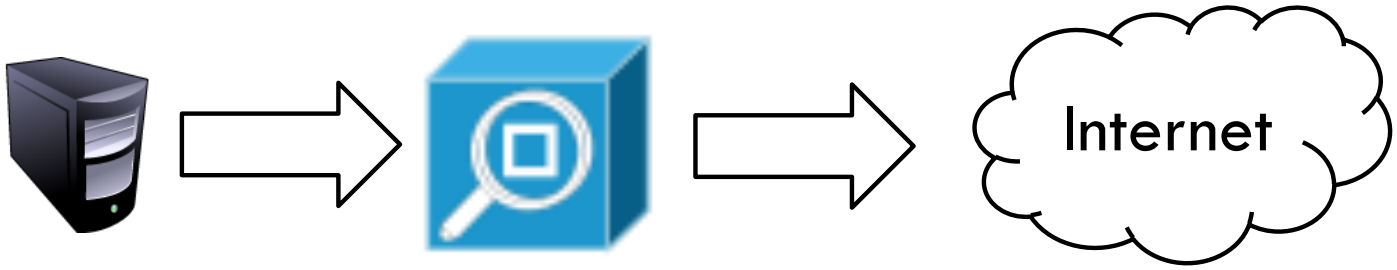
CSCI-351
Data communication and Networks

Lecture 11: Middleboxes and NAT
(Duct tape for IPv4)

The slide is built with the help of Prof. Alan Mislove, Christo Wilson, and David Choffnes's class

Middleboxes

- Devices in the network that interact with network traffic from the IP layer and up
- Common functions
  - **NAT**
  - Firewall and other security
  - Proxy
  - Filtering
  - Caching
  - …



Outline

- NAT
- Other middleboxes

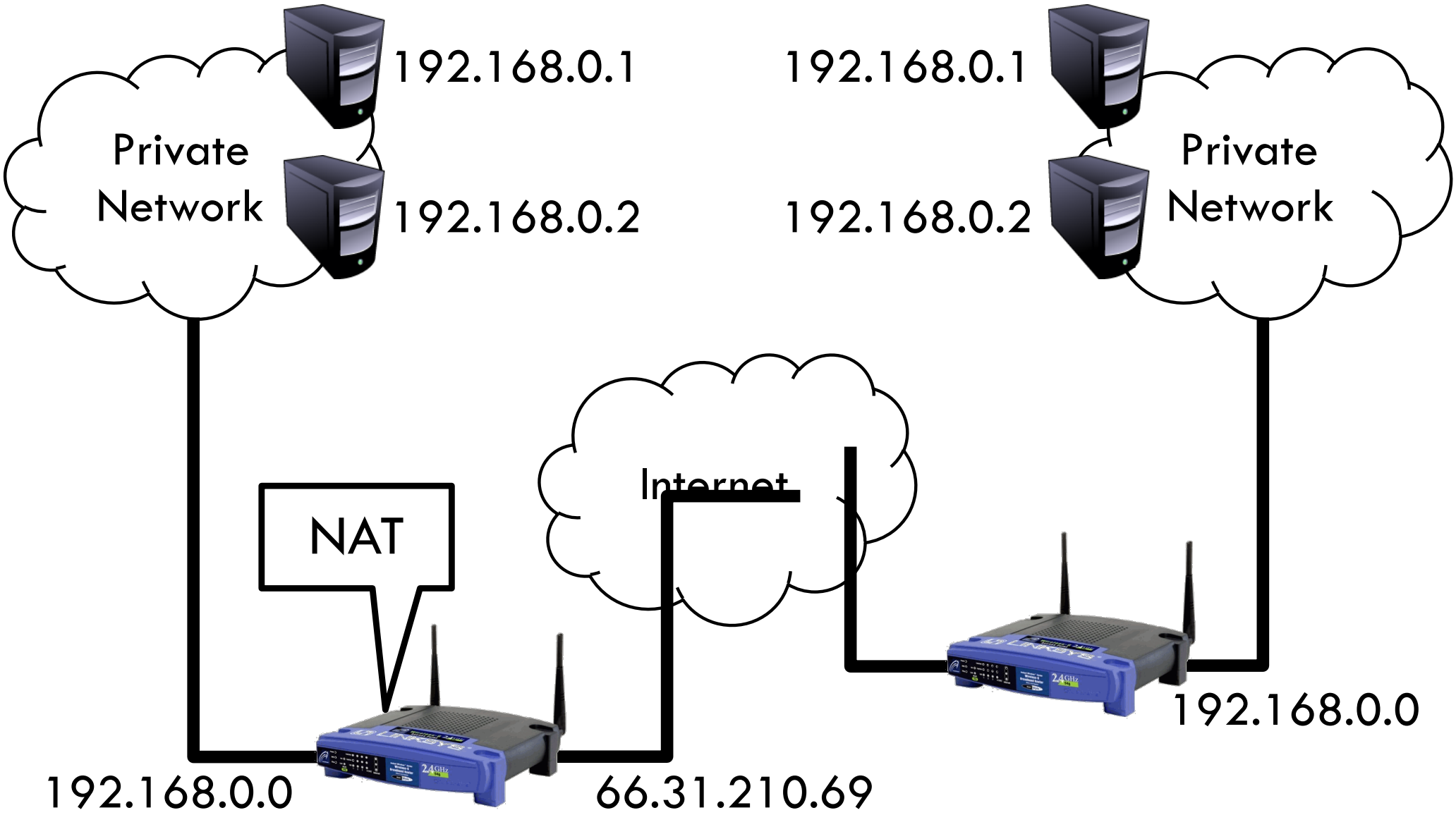
The IPv4 Shortage

- Problem: consumer ISPs typically only give one IP address per-household
  - Additional IPs cost extra
  - More IPs may not be available
- Today's households have more networked devices than ever
  - Laptops and desktops
  - TV, bluray players, game consoles
  - Tablets, smartphones, eReaders
- How to get all these devices online?

