


Computer Networks

CMSC 417 : Spring 2024

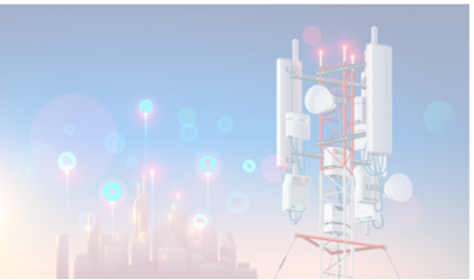
COMPUTER SCIENCE
UNIVERSITY OF MARYLAND

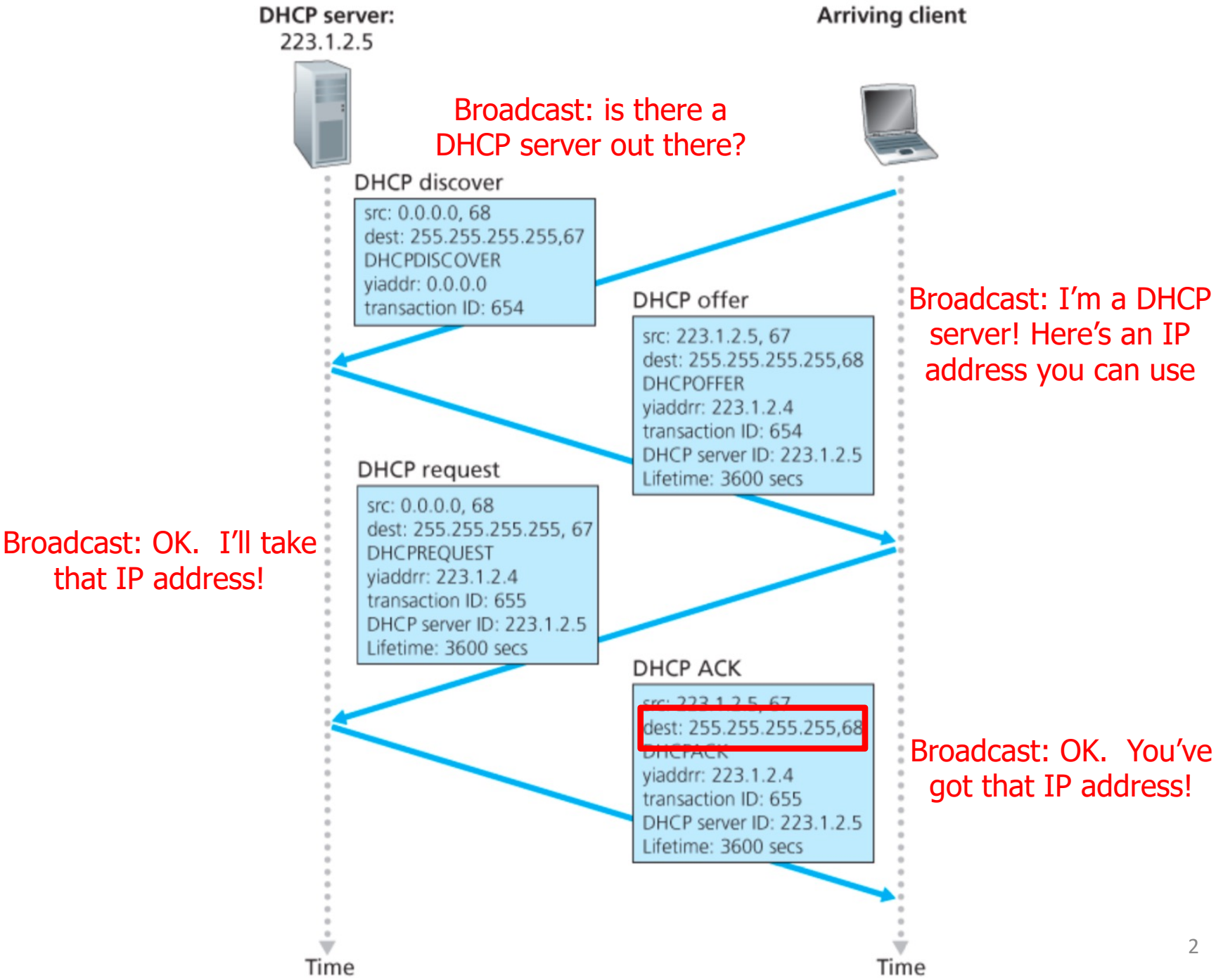
Topic: Internetworking: DHCP, NAT, ARP, ICMP (Textbook chapter 3)

