CS 352
Internet Protocol (IP)

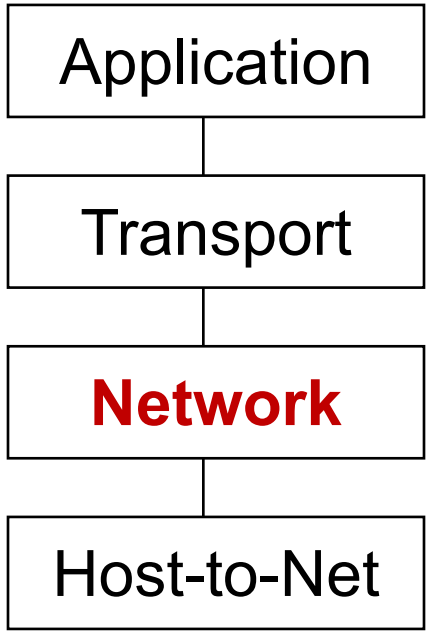
CS 352, Lecture 16.1

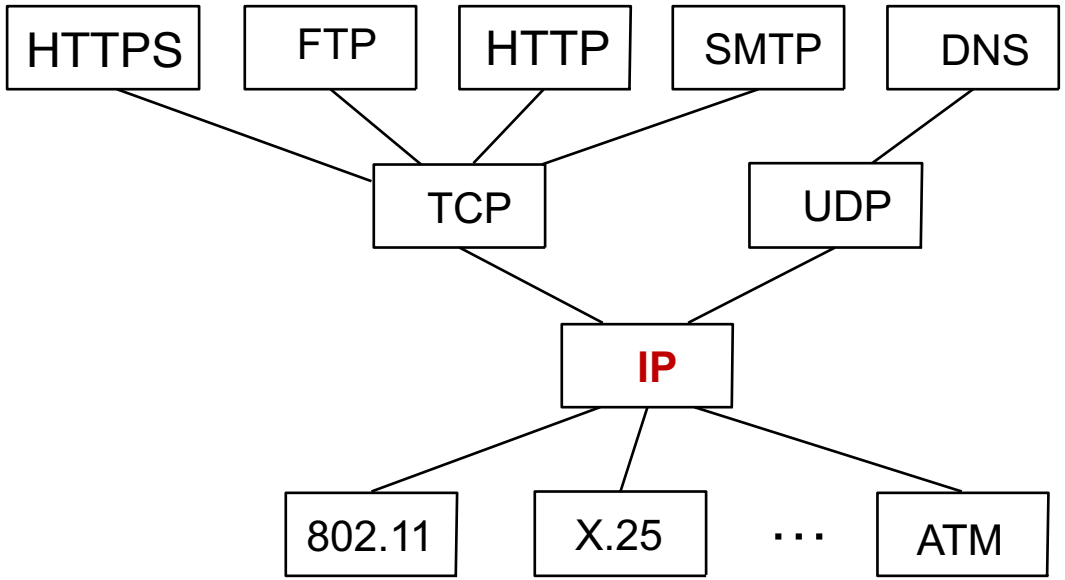
http://www.cs.rutgers.edu/~sn624/352

Srinivas Narayana

RUTGERS
UNIVERSITY | NEW BRUNSWICK

