

# Week 11: Network Layer – Internet Protocol

EE3017/IM2003 Computer Communications

School of Electrical and Electronic Engineering

Prof. Cheng Tee Hiang

Room: S1-B1a-29

Email: [ethcheng@ntu.edu.sg](mailto:ethcheng@ntu.edu.sg)

Phone: 6790-4534

The background features a light gray gradient with several decorative elements: two horizontal teal lines, one above and one below the text, and four large, overlapping teal arcs that curve from the top and bottom edges towards the center.

# Topic Outline

(Updated in February 2020)

## Network Layer – Internet Protocol

- Network Layer
- IP Datagram Format
- IP Fragmentation and Reassembly
- Number Systems
- IP Addressing
- Classful IP Addressing
- Special IP Addresses
- Subnet Addressing (Subnetting)
- Route Aggregation/Summarisation
- Dynamic Host Configuration Protocol (DHCP)



### **Recommended reading:**

Section 4.4, Pages 367 to 391 of the recommended textbook.

The background features a light gray gradient. Two horizontal teal bars, one above and one below the text, span the width of the slide. On the left side, there are several overlapping teal arcs of varying radii and opacities, creating a dynamic, layered effect. On the right side, there are also overlapping teal arcs, similar in style to the ones on the left.

# Learning Objectives

# Learning Objectives

By the end of this topic, you should be able to:

- Explain the following terms associated with Internet Protocol:
  - Network Layer
  - IP Datagram
  - IP Fragmentation and Reassembly
  - Number Systems
  - IP Addressing
  - Classful IP Addressing
  - Special IP Addresses
  - Subnet Addressing (Subnetting)
  - Route Aggregation/Summarisation
  - Dynamic Host Configuration Protocol (DHCP)

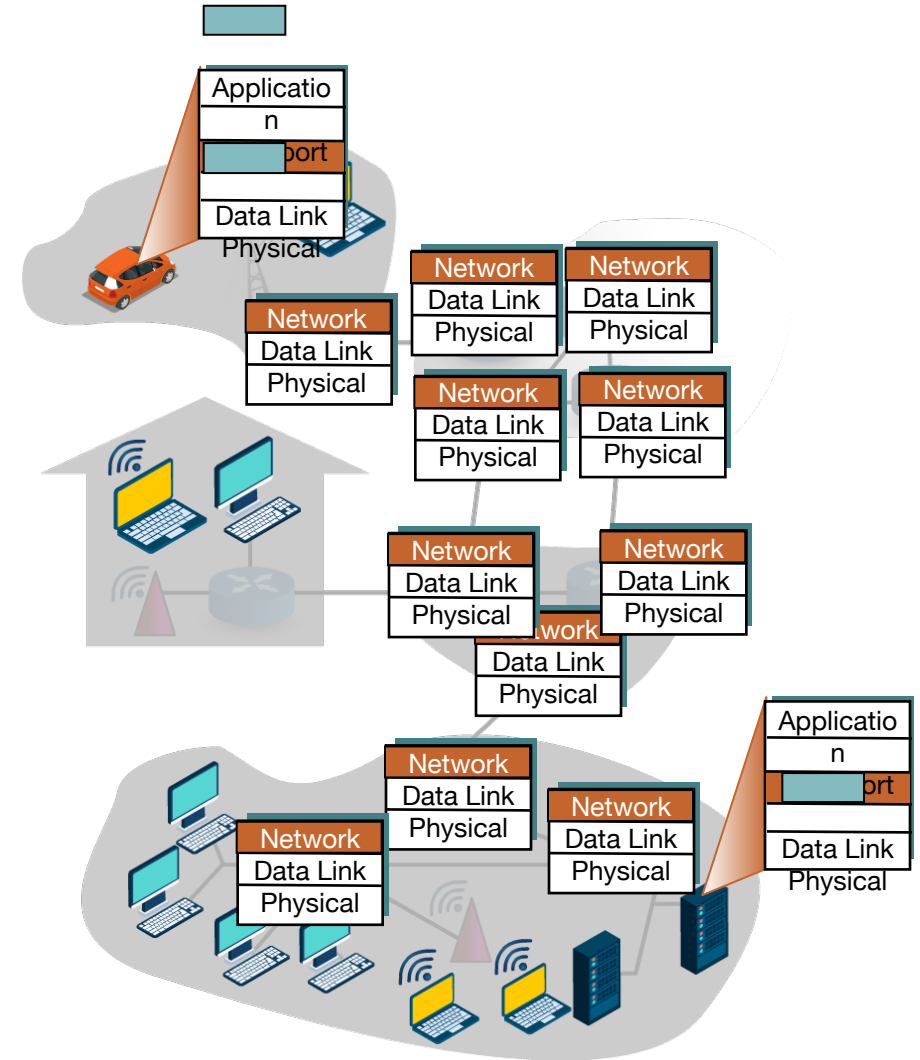




Network Layer

# Network Layer

- The Network Layer transports segments from a sending to the receiving host.
- On the sending side, it encapsulates segments into datagrams.
- On the receiving side, it delivers segments to the transport layer.
- Network layer protocols are present in every host and router.
- The router examines the header field of every Internet Protocol (IP) datagram passing through it.