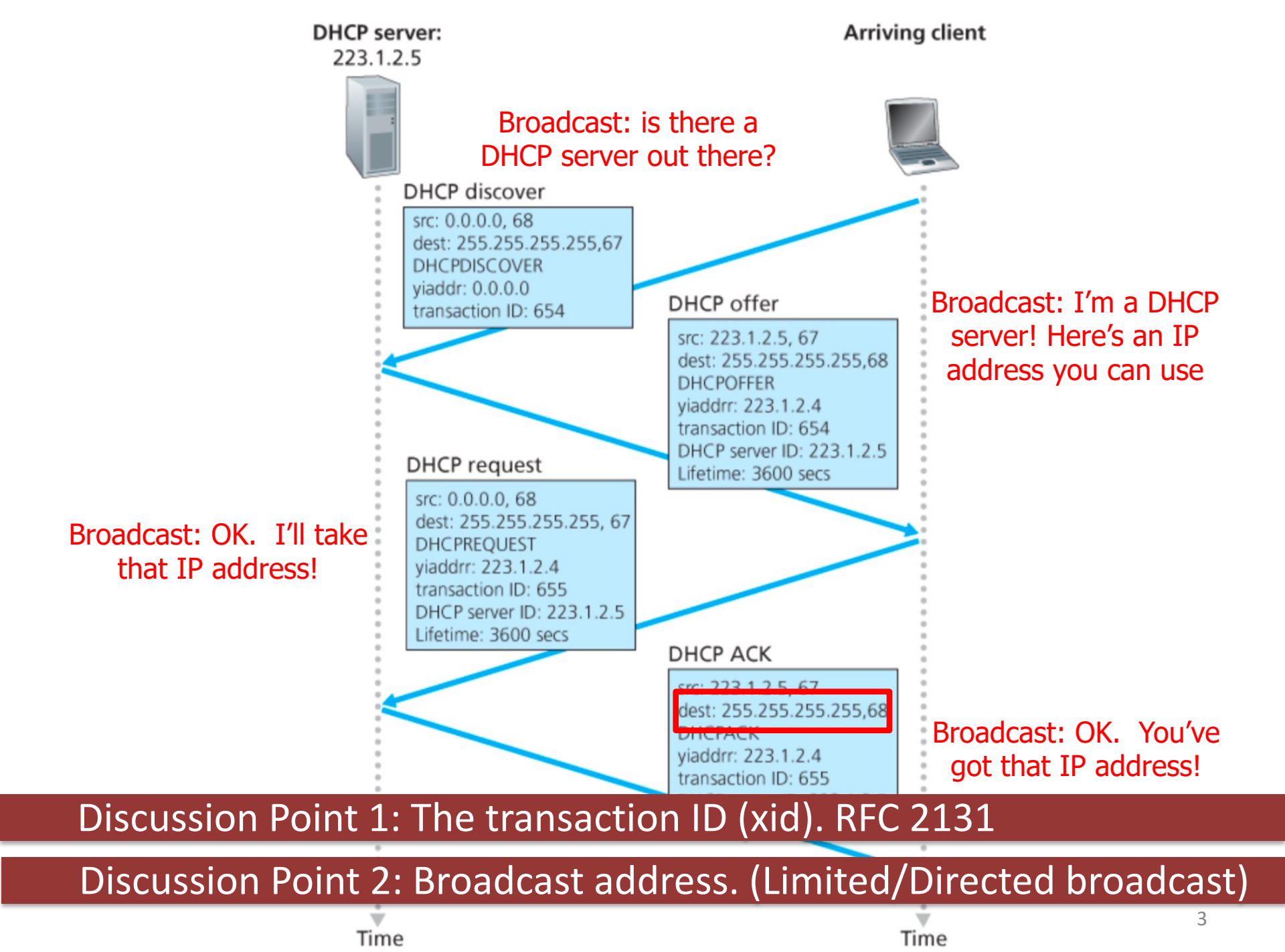
Nirupam Roy

Tu-Th 2:00-3:15pm
CSI 2117

Feb 29th, 2024





DHCP server:
223.1.2.5
Arriving client
Broadcast: is there a DHCP server out there?
DHCP discover
src: 0.0.0.0, 68
dest: 255.255.255.255,67
DHCPDISCOVER
yiaddr: 0.0.0.0
transaction ID: 654
DHCP offer
src: 223.1.2.5, 67
dest: 255.255.255.255,68
DHCPOFFER
yiaddrr: 223.1.2.4
transaction ID: 654
DHCP server ID: 223.1.2.5
Lifetime: 3600 secs
Broadcast: I'm a DHCP server! Here's an IP address you can use
DHCP request
src: 0.0.0.0, 68
dest: 255.255.255.255, 67
DHCPREQUEST
yiaddrr: 223.1.2.4
transaction ID: 655
DHCP server ID: 223.1.2.5
Lifetime: 3600 secs
Broadcast: OK. I'll take that IP address!
DHCP ACK
dest: 255.255.255.255,68
yiaddrr: 223.1.2.4
transaction ID: 655
DHCP server ID: 223.1.2.5
Lifetime: 3600 secs
Broadcast: OK. You've got that IP address!
Time
Time



Discussion Point 1: The transaction ID (xid). RFC 2131

Discussion Point 2: Broadcast address. (Limited/Directed broadcast)

DHCP: more than IP addresses

DHCP can return more than just allocated IP address on subnet:

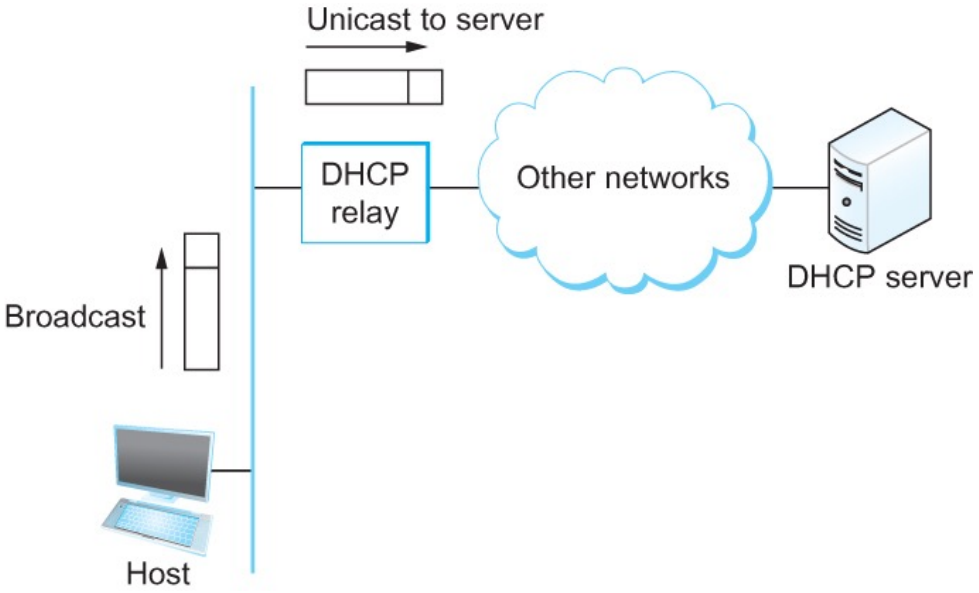
- address of first-hop router for client
- name and IP address of DNS sever
- network mask (indicating network versus host portion of address)

Dynamic Host Configuration Protocol (DHCP)

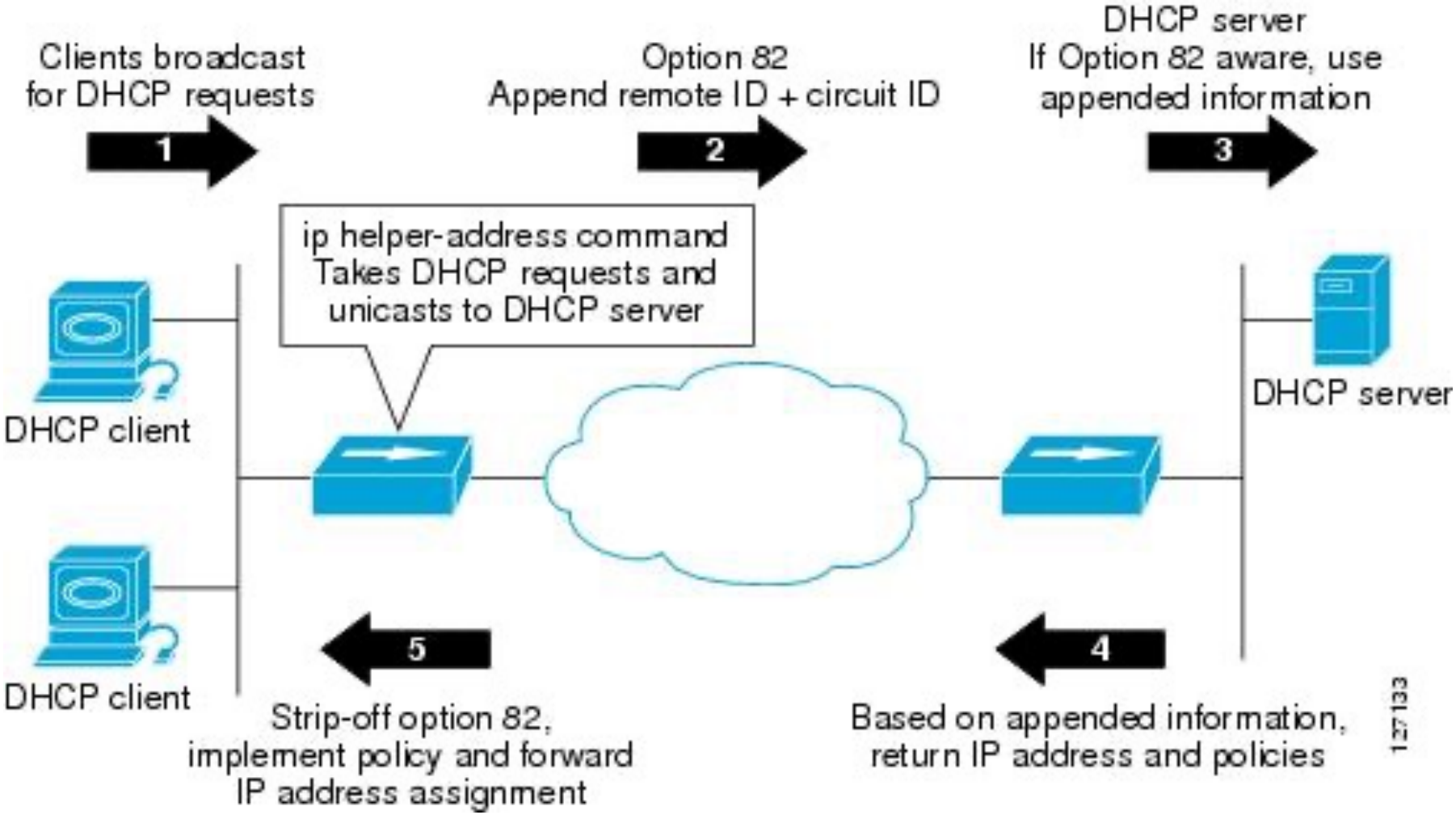
- DHCP server is responsible for providing configuration information to hosts
- DHCP server maintains a pool of available addresses
- There is at least one DHCP server for an administrative domain (a server or a relay agent per subnet)