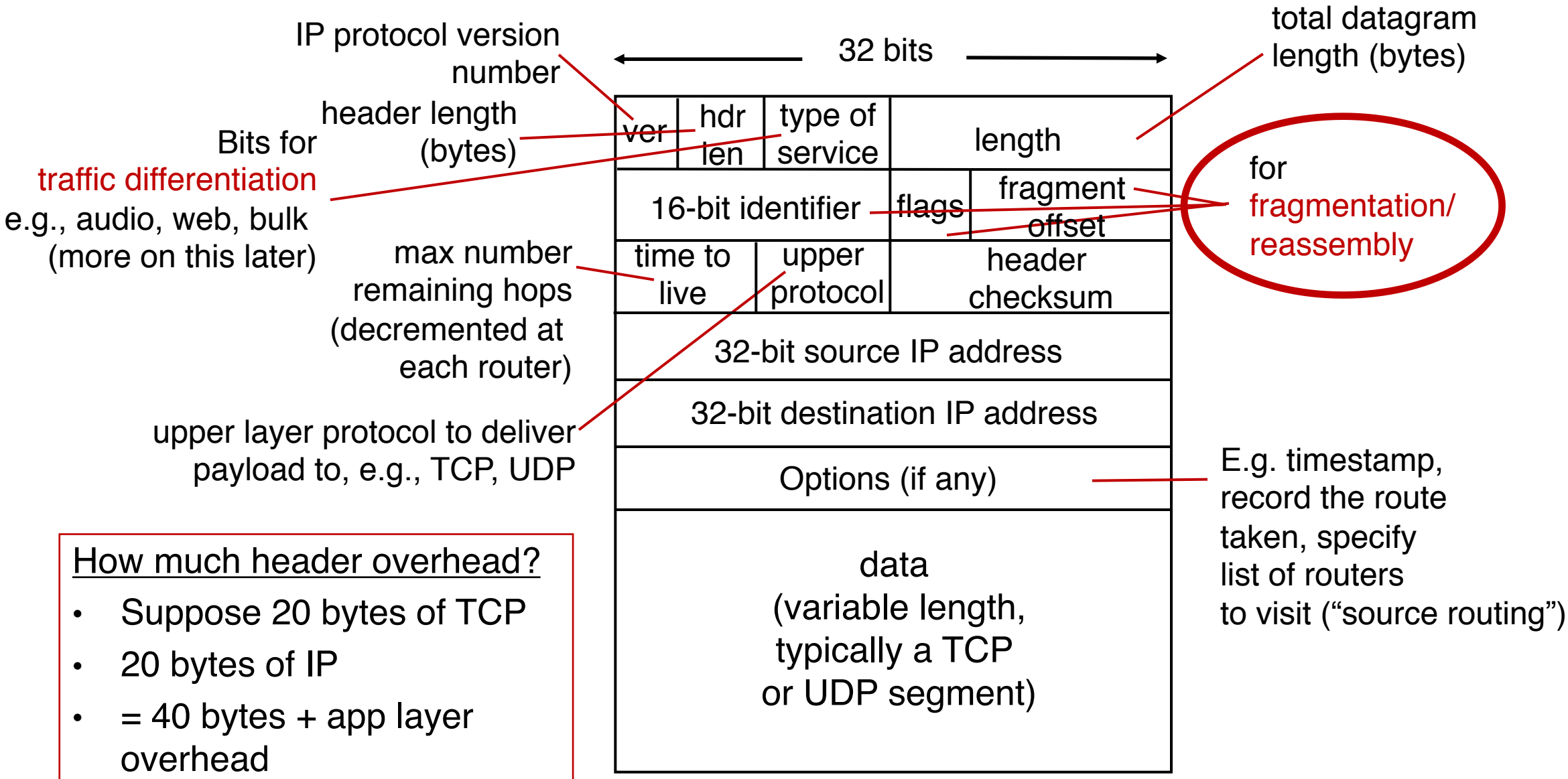
Network





The main function of the network layer is to
move packets from one endpoint to another.

IPv4 Datagram Format

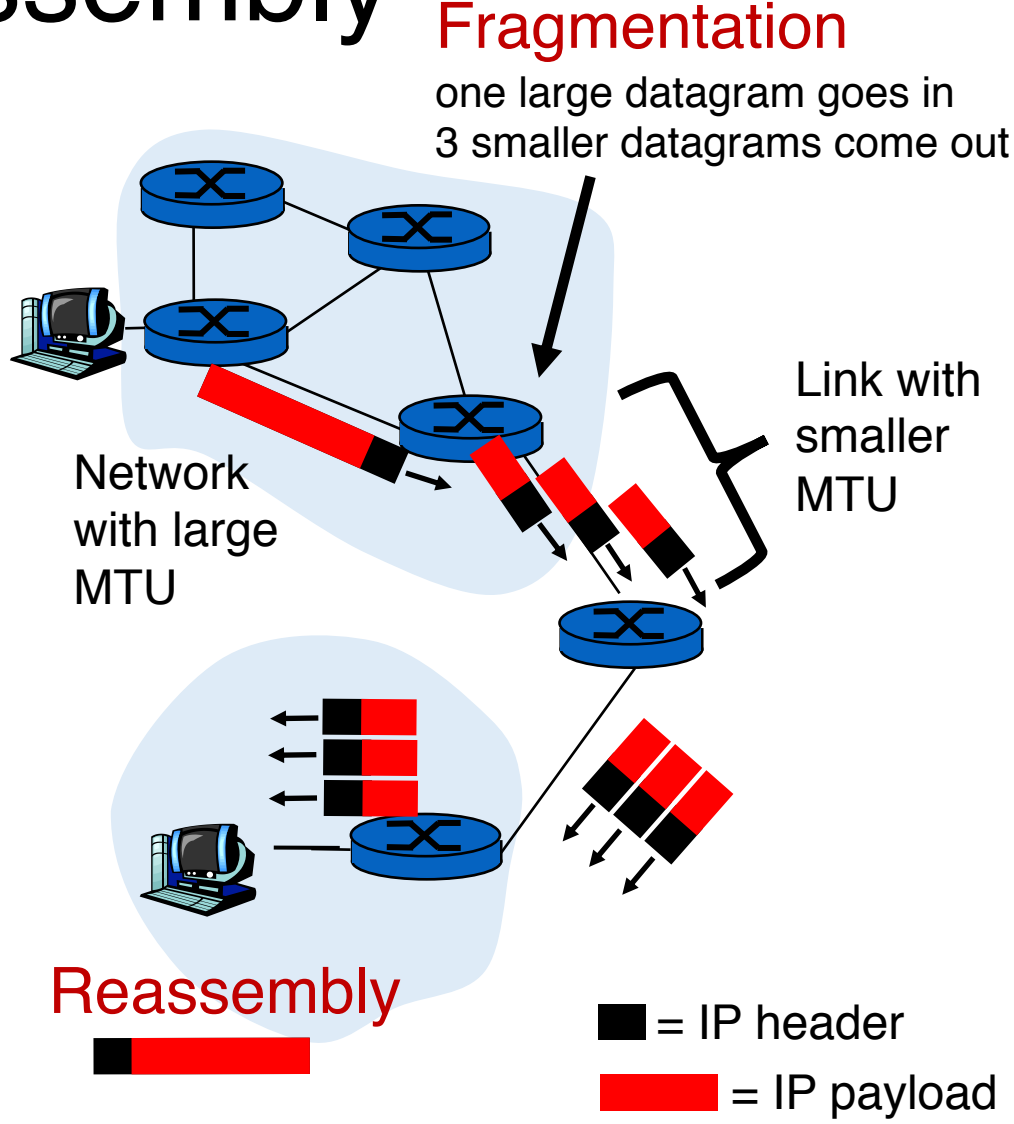


How much header overhead?

