CS3640

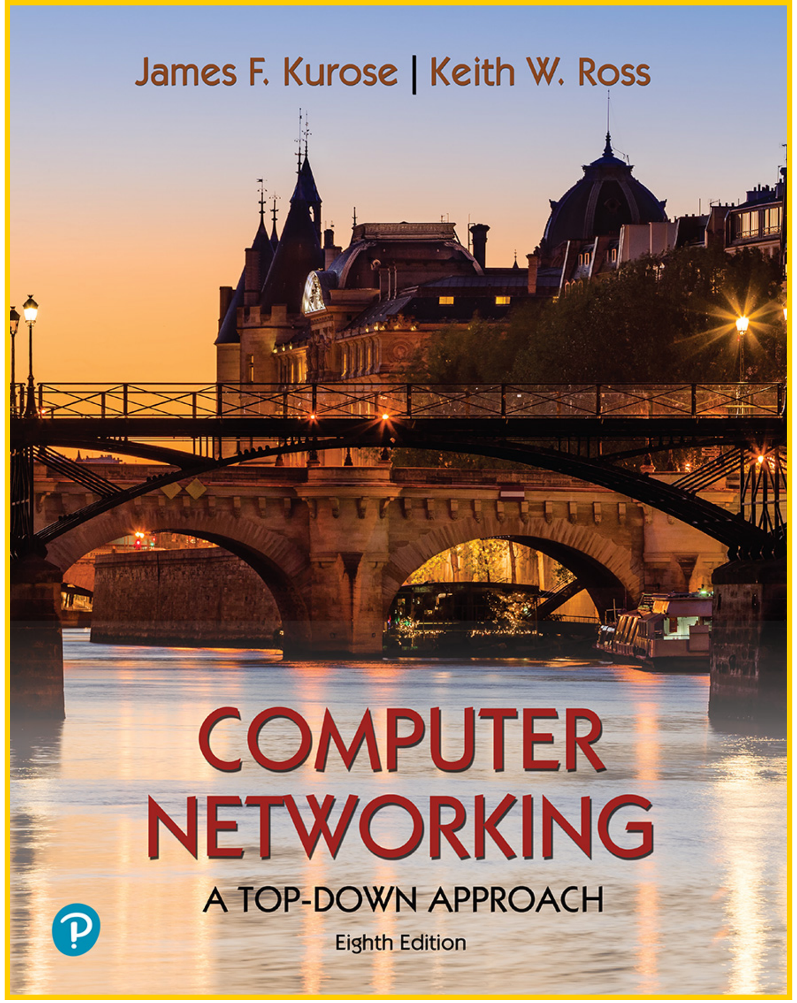
Network Layer (3): The Internet Protocol

Prof. Supreeth Shastri
Computer Science
The University of Iowa

Lecture goals

a two-part discussion on the Internet Protocol, its functionalities, shortcomings, and real-life solutions

- *IPv4 format and addressing*
- *Address management via DHCP*
- *IPv6*
- *NAT and Middleboxes*



Chapters 4.3, 4.5

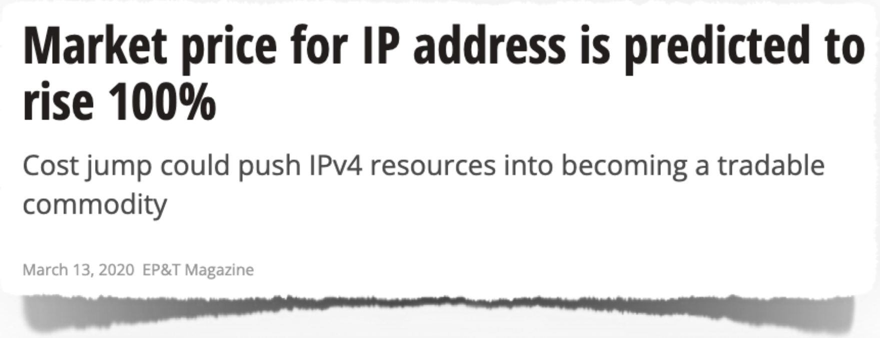
Previously on CS3640

IP address

- ➡ 32-bit unique ID associated with every network entity
- ➡ New nodes join the Internet by getting a new IP address
- ➡ IP routers learn about them, and forward packets