DHCP relay

- Newly booted or attached host sends DHCPDISCOVER message to a special IP address (255.255.255.255)
- DHCP relay agent unicasts the message to DHCP server and waits for the response



DHCP relay


Clients broadcast
for DHCP requests
1
Option 82
Append remote ID + circuit ID
2
DHCP server
If Option 82 aware, use
appended information
3
ip helper-address command
Takes DHCP requests and
unicasts to DHCP server
DHCP client
DHCP client
DHCP server
5
4
Strip-off option 82,
implement policy and forward
IP address assignment
Based on appended information,
return IP address and policies
127133

Check your IP addresses
(ifconfig/ipconfig)

```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 38:f9:d3:21:07:2a
        inet6 fe80::c84:8160:88c8:ea96%en0 prefixlen 64 secured scopeid 0xa
        inet 10.104.215.30 netmask 0xfffff000 broadcast 10.104.223.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
```

Check your IP addresses
(ifconfig/ipconfig)

```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 38:f9:d3:21:07:2a
        inet6 fe80::c84:8160:88c8:ea96%en0 prefixlen 64 secured scopeid 0xa
        inet 10.104.215.30 netmask 0xfffff000 broadcast 10.104.223.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
```

Private Address Space
&
NAT

ARIN
American Registry for Internet Numbers

Search Site or Whois

IP Addresses & ASNs | Policy & Participation | Reference & Tools | About

Home > Reference & Tools > Research > Statistics & Reporting > IPv4 Private Address Space and Filtering

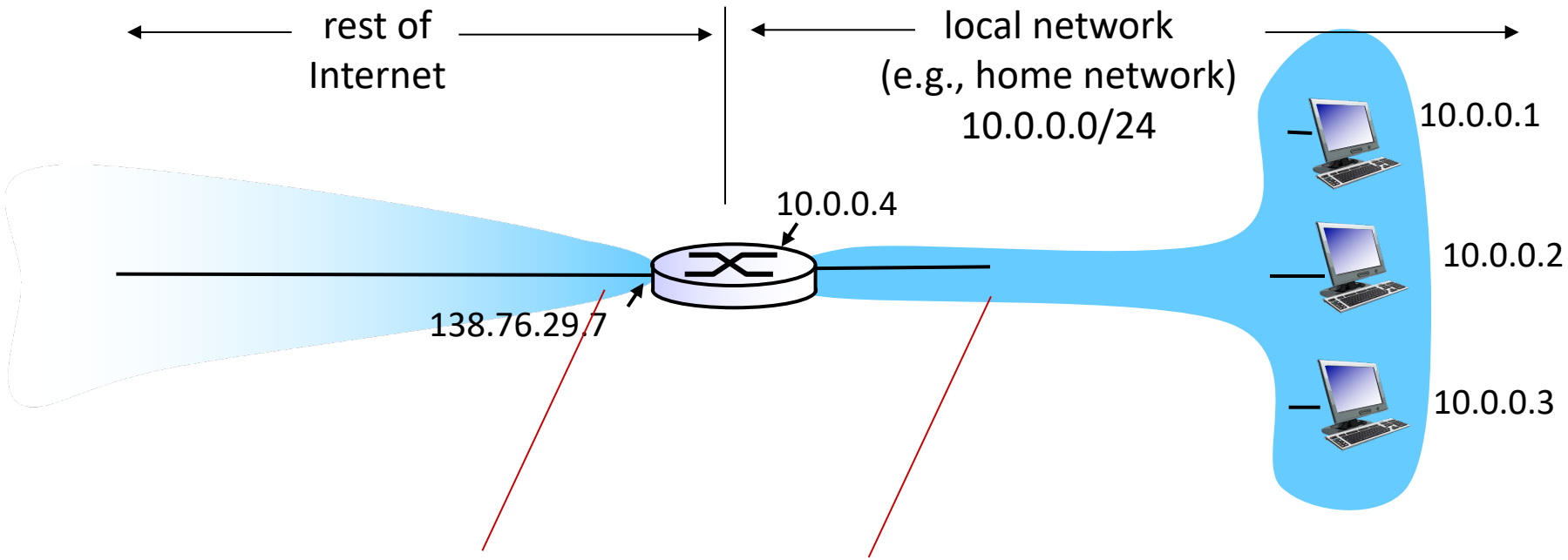
IPv4 Private Address Space and Filtering

According to standards set forth in Internet Engineering Task Force (IETF) document RFC-1918, the following IPv4 address ranges are reserved by the IANA for private internets, and are *not* publicly routable on the global internet:

- **10.0.0.0/8 IP addresses:** 10.0.0.0 – 10.255.255.255
- **172.16.0.0/12 IP addresses:** 172.16.0.0 – 172.31.255.255
- **192.168.0.0/16 IP addresses:** 192.168.0.0 – 192.168.255.255

Note that only a *portion* of the "172" and the "192" address ranges are designated for private use. The remaining addresses are considered "public," and thus are routable on the global Internet.

