CS2105 Introduction to Computer Networks

Lecture 6

Network Layer: Data Plane

17 September 2018

Assignments

Assignment 1 due this weekend

- Submit on IVLE
- Zip your file correctly
- Test on `sunfire` using our autotester

Assignment 2 released

- RDT using UDP
- Timings subject to changes

PREVIOUS LECTURE

UDP Overview

Connection-less

- No setup needed → Reduce delay

No connection state at sender or receiver

- Need less resources

Small header size

- Less overhead

No congestion control

- Can blast as fast as desired

PREVIOUS LECTURE

TCP Overview

Connection-oriented

- handshaking (exchange of control messages) before sending app data

Reliable, in-order stream abstraction

- Application passes data to TCP and TCP forms packets in view of MSS (maximum segment size)
- Protocol is rather complicated

Flow control and congestion control

PREVIOUS LECTURE

TCP's Reliable Transfer Algorithm

Sequence number

- in terms of bytes, not packets/segments

Acknowledgements are

- Cumulative
- Piggybacked on data segments

Retransmit segments on

- Timeout (RTO estimated from taking EWMA of RTT)
- 3 Duplicate ACKs received

TCP Connection Establishment

PREVIOUS LECTURE

3-way handshake to establish connection

- → SYN
- ← SYN/ACK
- → ACK

Teardown procedure

- Each side closes their own connection by sending FIN

Learning Outcomes

After this class, you are expected to:

- describe the basic services the network layer provides.
- know the purpose of DHCP and how it works.
- know IP address, subnet, subnet mask and address allocation
- know how ping and traceroute are implemented with ICMP
- know how longest prefix forwarding in a router works.

Chapter 4: Roadmap

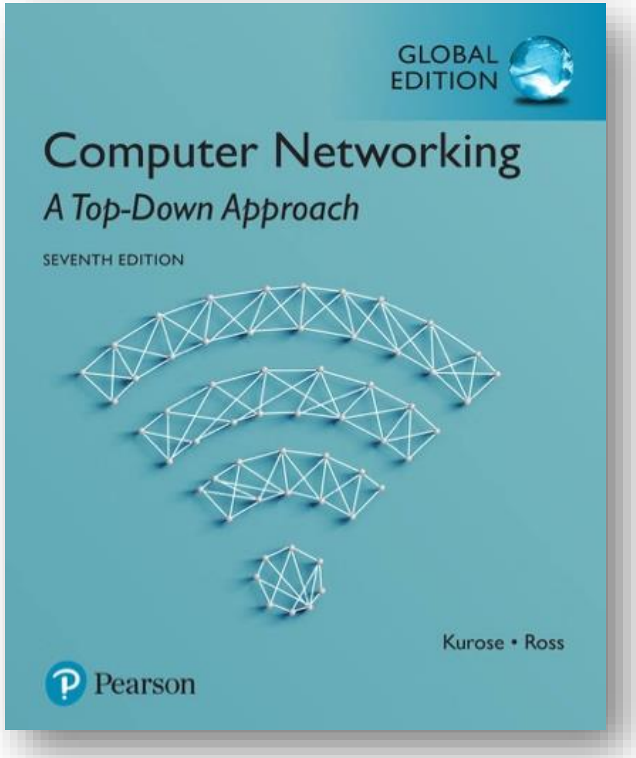
4.1 Introduction

4.3 The Internet Protocol (IP)

- 4.3.1 Datagram Format
- 4.3.2 Datagram Fragmentation

Next Lecture

- 4.3.3 IPv4 Addressing
- 4.3.4 NAT

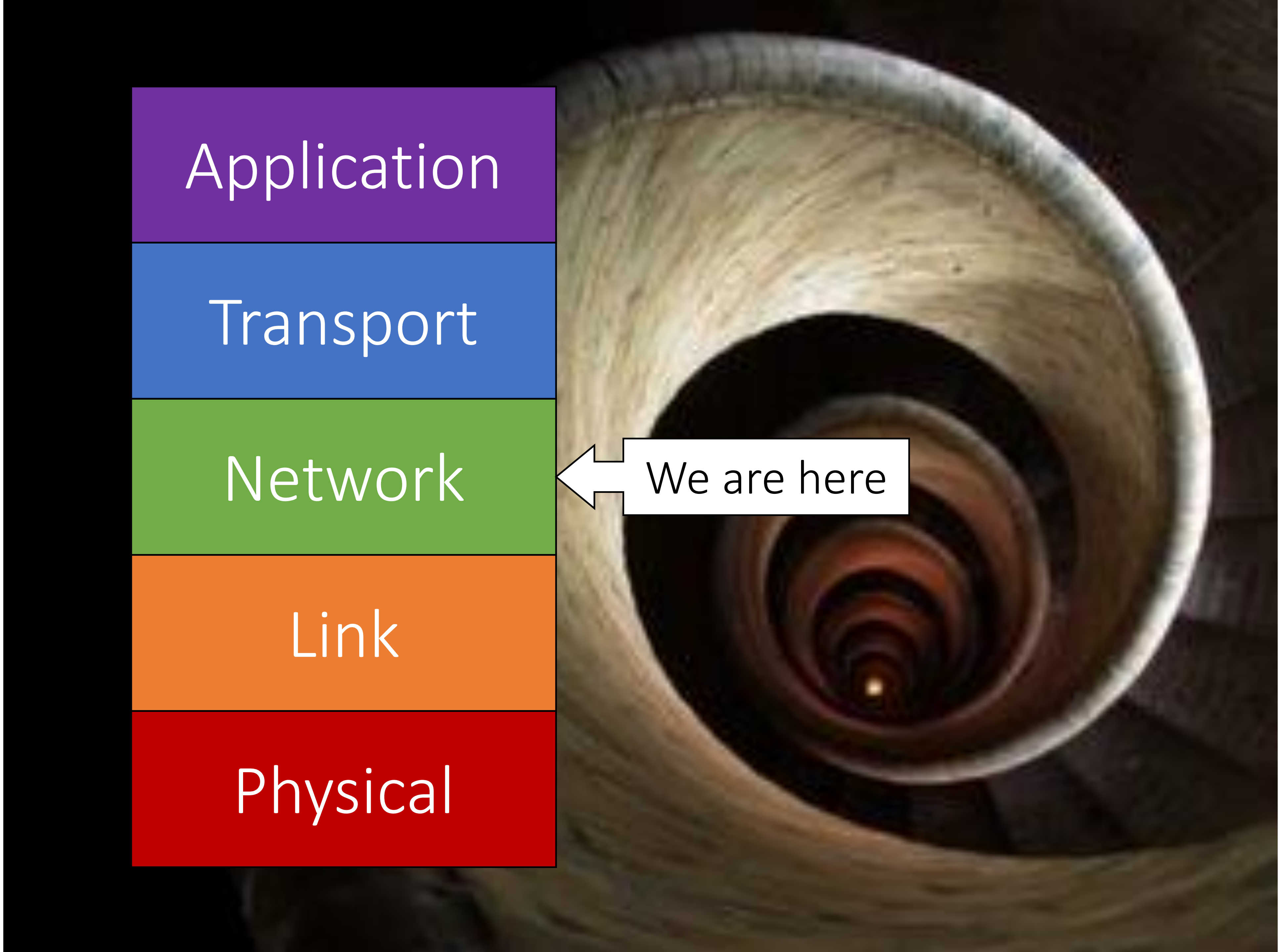


IPv4 addresses has 32 bits

4,294,967,296 possible addresses

The Internet has ran out of IPv4 addresses in 2012

The hacks used to keep the Internet growing, are brilliant



Application

Transport

Network

Link

Physical

We are here

Layering

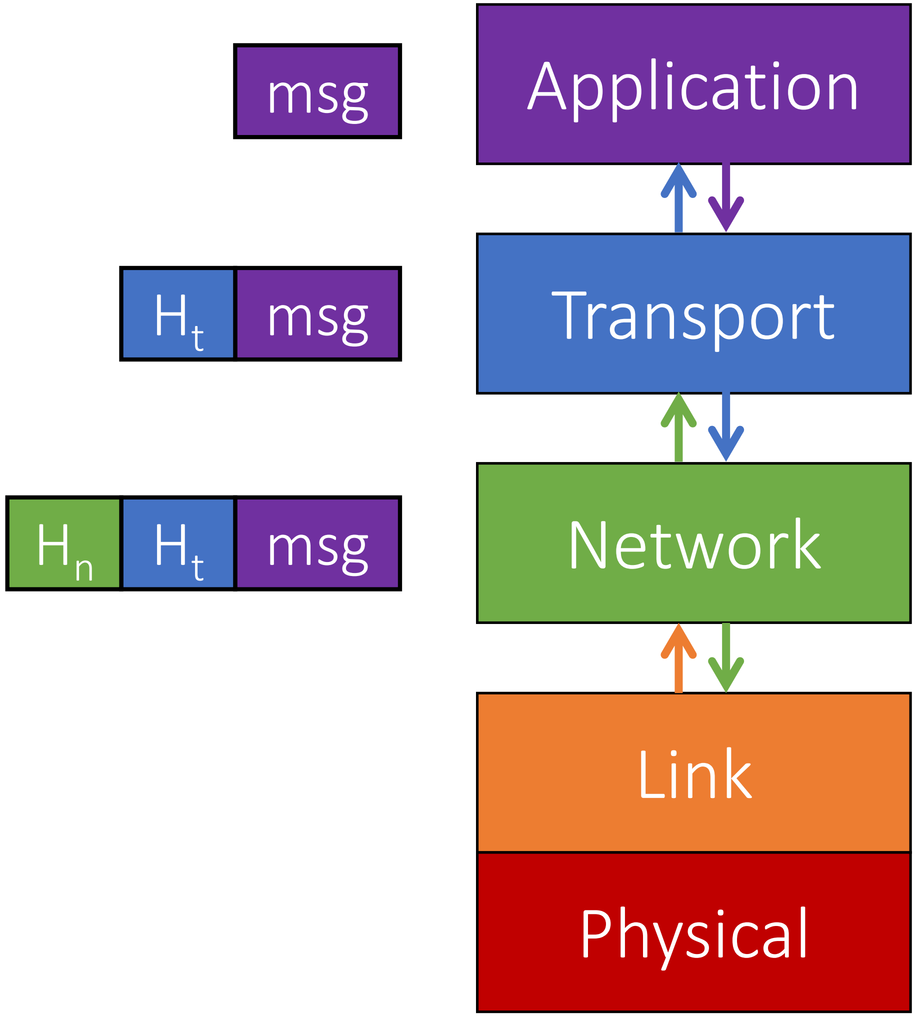
message

segment

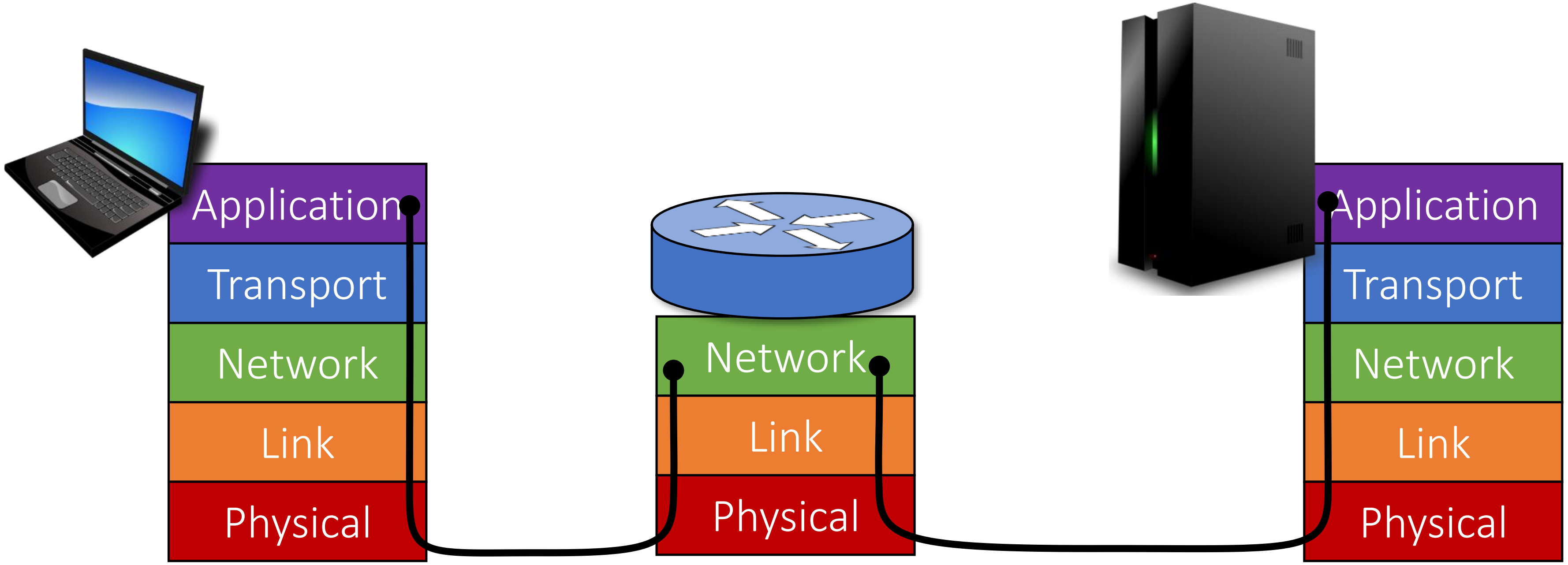
H_t contains source and destination port

datagram

H_n contains source and destination IP address



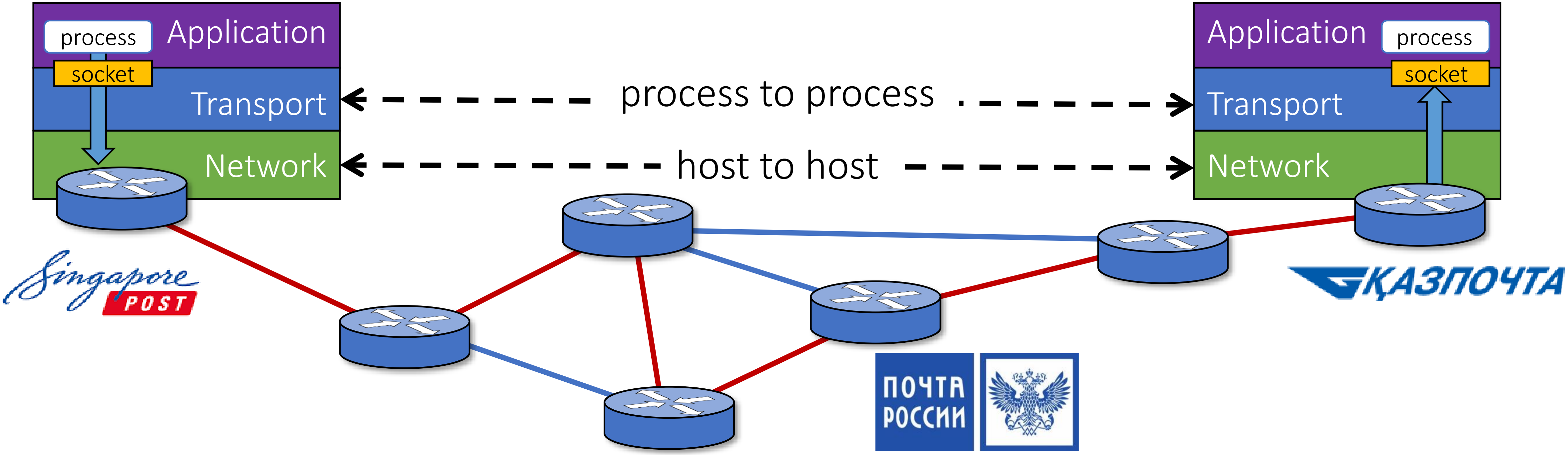
The network layer resides on end hosts and routers

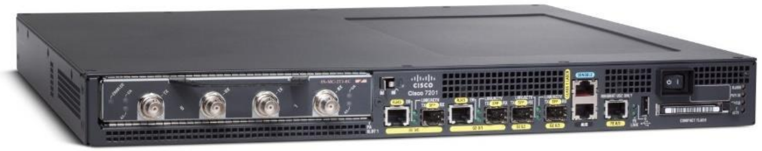


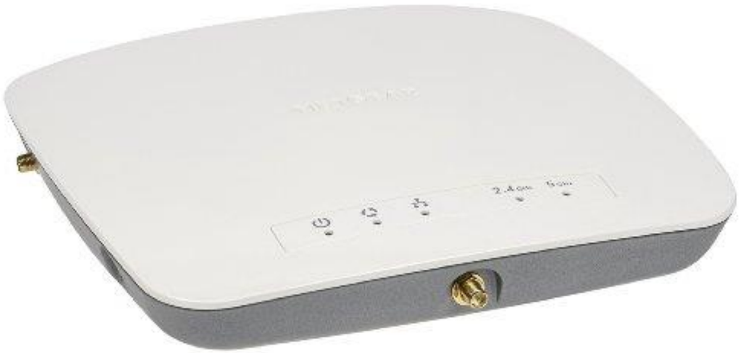
Responsibility of Network layer

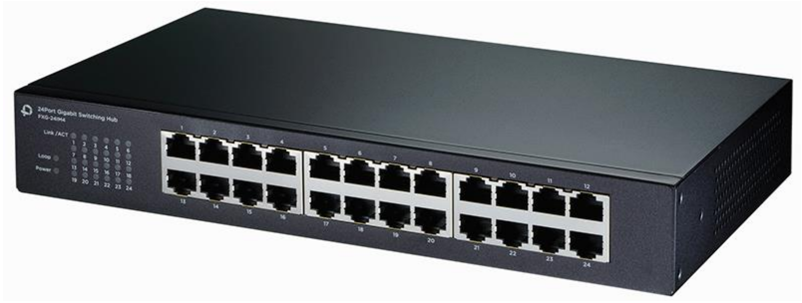
Host-to-host communication

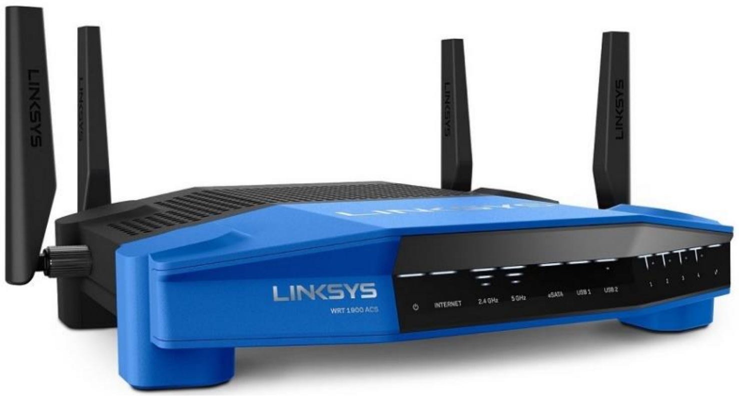
- Forwarding: determining which output link to forward a packet
- Routing: determining the route or path that packets should follow