Total available IP addresses ≈ **4 billion**

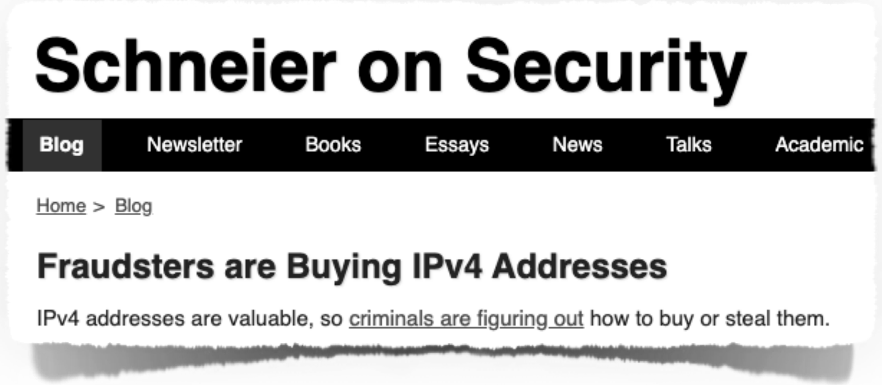
- ➡ In 1981 (when IPv4 was standardized), no one expected the Internet to have billions of nodes
- ➡ However, the rapid growth of the Internet started depleting this resource



Market price for IP address is predicted to rise 100%

Cost jump could push IPv4 resources into becoming a tradable commodity

March 13, 2020 EP&T Magazine



Schneier on Security

Fraudsters are Buying IPv4 Addresses

IPv4 addresses are valuable, so criminals are figuring out how to buy or steal them.

ICANN allocated the last chunk of IPv4 addresses in 2011

Then, how do new hosts obtain and manage their IP addresses?

1

Create a new version of the Internet Protocol w/ larger range of addresses

2

Figure out a way to reuse the existing 32-bit address space

IPv6

(or what the Internet visionaries proposed)