Private IP Networks

- Idea: create a range of private IPs that are separate from the rest of the network
  - Use the private IPs for internal routing
  - Use a special router to bridge the LAN and the WAN
- Properties of private IPs
  - Not globally unique
  - Usually taken from non-routable IP ranges (why?)
- Typical private IP ranges
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255

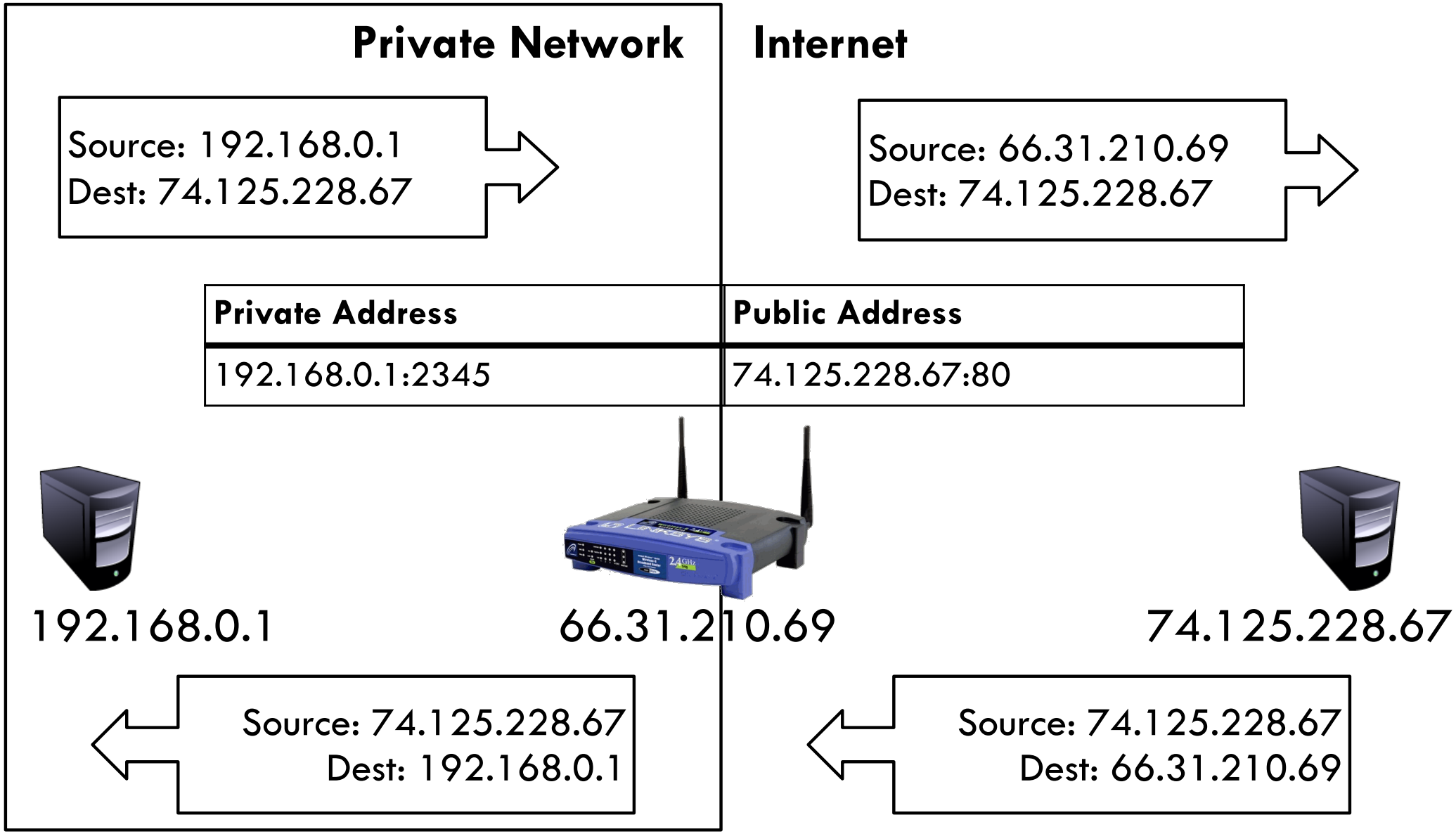
Private Networks



Network Address Translation (NAT)