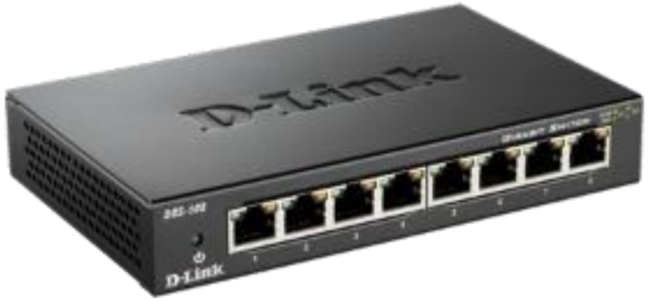










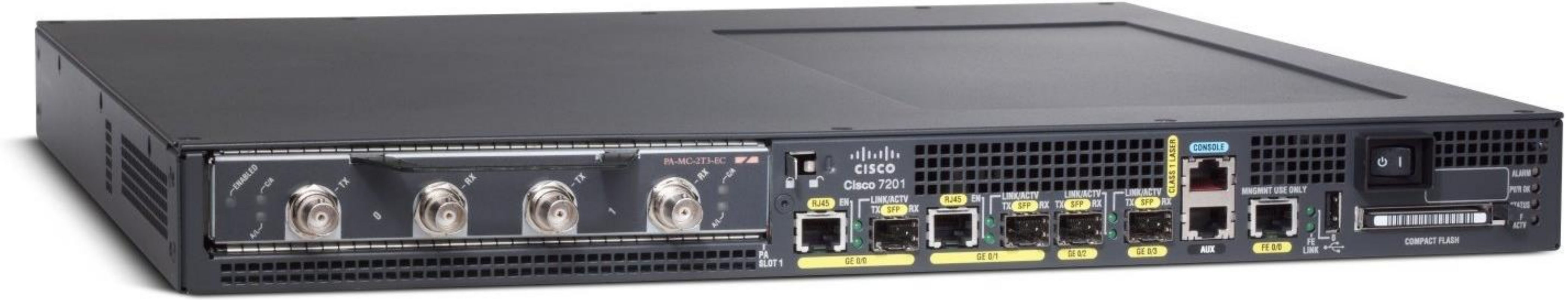


Which of these is a router?

What is a router

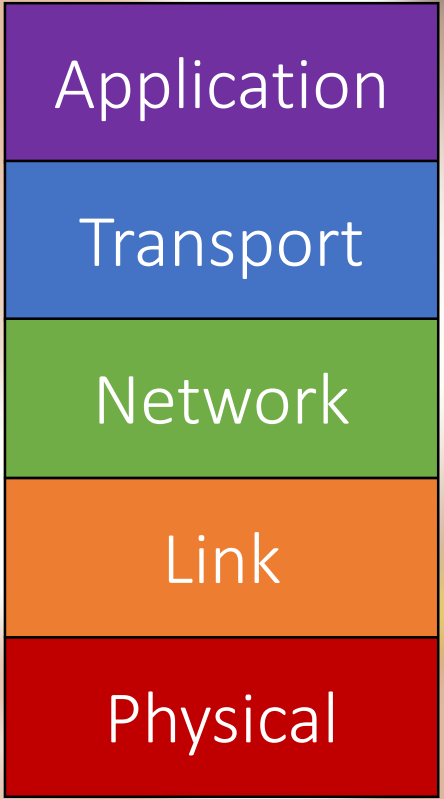
A device that

- forward packets between networks
- perform routing protocols



A Cisco router. Note the number of “LAN” ports

“Narrow waist” of the Internet



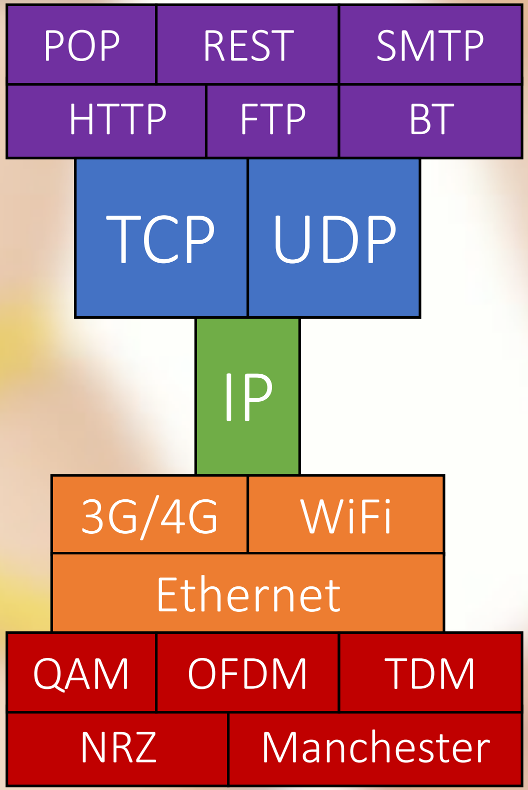
Application

Transport

Network

Link

Physical



POP REST SMTP

HTTP FTP BT

TCP UDP

IP

3G/4G WiFi

Ethernet

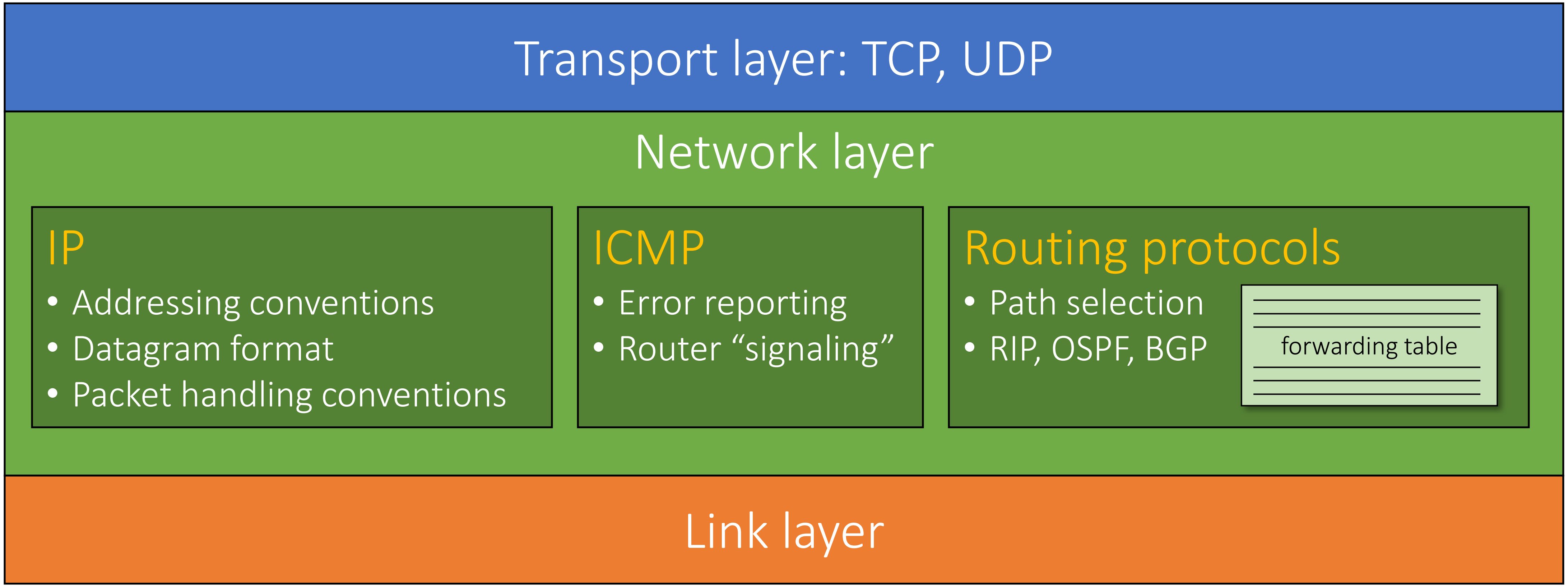
QAM OFDM TDM

NRZ Manchester

Focus of CS2105 is on datagram networks.

You can read about virtual circuit in your own time.

Network Layer Services



Transport layer: TCP, UDP

Network layer

IP
- Addressing conventions
- Datagram format
- Packet handling conventions

ICMP
- Error reporting
- Router “signaling”

Routing protocols
- Path selection
- RIP, OSPF, BGP

forwarding table

Link layer

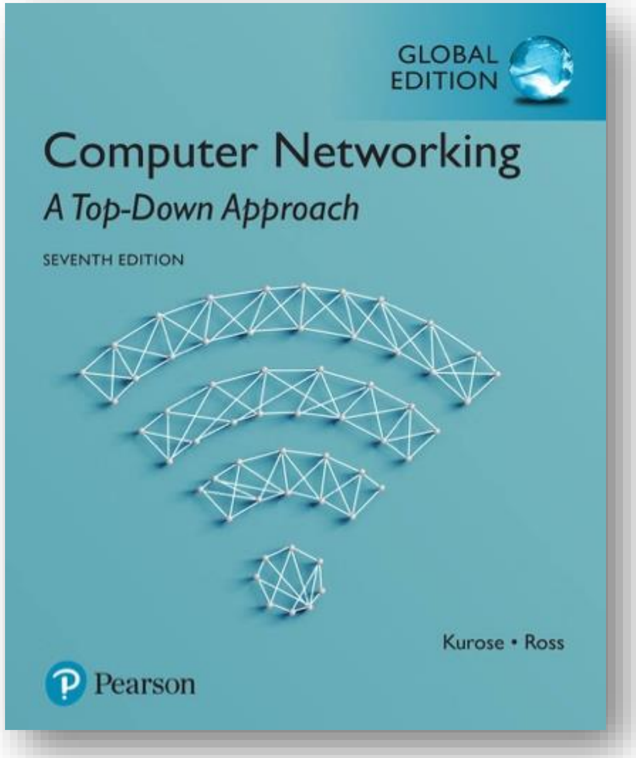
Chapter 4: Roadmap

4.1 Introduction

4.4 The Internet Protocol (IP)

- 4.4.1 Datagram Format
- 4.4.2 IPv4 Addressing
- 4.4.3 ICMP

4.5 Routing Algorithms



Internet Protocol

version 4

IPv4

IPv4 is still the dominant version today.

IPv6 will eventually replace IPv4, just *not so soon*.

Interested? Read Chapter 4.4.4

IP Address

An IP address is associated with an interface

4GLTE
4G
SAMSUNG

83.154.223.121

Wi-Fi
802.11

203.162.32.129

Ethernet
802.3

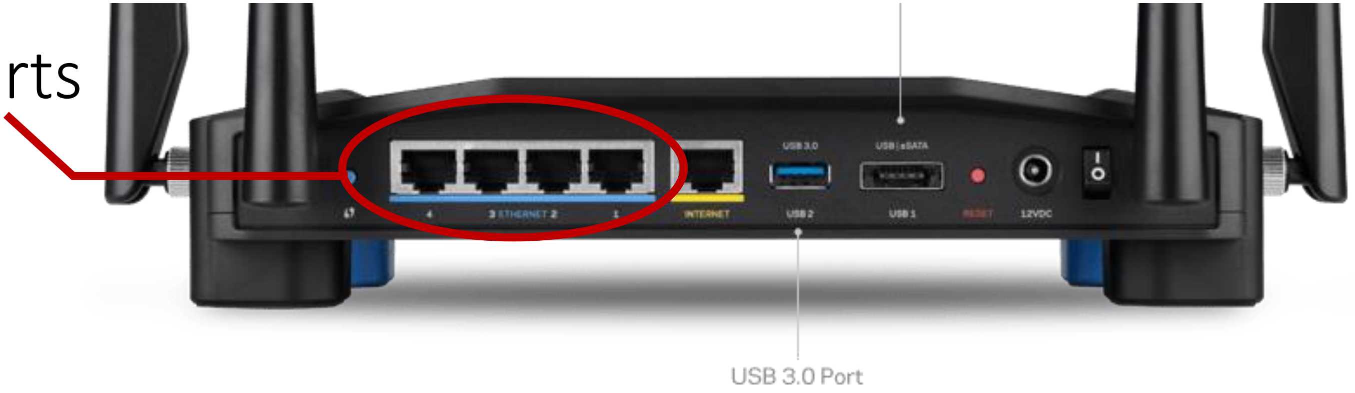
174.163.229.152

127.0.0.1

Network Interface

A router has multiple interfaces → multiple IP addresses

– Not to be confused with ports



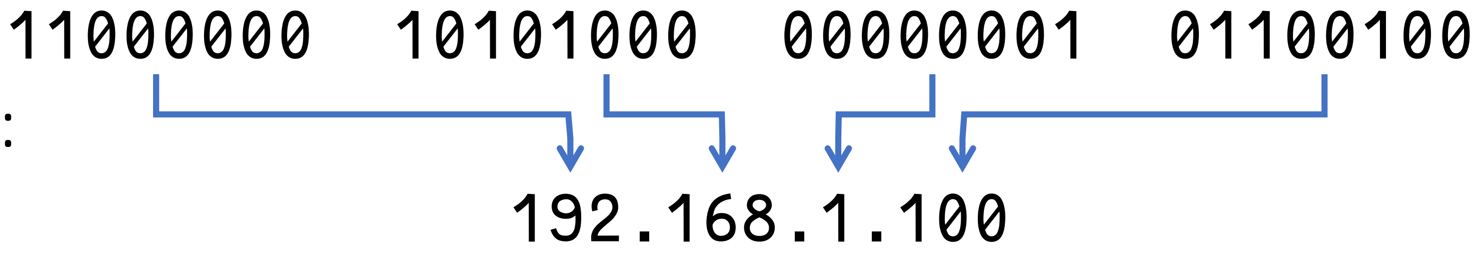
IP Address

Used to identify a host (or router)

- Since an interface needs to be on a host or router

IPv4

- 32-bit integer, typically expressed in dot-decimal notation
- Binary:
- Decimal:



```
11000000 10101000 00000001 01100100
```

```
192.168.1.100
```

Did you configure an IP address on your hosts (phone, laptop, desktop)?

Probably not. It was configured automatically

Dynamic Host Configuration Protocol

Allows a host to dynamically obtain an IP address from a DHCP server when it joins a network

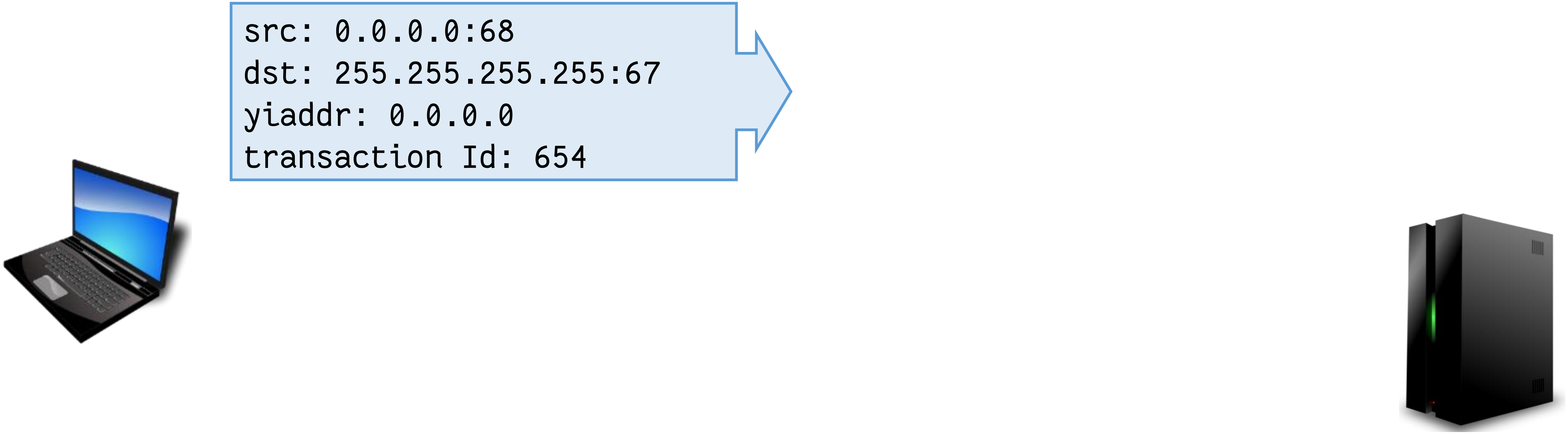
- IP address is renewable
- IP address is reusable (other hosts can use if you leave)
- Supports mobile users who want to join different networks

Four step process

1. Host broadcast a Discover message
2. DHCP server(s) responds with an Offer
3. Host Request for the IP address
4. DHCP server ACK-nowledges assignment