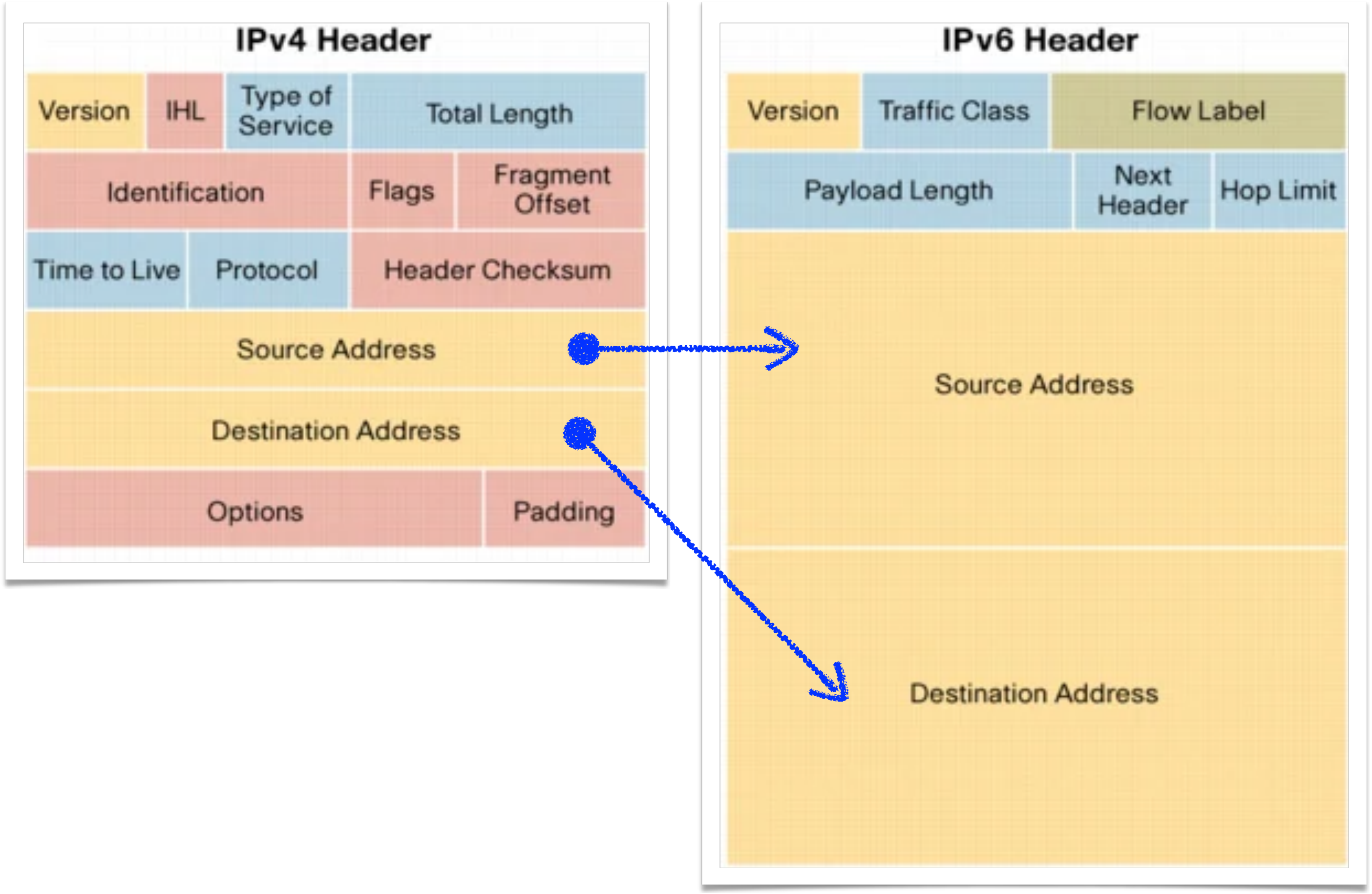
IPv6

Expanded addressing

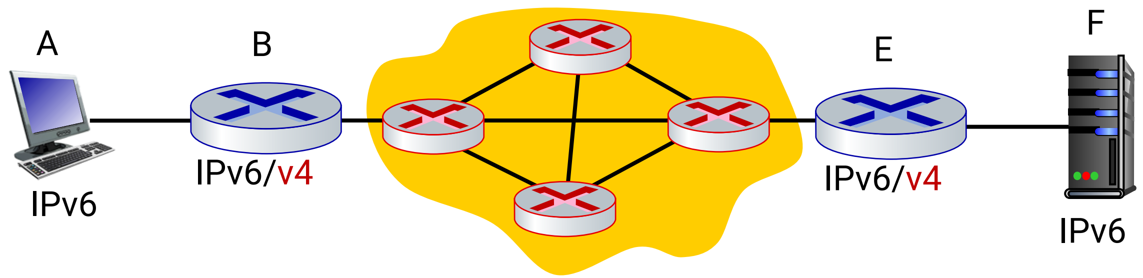
The available address space increased from 2^{32} (4 billion) to 2^{128} (340 trillion trillion trillion)

Transition from v4 to v6

- To transition from IPv4 to v6, all routers need to be upgraded. This is unlikely to happen at once. ***Why?***
- So, the Internet has to operate with a mix of IPv4 and IPv6 routers. ***How?***



An IPv4 network (in yellow) connects two IPv6 routers



Tunneling

- ➡ Tunnel is a mechanism for shipping a foreign protocol across a network that does not support it
- ➡ Tunneling works via *packet encapsulation* i.e., nesting one type of packet within an other