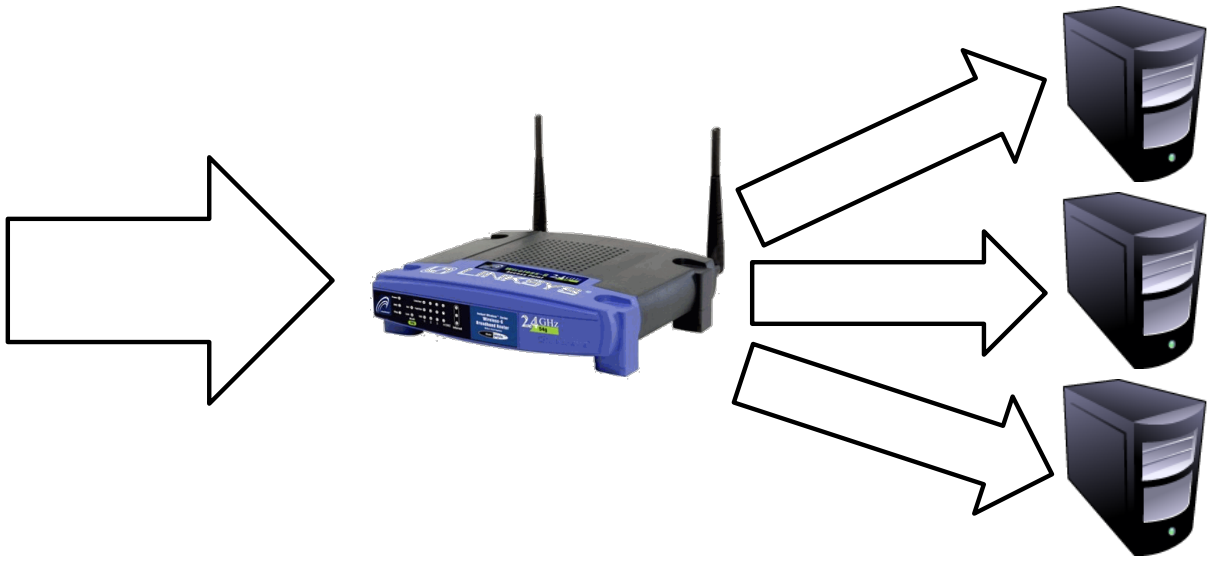
- NAT allows hosts on a private network to communicate with the Internet
  - Warning: connectivity is not seamless
- Special router at the boundary of a private network
  - Replaces internal IPs with external IP
    - This is "Network Address Translation"
  - May also replace TCP/UDP port numbers
- Maintains a table of active flows
  - Outgoing packets initialize a table entry
  - Incoming packets are rewritten based on the table

Basic NAT Operation



Advantages of NATs

- Allow multiple hosts to share a single public IP
- Allow migration between ISPs
  - Even if the public IP address changes, you don't need to reconfigure the machines on the LAN
- Load balancing
  - Forward traffic from a single public IP to multiple private hosts



