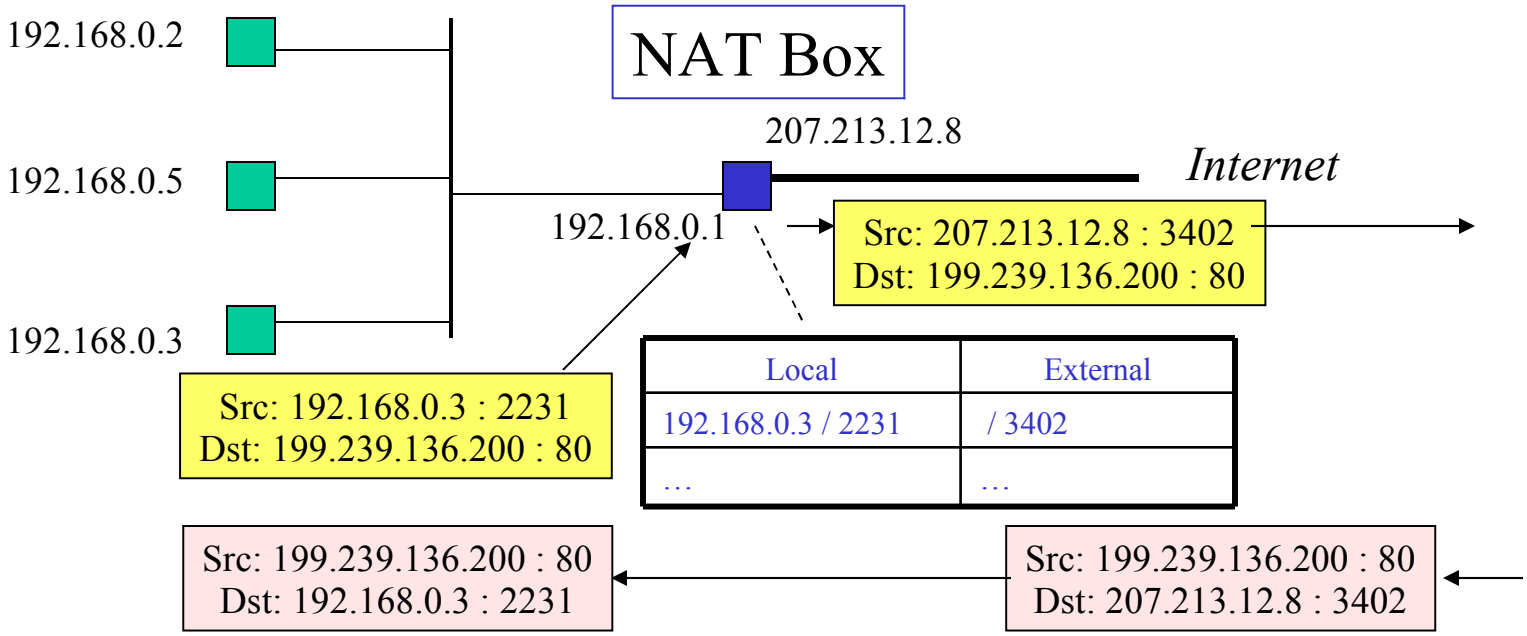
(As always, the actual protocol is richer than what is shown here.)

Topic 3: Network Address Translation (NAT)

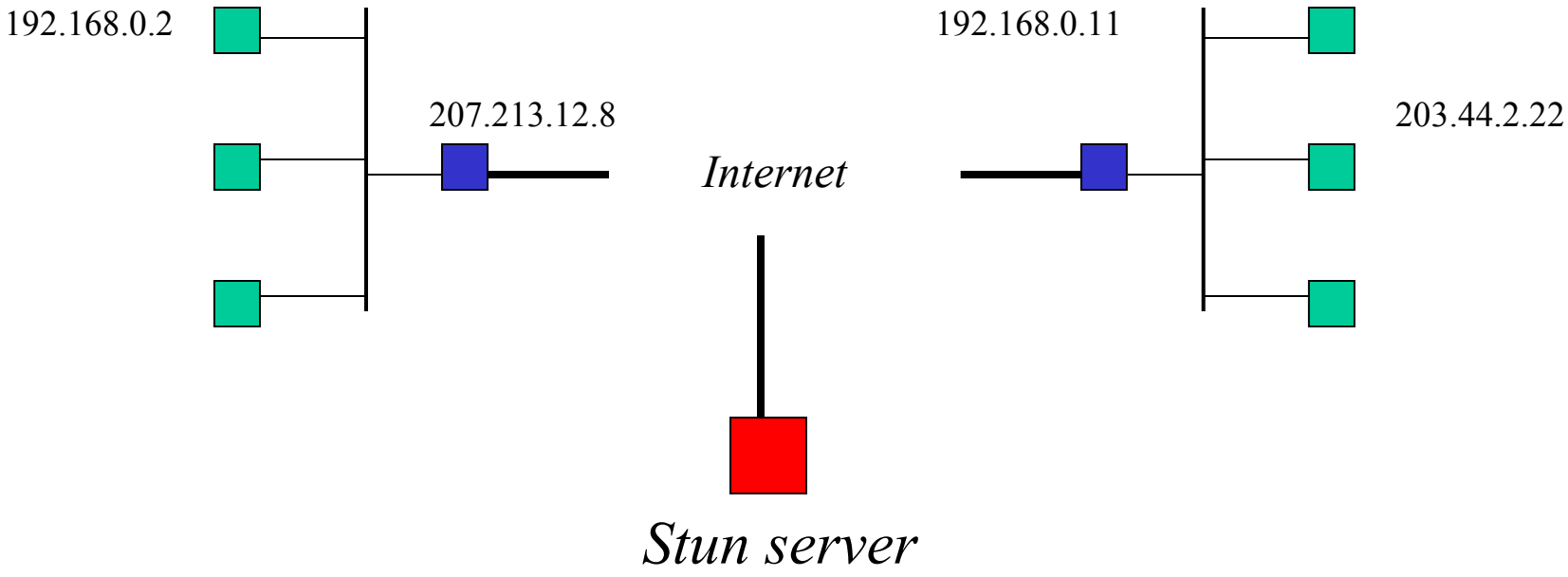
- Turns out that there aren't all that many 32-bit strings (i.e., IP addresses)
  - The world needs more…
  - An individual network needs more…
  - You need more…
    - Your ISP will give you only one (using DHCP), but you want to connect five machines to the Internet
- NAT exploits *non-routable addresses* to let you build your own private network "behind the NAT box"
  - Non-routable addresses are, well, never routed
  - do not have to be globally unique (just locally unique)
- The NAT box substitutes its own IP address for outgoing packets, and the local address of the actual destination for incoming packets

NAT Overview

- Recall that IP addresses are 32-bits (e.g., 192.168.10.3)
- Recall that TCP addresses are IP addresses plus a port number
- These IP address ranges are "non-routable":
  - 10.0.0.0 - 10.255.255.255
  - 172.16.0.0 - 172.31.255.255
  - 192.168.0.0 - 192.168.255.255



NAT and Peer-to-Peer (P2P)



- STUN (Session Traversal Utilities for NAT)
  - Heuristic designed to discover "routable" address (NAT entry) for hosts behind NATs
  - IETF RFC 5389 (http://tools.ietf.org/html/rfc5389)

Key Concepts

- DHCP provides convenient management of host startup information
- ARP learns the mapping from IP to MAC address
- NAT hides local names behind a single global name
- STUN permits interactions between machines behind (distinct) NATs