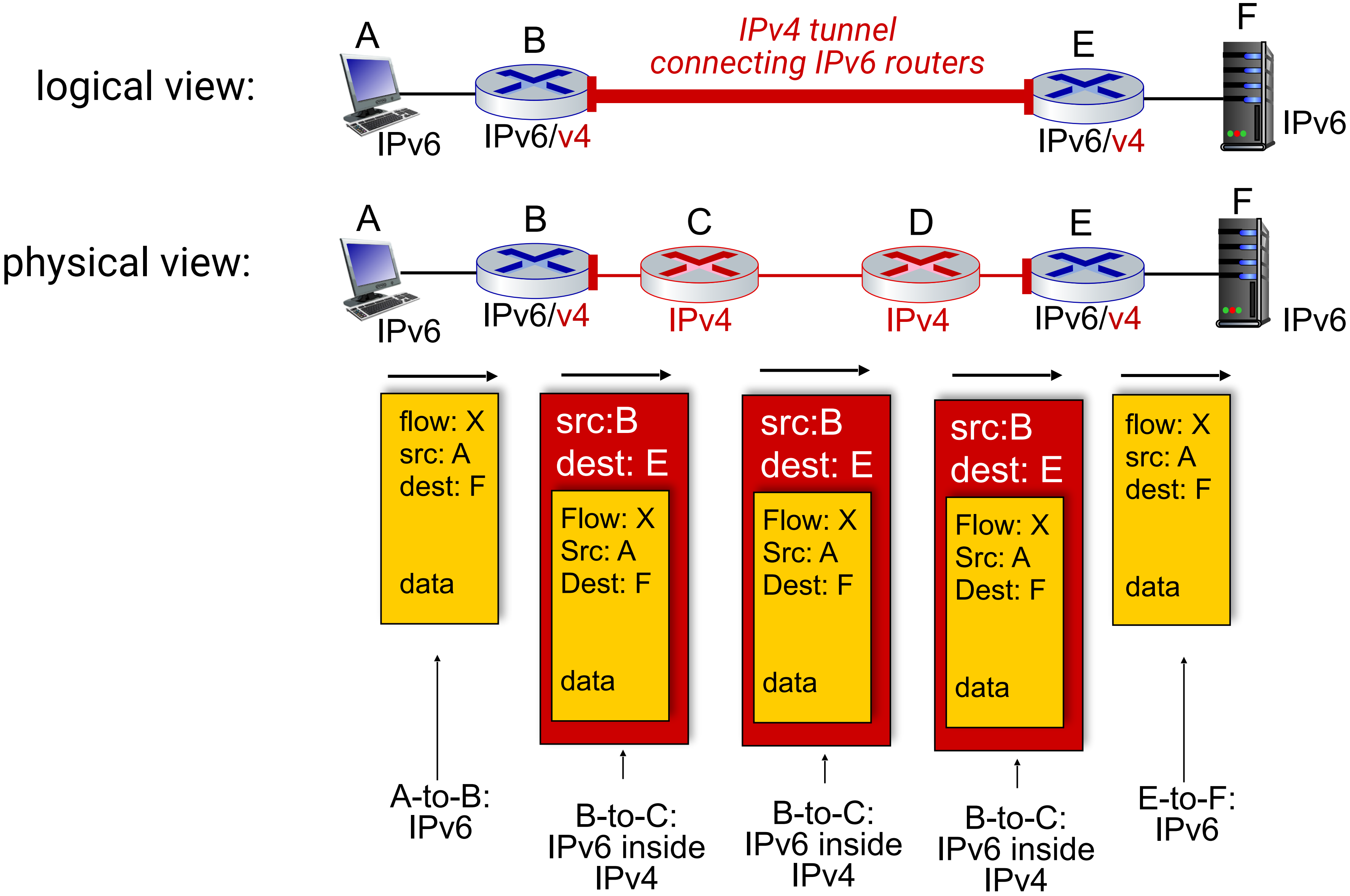
Examples

IPv6-in-IPv4
carry IPv6 datagram as payload in IPv4 datagram among IPv4 routers

Virtual Private Network
extends a private network across the Internet to allow users to communicate as if they are directly connected to the private network