Natural Firewall

10

Private Network | **Internet**

Private Address	Public Address

192.168.0.1

66.31.210.69

74.125.228.67

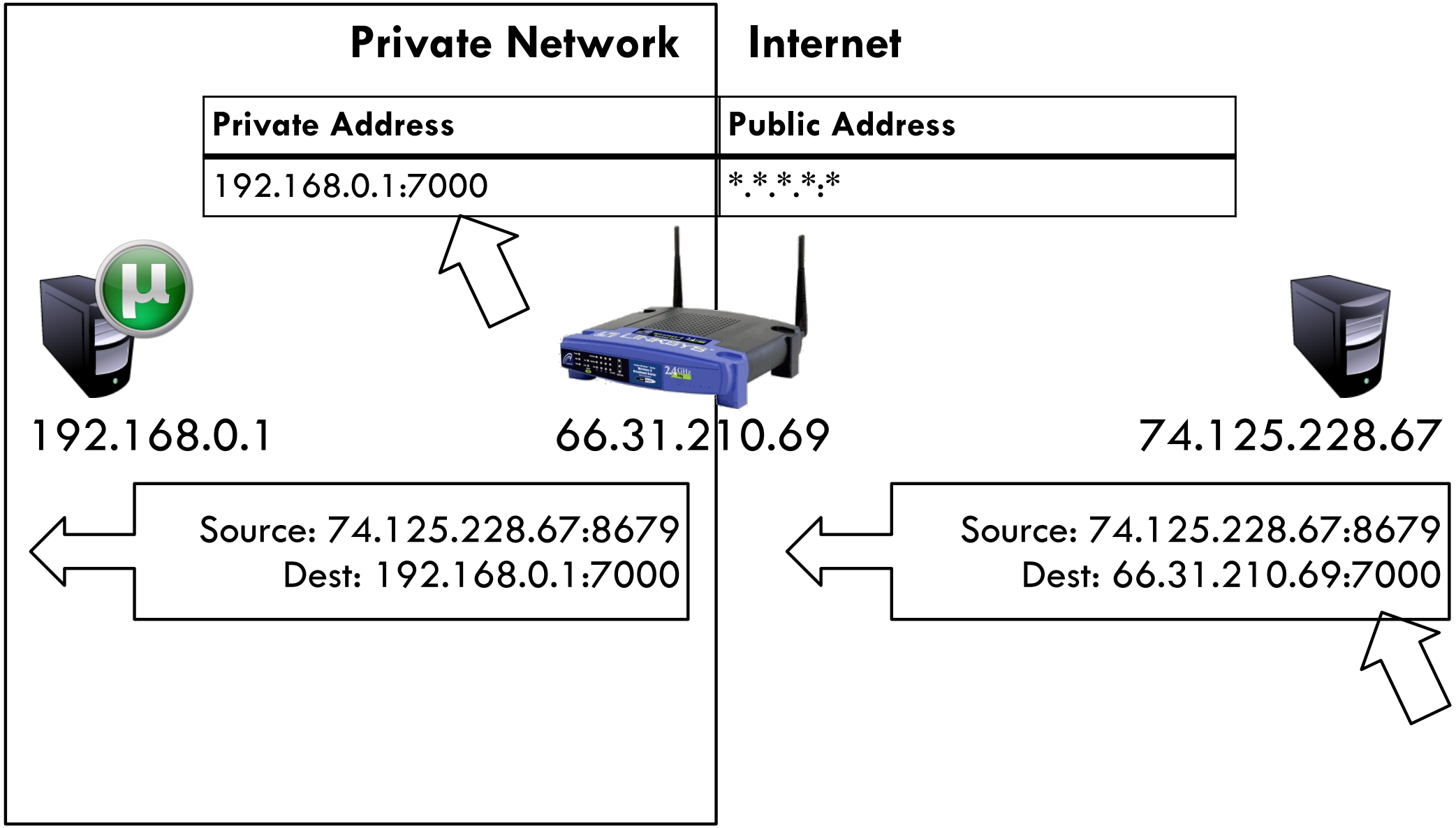
Source: 74.125.228.67

Dest: 66.31.210.69

Concerns About NAT

- Performance/scalability issues
  - Per flow state!
  - Modifying IP and Port numbers means NAT must recompute IP and TCP checksums
- Breaks the layered network abstraction
- Breaks end-to-end Internet connectivity
  - 192.168.*.* addresses are private
  - Cannot be routed to on the Internet
  - Problem is worse when both hosts are behind NATs
- What about IPs embedded in data payloads?

Port Forwarding



Outline

- NAT
- Other middleboxes

Firewall

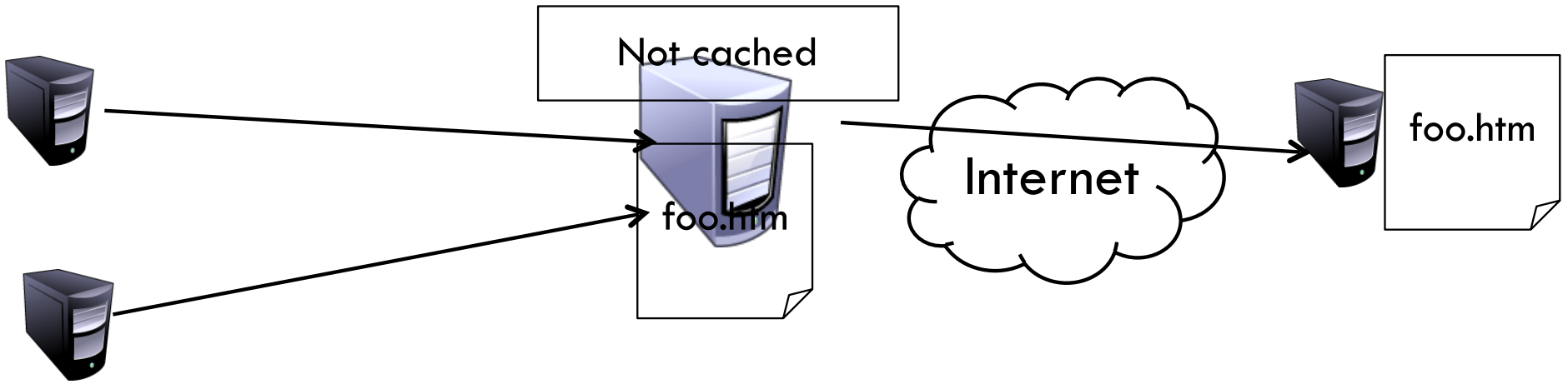
- A device that blocks traffic according to a set of rules
  - Why?
  - Services with vulnerabilities turned on by default
  - ISP policy forbidding certain traffic due to ToS
- Typically specified using a 5-tuple
  - E.g., block outbound SMTP; block inbound SQL server reqs
- GFC (Great Firewall of China)
  - Known to block based on IP, filter DNS requests, etc

Web caching

- ISP installs cache near network edge that caches copies of Web pages
  - Why?
  - **Performance:** Content is closer to clients, TCP will perform better with lower RTTs
  - **Cost:** "free" for the ISP to serve from inside the network
- Limitations
  - Much of today's content is not static (why does this matter?)
  - Content ownership
  - Potential privacy issues
  - Long tail of content popularity