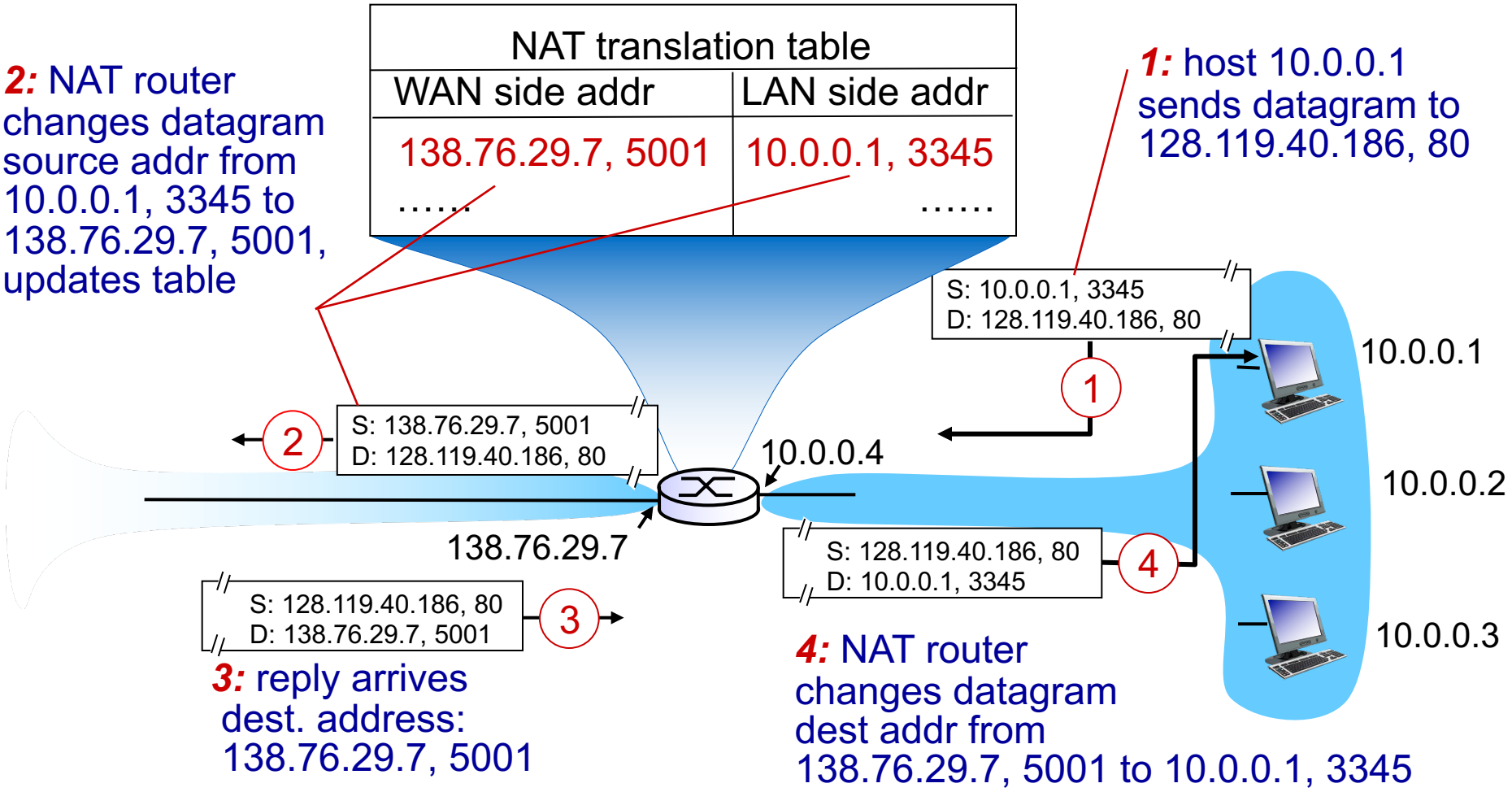
NAT: network address translation



all datagrams *leaving* local network have *same* single source NAT IP address: 138.76.29.7,different source port numbers

datagrams with source or destination in this network have 10.0.0.0/24 address for source, destination (as usual)

NAT: network address translation



NAT: network address translation

motivation: local network uses just one IP address as far as outside world is concerned:

- range of addresses not needed from ISP: just one IP address for all devices
- can change addresses of devices in local network without notifying outside world
- can change ISP without changing addresses of devices in local network
- devices inside local net not explicitly addressable, visible by outside world (a security plus)

NAT: network address translation

implementation: NAT router must:

- *outgoing datagrams: replace* (source IP address, port #) of every outgoing datagram to (NAT IP address, new port #)

  . . . remote clients/servers will respond using (NAT IP address, new port #) as destination addr

- *remember (in NAT translation table)* every (source IP address, port #) to (NAT IP address, new port #) translation pair

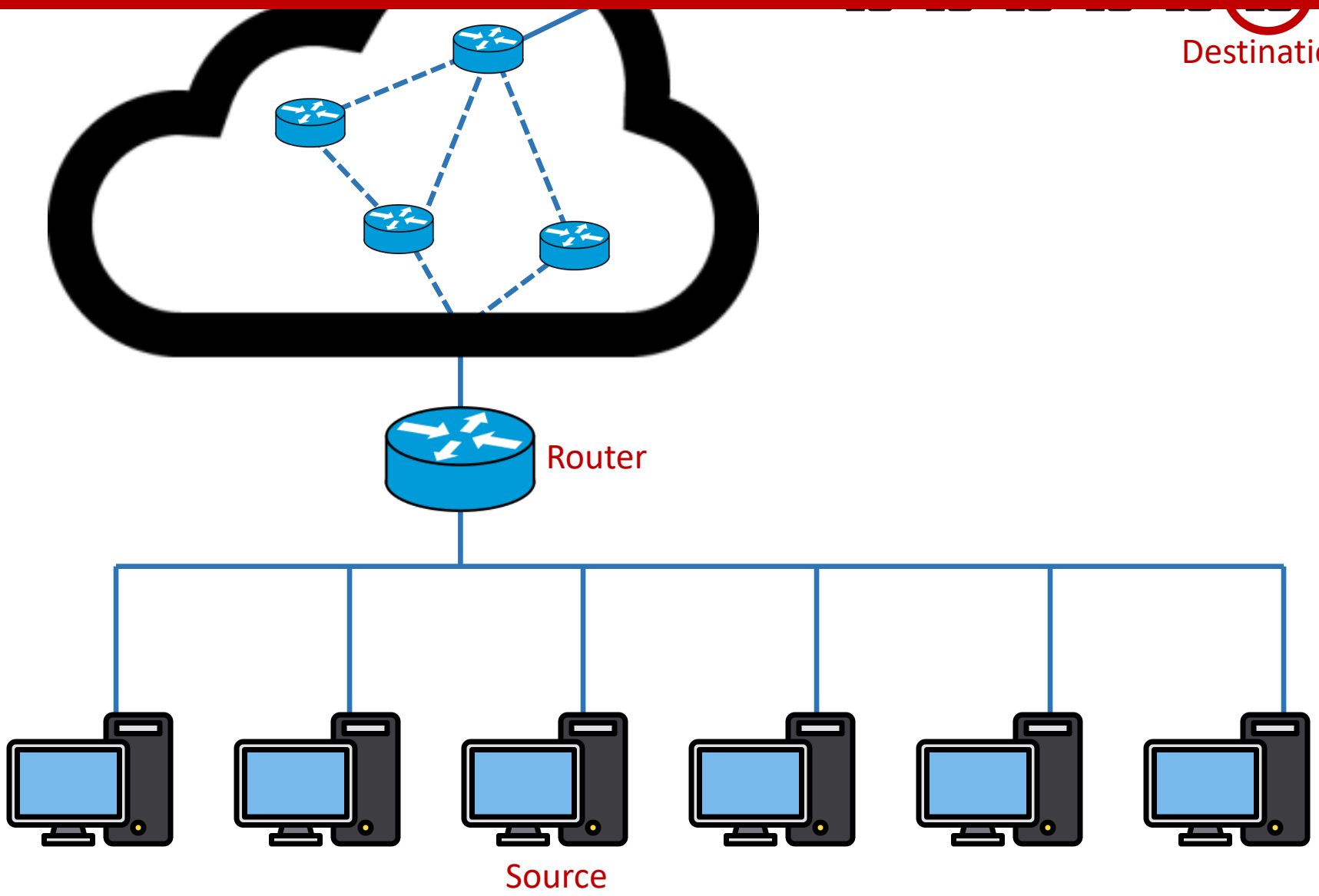
- *incoming datagrams: replace* (NAT IP address, new port #) in dest fields of every incoming datagram with corresponding (source IP address, port #) stored in NAT table