# Two Key Network-Layer Functions

## Routing algorithms:

- Routing: Determining the route taken by packets from the source to destination.
- Forwarding: Moving packets from the router's input to the appropriate router output.

## Analogy:

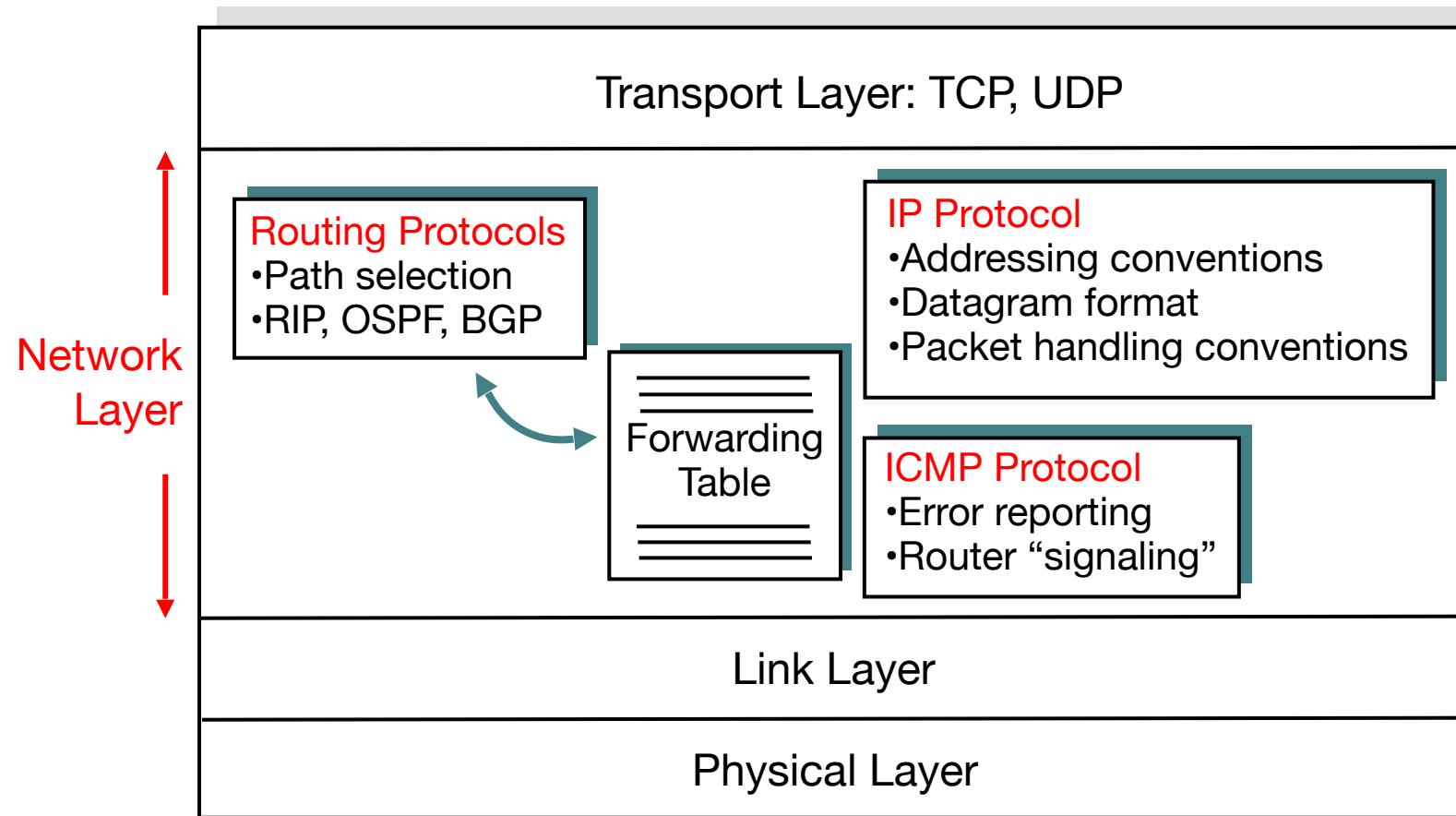
- Routing: Process of planning the trip from source to destination.
- Forwarding: Process of getting through a single interchange.





# Internet Network Layer

Host, router network layer functions:



*We will focus on IP protocol in this module. Routing protocols and ICMP are not in the scope.*

## Notes: Network Layer

- Network layer is present in every host and router. It is responsible for host-to-host communications. It does so by transporting segments receiving from the Transport Layer of a host as IP packets to another host across the network.
- IP packets are forwarded by routers in the network. When a router receives an IP packet, it will examine the IP packet header. It will look at the destination IP address, from which it will extract the subnet address and access its routing table to find out which router interface it should forward the IP packet to.
- Extracting the subnet address is equivalent to using the postal code in the full address to extract the block number and street name but ignore the unit number in the full address. This is known as the forwarding function.
- Routers exchange routing information with other routers to set up the routing table and determine the best route to forward packets from a particular subnet to another subnet. This function is known as the routing function.