- Suppose 20 bytes of TCP
- 20 bytes of IP
- = 40 bytes + app layer overhead

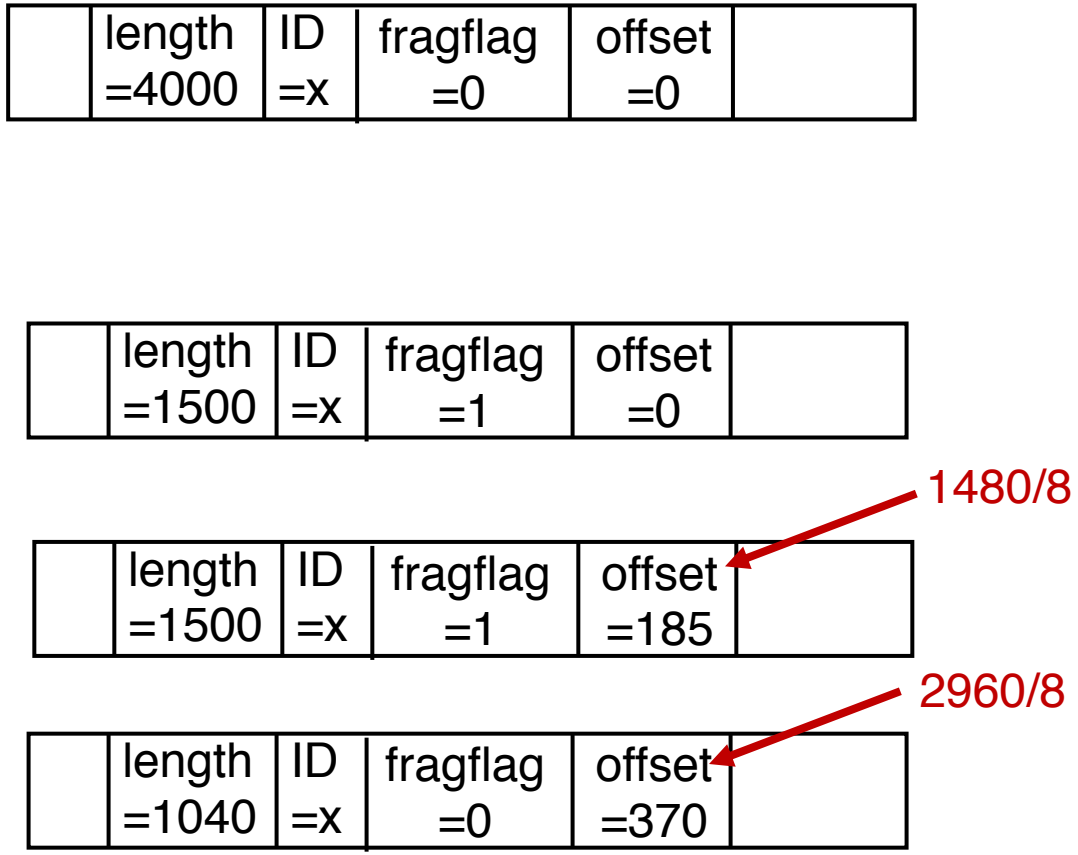
IP fragmentation and reassembly

- Links and transmission media have MTUs (maximum transmission unit):
  - Largest possible link-level frame
- On a network path, a packet might traverse links with different MTUs
- This may result in a large IP datagram to be divided (fragmented) by a router
  - Fragments reassembled only at the destination endpoint, at the IP layer
  - IP header bits used to identify and reassemble related fragments