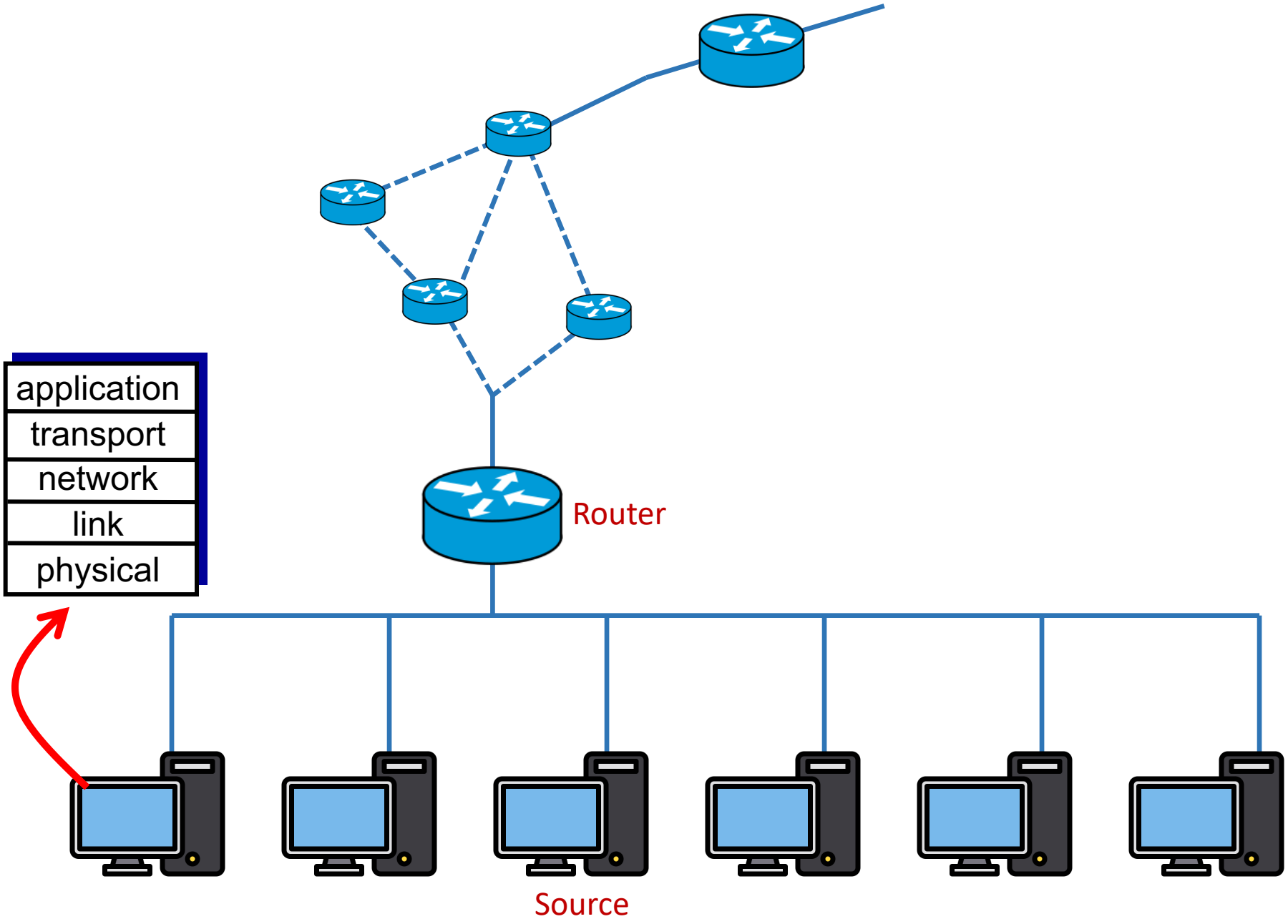
NAT: network address translation

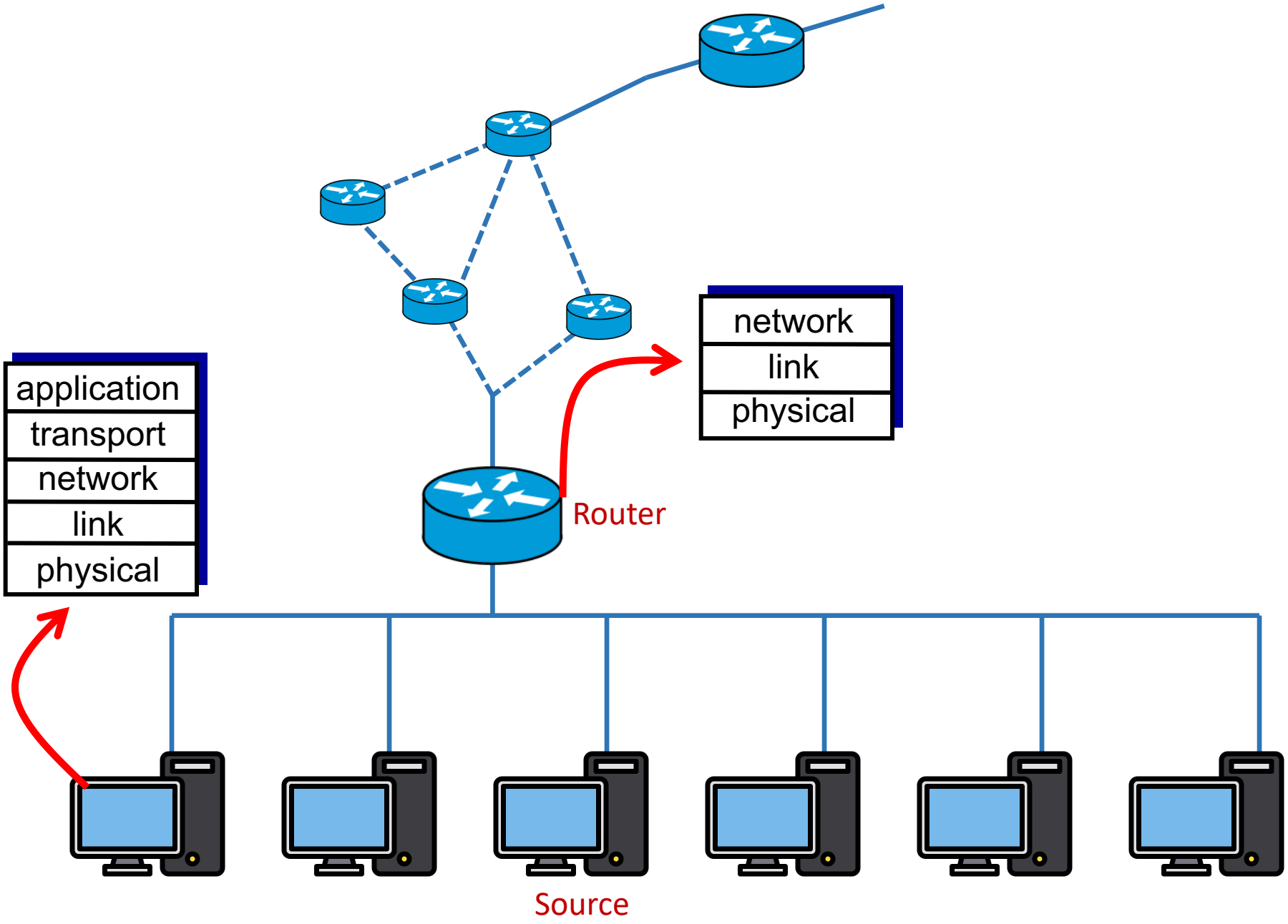
- 16-bit port-number field:
  - Over 60,000 simultaneous connections with a single LAN-side address!
- NAT challenges:
  - violates end-to-end argument
    - NAT possibility must be taken into account by app designers, e.g., P2P applications
  - NAT traversal: what if client wants to connect to server behind NAT?