## Notes: Network Layer

---

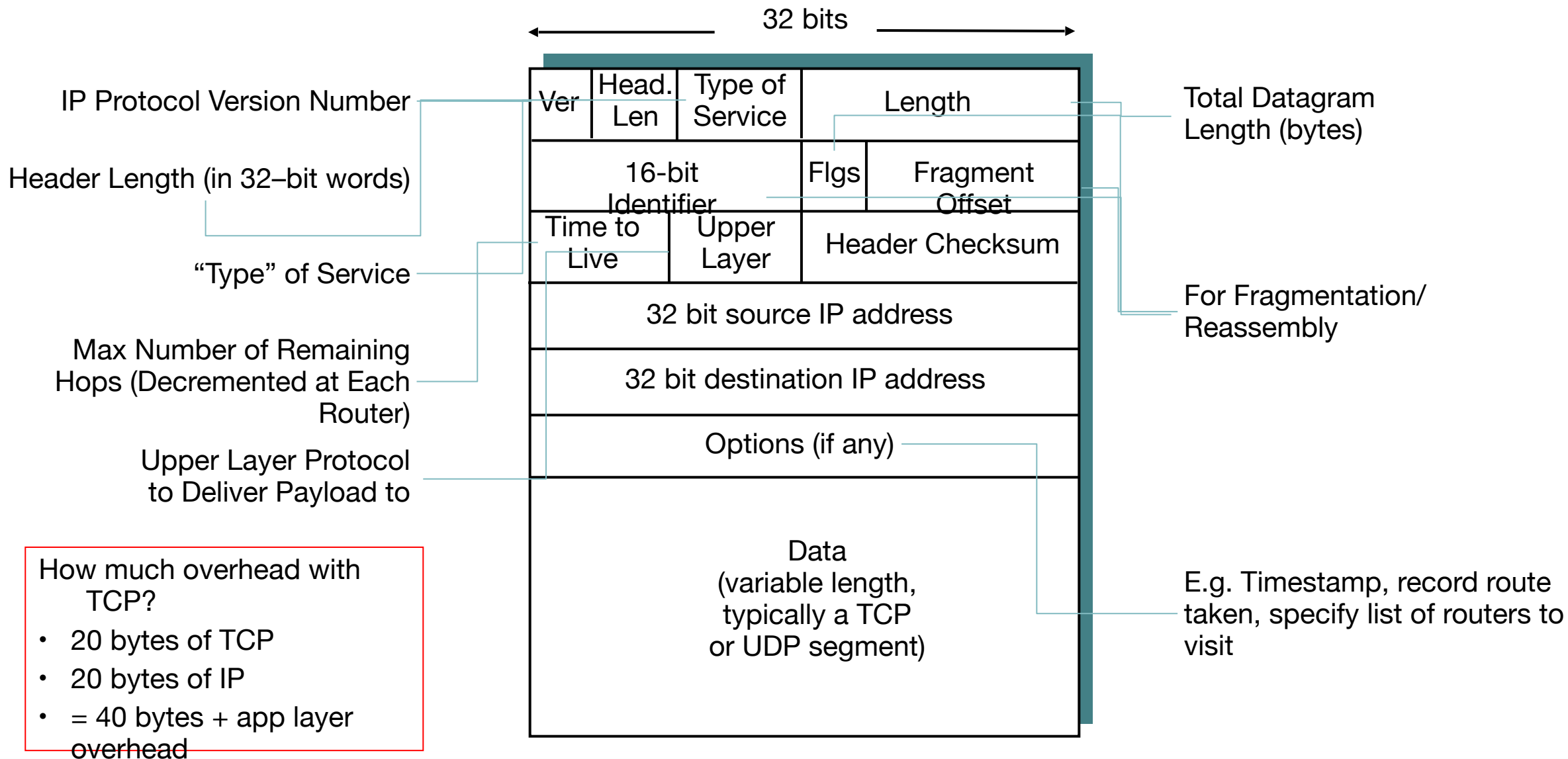
- Routing function of a router is performed by a routing protocol. Widely used routing protocols are Open Shortest Path First (OSPF), Routing Information Protocol (RIP), and Border Gateway Protocol (BGP). The dominant router vendor, Cisco Systems, also has its own proprietary Interior Gateway Routing Protocol (IGRP) and Enhanced Interior Gateway Routing Protocol (EIGRP).
- Network Layer also contains the Internet Control Message Protocol (ICMP). ICMP is an error-reporting protocol. It allows network devices such as routers to generate error messages to inform the source IP address when network problems prevent delivery of IP packets. ICMP also allows network devices to exchange information for signaling purposes; e.g., a source host could use an ICMP 'echo reply' message to request routers along the path towards the destination host to reply, which can then be used for diagnostic purpose.

*Routing protocols and ICMP are not in the scope of this module.*



# IP Datagram Format

# IP Datagram Format



# Notes: IP Datagram Format

**Version Number:** These 4 bits specify the IP protocol version of the datagram. The IP datagram format shown is for IP version 4 (IPv4), which is the version we use today. IP version 6 (IPv6) is a new IP protocol which is gaining traction and you will learn about IPv6 in EE4718 Enterprise Network Design.