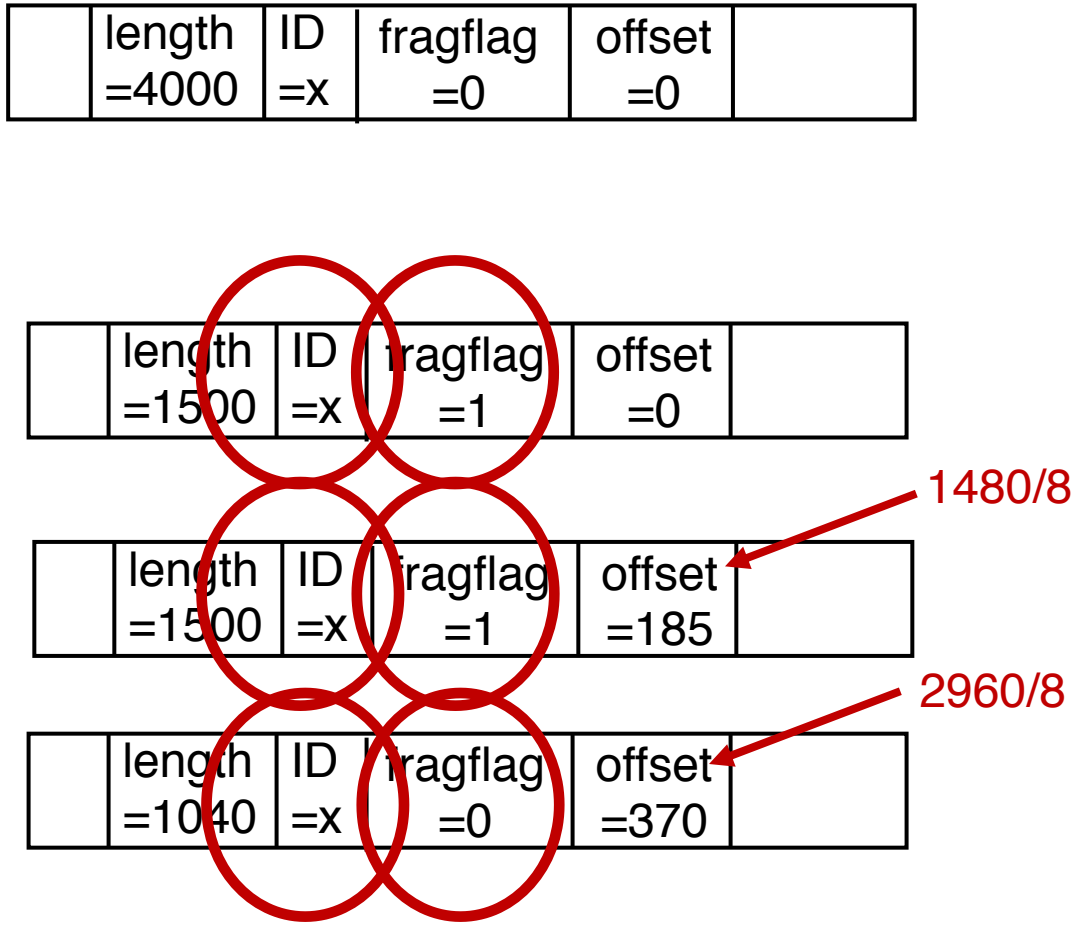
IP fragmentation and reassembly

- Suppose a large 4000-byte datagram reaches a router. The next link has MTU 1500 bytes.
  - Note: MTU includes IP headers, so does the length field of the IP header. IP payload = 3980 bytes.
- Result: 3 datagrams of length 1500, 1500, 1040 bytes resp.
  - IP payload = 1480, 1480, 1020 bytes resp. (adds to 3980)
- Offset field = index of payload byte / 8



IP fragmentation and reassembly

- At the destination endpoints, the fragments are reassembled using the IP identifier field
  - Fragments of the same original datagram share the same IP ID
- The fragmentation flag is set to 0 for the terminal fragment, and 1, if other fragments follow
- The offset field allows the IP stack to reassemble the fragments in order into a single IP datagram



The rest of this lecture and the next

- We'll talk about some support protocols and mechanisms for the network layer
  - Protocols: DHCP, ICMP, ARP
  - Mechanisms: NAT
  - We'll also talk about IP version 6 (IPv6)

- Some of these protocols use an IP header underneath their own header (ICMP) or replace the IP header with their own (ARP)
  - But these shouldn't be construed as transport/network protocols
  - They are fundamental to supporting IP/network layer functionality
  - More appropriately discussed as support protocols for the network layer

CS 352
Dynamic Host Configuration

CS 352, Lecture 16.2

http://www.cs.rutgers.edu/~sn624/352

Srinivas Narayana

RUTGERS
UNIVERSITY | NEW BRUNSWICK

How does an endpoint get its IP addr?

- One possibility: hard-code the IP address on the endpoint
  - e.g., a system admin writing addresses in a file
  - UNIX: /etc/network/interfaces
  - Windows: control panel → network → configuration → TCP/IP → properties
- Another possibility: dynamically receive an address “from the network”
  - DHCP: Dynamic Host Configuration Protocol
  - Provide plug-and-play functionality for endpoints (e.g., phones, laptops)

Many similar bootstrapping problems

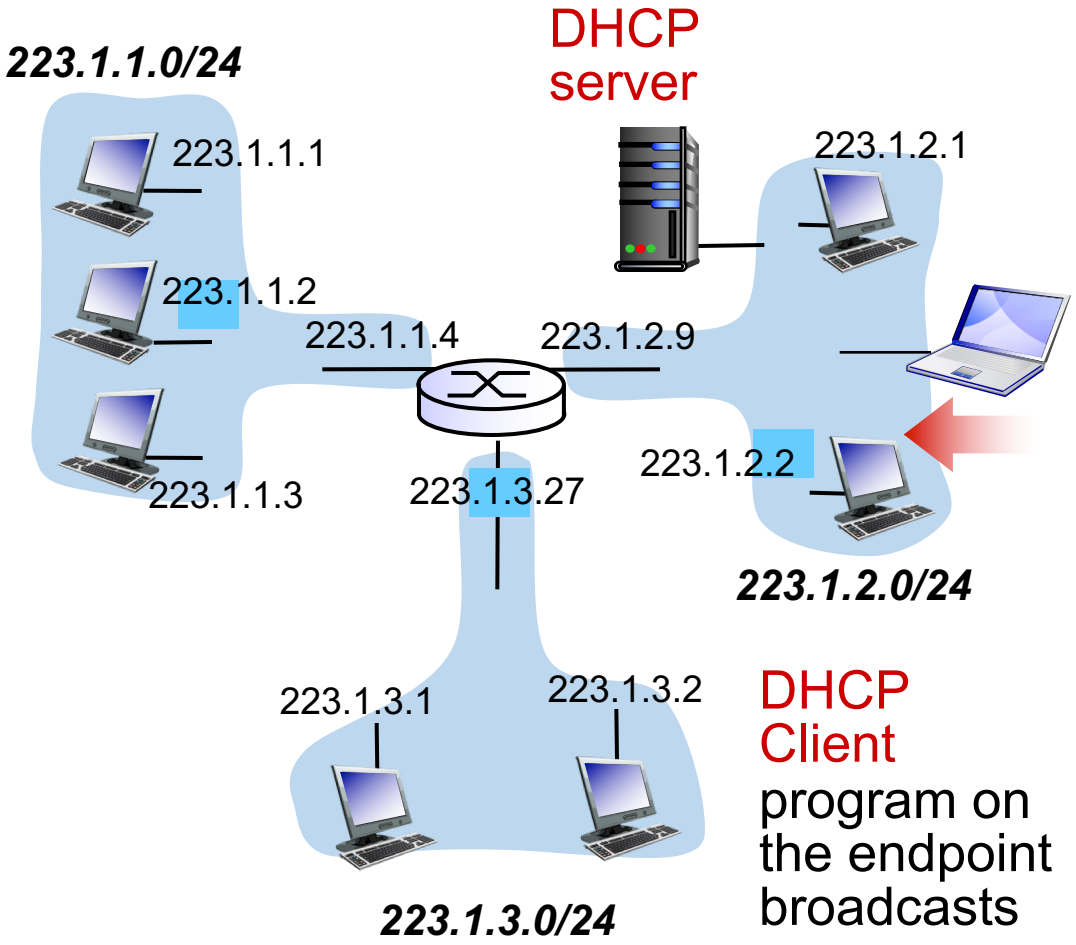
- How does a host get its IP address?
- How does a host know its local DNS server?
- How does a host know its netmask?
  - i.e., so that it can know which other hosts are in the same network
- How does a host know how to reach other networks?
  - i.e., which router is at the “border” of the current network?
  - This router is also called the gateway router: crucial for an endpoint to communicate with another endpoint external to the network