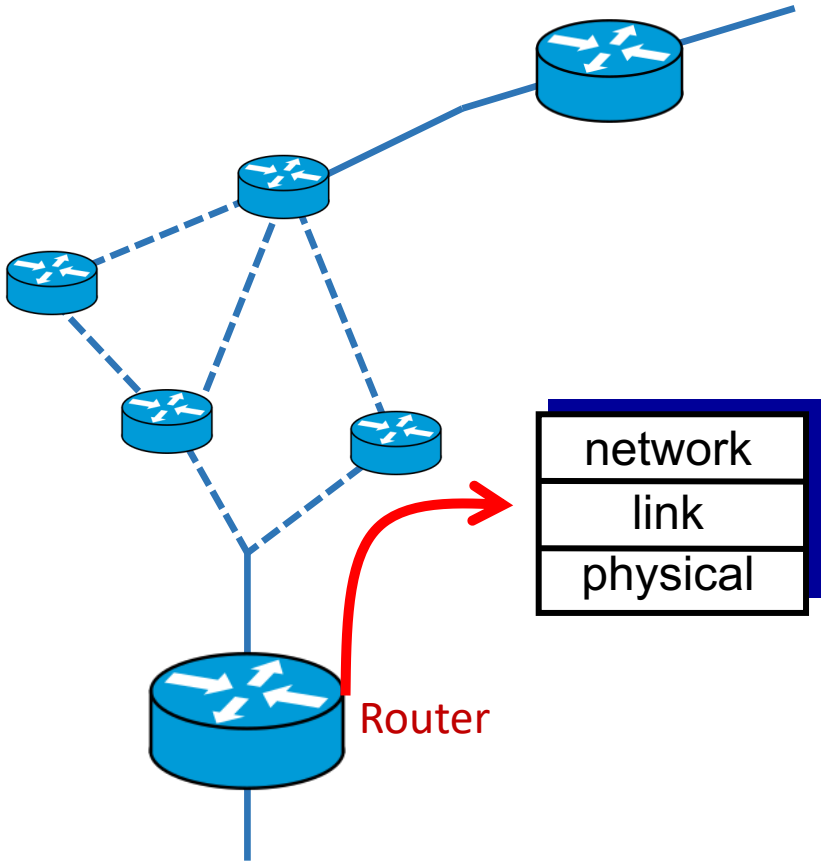
Network-specific address (IP address) vs LAN-specific address (HW address)