Step 1: DHCP Discover

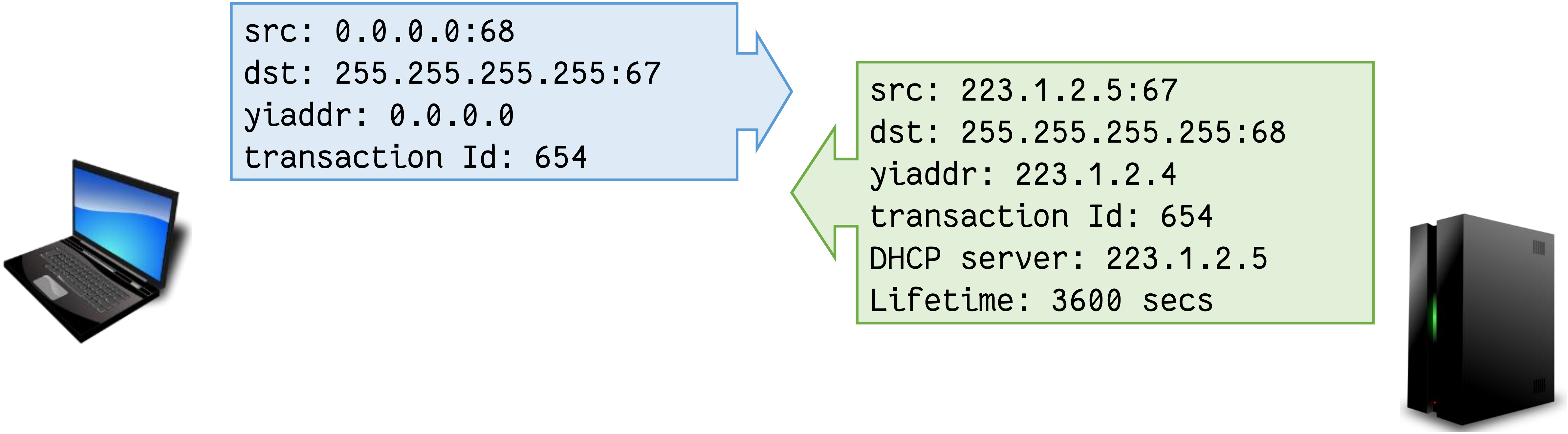
New host broadcasts DHCP discover msg



```
src: 0.0.0.0:68
dst: 255.255.255.255:67
yiaddr: 0.0.0.0
transaction Id: 654
```

Step 2: DHCP Offer

DHCP server(s) responds with DHCP offer

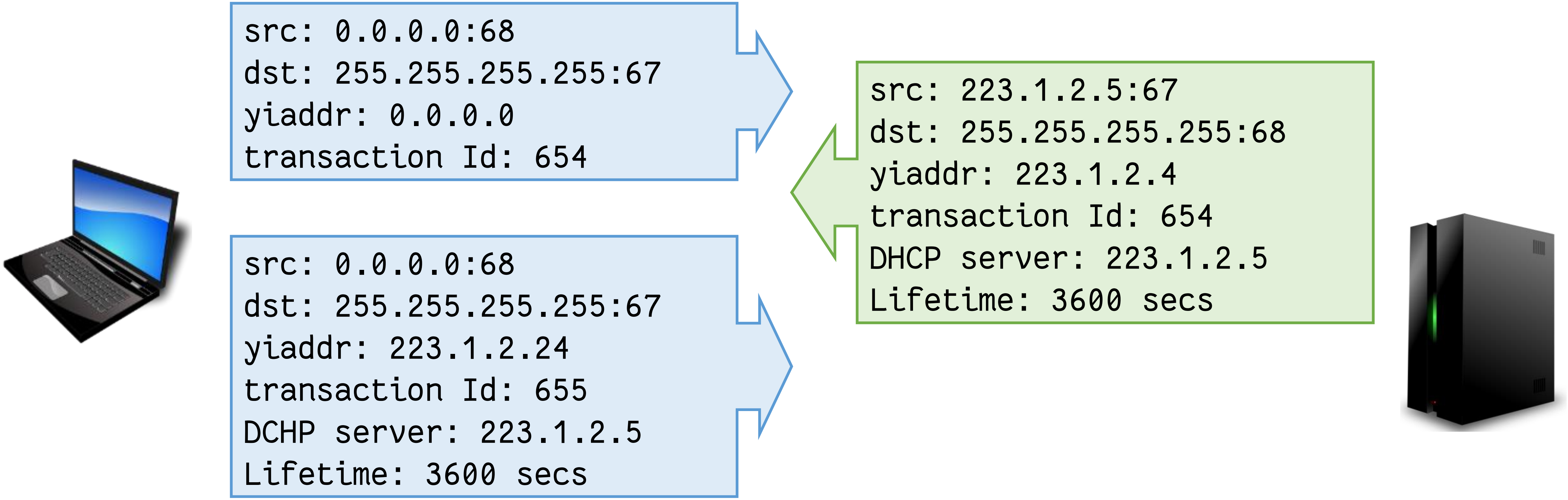


```
src: 0.0.0.0:68
dst: 255.255.255.255:67
yiaddr: 0.0.0.0
transaction Id: 654
```

```
src: 223.1.2.5:67
dst: 255.255.255.255:68
yiaddr: 223.1.2.4
transaction Id: 654
DHCP server: 223.1.2.5
Lifetime: 3600 secs
```

Step 3: DHCP Request

Host selects from offers and send request



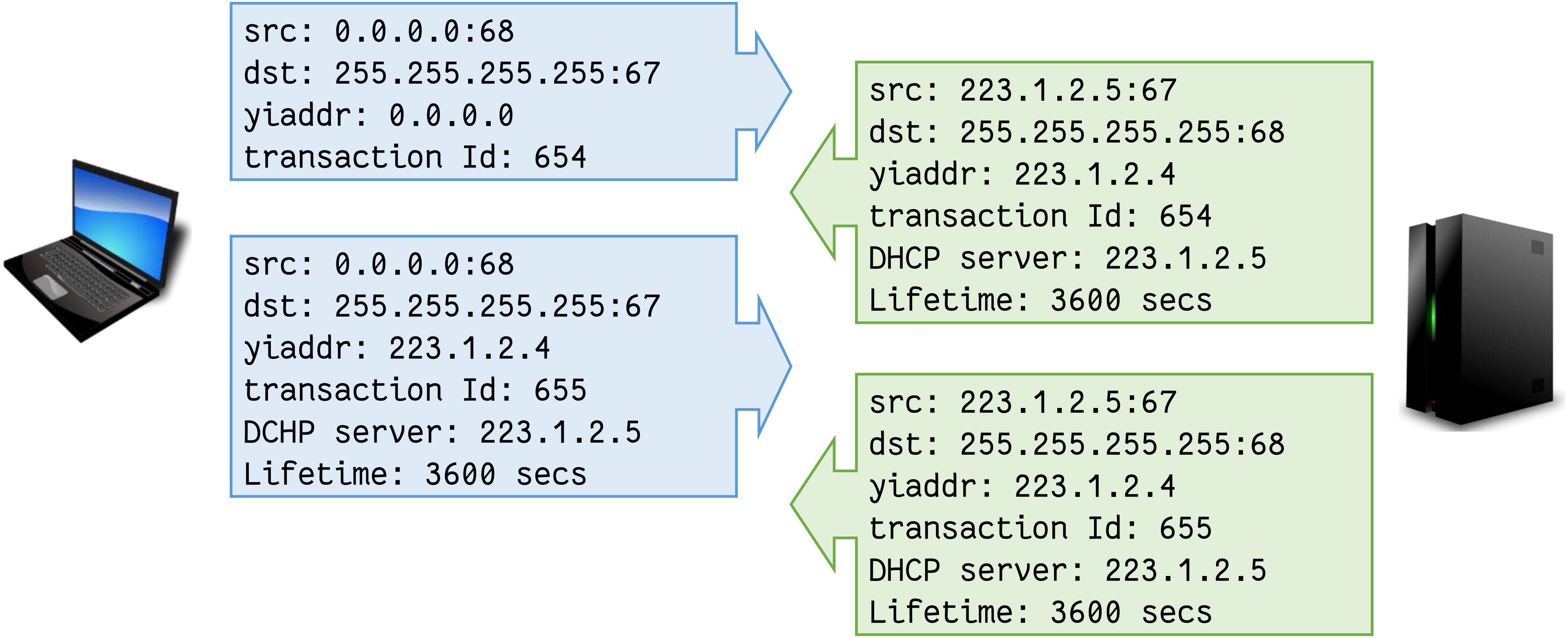
```
src: 0.0.0.0:68
dst: 255.255.255.255:67
yiaddr: 0.0.0.0
transaction Id: 654
```

```
src: 223.1.2.5:67
dst: 255.255.255.255:68
yiaddr: 223.1.2.4
transaction Id: 654
DHCP server: 223.1.2.5
Lifetime: 3600 secs
```

```
src: 0.0.0.0:68
dst: 255.255.255.255:67
yiaddr: 223.1.2.24
transaction Id: 655
DCHP server: 223.1.2.5
Lifetime: 3600 secs
```

Step 4: DHCP ACK

Server confirms requested parameters



```
src: 0.0.0.0:68
dst: 255.255.255.255:67
yiaddr: 0.0.0.0
transaction Id: 654
```

```
src: 223.1.2.5:67
dst: 255.255.255.255:68
yiaddr: 223.1.2.4
transaction Id: 654
DHCP server: 223.1.2.5
Lifetime: 3600 secs
```

```
src: 0.0.0.0:68
dst: 255.255.255.255:67
yiaddr: 223.1.2.4
transaction Id: 655
DCHP server: 223.1.2.5
Lifetime: 3600 secs
```

```
src: 223.1.2.5:67
dst: 255.255.255.255:68
yiaddr: 223.1.2.4
transaction Id: 655
DHCP server: 223.1.2.5
Lifetime: 3600 secs
```

More on DHCP

In addition to host IP address assignment, DHCP may also provide a host additional network information:

- IP address of first-hop router
- IP address of local DNS server
- Network mask (indicating network prefix versus host ID of an IP address)

DHCP runs over UDP

- DHCP server port number: 67
- DHCP client port number: 68

Special IP Addresses

`127.0.0.1/8`	Loopback address. Typically using 127.0.0.1/32

`10.0.0.0/8`
`172.16.0.0/12`
`192.168. 0.0/16`
	Private addresses. Local communication in a private network.

`255.255.255.255/32`	Broadcast address. All hosts on the same subnet will receive the datagram
`0.0.0.0/8`	Non-routable meta-address for special use

Full list of special addresses in RFC 5735

4,294,967,296 possible addresses

ran out in 2012

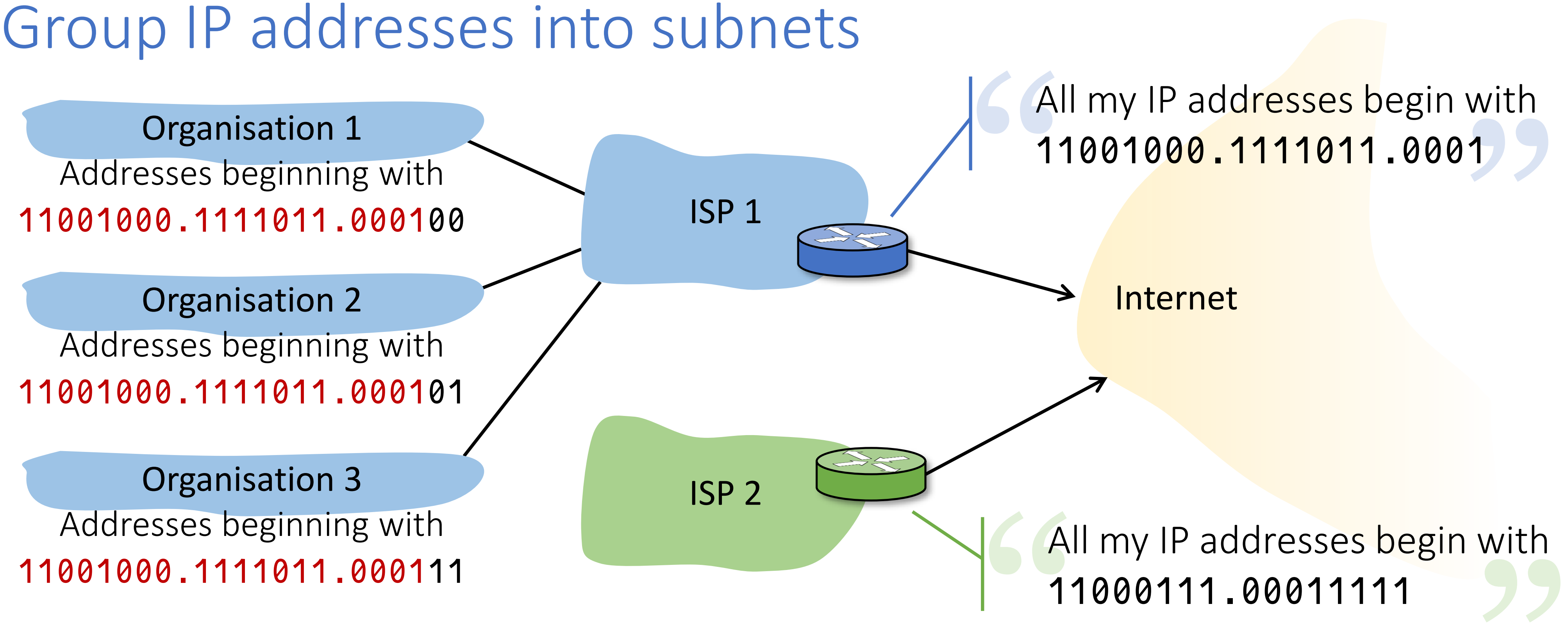
But only 2.497 billion hosts (Why?)

Hierarchical Addressing

It is impossible to forward/route with random IP addresses

- Hierarchical addressing to aggregate IP addresses

Group IP addresses into subnets



Organisation 1
Addresses beginning with
11001000.1111011.000100

Organisation 2
Addresses beginning with
11001000.1111011.000101

Organisation 3
Addresses beginning with
11001000.1111011.000111

ISP 1

ISP 2

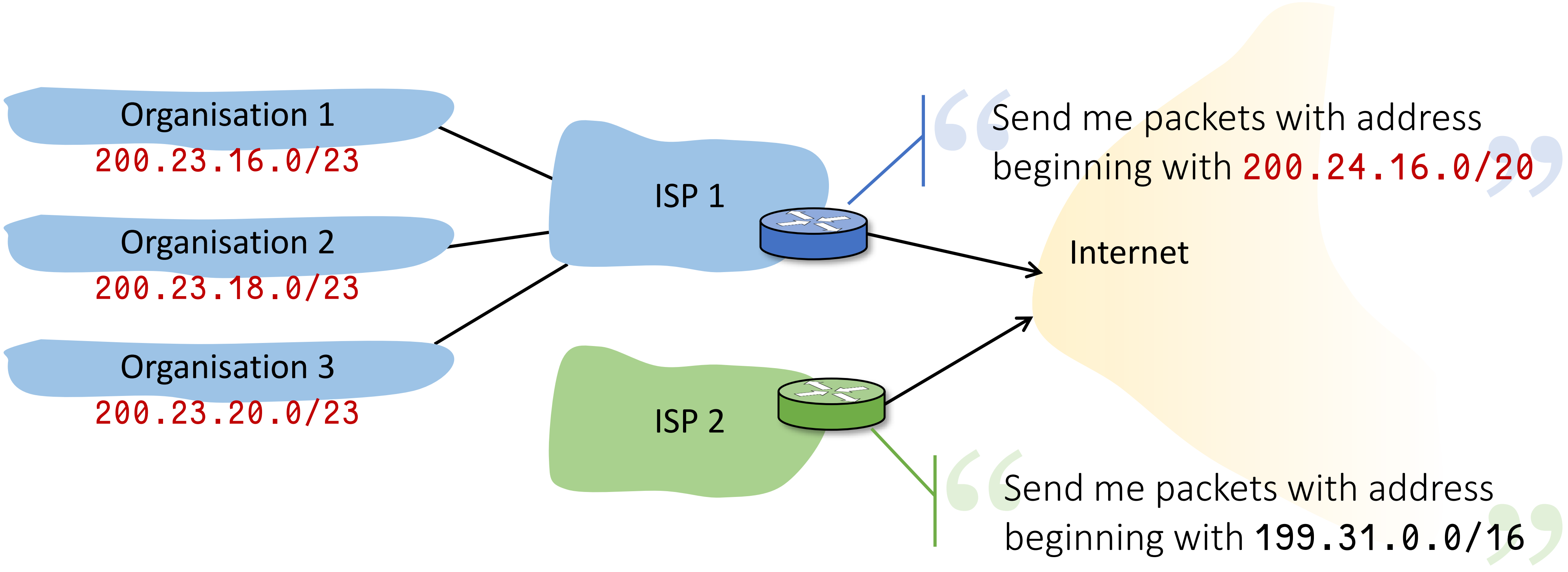
Internet

“All my IP addresses begin with
11001000.1111011.0001”

“All my IP addresses begin with
11000111.00011111”