**Header Length:** IPv4 datagram can contain a variable number of options, which are included in the IPv4 datagram header; hence, these 4 bits are needed to determine where in the IP datagram the data actually begins.

**Type of Service:** This field allows different types of IP datagrams to be differentiated, for example, it might be useful to distinguish datagrams from real-time applications (such as IP telephony) and those from non-real-time applications (such as file transfer) so that the router administrator could decide if there is a need to accord different priorities to different types of service.

# Notes: IP Datagram Format

**Datagram Length:** This is the total length of the IP datagram (header plus data) measured in bytes. Since this field is 16 bits long, the theoretical maximum size of the IP datagram is 65,535 bytes. However, datagrams are rarely larger than 1,500 bytes.

**Identifier, Flags, Fragmentation Offset:** These 3 fields are used when an IP datagram needs to be fragmented. This will be elaborated later.

**Time-to-live (TTL):** This is used to ensure that datagrams do not circulate forever in the network. This field is decremented by one each time the datagram is processed by a router. When the TTL field reaches 0, the datagram will be dropped.

**Protocol:** This field is used when an IP datagram reaches its final destination. The value of this field indicates the specific transport-layer protocol to which the data portion of the datagram should be passed to. For example, 16 indicates TCP and 17 indicates UDP.

# Notes: IP Datagram Format



**Header Checksum:** This is used for detecting bit errors in the IP header. This topic will be discussed under Internet Checksum.

**Source and Destination IP Addresses:** These contain the IP address of the source host and that of the destination host.

**Options:** The option fields allow the IP header to be extended and they are rarely used.

**Data (Payload):** The data field contains the transport-layer segment and may also carry other types of data, such as ICMP messages.





# IP Fragmentation and Reassembly

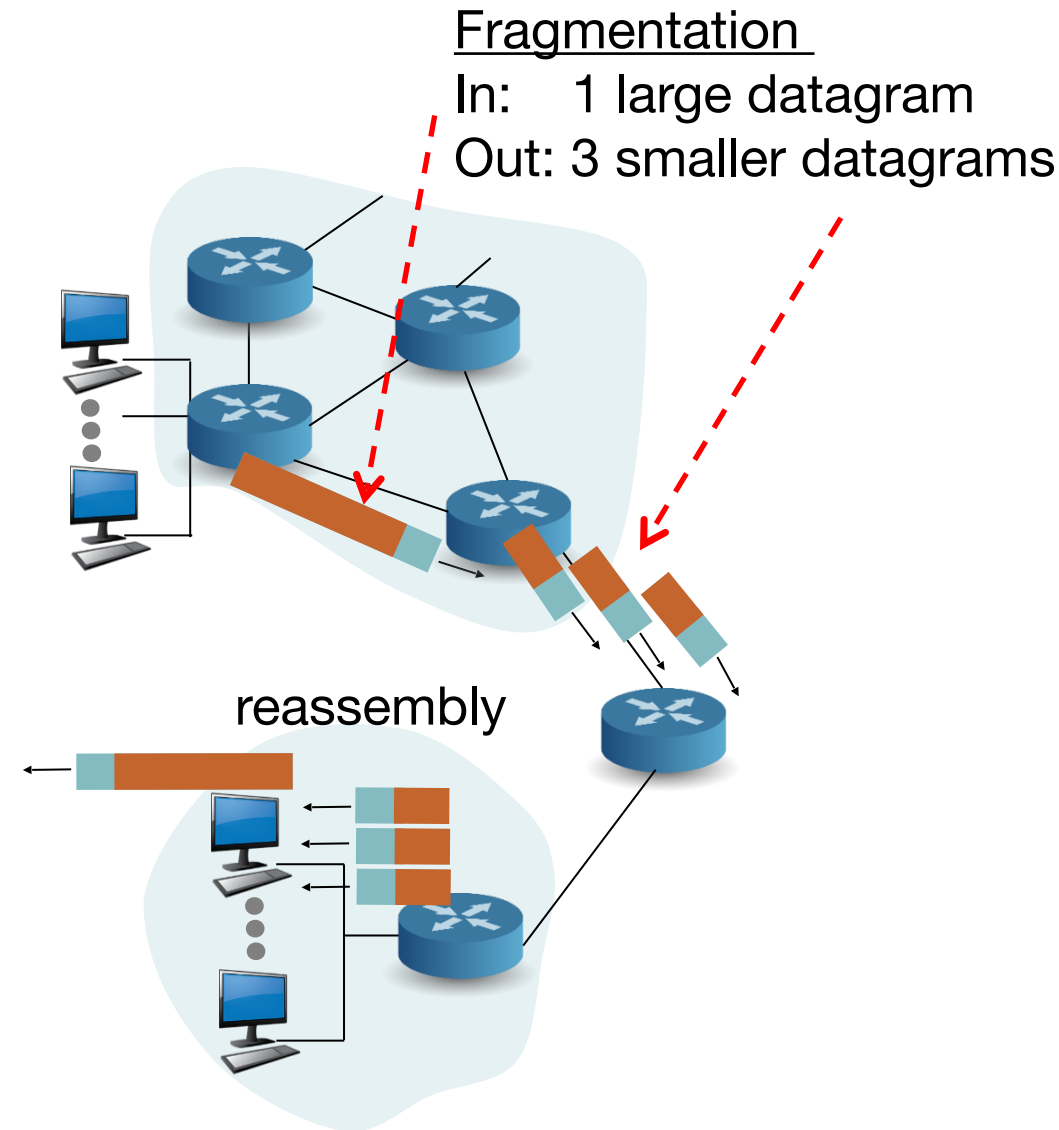
# IP Fragmentation and Reassembly

Network links have a Maximum Transfer Unit (MTU) – largest possible link-level frame:

- Different link types, different MTUs

Large IP datagram divided (“fragmented”) within net:

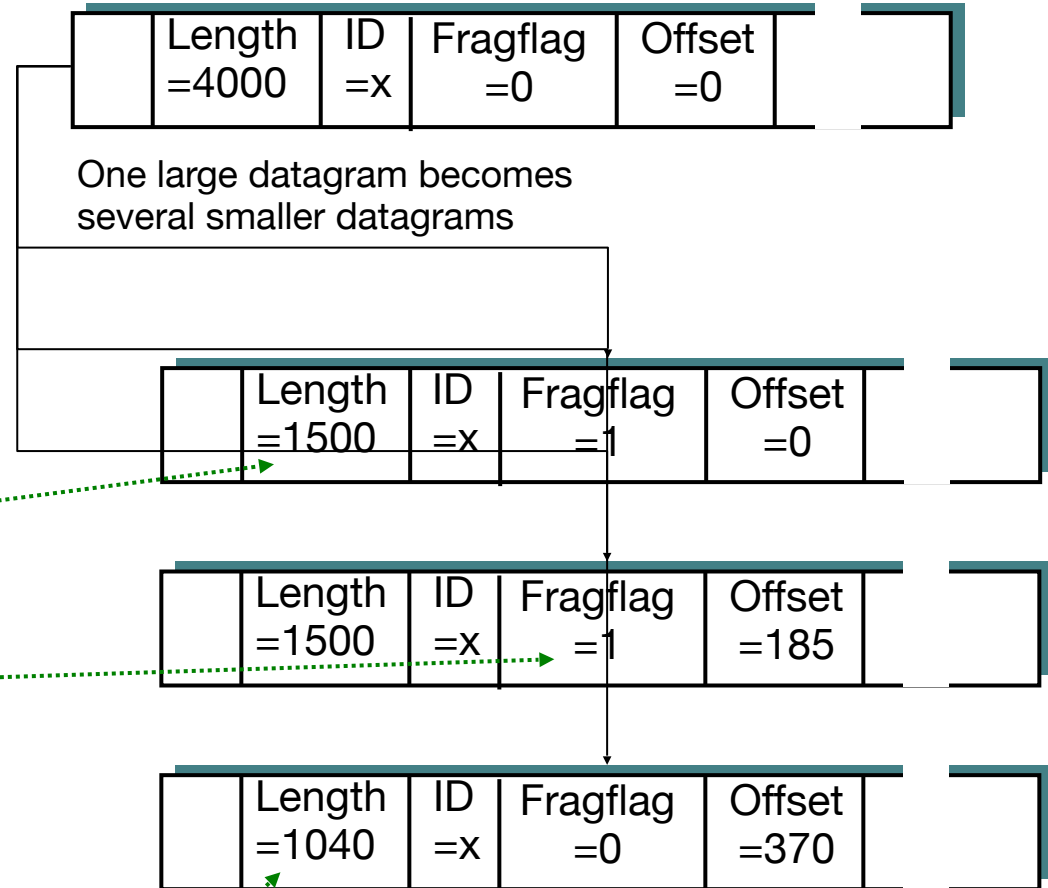
- One datagram becomes several datagrams
- “Reassembled” only at final destination
- IP header bits used to identify, order related fragments



# IP Fragmentation and Reassembly

Example:

- 4000 byte datagram (3980 of data + 20 bytes of header)
- MTU = 1500 bytes (1480 bytes of data in data field)
- Remember that each IP packet has 20 bytes of header!



1480 bytes in data field

Offset = 1480/8

(Offset value is specified in 8-byte chunks)

$$3980 - 1480 - 1480 + 20 = 1040$$

## Notes: IP Fragmentation and Reassembly

- Not all link-layer protocols can carry network-layer packets of the same size. Some protocols can carry big datagrams, whereas other protocols can carry only little packets.
- The maximum amount of data that a link-layer frame can carry is called the MTU. Because each IP datagram is encapsulated within the link-layer frame for transport from one router to the next router, the MTU of the link-layer protocol places a hard limit on the length of an IP datagram.
- When an IP datagram is received by a router and its size is bigger than the MTU of the outgoing link, the IP datagram will need to be fragmented into two or more smaller IP datagrams. These IP datagram fragments only need to be reassembled at the destination host.
- In the given example, a datagram of 4,000 bytes (20 bytes of IP header plus 3,980 bytes of IP payload) arrives at a router must be forwarded to a link with an MTU of 1,500 bytes.
- This leads to 3,980 data bytes in the original datagram to be divided to three separate fragments (each of which is also an IP datagram).