Secure Shell (SSH)
create an encrypted channel over an unsecured network

IPv6 Tunneling



IPv6 Slow Adoption

30%

client access to Google search are via IPv6

33%

of all US government domains are IPv6 capable

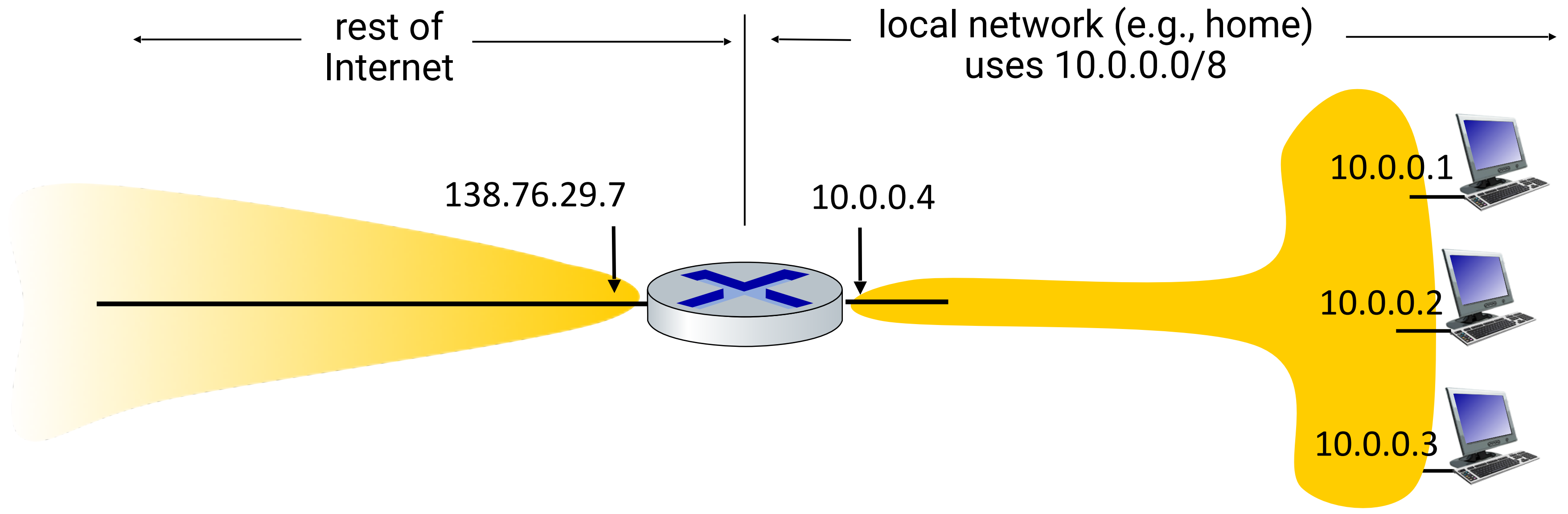
25

years since IPv6 was standardized

NAT

(or how folks actually solved the problem in the real world)

Network Address Translation



When communicating with the outside world, all devices in local network share just one (or a limited set of) public IPv4 address

All devices in local network have addresses from the ***private IP address space*** *(10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16) that can only be used in local network*

NAT

NAT is a mechanism of mapping one IP address space into another by modifying the source/ destination information in the IP header when packets transit across an IP router

Why is NAT useful?

- **Address reusability:** Just one IP address needed from provider ISP for all devices
- **Administrative flexibility:** can change addresses of host in local network without notifying outside world
- **Administrative flexibility:** can change ISP without changing addresses of devices in local network
- **Security**: devices internal to the local network are neither directly addressable nor visible to the outside world