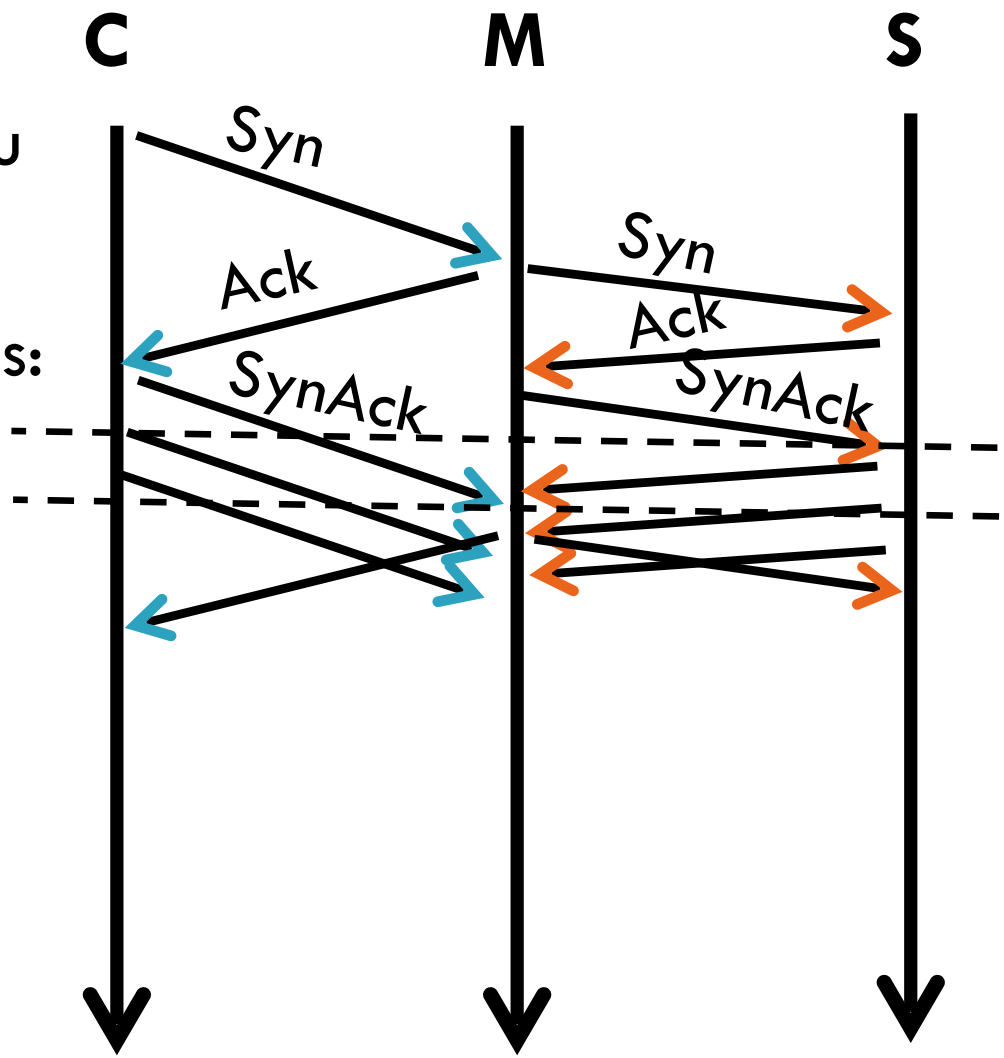
Web caching

- ISP installs cache near network edge that caches copies of Web pages
  - Why?
  - **Performance:** Content is closer to clients, TCP will perform better with lower RTTs
  - **Cost:** "free" for the ISP to serve from inside the network



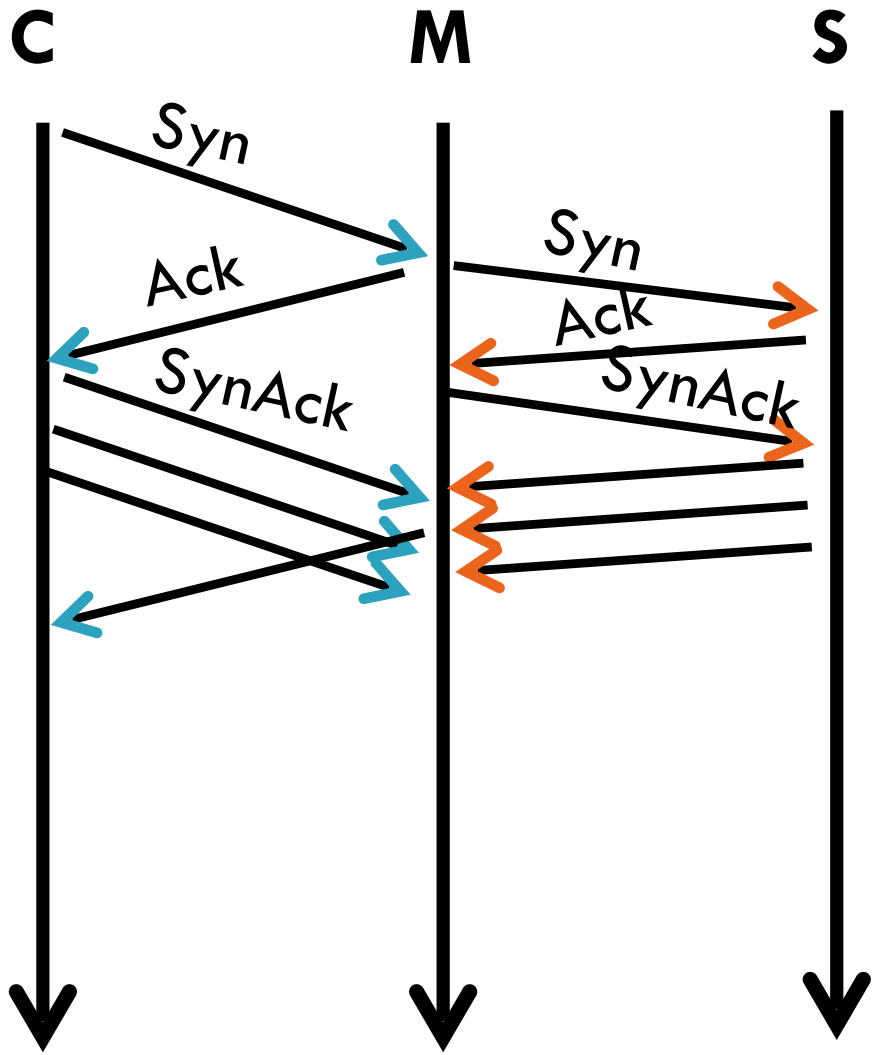
Proxying

- Non-split connections
  - Like NAT, but IP address is no longer the one assigned to you
- Split connections
  - Middlebox maintains two flows: C-M and M-S
  - Can be done transparently
    - How?