How DHCP works

- A new endpoint that just joins a network knows nothing about the network
  - It doesn't even have a network address for its point of attachment
- It makes no sense to have it contact a "known" server to receive this information.
- The only known mechanism that might work is broadcast:
  - Ask everyone!

How DHCP works

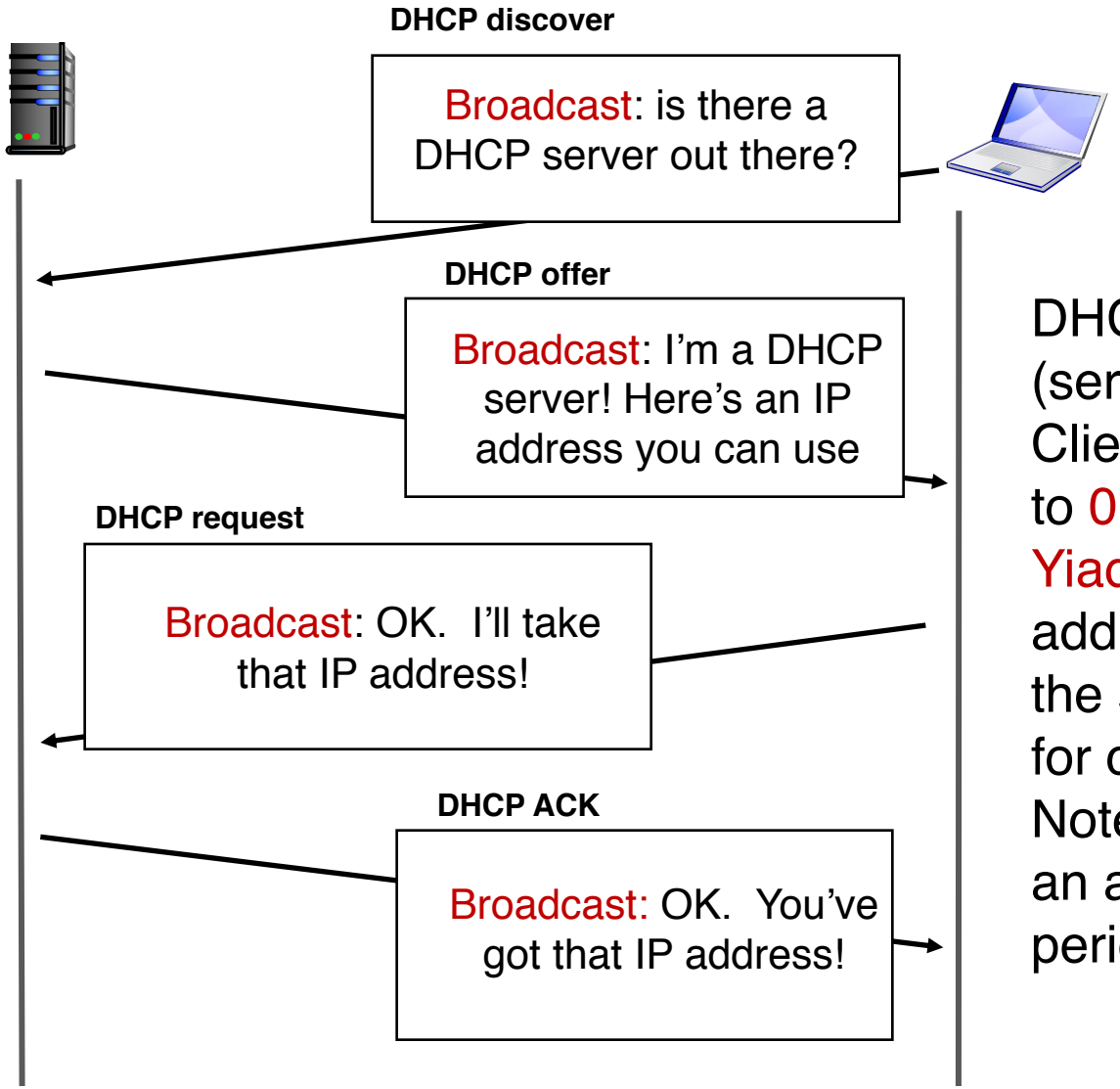
- DHCP allows a host to dynamically obtain its IP address from a server on a network when it joins the network
- DHCP can allow a host to be mobile across different networks, obtaining IP addresses as needed
- DHCP uses leases on addresses
  - Host must renew lease periodically
  - Allows network to reuse an IP with an expired lease, reclaiming addresses from inactive hosts



DHCP Client program on the endpoint broadcasts message requesting an IP address.