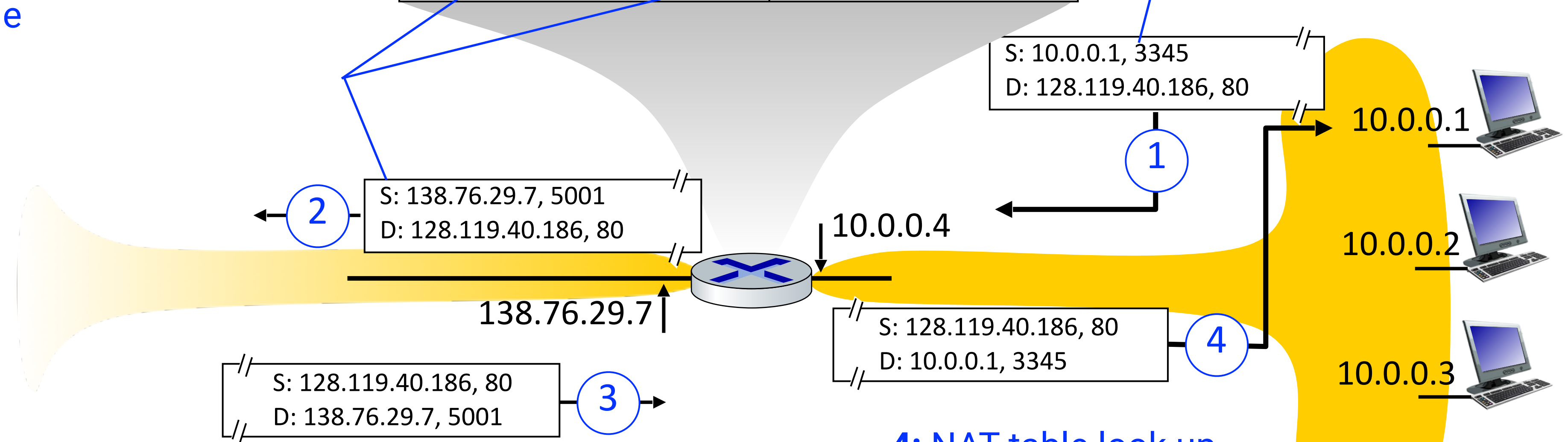
Implementation of NAT

2: NAT router changes datagram source address from 10.0.0.1 port 3345 to 138.76.29.7 port 5001; creates an entry in the NAT translation table

NAT translation table

WAN side addr	LAN side addr
138.76.29.7, 5001	10.0.0.1, 3345
……	……

1: host 10.0.0.1 sends datagram to 128.119.40.186



3: reply arrives for destination address: 138.76.29.7 port 5001

4: NAT table look up, followed by a source IP and port number rewrite

Implementation of NAT

A NAT router must (transparently) perform the following:

1. **For all outgoing datagrams**: replace (source IP address, port #) to (NAT IP address, new port #). Remote clients/servers will perceive (NAT IP address, new port #) as the end host they are communicating with, and will address their packets to that.

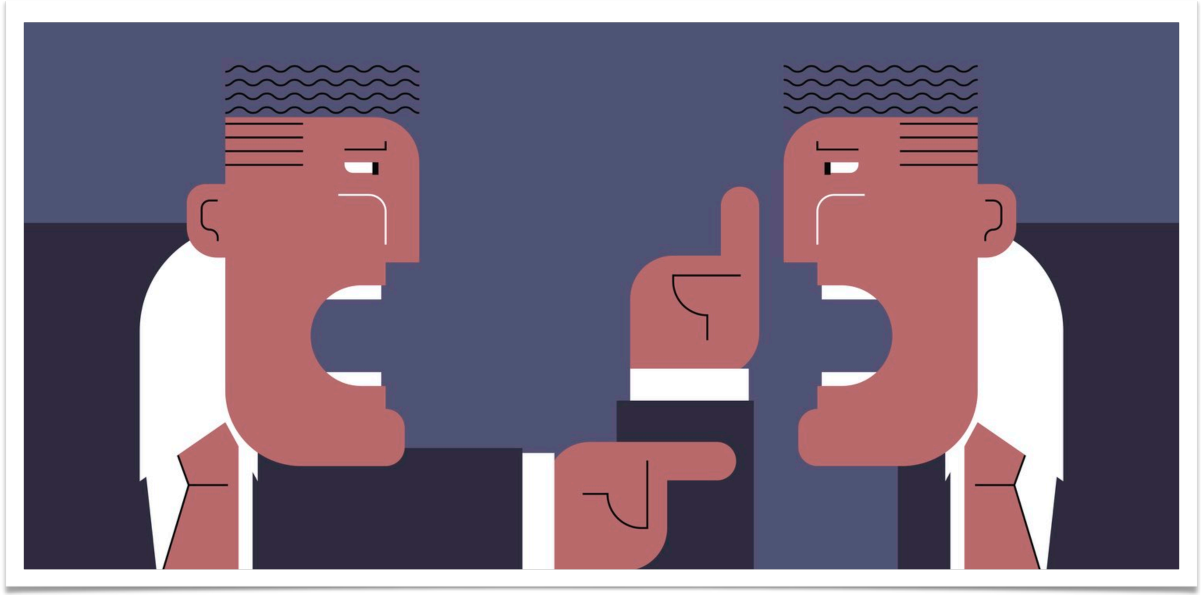
2. **Maintain a NAT translation table**: record all mappings from (source IP address, port #) to (NAT IP address, new port #) in a look up table.