Proxying

- Advantages
  - RTT is lower on each end
  - Can use different MTUs
  - Particularly useful in cell ntwks
- Disadvantages
  - Extra delay can be bad for small flows
  - Buffering/state makes it potentially costly



Questions

- Middleboxes that breaks end-to-end integrity
  - APs?
- How can we tell if middle boxes does do that?
  - ISP? Software on your computer? How can we tell that?
- Net-neutrality
-

CSCI-351
Data communication and Networks

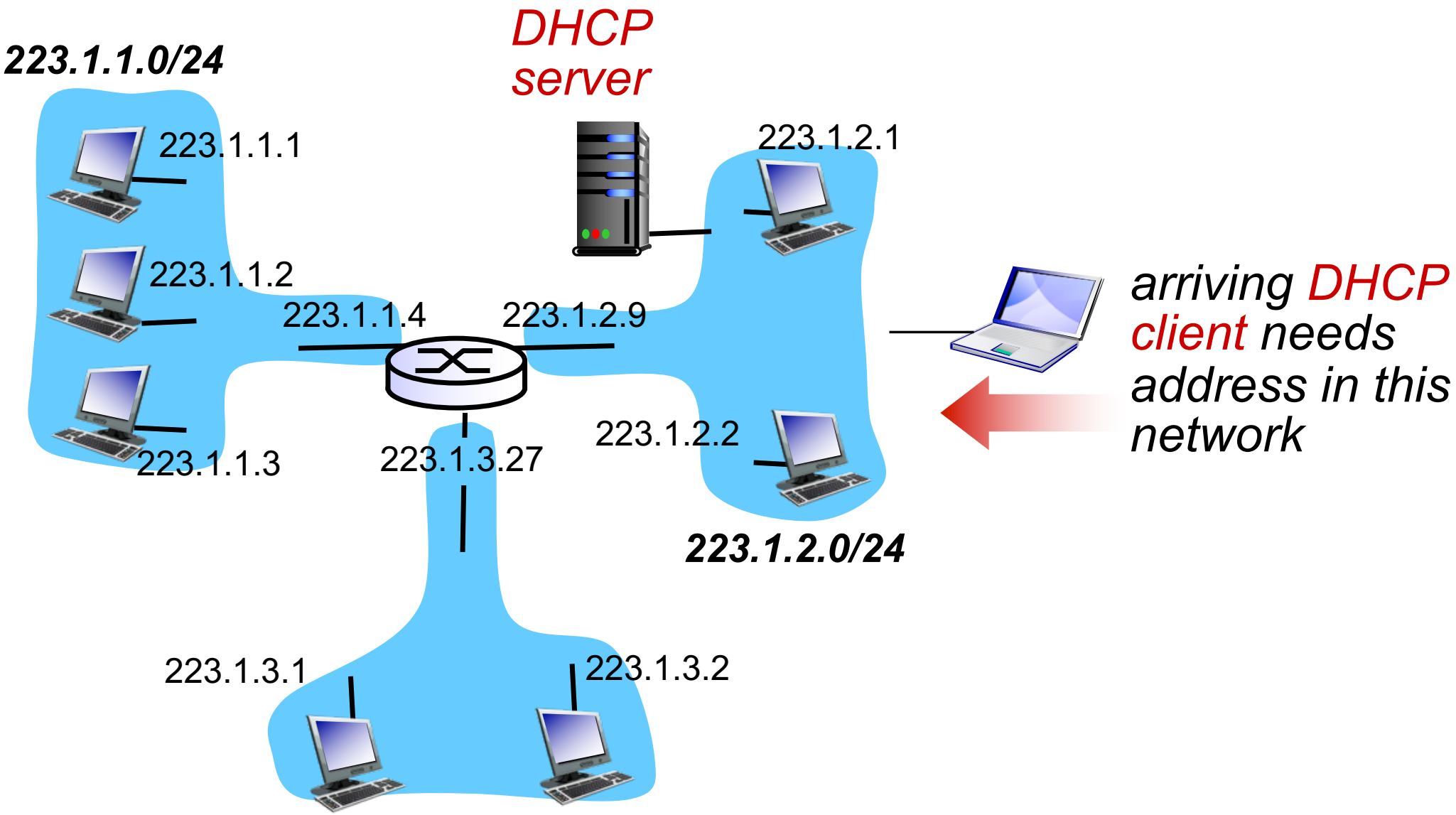