Hierarchical Addressing

Allows efficient routing advertisement



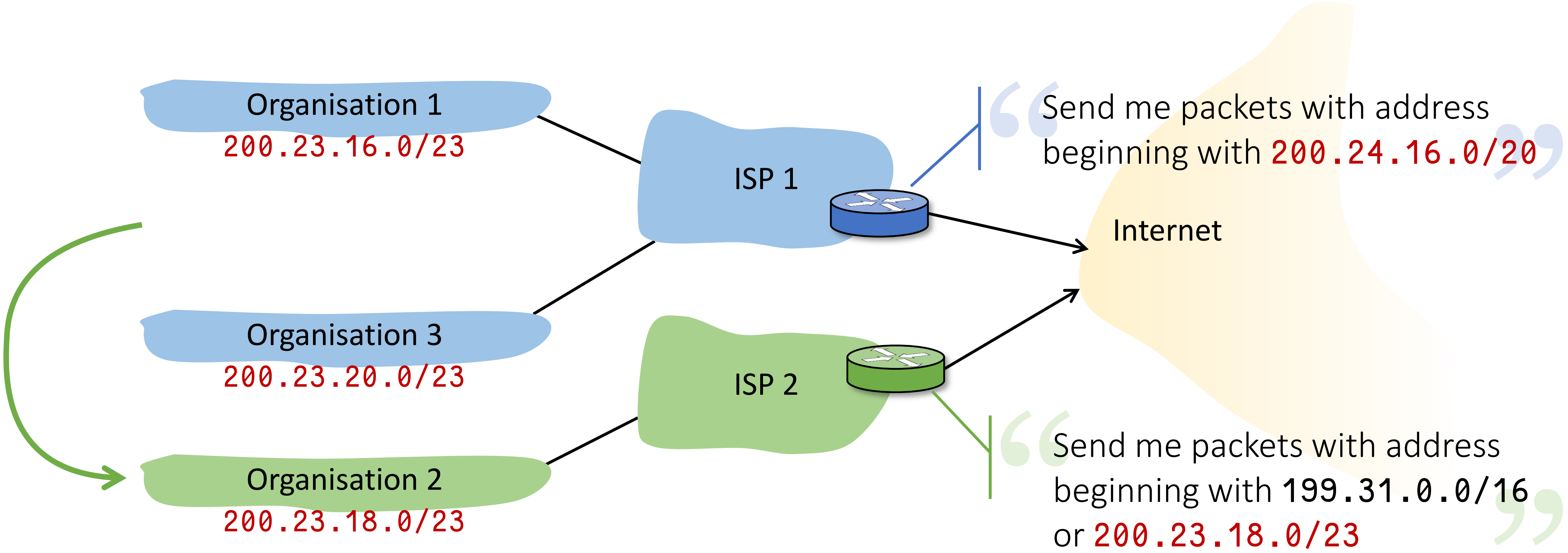
"Send me packets with address beginning with 200.24.16.0/20"

"Send me packets with address beginning with 199.31.0.0/16"

Longest Prefix Match

Suppose Organisation 2 switches ISP

- But wants to retain its IP address block



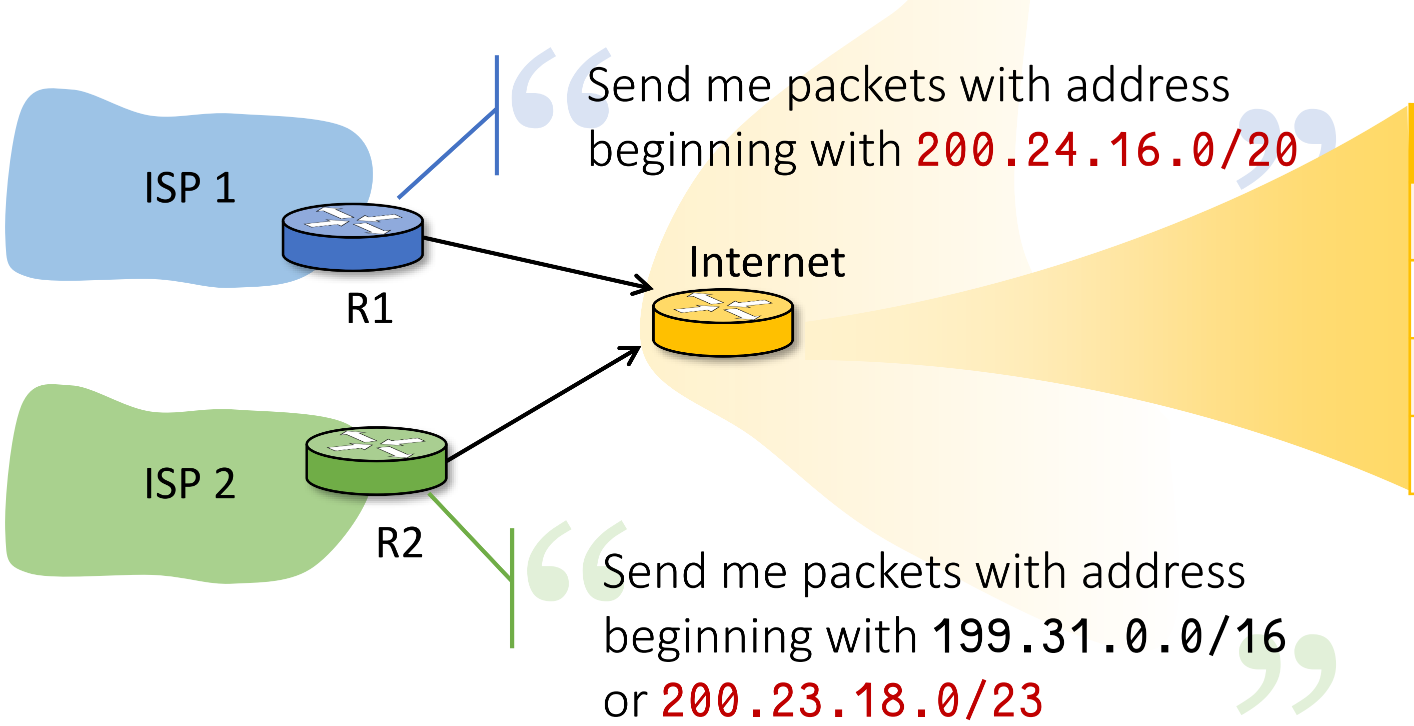
"Send me packets with address beginning with 200.24.16.0/20"

"Send me packets with address beginning with 199.31.0.0/16 or 200.23.18.0/23"

Longest Prefix Match

Question: Which router to forward

- packet with destination IP 200.23.20.2?
- packet with destination IP 200.23.19.3?



“Send me packets with address beginning with 200.24.16.0/20”

“Send me packets with address beginning with 199.31.0.0/16 or 200.23.18.0/23”

Net Mask	Next hop
200.23.16.0/20	R1
200.23.18.0/23	R2
199.31.0.0/16	R2
...	...

Longest Prefix Match

– packet with destination IP 200.23.20.2? → R1

11001000 00010111 00010100 00000010

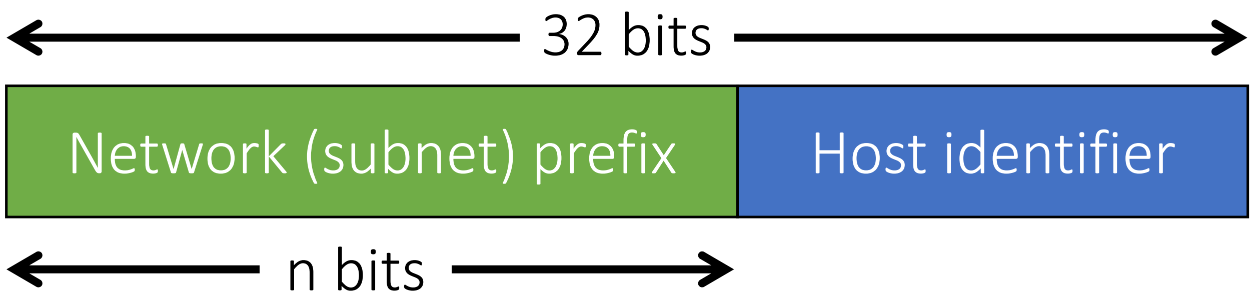
– packet with destination IP 200.23.19.3? → R2

11001000 00010111 00010011 00000011

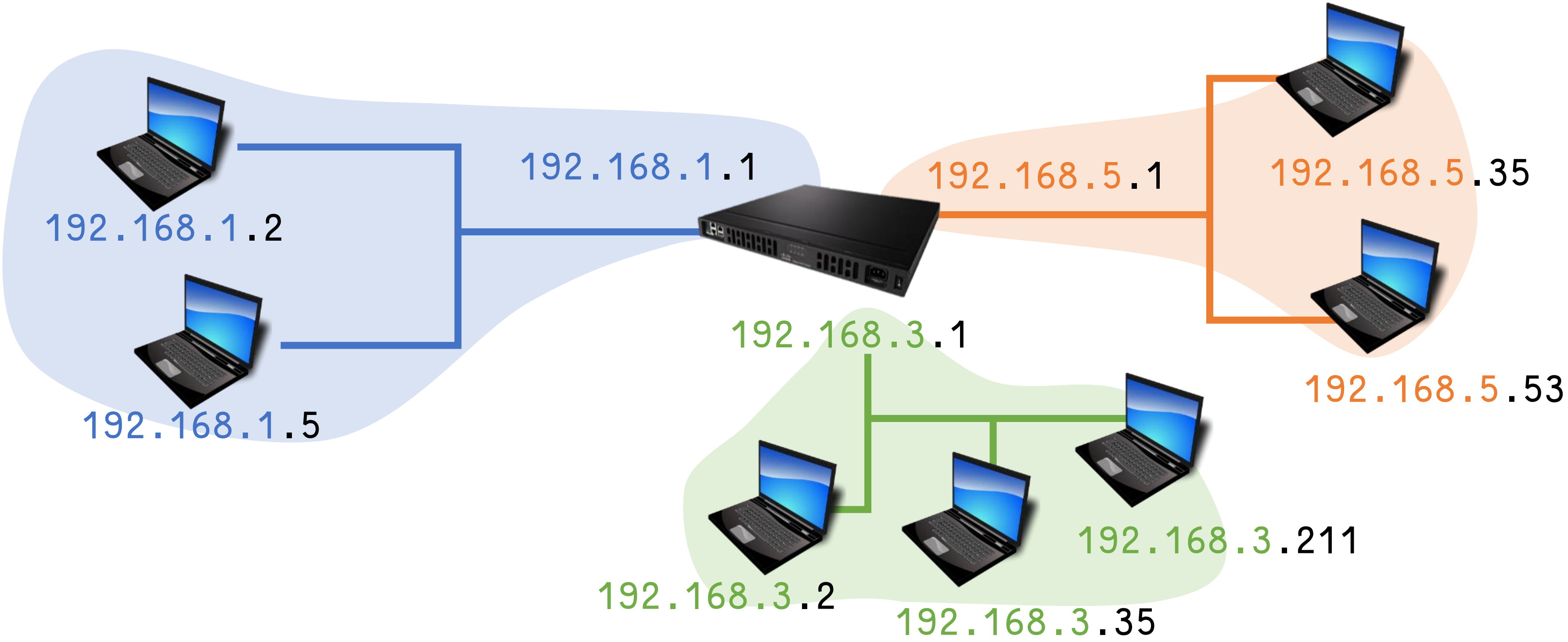
Net Mask	Net mask in binary	Next hop
200.23.16.0/20	11001000 00010111 00010000 00000000	R1
200.23.18.0/23	11001000 00010111 00010010 00000000	R2
199.31.0.0/16	11000111 00011111 00000000 00000000	R2
…		…

IP Address and Subnet

An IP address has two parts



Subnet



Subnet is a network formed by “directly” interconnected hosts

- Hosts in the same subnet have the same network prefix
- Hosts can reach other hosts on the same subnet without needing the router
- Router is needed to reach other networks, or the outside world

Subnet Mask

Used to determine which subnet an IP address belongs to.

- made by setting all subnet prefix bits to “1”s and host ID bits to “0”s.

Example: for IP address 200.23.16.42/23:

IP address:	11001000	00010111	00010000	00101010
Subnet mask:	11111111	11111111	11111110	00000000

- Subnet mask in dot-decimal:

255.255.254.0

Classful Addressing

In 1981, RFC 791

- Class A: 8-bit prefix

0	127 networks	$2^{24} \approx$ 16 million addresses

- Class B: 16-bit prefix

1	0	2^{14} = 16,384 networks	2^{16} = 65,536 addresses

- Class C: 24-bit prefix

1	1	0	$2^{21} \approx$ 2 million networks	2^{8} = 256 addresses

Organizations can buy Class A, B or C address blocks

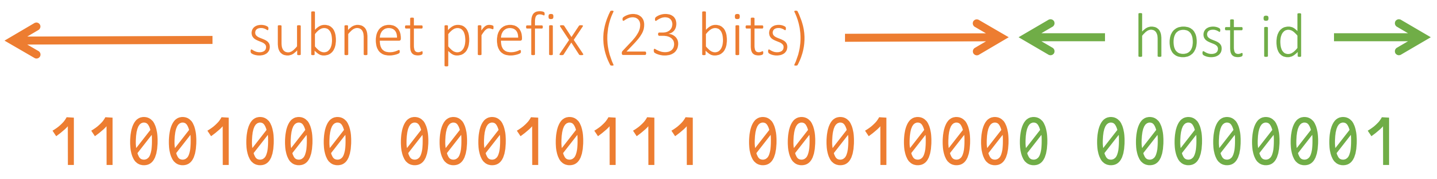
- Class C too small, and Class B too big
- Lots of unused addresses

Classless Inter-Domain Routing

Replaced classful networking in 1993

The Internet today uses CIDR

- Subnet of arbitrary length
- Address format: `x.x.x.x/y` where `y` is the subnet mask



subnet prefix (23 bits)

host id

`11001000 00010111 00010000 00000001`

`200.23.16.1/23`

This subnet has 2^9 IP addresses

IP Address Allocation

Organizations obtains a block of IP address from ISP's address space

	Binary address	Decimal address
ISP's Block	11001000 00010111 00010000 00000000	200.23.16.0/20
Organization 1	11001000 00010111 00010000 00000000	200.23.16.0/23
Organization 2	11001000 00010111 00010010 00000000	200.23.18.0/23
…	…	…
Organization 8	11001000 00010111 00011110 00000000	200.23.30.0/23

IPv4 address space registry

http://www.iana.org/assignments/ipv4-address-space/

Use whois command to query owner

```
whois 137.132.0.0/16
```

IP Address Allocation

How does an ISP get a block of addresses?

ICANN: Internet Corporation for Assigned Names and Numbers

- Allocates addresses
- Manages DNS
- Assigns domain names, resolves disputes

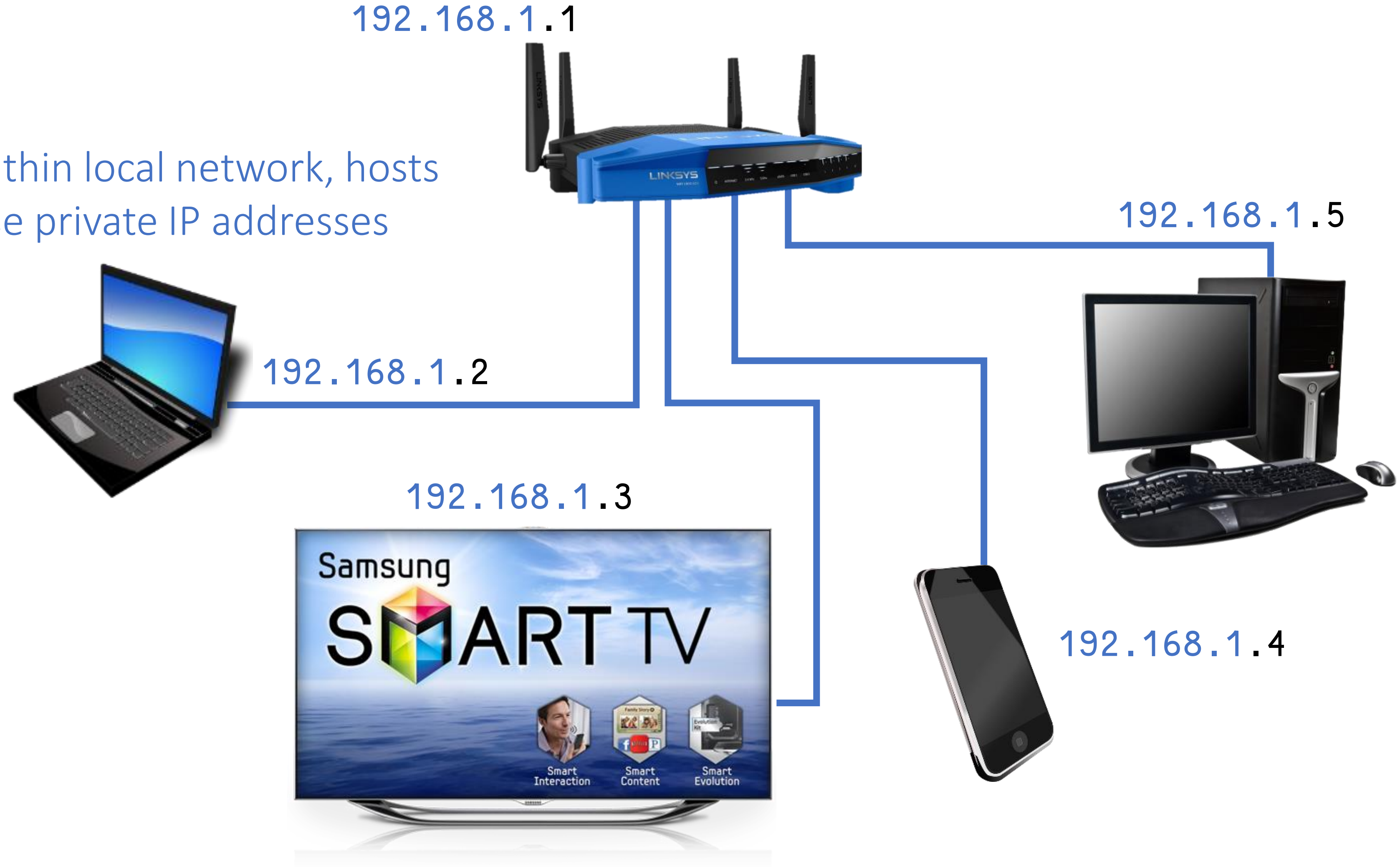
How to solve the lack of IPv4 addresses?

Private networks

Your ISP only gives you one IP address. But you have several hosts.

HOW?