3. **For all incoming datagrams**: replace (NAT IP address, new port #) in destination field of every incoming datagram with the corresponding (source IP address, port #) stored in NAT table.

Since early days

NAT has been

controversial



not an elegant fix

- ➡ address shortage should be solved by IPv6
- ➡ NAT leads to undesirable second order effects: for e.g., the service discovery problem

violates the end-to-end principle

- ➡ Intelligence resides in end hosts but not the network
- ➡ Packet/address manipulation by NAT routers violates this founding principle of the Internet

Middleboxes

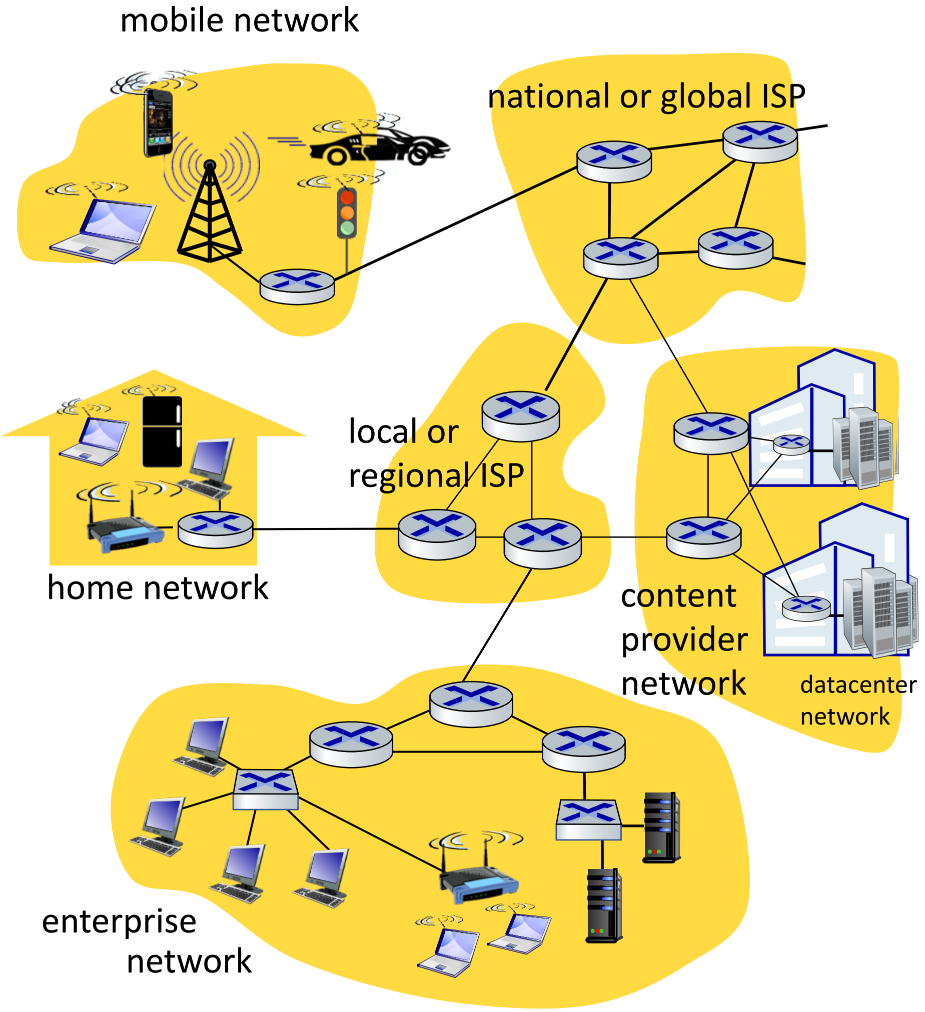
(or why stop at NAT when one can rock the boat harder!)