Lecture 11 ext: DHCP

The slide is built with the Prof. Kurose's materials

DHCP: Dynamic Host Configuration Protocol

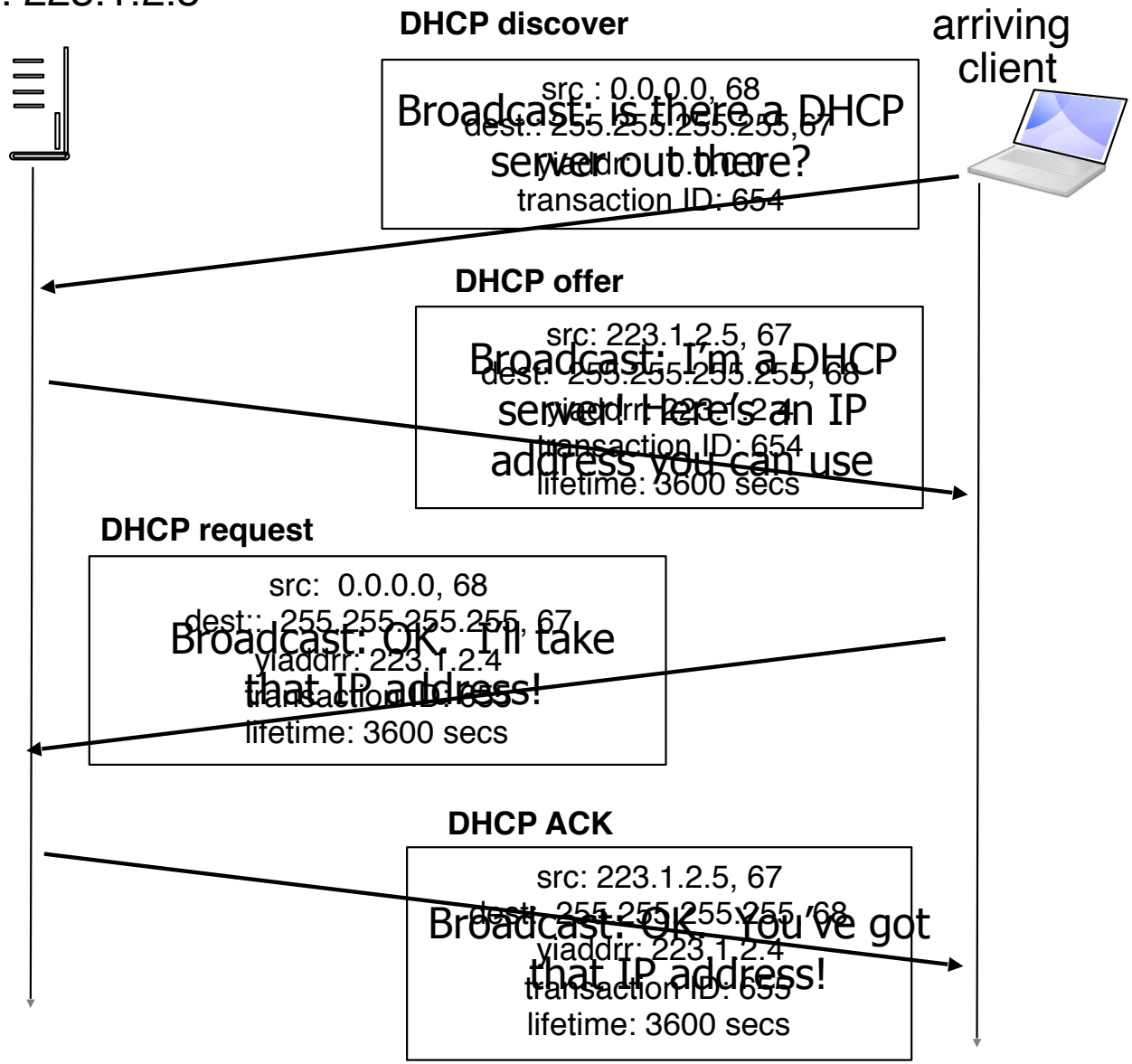
- Let's say that a ISP has X customers, How many IPs does it need to have?
  - X?
- Goal: allow host to *dynamically* obtain its IP address from network server when it joins network
  - can renew its lease on address in use
  - allows reuse of addresses (only hold address while connected/"on")
  - support for mobile users who want to join network (more shortly)