Create a private network



192.168.1.1

within local network, hosts use private IP addresses

192.168.1.2

192.168.1.3

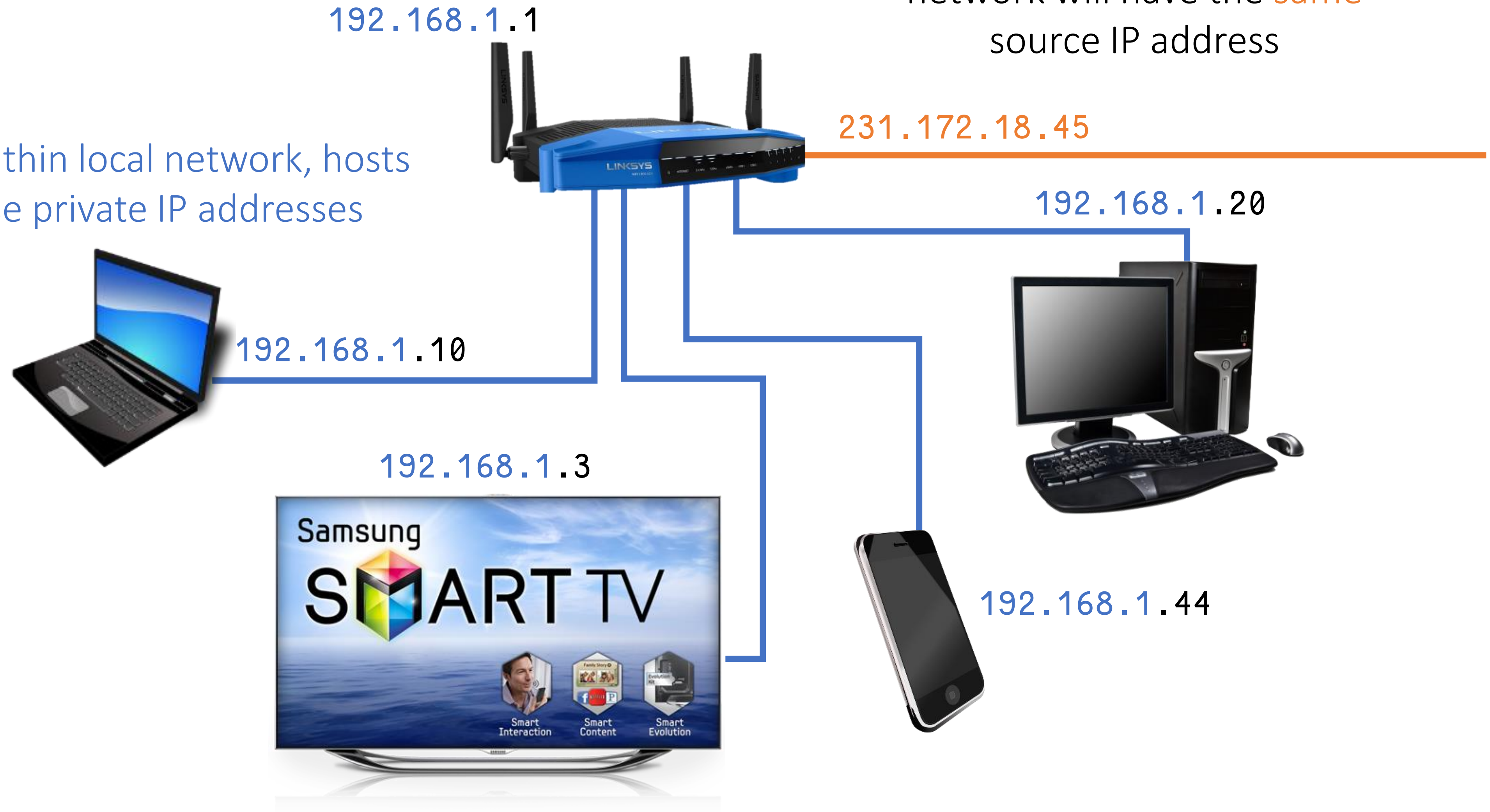
192.168.1.4

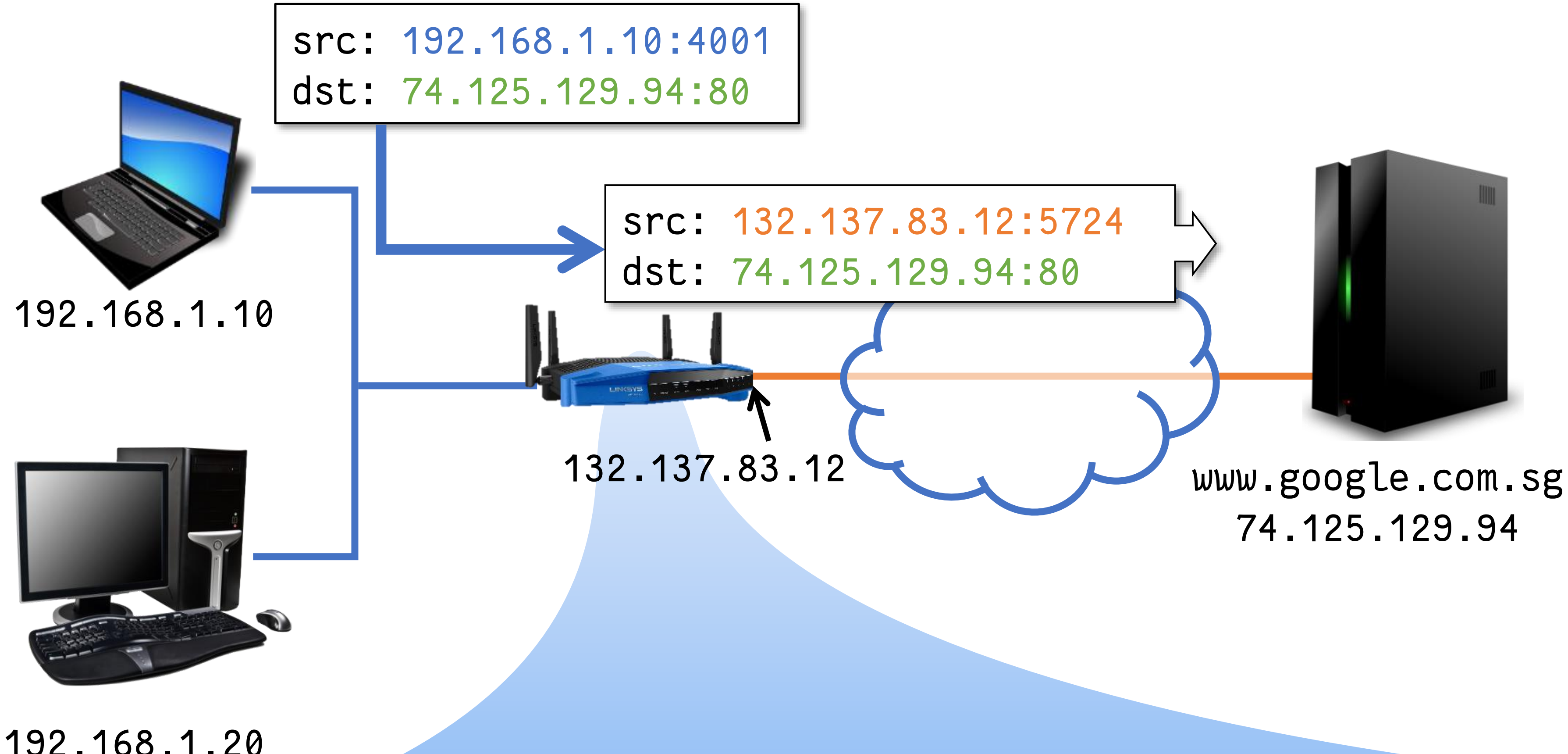
192.168.1.5

Perform NAT

all datagrams leaving local network will have the same source IP address

within local network, hosts use private IP addresses





src: 192.168.1.10:4001
dst: 74.125.129.94:80

src: 132.137.83.12:5724
dst: 74.125.129.94:80

192.168.1.10

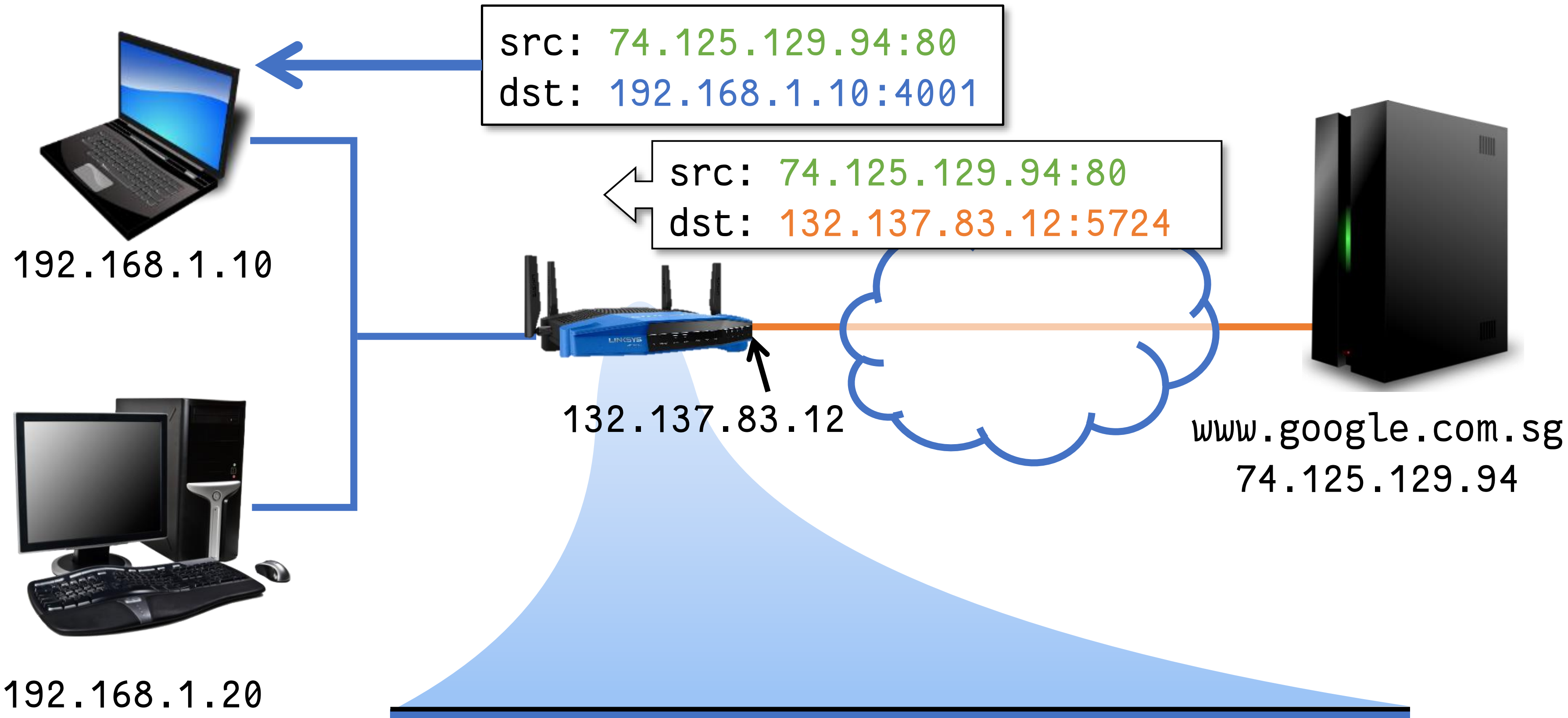
192.168.1.20

132.137.83.12

www.google.com.sg
74.125.129.94

Network Address Translation Table

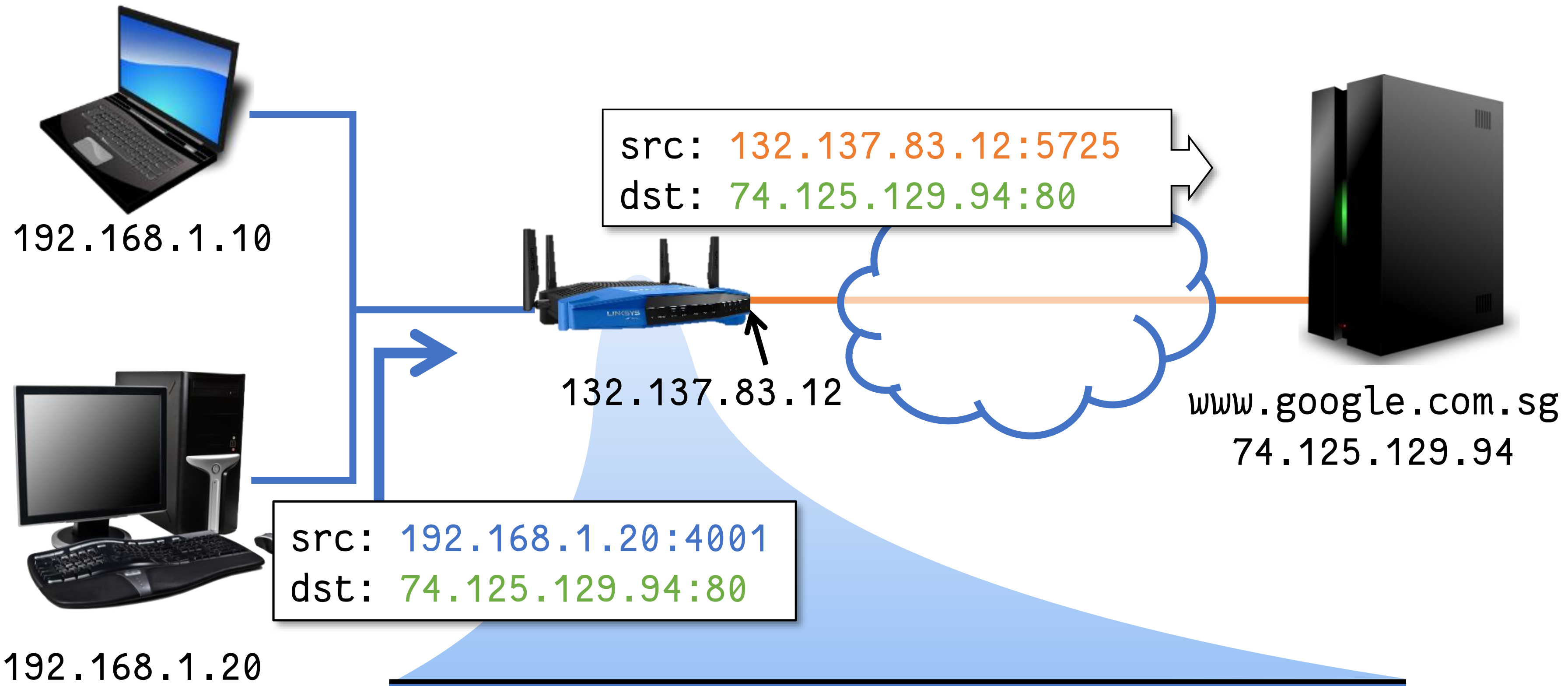
LAN		WAN
192.168.1.10:4001	⟷	132.137.83.12:5724



src: 74.125.129.94:80
dst: 192.168.1.10:4001

src: 74.125.129.94:80
dst: 132.137.83.12:5724

Network Address Translation Table		
LAN		WAN
192.168.1.10:4001	⟷	132.137.83.12:5724



src: 132.137.83.12:5725
dst: 74.125.129.94:80

192.168.1.10

132.137.83.12

www.google.com.sg
74.125.129.94

src: 192.168.1.20:4001
dst: 74.125.129.94:80

192.168.1.20

Network Address Translation Table

LAN		WAN
192.168.1.10:4001	⟷	132.137.83.12:5724
192.168.1.20:4001	⟷	132.137.83.12:5725

Advantages of NAT

Only need one public IP address

- Can change ISP without changing internal host addresses

All hosts use private address

- Can change internal IP without affecting outside world

Hosts within local network not explicitly addressable and visible to outside world