Middlebox (RFC 3234)

any intermediary box performing functions apart from normal, standard functions of an IP router on the data path between a source host and destination host

Middleboxes are everywhere!

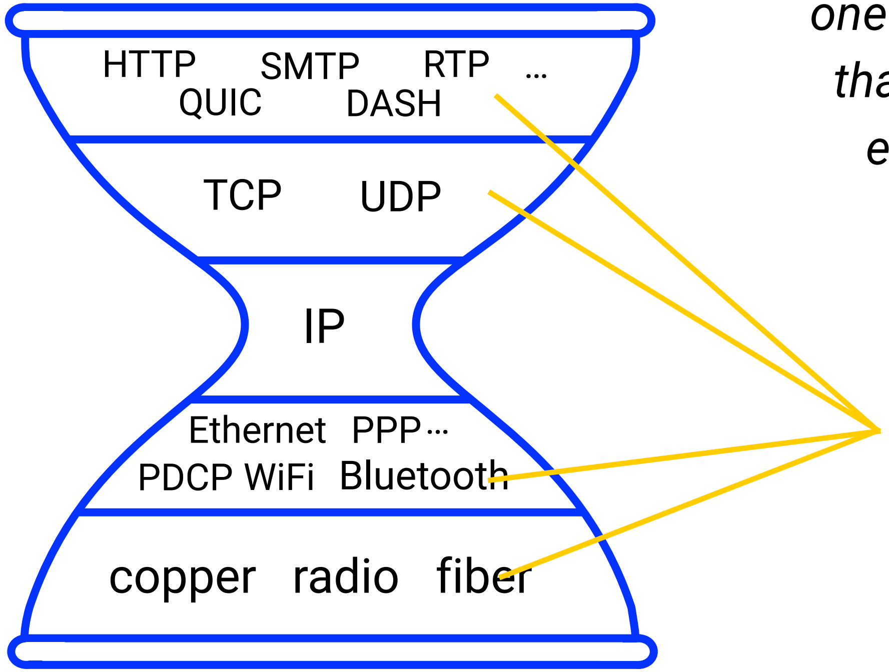
- **NAT**: home, mobile, enterprise networks
- **Firewalls** and **Intrusion detection**: enterprise networks
- **Load balancers**: service providers, mobile networks
- **Network Function Virtualization (NFV)**



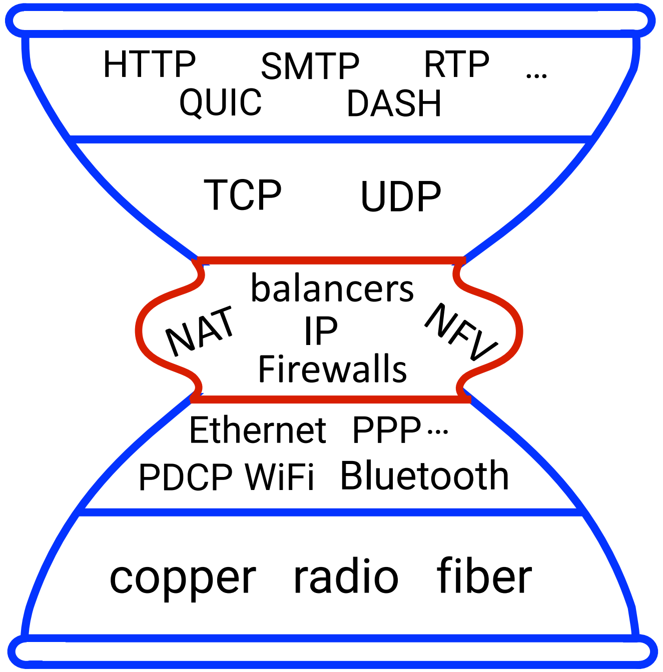
The IP hourglass: *An Organizing Principle for Internet Protocols*

Internet's "thin waist"

one core network layer protocol that ***must*** *be implemented by every (billions of) Internet-connected device*



allows many protocols in physical, link, transport, and application layers



As the Internet enters its "**middle age**", its waist has expanded!

Spot Quiz (ICON)