DHCP client-server scenario

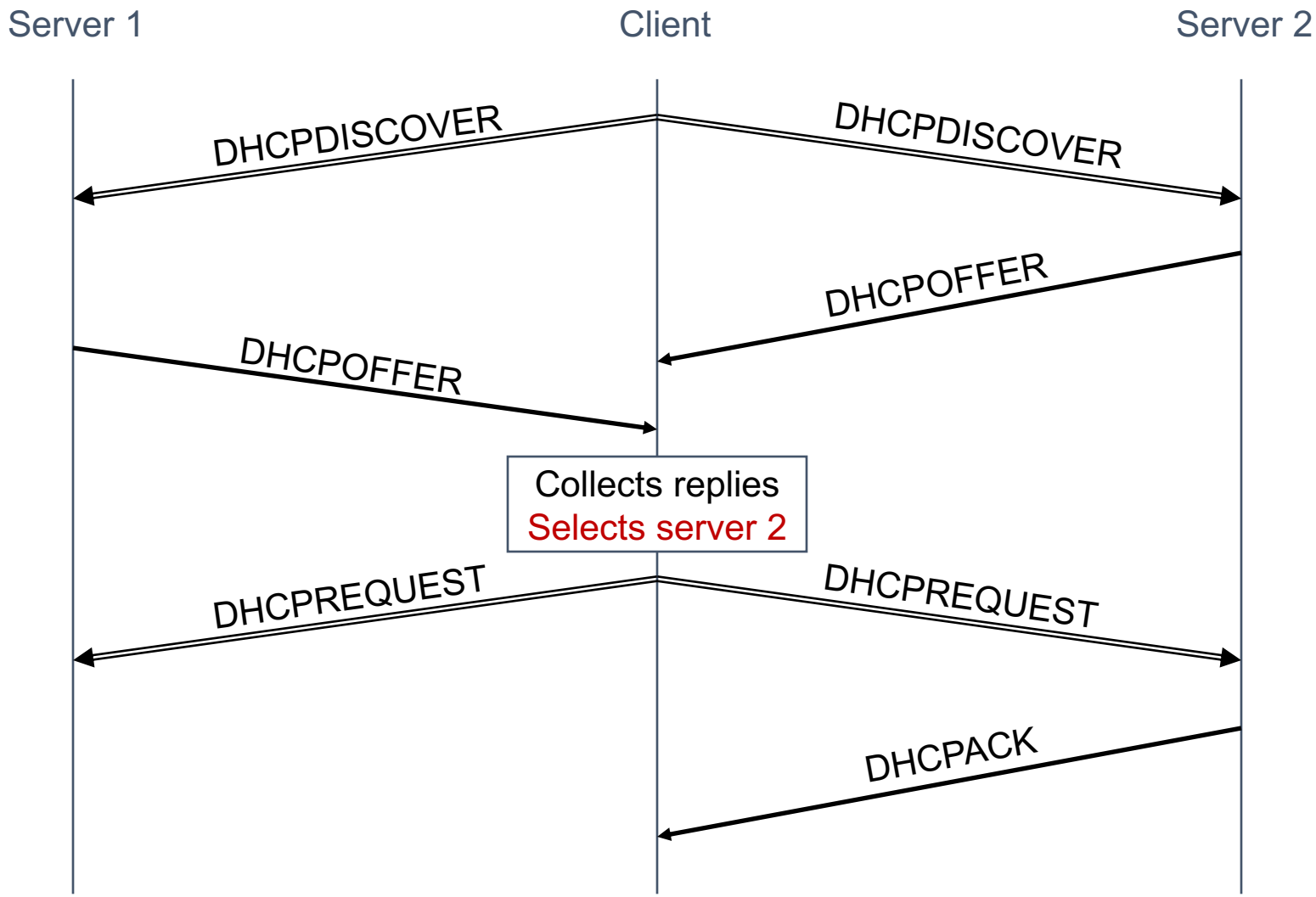
DHCP server:
223.1.2.5



223.1.2.4
Arriving client

DHCP runs on UDP ports 67 (server) and 68 (client)
Client's initial IP address is set to 0.0.0.0
Yiaddr stands for "your IP address" – an address value the server sends to the client for consideration
Note that the IP allocation has an associated lifetime (lease period)

Multiple DHCP servers can coexist



DHCP returns more than an IP address

- Name and IP address of the local DNS server
- Netmask of the IP network the host is on
  - Useful to know whether another endpoint is inside or outside the current IP network
- Address of the gateway router to enable the endpoint to reach other IP networks

Your home router runs DHCP

- Likely, your home devices (laptops, tablets, phones) are all using DHCP-assigned IP addresses
- The DHCP server is running on the control processor of your home's access router (e.g., WiFi router)
- You can access the DHCP client program on Linux using the command `dhclient` and on Linux using `sudo ipconfig <interface> DHCP`

Summary of DHCP

- Want endpoints to have plug and play functionality
  - Avoid tedious manual configuration of IP addresses and other information
- DHCP: a general bootstrapping mechanism for critical information required for network layer functionality
- Hosts can be simple: receive information from DHCP servers by broadcasting over the network