## Notes: IP Fragmentation and Reassembly

- Note that all the 3 new IP datagrams will carry the same identification number of  $x$  as in the original datagram.
- The flags of the first two new datagrams are both '1', indicating that they are not the last fragment. The flag of the third new datagram is '0', which indicates that it is the last fragment in the fragmented datagram.
- For the 1st new IP datagram, there are 1,480 bytes in the data field. The offset is 0, meaning that the data should be inserted beginning at byte 0.
- For the 2nd new IP datagram, there are 1,480 bytes in the data field. The offset is 185, meaning that the data should be inserted beginning at byte  $185 \times 8 = 1,480$ .
- For the 3rd new IP datagram, there are  $1,020 (= 3,980 - 1,480 - 1,480)$  bytes in the data field; as such, the length is  $1,020 + 20 = 1,040$ . The offset is  $185 + 185 = 370$ , meaning that the data should be inserted beginning at byte  $370 \times 8 = 2,960$ .

The background features a light gray gradient with abstract teal-colored curved lines and segments. A solid teal horizontal band runs across the middle of the image, passing behind the title text.

# Number Systems

# Number Systems

Base 10				
Place Value	$\frac{4}{1000}$	$\frac{8}{100}$	$\frac{2}{10}$	$\frac{5}{1}$
Base Exponent	$10^3 = 1000$ $10^2 = 100$ $10^1 = 10$ $10^0 = 1$			
Number of Symbols	10			
Symbols	0, 1, 2, 3, 4, 5, 6, 7, 8, 9			
Rationale	Typical number of fingers is ten			

# Number Systems

Base 2								
Place Value	$\frac{1}{128}$	$\frac{0}{64}$	$\frac{1}{32}$	$\frac{1}{16}$	$\frac{0}{8}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{1}$
Base Exponent	$2^7 = 128$ $2^6 = 64$ $2^5 = 32$ $2^4 = 16$ $2^3 = 8$ $2^2 = 4$ $2^1 = 2$ $2^0 = 1$							
Number of Symbols	2							
Symbols	0, 1							
Rationale	Two-state (discrete binary) voltage systems made from transistors can be diverse, powerful, inexpensive, tiny and relatively immune to noise.							



# Number Systems

Converting a binary number into a decimal number:

$(b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0)_{\text{base}2}$

$$= b_7 \times 2^7 + b_6 \times 2^6 + b_5 \times 2^5 + b_4 \times 2^4 + b_3 \times 2^3 + b_2 \times 2^2 + b_1 \times 2^1 + b_0 \times 2^0$$

$$= b_7 \times 128 + b_6 \times 64 + b_5 \times 32 + b_4 \times 16 + b_3 \times 8 + b_2 \times 4 + b_1 \times 2 + b_0 \times 1$$

**Example:**

$$\begin{aligned} 10110111_2 &= 1 \times 2^7 + 0 \times 2^6 + 1 \times 2^5 + 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 \\ &= 1 \times 128 + 0 \times 64 + 1 \times 32 + 1 \times 16 + 0 \times 8 + 1 \times 4 + 1 \times 2 + 1 \times 1 \\ &= 128 + 32 + 16 + 4 + 2 + 1 \\ &= 183 \end{aligned}$$

*You can use a calculator to do the conversion!*

# Number Systems

Converting a decimal number into a binary number:

$$2 \overline{)183} \quad \text{-- 1}$$

$$2 \overline{)91} \quad \text{-- 1}$$

$$2 \overline{)45} \quad \text{-- 1}$$

$$2 \overline{)22} \quad \text{-- 0}$$

$$2 \overline{)11} \quad \text{-- 1}$$

$$2 \overline{)5} \quad \text{-- 1}$$

$$2 \overline{)2} \quad \text{-- 0}$$

$$2 \overline{)1} \quad \text{-- 1}$$

0

$$183 = 10110111_2$$



# IP Addressing

# IP Addressing

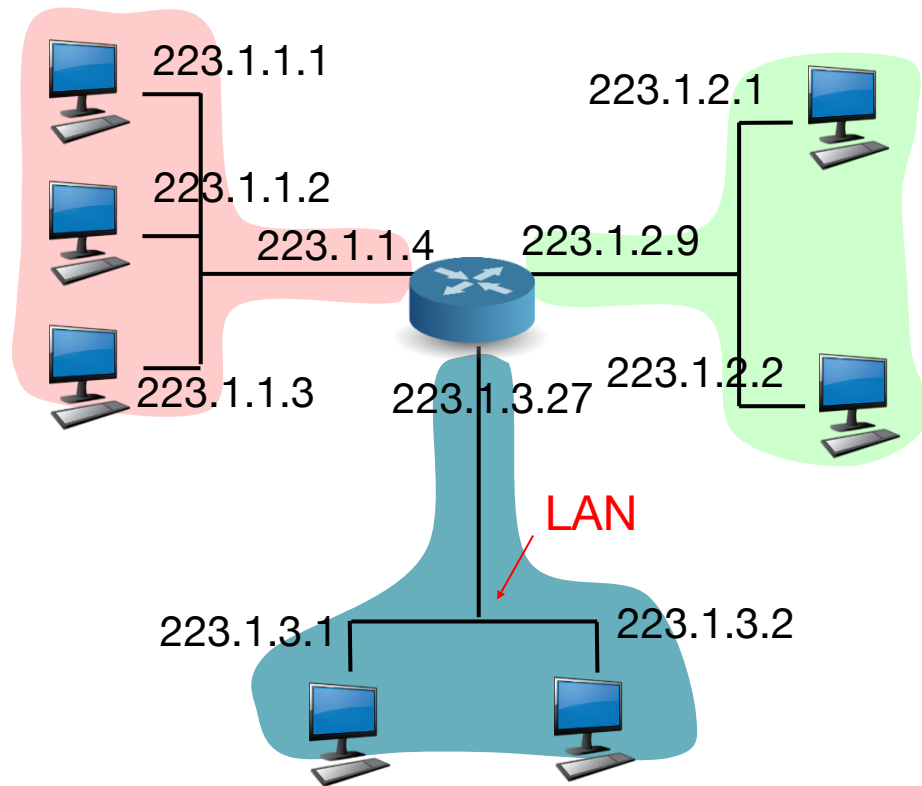
An **Interface** is the connection point between host/router and physical link. An **IP address** is a 32-bit identifier for an interface that is written in [dotted-decimal notation](#).

For example, the IP address 223.1.1.1 represents:

11011111	00000001	00000001	00000001
└──────────┘	└──────────┘	└──────────┘	└──────────┘
223	1	1	1

# IP Addressing

Each interface must have a unique address in the network. In this example, the network address consists of 24 bits or 3 bytes.



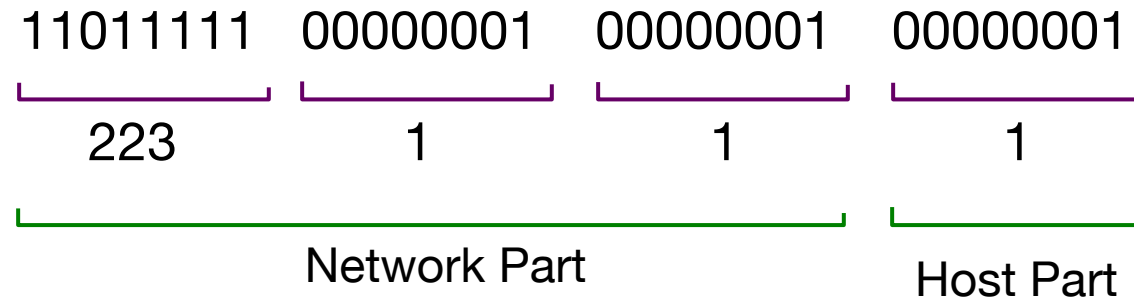
Network Consisting of 3 IP  
subnets

# IP Addressing

A router usually has multiple interfaces. A host usually has one interface but in some cases, it can have multiple interfaces.

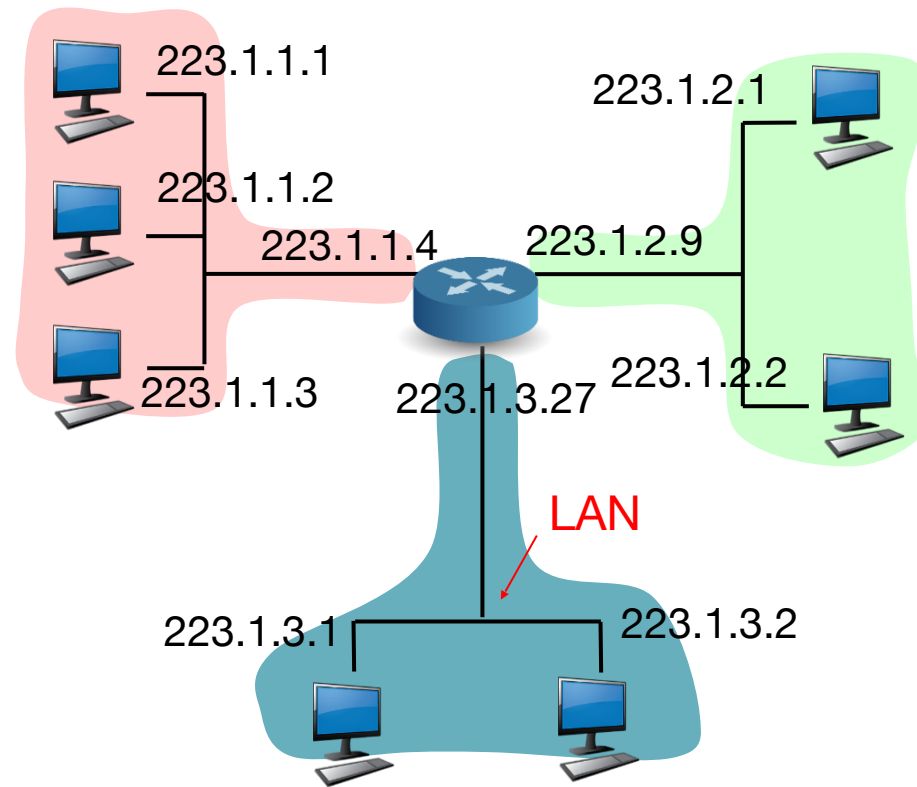
IP address consists of 2 parts:

- Network part or prefix (high order bits)
- Host part or suffix (low order bits)



# IP Addressing

Let's see what an IP subnet is from an IP address perspective. All interfaces in an IP subnet have the same network part of IP address. It can physically reach each other without an intervening the router.