Two perspectives of addresses: (1)Network-to-network & (2)machine-to-machine

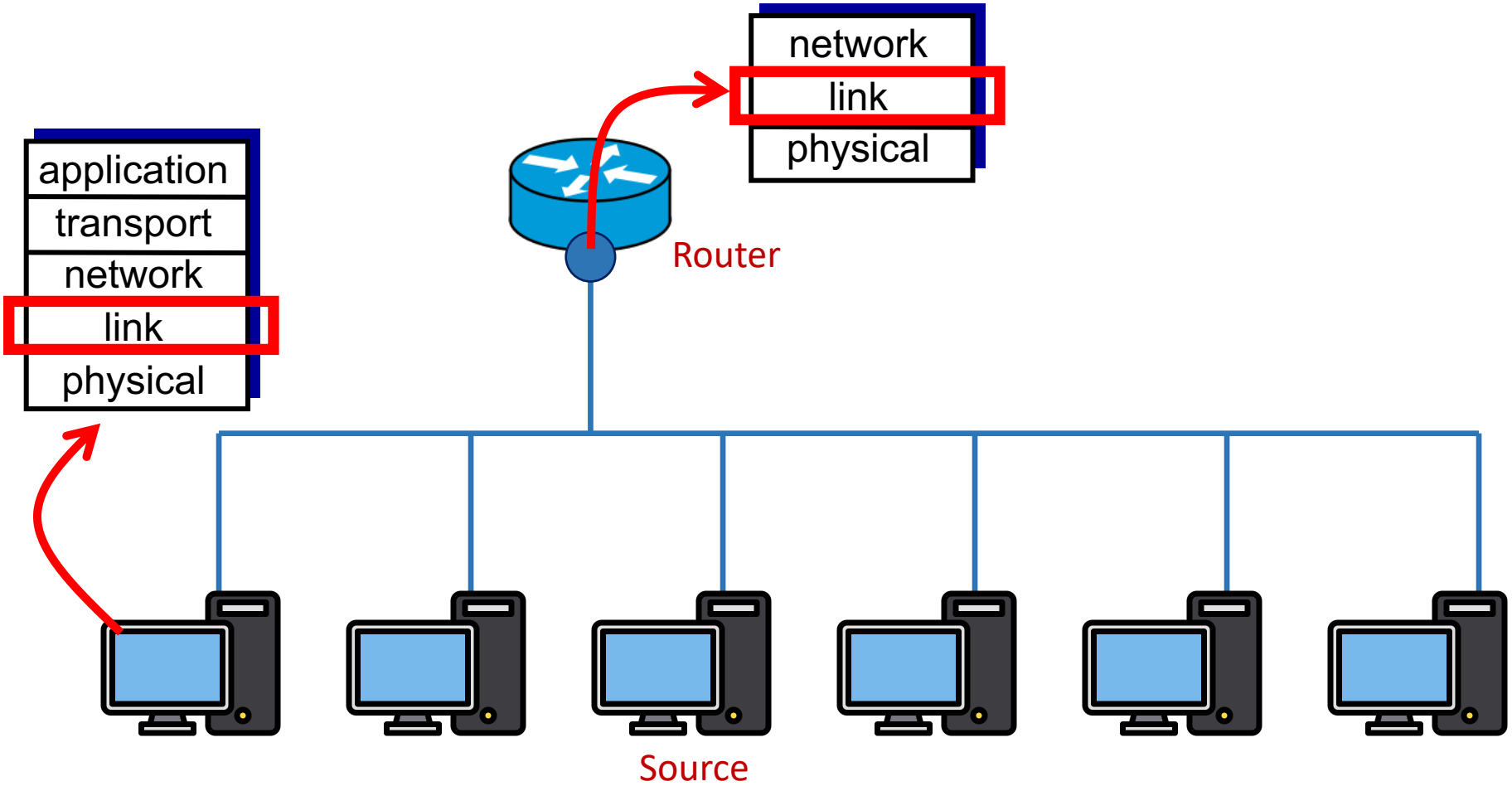



application
transport
network
link
physical
Router
Source

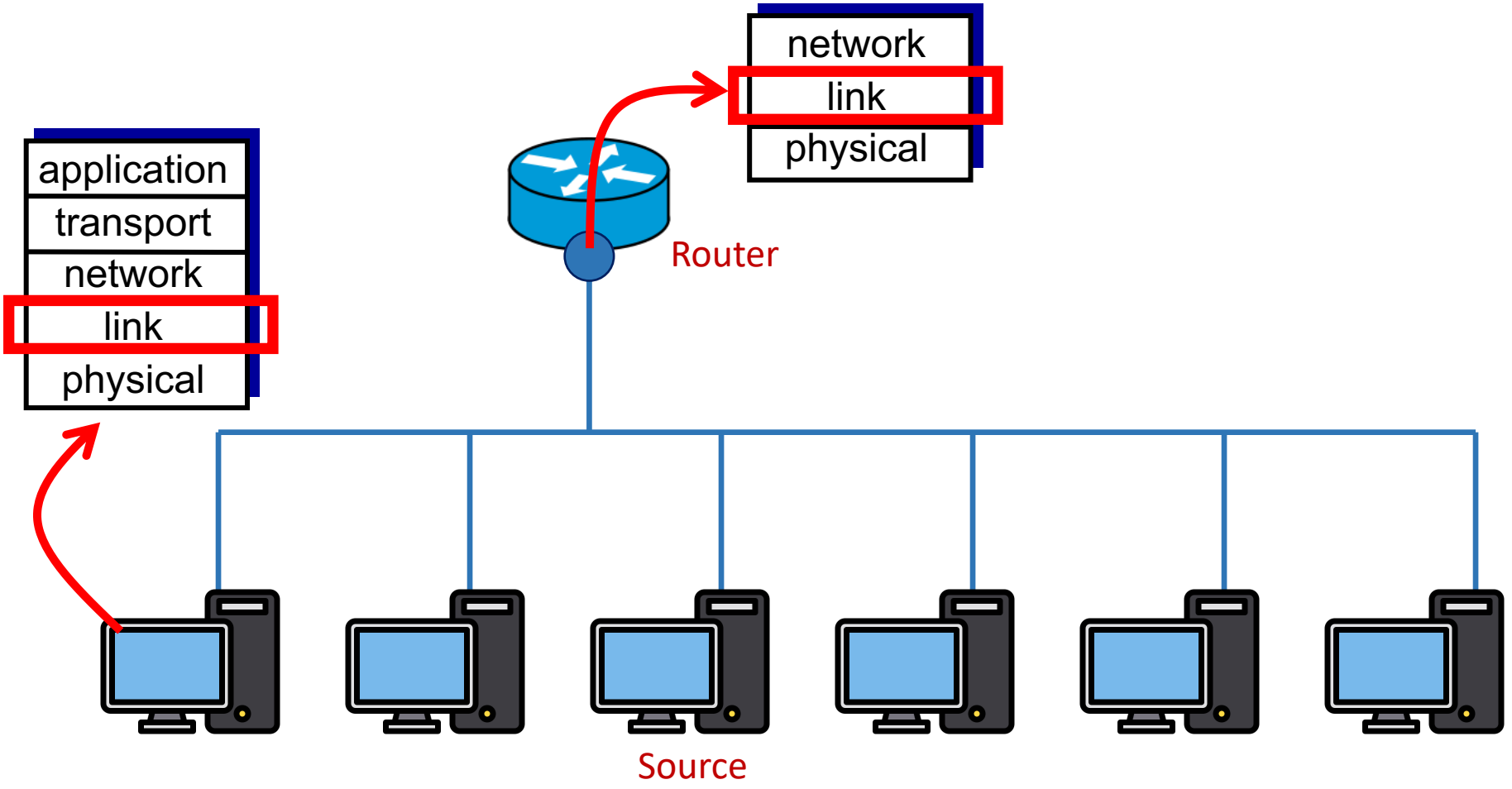

application
transport
network
link
physical
network
link
physical
Router
Source



Hierarchical address for addressing networks
(IP address)


network
link
physical
application
transport
network
link
physical
Router
Source

Flat address for addressing machines at the link-layer (MAC address)



Address Resolution Protocol (ARP)

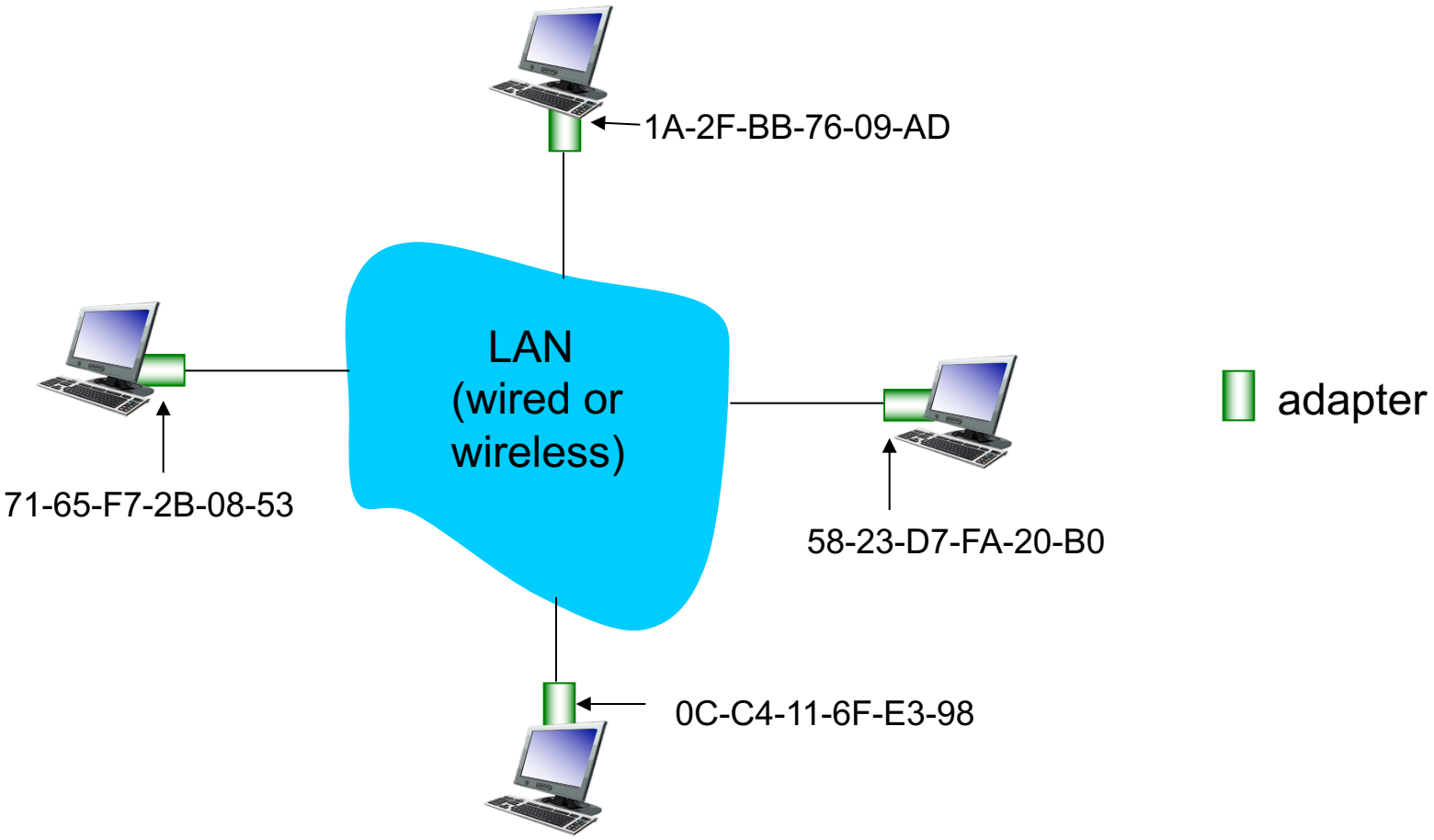
MAC addresses and ARP

- 32-bit IP address:
  - *network-layer* address for interface
  - used for layer 3 (network layer) forwarding
- MAC (or LAN or physical or Ethernet) address:
  - function: *used "locally" to get frame from one interface to another physically-connected interface (same network, in IP-addressing sense)*
  - 48 bit MAC address (for most LANs) burned in NIC ROM, also sometimes software settable
  - e.g.: 1A-2F-BB-76-09-AD

hexadecimal (base 16) notation
(each "numeral" represents 4 bits)

MAC addresses and ARP

each adapter on LAN has unique *LAN* addr. or MAC addr.