CS 352
Internet Control Message Protocol

CS 352, Lecture 16.3

http://www.cs.rutgers.edu/~sn624/352

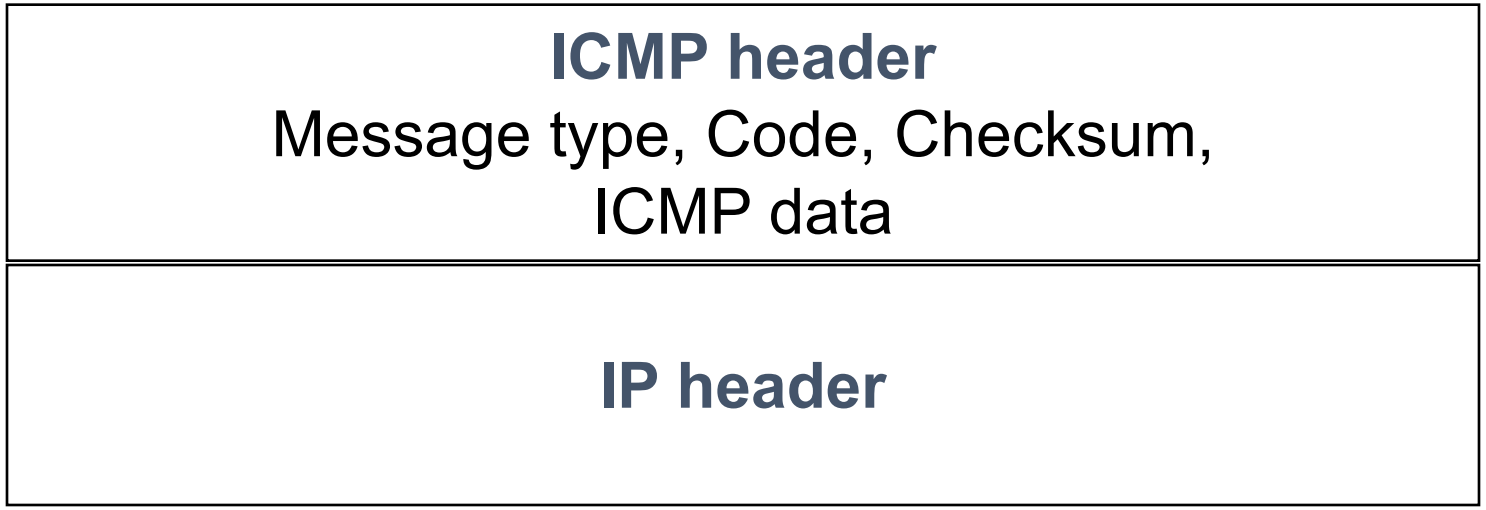
Srinivas Narayana

RUTGERS
UNIVERSITY | NEW BRUNSWICK

Internet Control Message Protocol

- A protocol for troubleshooting and diagnostics
- Works over IP: unreliable delivery of packets
- Some functions of ICMP:
  - Determine reachability and network errors
  - Specify that packets have been in the network for too long

ICMP message



https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol#Control_messages

Specific uses of ICMP

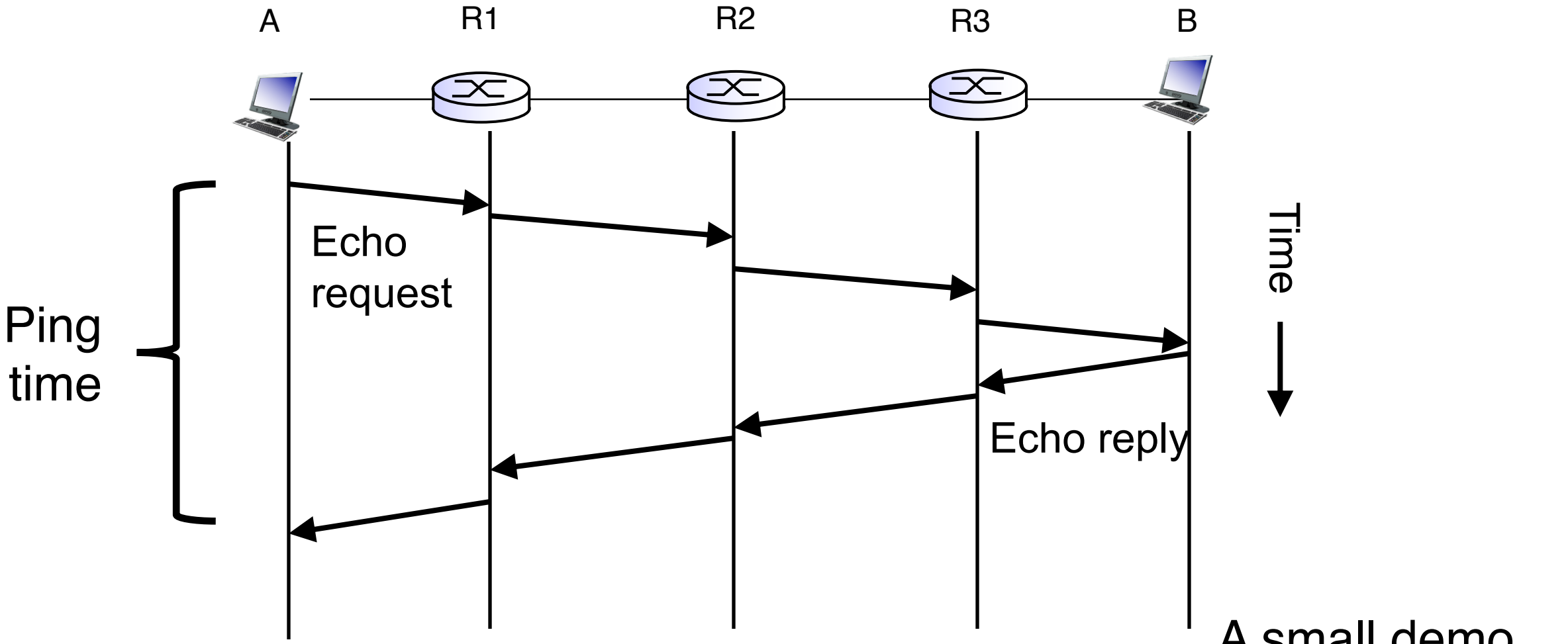
- Echo request reply
  - Check remotely if an endpoint is alive and connected
- An unreachable destination
  - Invalid address and/or port
- Knowing if packet's IP time-to-live expired
  - Example, due to routing loops