DHCP Client-Server



DHCP Client-Server

DHCP server: 223.1.2.5



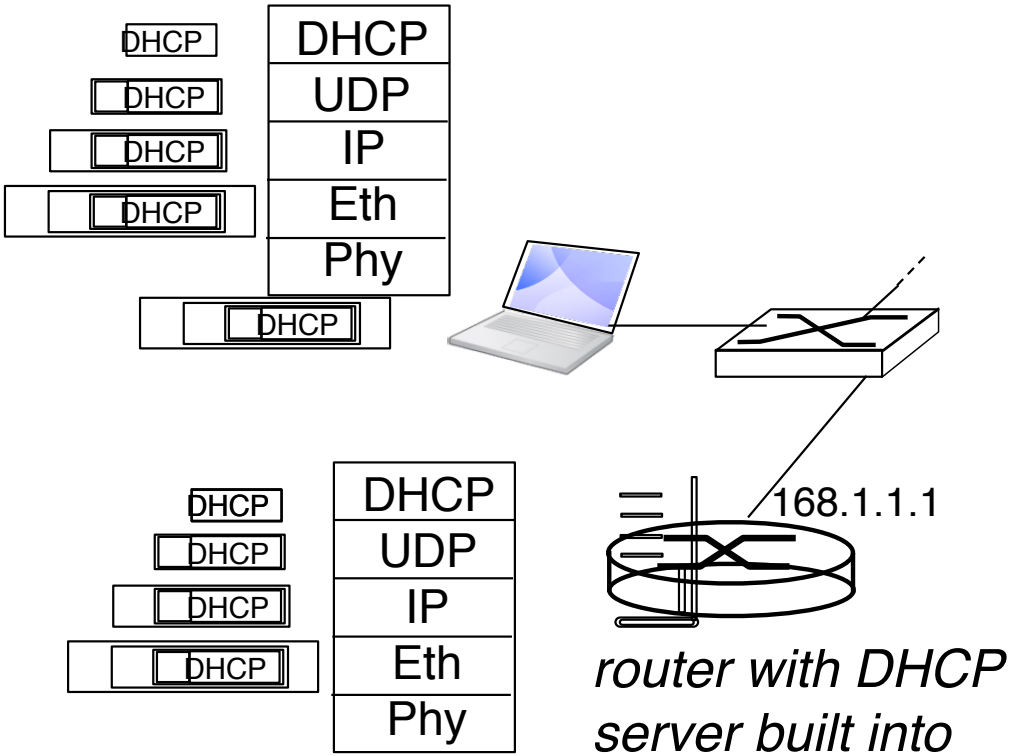
DHCP: More than IP address

- DHCP can return more than just allocated IP address on subnet
  - address of first-hop router for client
  - name and IP address of DNS sever
  - network mask (indicating network versus host portion of address)

DHCP Header (Do not memorize)

Dynamic Host Configuration Protocol				
Bit Offset	0–15		16–31	
0	OpCode	Hardware Type	Hardware Length	Hops
32	Transaction ID			
64	Seconds Elapsed		Flags	
96	Client IP Address			
128	Your IP Address			
160	Server IP Address			
196	Gateway IP Address			
228+	Client Hardware Address (16 bytes)			
	Server Host Name (64 bytes)			
	Boot File (128 bytes)			
	Options			

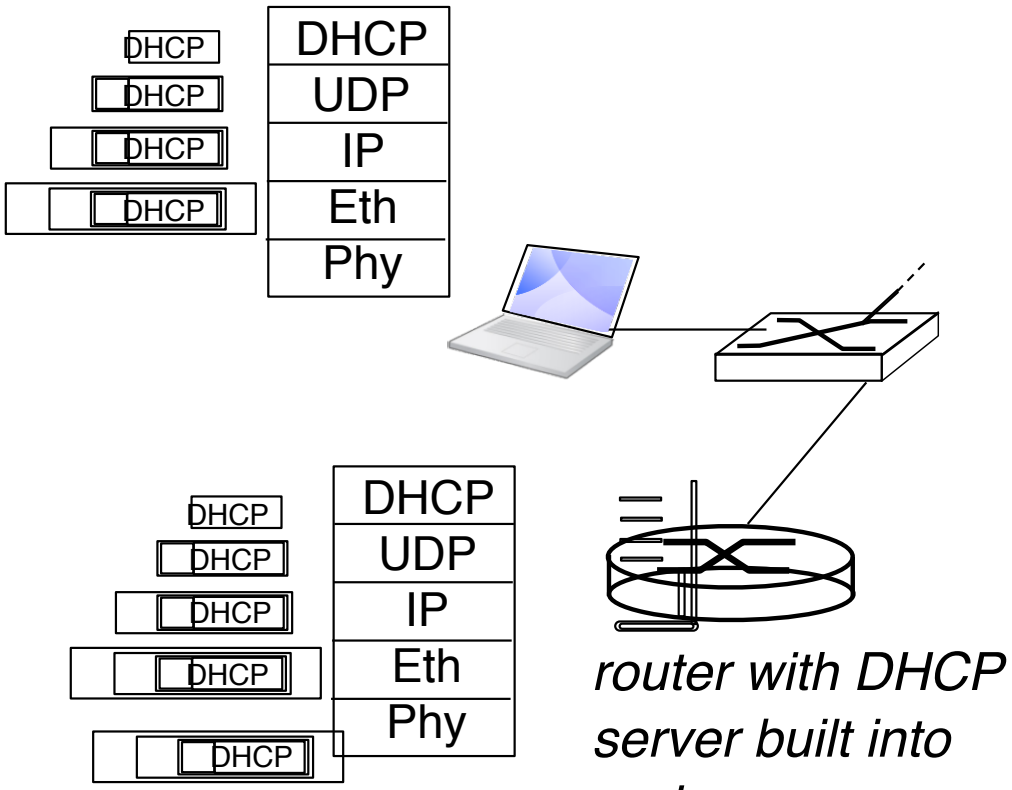
DHCP: example



router with DHCP server built into router

- connecting laptop needs its IP address, addr of first-hop router, addr of DNS server: use DHCP
- DHCP request encapsulated in UDP, encapsulated in IP, encapsulated in 802.1 Ethernet
- Ethernet frame broadcast (dest: FFFFFFFFFFFF) on LAN, received at router running DHCP server
- Ethernet demuxed to IP demuxed, UDP demuxed to DHCP

DHCP: example



router with DHCP server built into router

- DCP server formulates DHCP ACK containing client's IP address, IP address of first-hop router for client, name & IP address of DNS server
- encapsulation of DHCP server, frame forwarded to client, demuxing up to DHCP at client
- client now knows its IP address, name and IP address of DSN server, IP address of its first-hop router