- Effectively firewalled

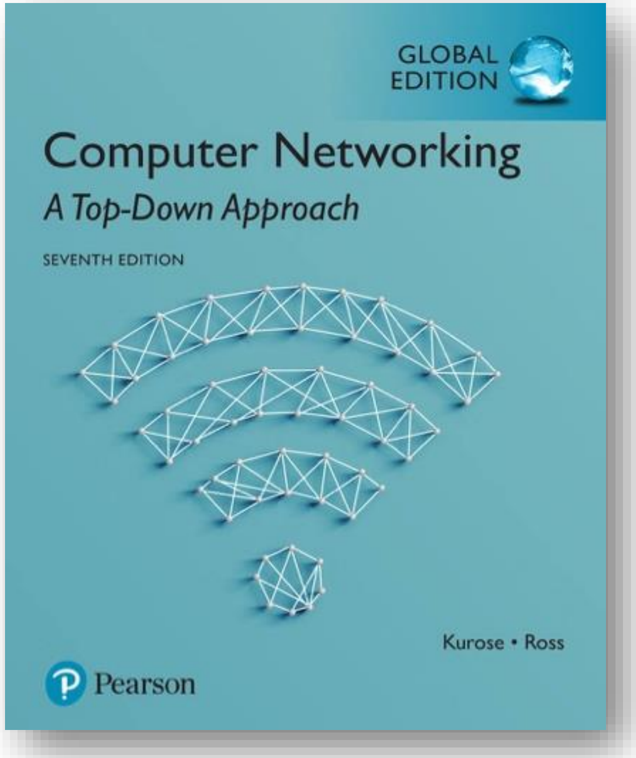
Chapter 4: Roadmap

4.1 Introduction

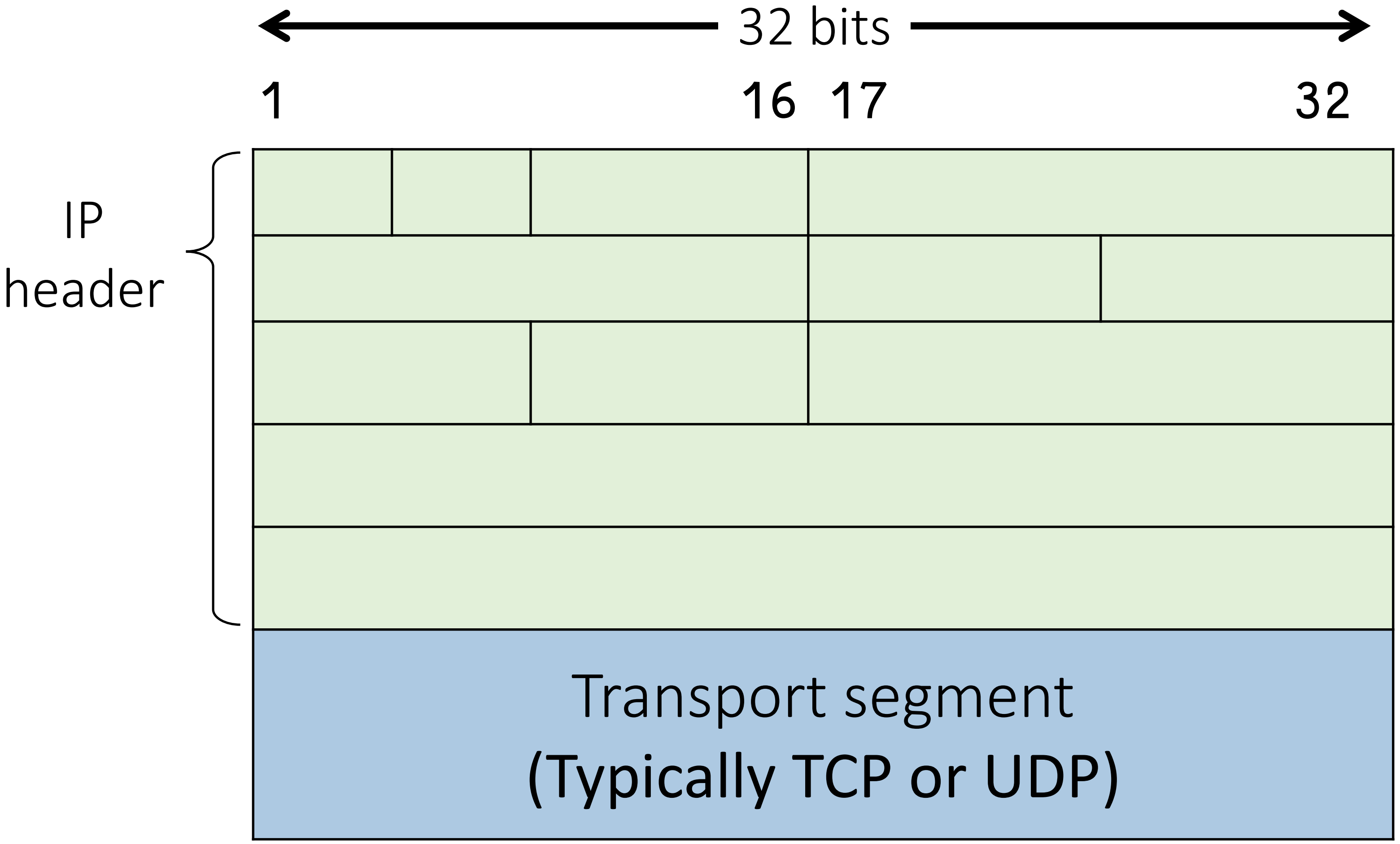
4.4 The Internet Protocol (IP)

- 4.4.1 Datagram Format
- 4.4.2 IPv4 Addressing
- 4.4.3 ICMP

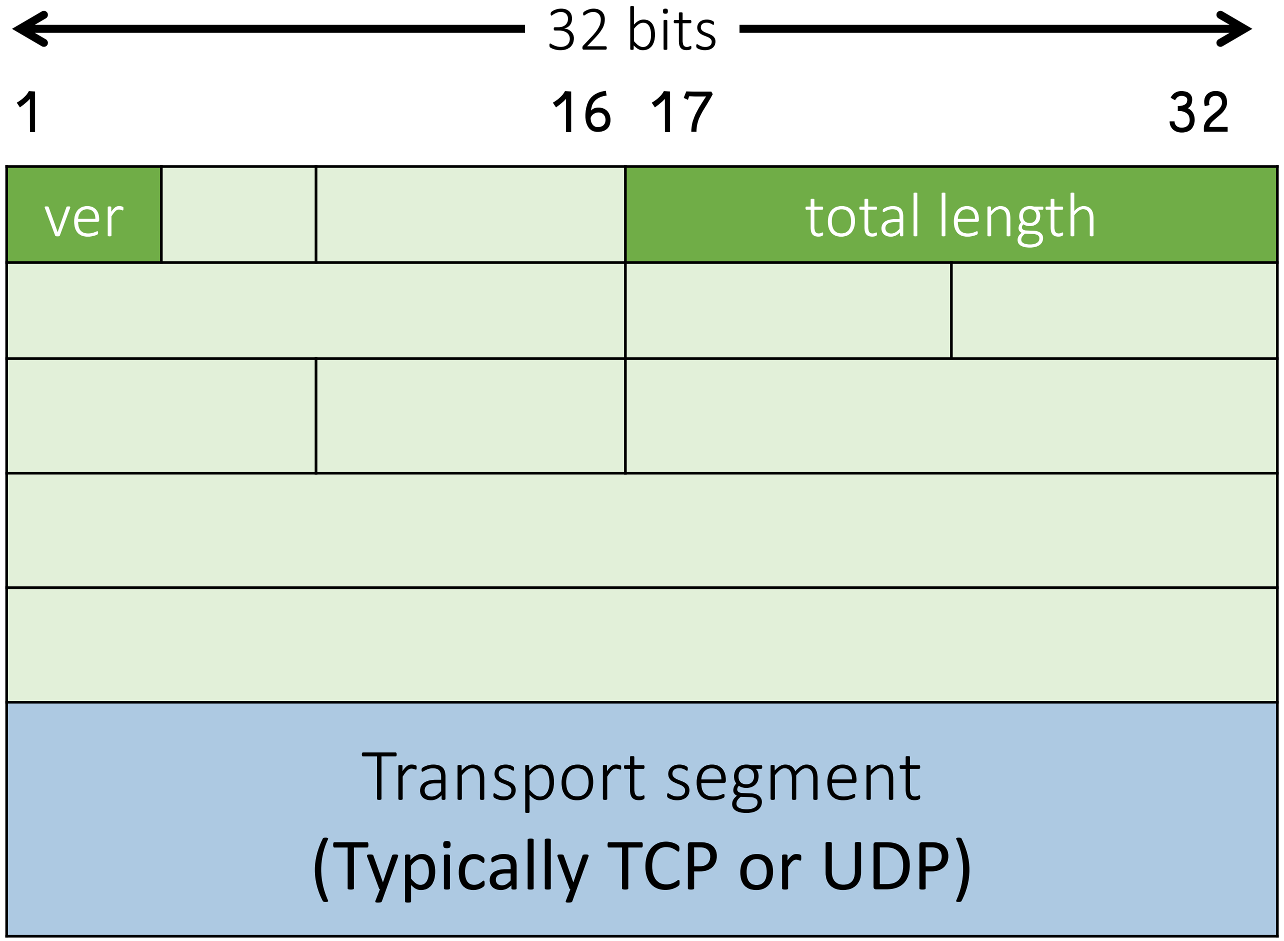
4.5 Routing Algorithms



IP datagram structure



IP datagram structure



32 bits

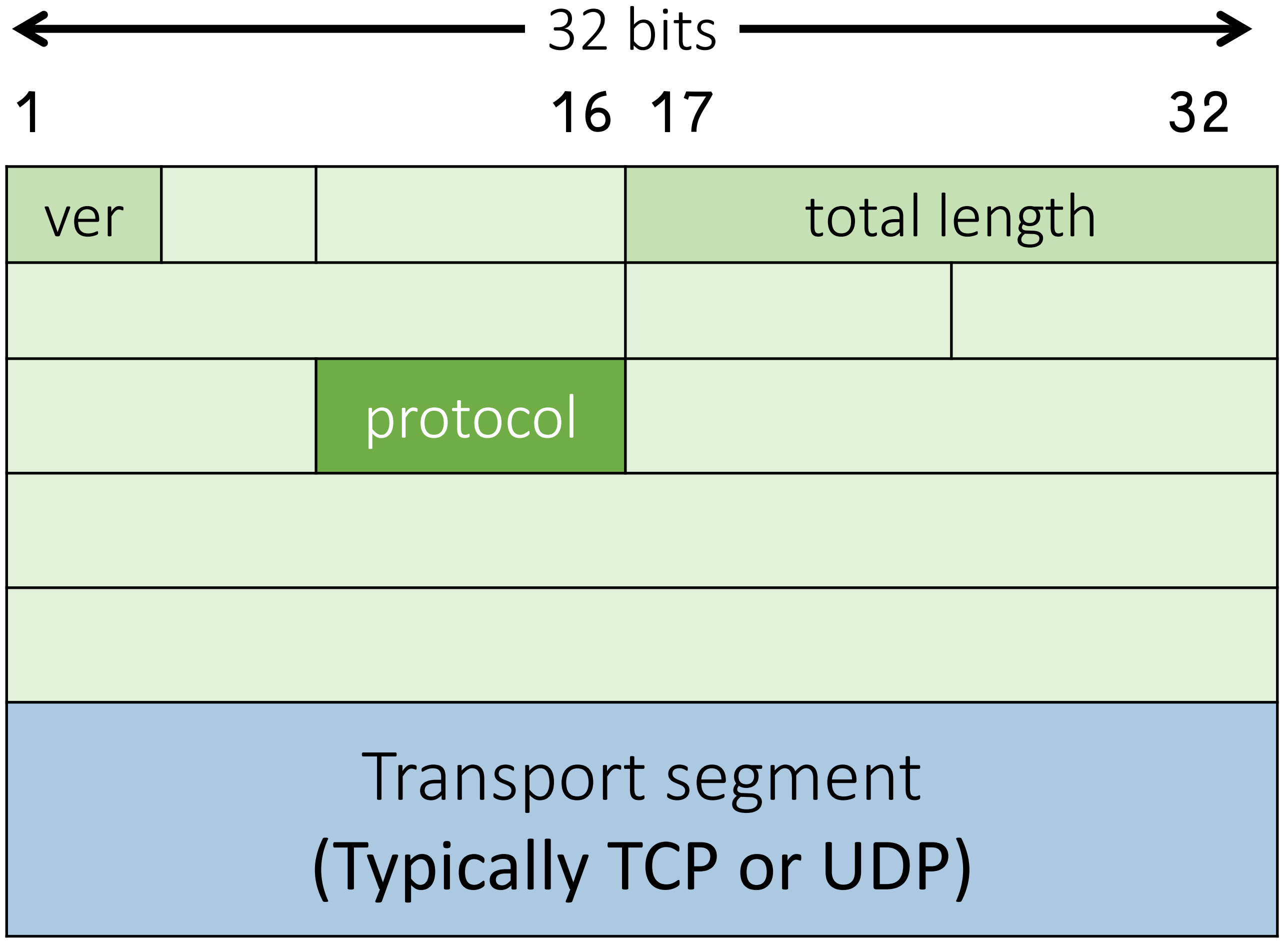
1 16 17 32

ver

total length

Transport segment
(Typically TCP or UDP)

IP datagram structure



32 bits

1 16 17 32

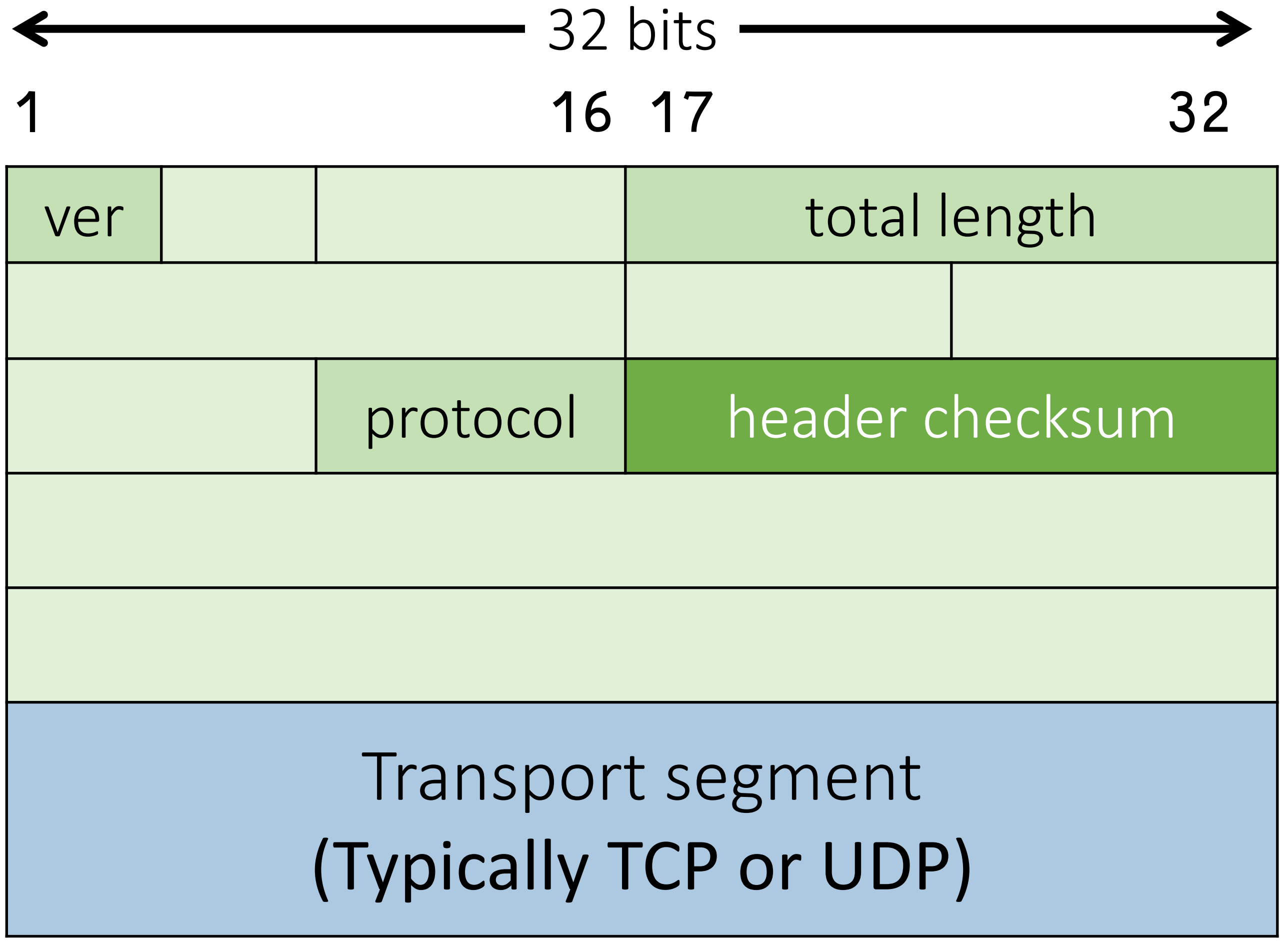
ver

total length

protocol

Transport segment
(Typically TCP or UDP)

IP datagram structure



32 bits

1

16

17

32

ver

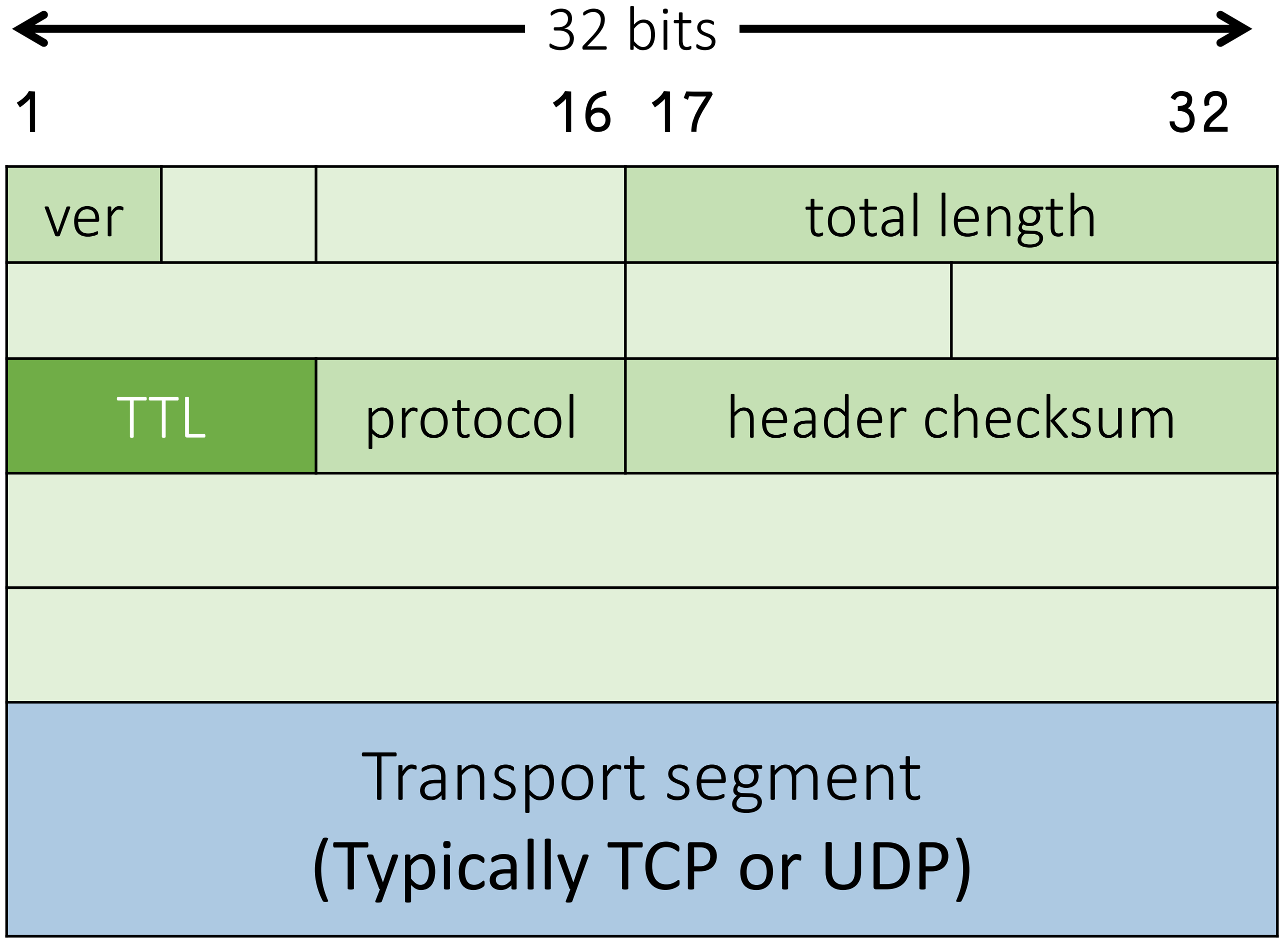
total length

protocol

header checksum

Transport segment
(Typically TCP or UDP)