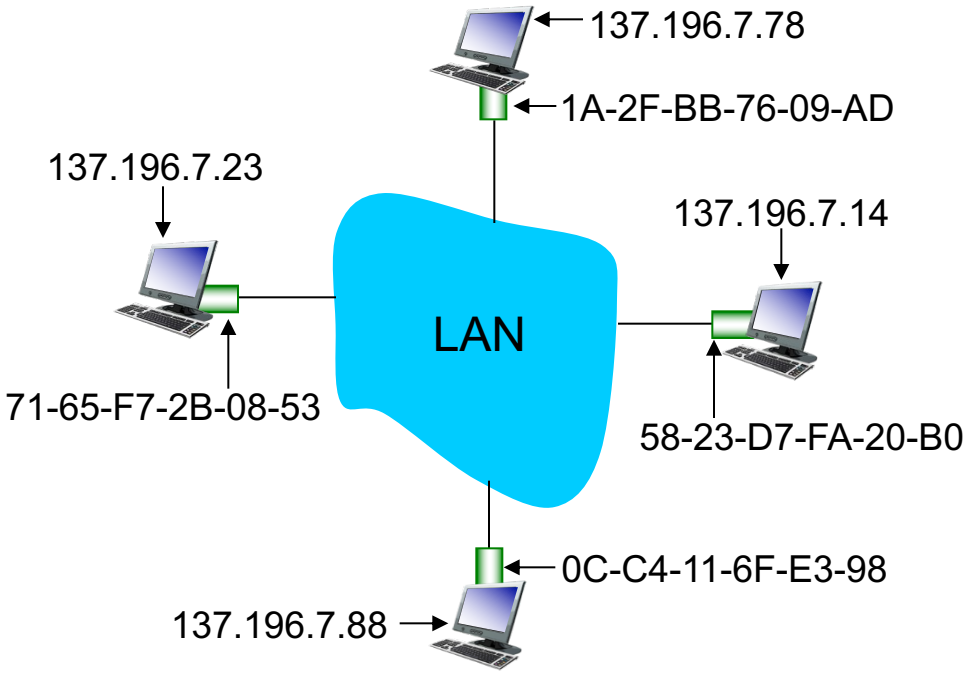


MAC addresses (more)

- MAC address allocation administered by IEEE
- manufacturer buys portion of MAC address space (to assure uniqueness)
- analogy:
  - MAC address: like Social Security Number
  - IP address: like postal address
- MAC flat address ➜ portability
  - can move LAN card from one LAN to another
- IP hierarchical address *not* portable
  - address depends on IP subnet to which node is attached

ARP: address resolution protocol

Question: how to determine interface's MAC address, knowing its IP address?



ARP table: each IP node (host, router) on LAN has table

- IP/MAC address mappings for some LAN nodes:

  < IP address; MAC address; TTL>

- TTL (Time To Live): time after which address mapping will be forgotten (typically 20 min)

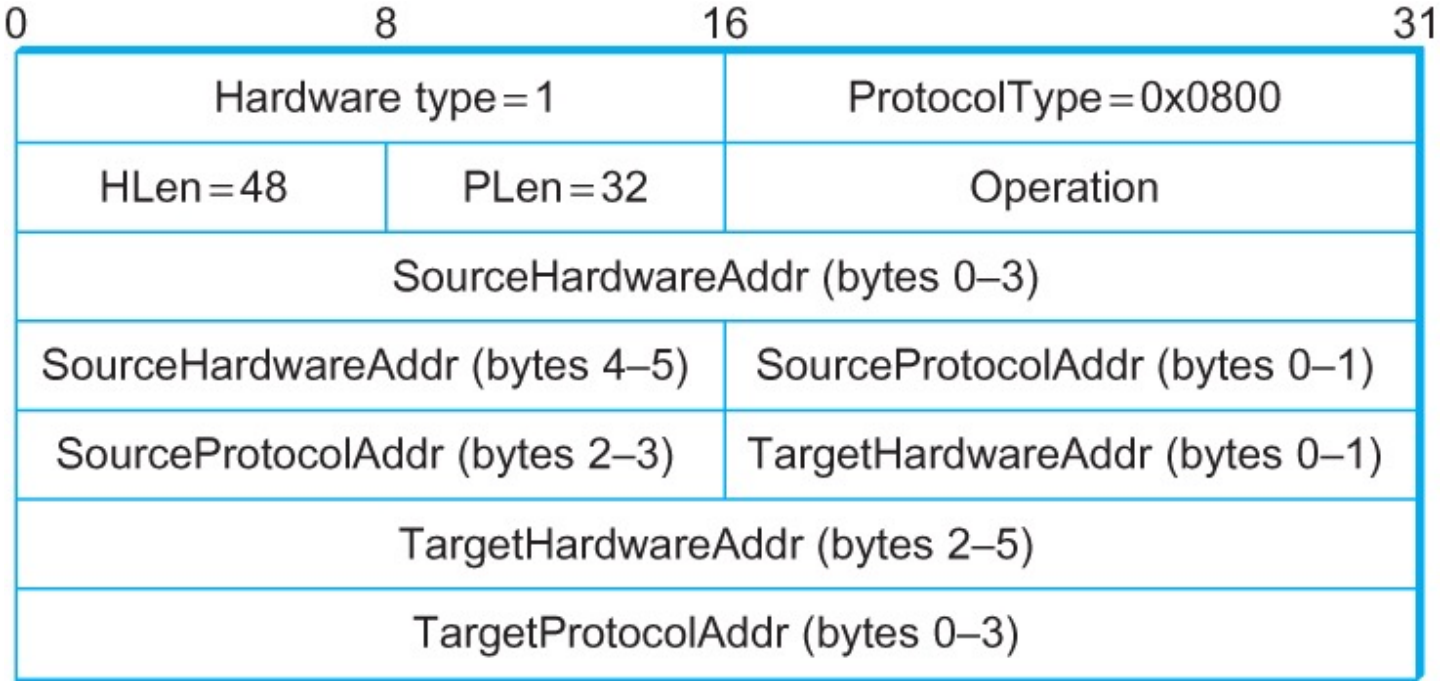
ARP protocol: same LAN

1. A wants to send datagram to B
   - B's MAC address not in A's ARP table.
2. A broadcasts ARP query packet, containing B's IP address
   - destination MAC address = FF-FF-FF-FF-FF-FF
   - all nodes on LAN receive ARP query
3. B receives ARP packet, replies to A with its (B's) MAC address
   - frame sent to A's MAC address (unicast)
4. A caches (saves) IP-to-MAC address pair in its ARP table until information becomes old (times out)
   - soft state: information that times out (goes away) unless refreshed
5. ARP is "plug-and-play":
   - nodes create their ARP tables *without intervention from net administrator*

Address Translation Protocol (ARP)

- Map IP addresses into physical addresses
  - destination host
  - next hop router
- Techniques
  - encode physical address in host part of IP address
  - table-based
- ARP (Address Resolution Protocol)
  - table of IP to physical address bindings
  - broadcast request if IP address not in table
  - target machine responds with its physical address
  - table entries are discarded if not refreshed
  - Query message include the physical address of the sending host. Why?

ARP Packet Format



- HardwareType: type of physical network (e.g., Ethernet)
- ProtocolType: type of higher layer protocol (e.g., IP)
- HLEN & PLEN: length of physical and protocol addresses
- Operation: request or response
- Source/Target Physical/Protocol addresses