- Look at two tools built using ICMP: ping and traceroute

Ping

- Uses ICMP echo request (type=8, code=0) and reply (type=0, code=0)
- Source sends ICMP echo request message to dst address
- Destination replies with an ICMP echo reply message containing the data in the original echo request message
- Source can calculate round trip time (RTT) of packets
- If no echo reply comes back, then the destination is unreachable
- Don’t need to have a server program running on the other side
  - In general, the remote endpoint can be completely outside your control

Ping



A small demo…

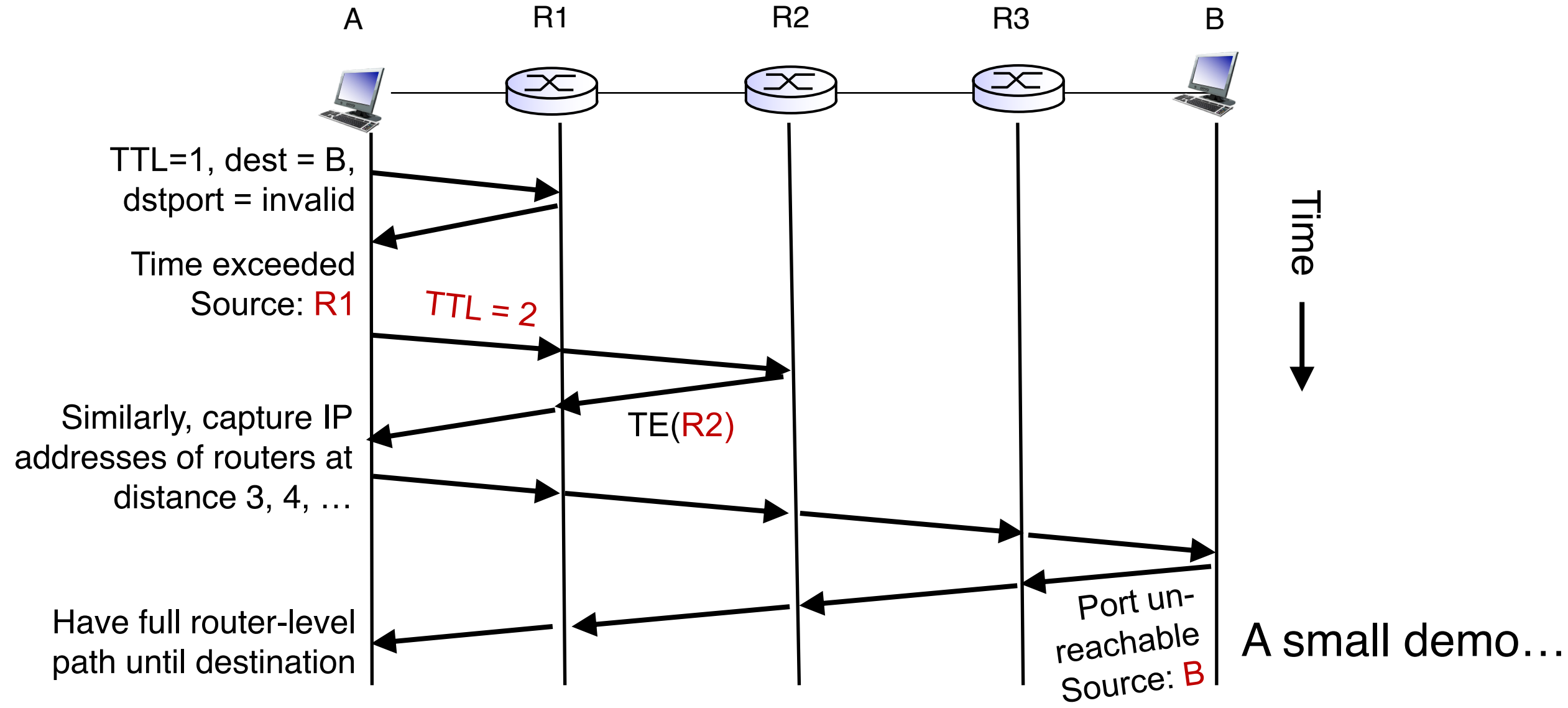
Traceroute

- A tool that can record the router-level path taken by packets
- A clever use of the IP time-to-live (TTL) field
- In general, when a router receives an IP packet, it decrements the TTL field on the packet
  - A failsafe mechanism to ensure packets don't keep taking up network resources for too long
- If a router receives a packet with TTL=0, it sends an ICMP time exceeded message (type=11, code=0) to the source endpoint

Traceroute

- Traceroute sends multiple packets to a destination endpoint
- But it progressively increases the TTL on those packets: 1, 2, ...
- Every time a time exceeded message is received, record the router's IP address
- Process repeated until the destination endpoint is reached
- If the packet reaches the destination endpoint (i.e.: TTL is high enough), then the endpoint sends a port unreachable message

Traceroute



A small demo…

Summary of ICMP

- A protocol for network diagnostics and troubleshooting
- Two useful tools: ping and traceroute
- Ping: test connectivity to a machine totally outside your control
  - Use ICMP echo request and reply
- Traceroute: determine router-level path to a remote endpoint
  - A smart use of the TTL field in the IP header