IP datagram structure



32 bits

1 16 17 32

ver

total length

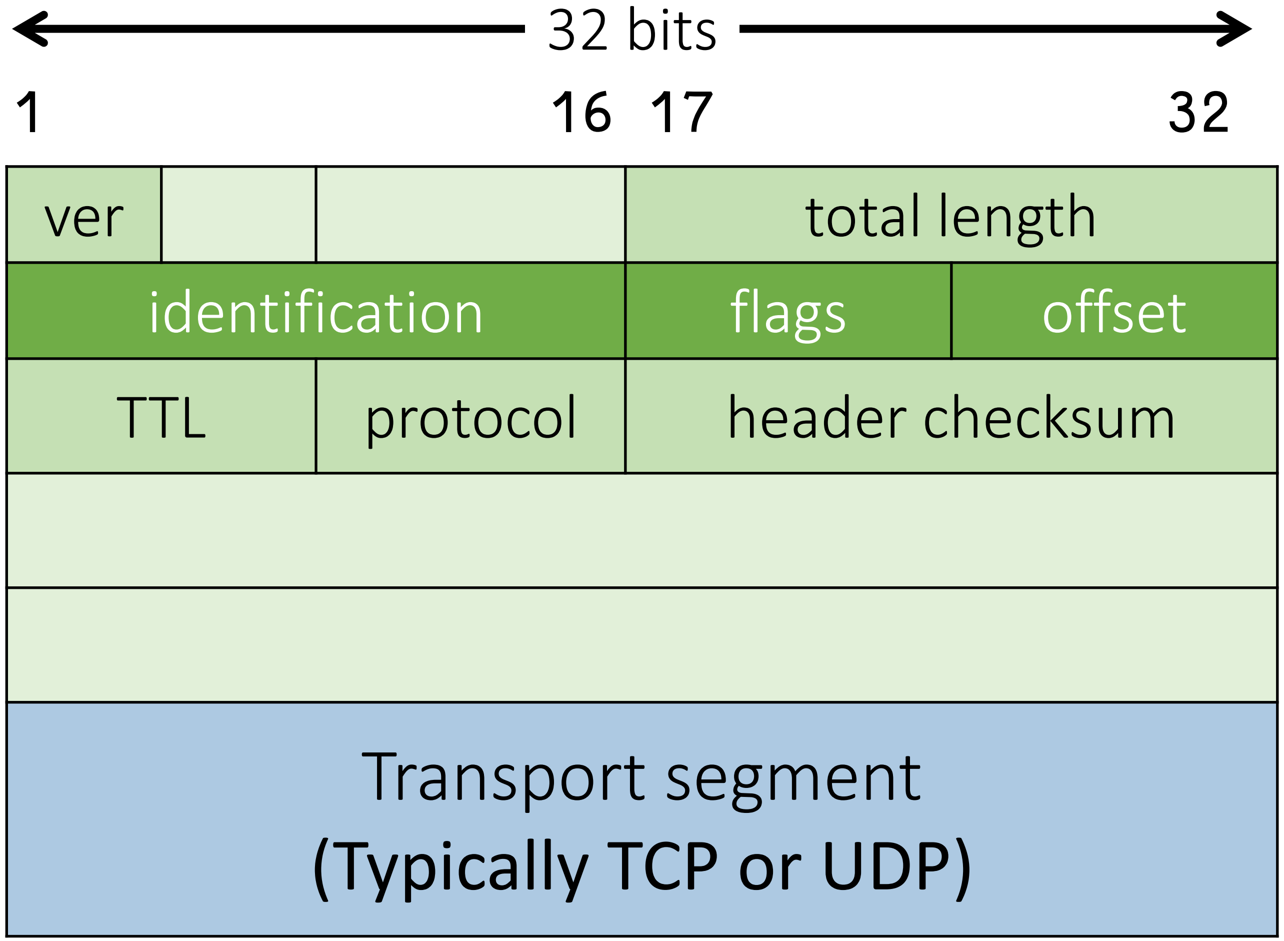
TTL

protocol

header checksum

Transport segment
(Typically TCP or UDP)

IP datagram structure



32 bits

1 16 17 32

ver | | | total length

identification | flags | offset

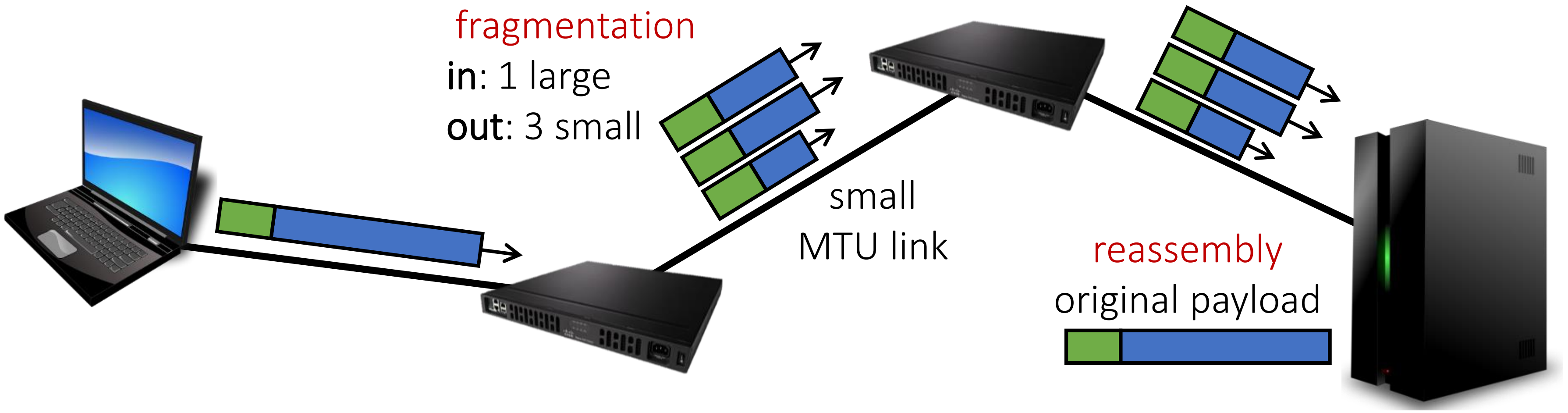
TTL | protocol | header checksum

Transport segment
(Typically TCP or UDP)

Datagram Fragmentation

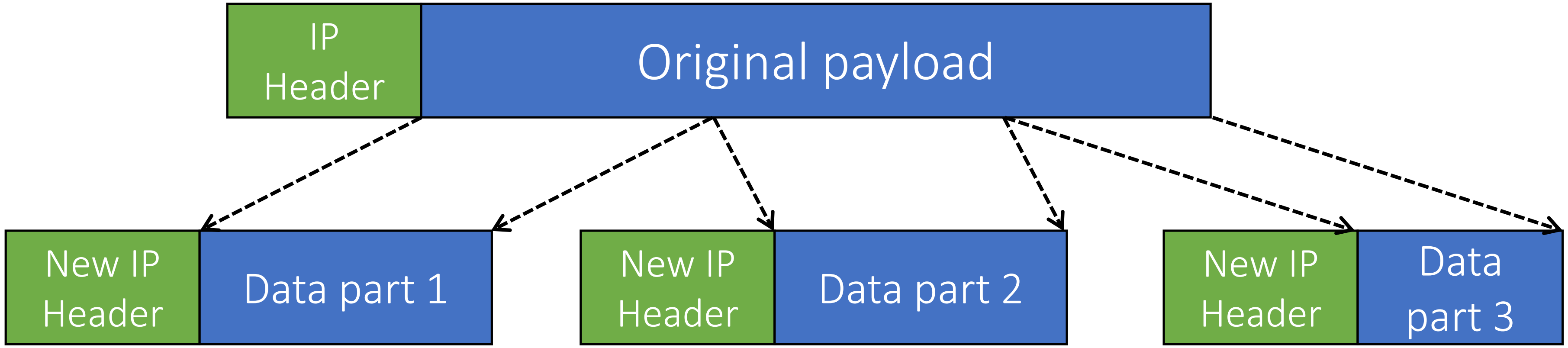
Different links may have different MTU

Large datagrams have to be fragmented by router



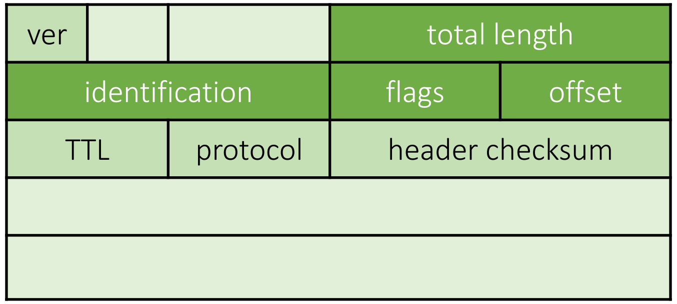
Destination host will reassemble the datagram

Illustration



Header fields to identify fragments

Example

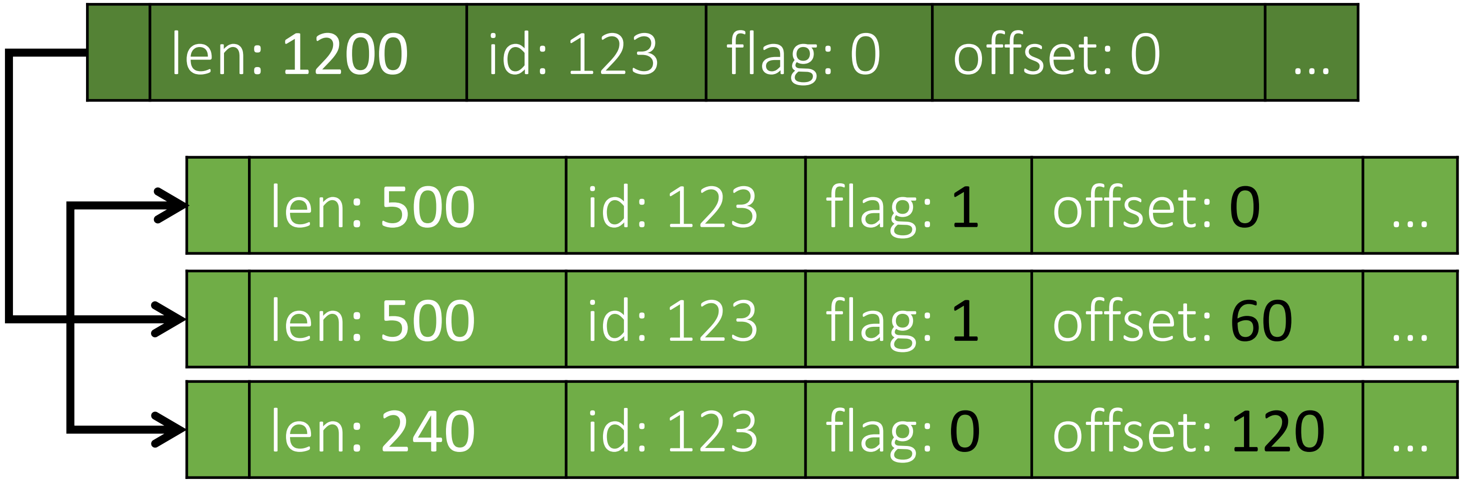


Frag Flag set to:

- 1 if there is next fragment
- 0 if this is last fragment

Offset is in multiple of 8-bytes

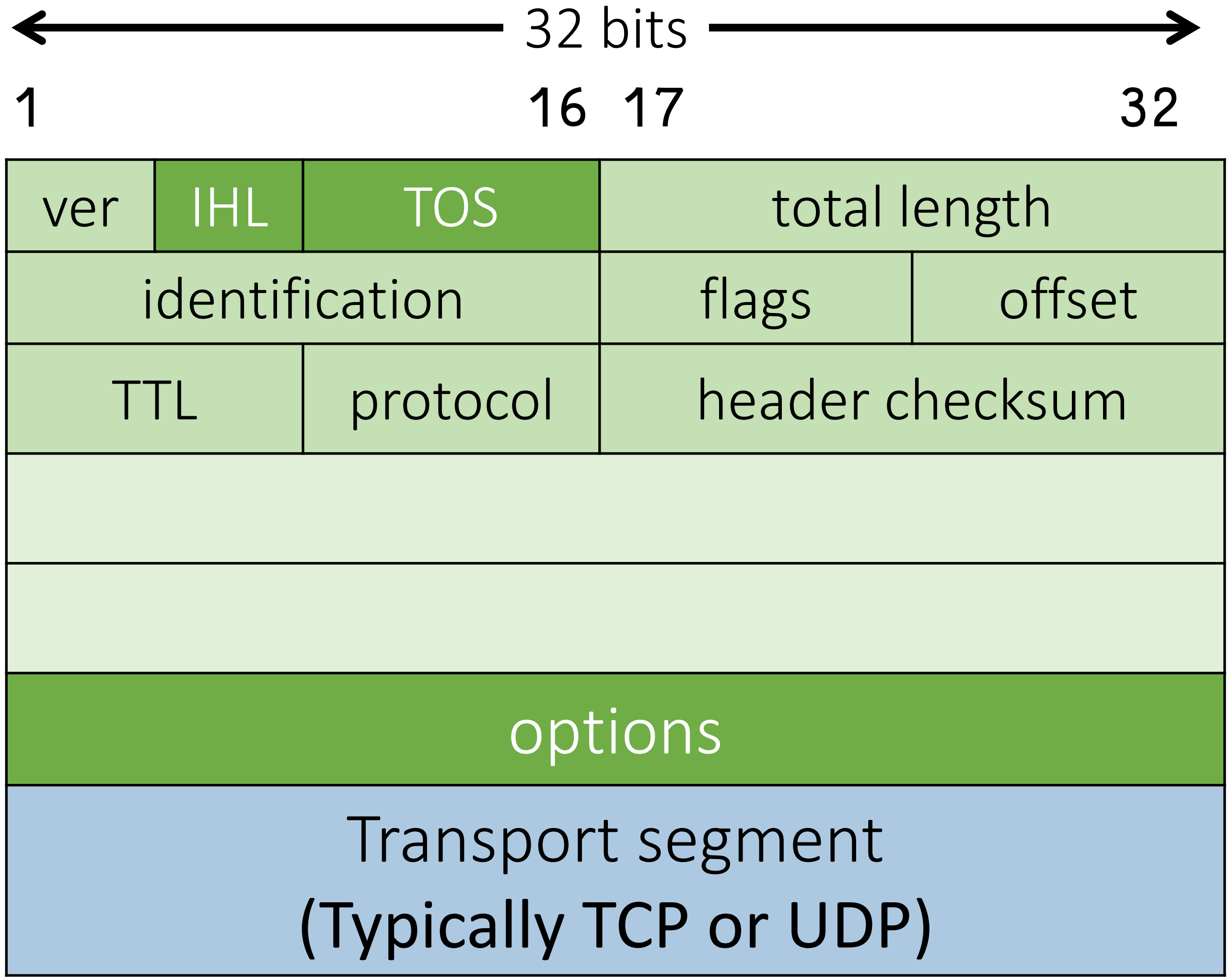
e.g. MTU = 500 bytes



	len: 1200	id: 123	flag: 0	offset: 0	...
	len: 500	id: 123	flag: 1	offset: 0	...
	len: 500	id: 123	flag: 1	offset: 60	...
	len: 240	id: 123	flag: 0	offset: 120	...

Header: 20 b
Payload: 480 b

IP datagram structure



32 bits

1

16

17

32

ver

IHL

TOS

total length

identification

flags

offset

TTL

protocol

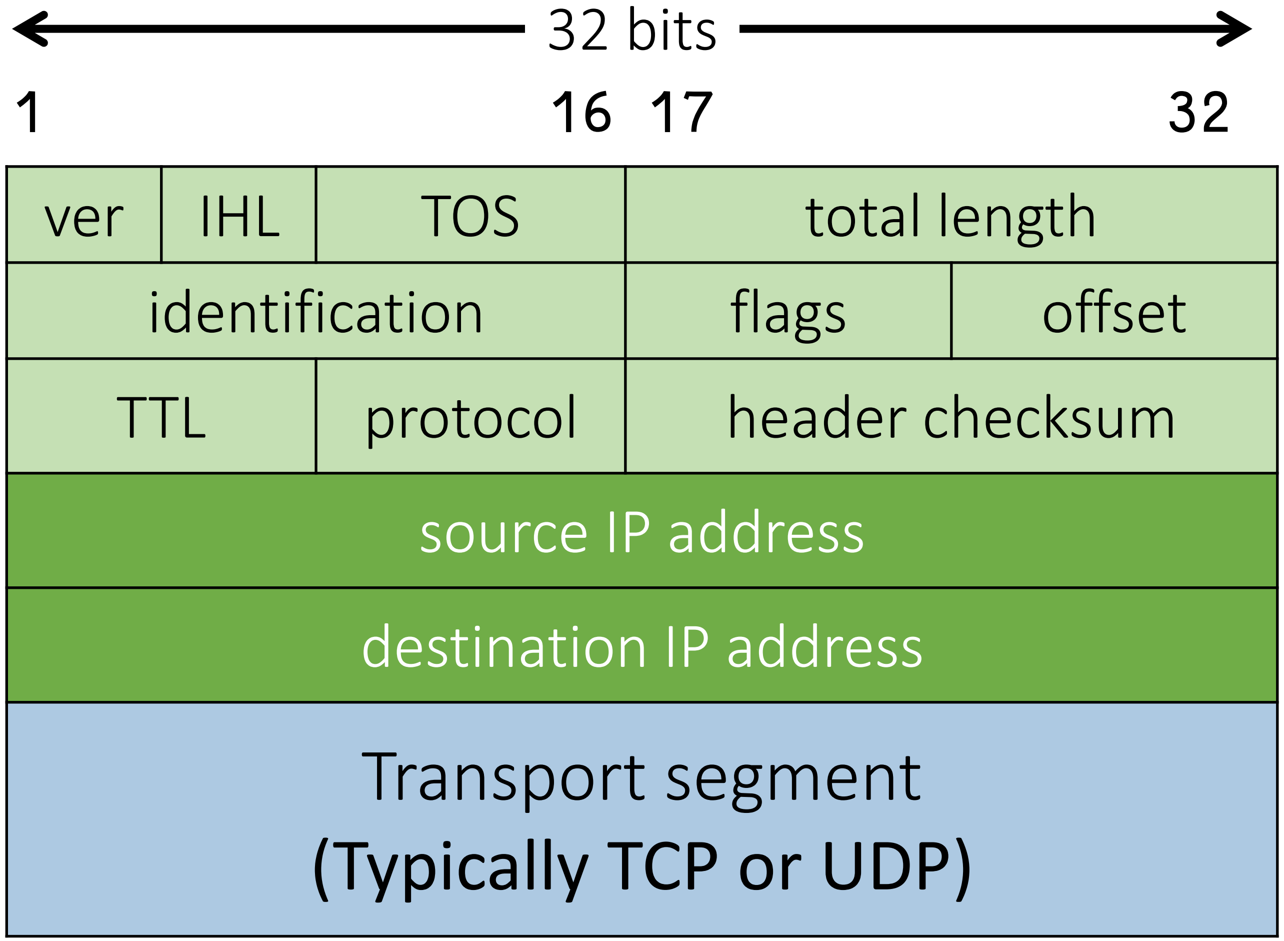
header checksum

options

Transport segment

(Typically TCP or UDP)

IP datagram structure



32 bits

1 16 17 32

ver | IHL | TOS | total length

identification | flags | offset

TTL | protocol | header checksum

source IP address

destination IP address

Transport segment
(Typically TCP or UDP)

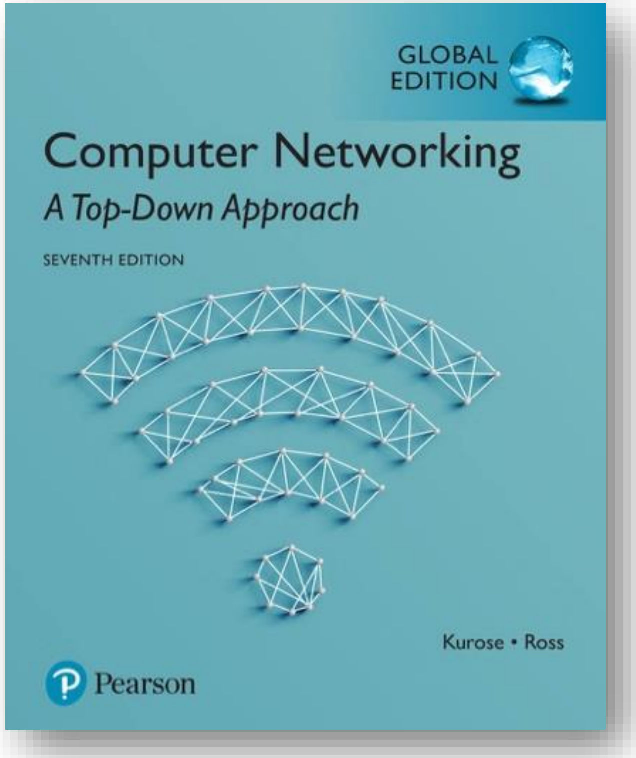
Chapter 4: Roadmap

4.1 Introduction

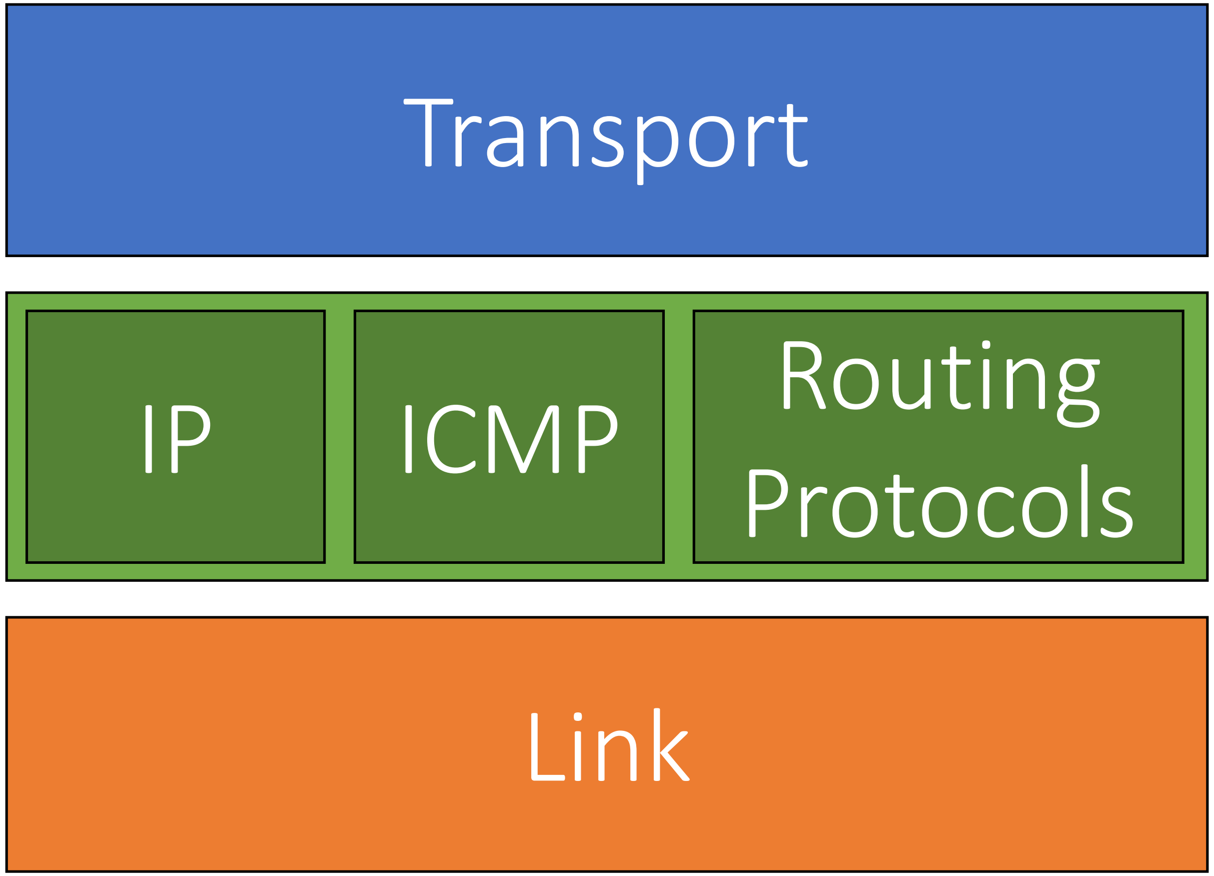
4.4 The Internet Protocol (IP)

- 4.4.1 Datagram Format
- 4.4.2 IPv4 Addressing
- 4.4.3 ICMP

4.5 Routing Algorithms



Network Layer Services



Transport

IP

ICMP

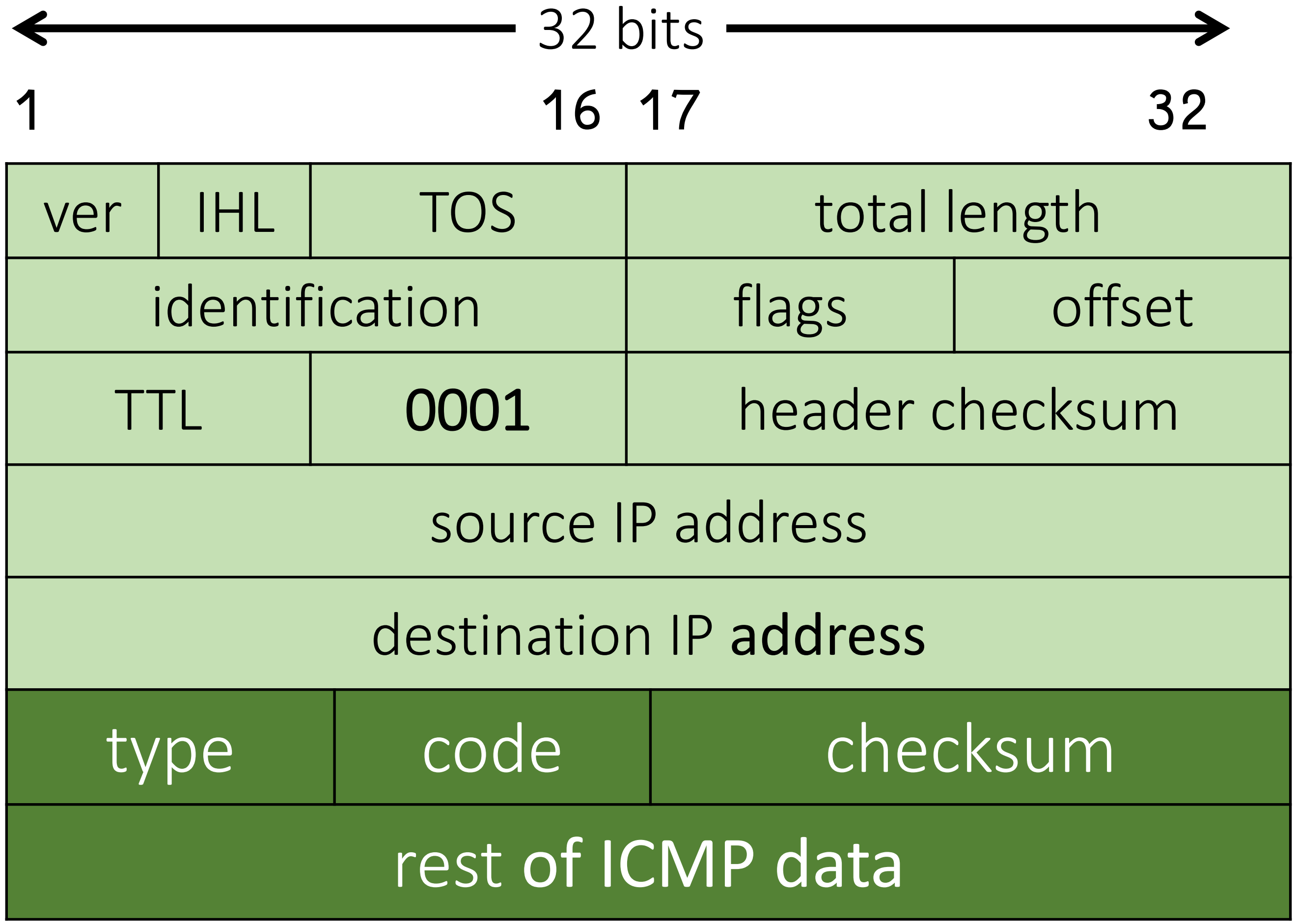
Routing Protocols

Link

ICMP

Internet Control Message Protocol

ICMP Header



32 bits

1 16 17 32

ver IHL TOS total length

identification flags offset

TTL **0001** header checksum

source IP address

destination IP **address**

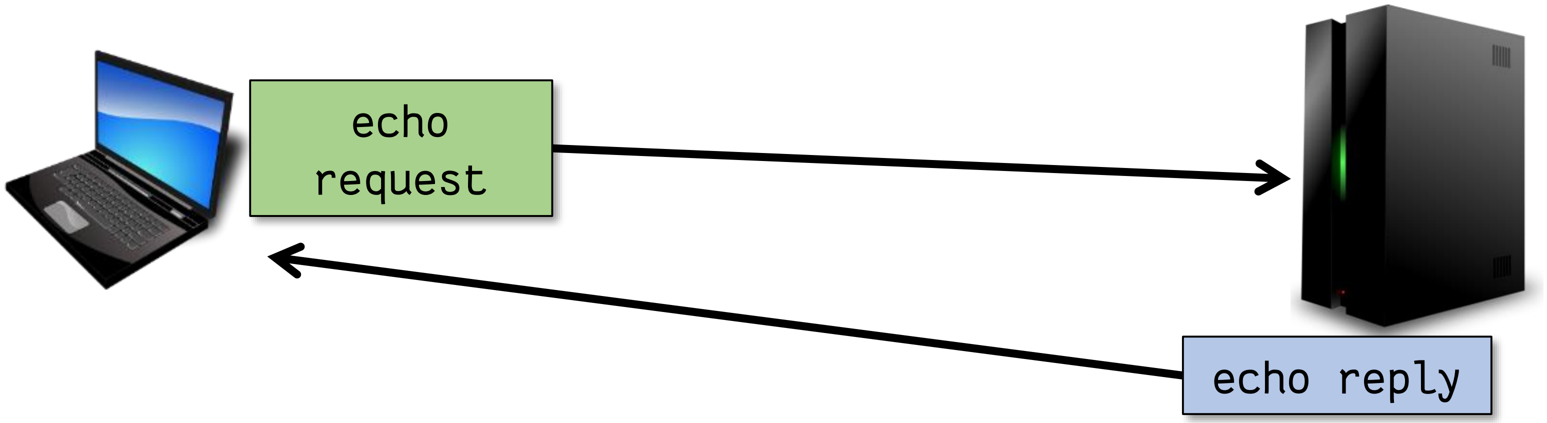
type code checksum

rest of **ICMP data**

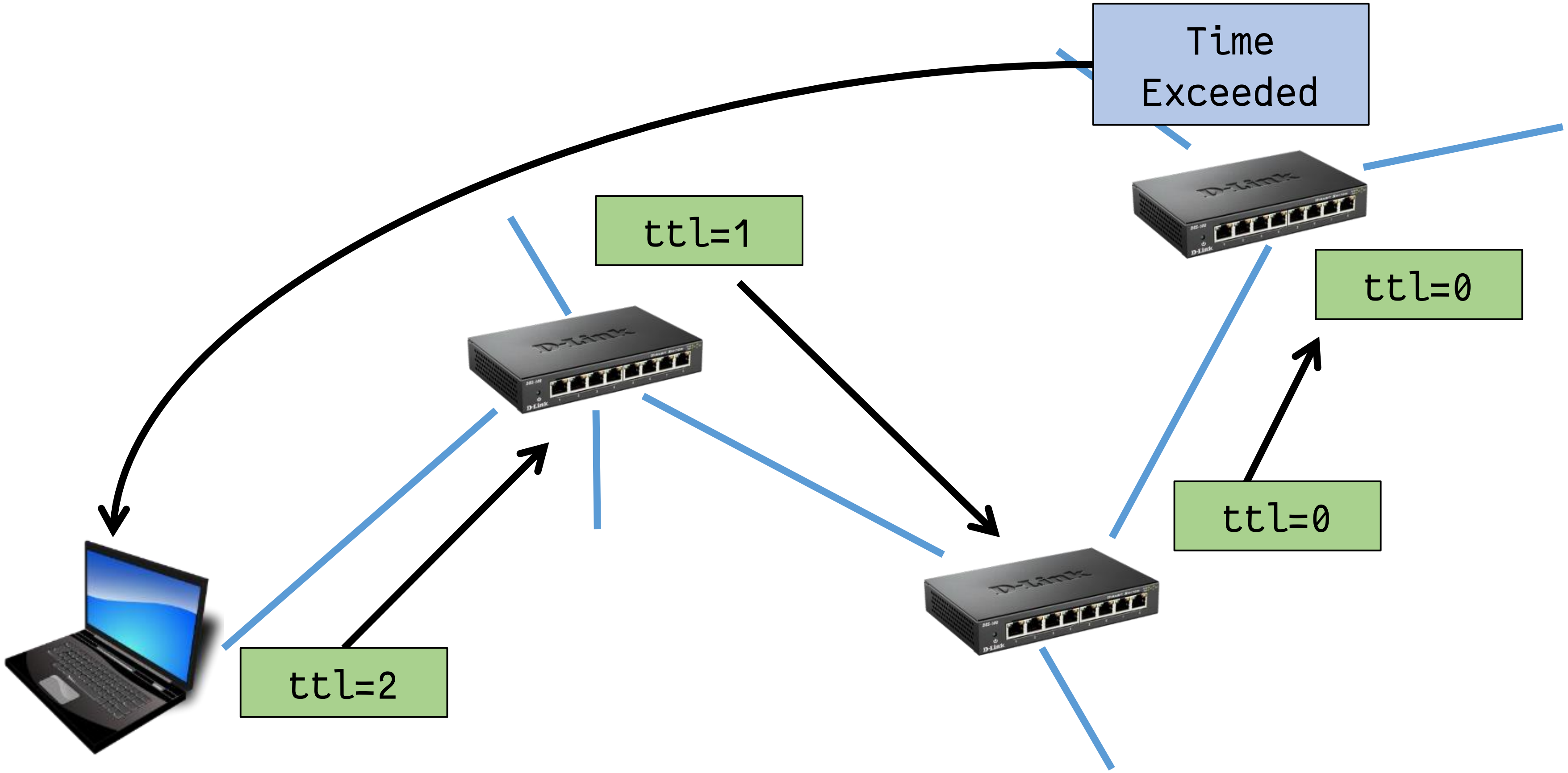
ICMP Type and Code

Type	Code	Description
8	0	echo **request**
0	0	echo **respond**
3	1	destination host unreachable
3	3	destination port unreachable
11	0	TTL expired
12	0	bad IP header

ping



traceroute



For your own interest

Virtual Circuit

What’s Inside a Router

IPv6

IPSec