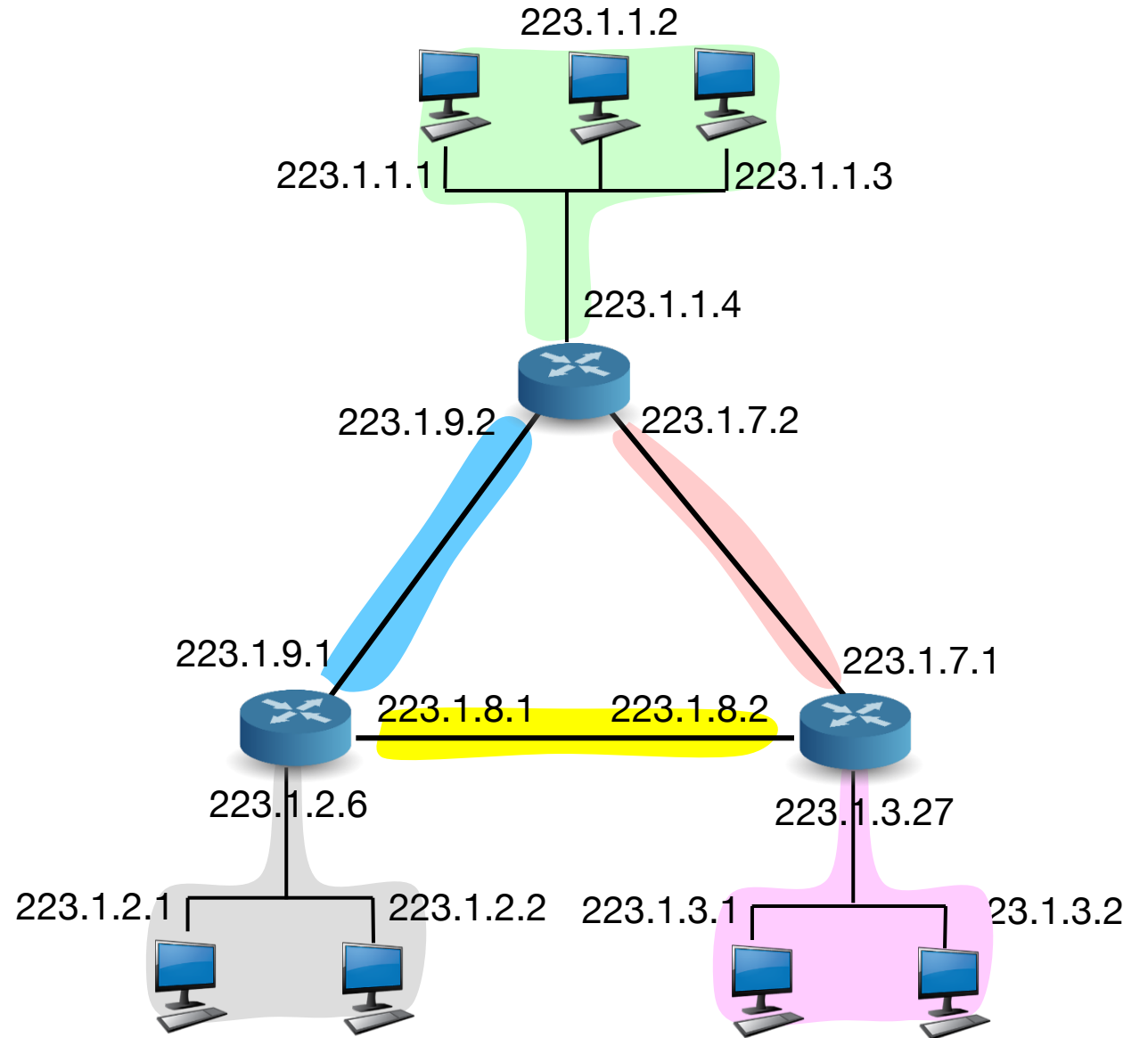
Network Consisting of 3 IP subnets

# IP Addressing

How many IP networks are there?

1. Remove the routers
2. Create islands of isolated networks

6 IP networks





## Notes: IP Addressing

- An IPv4 address is 32 bits (4 bytes) long, and theoretically there are  $2^{32}$  (or approximately 4 billion) possible IP addresses. These addresses are typically written in so-called dotted-decimal notation.
- In the given example, one router is used to interconnect 7 hosts. Note that hosts that are connected to the same router interface has the same network part; e.g., 223.1.1 for the hosts that are connected to the router interface with the IP address of 223.1.1.4. In IP terms, the hosts 223.1.1.1, 223.1.1.2, 223.1.1.3 and the router interface with IP address 223.1.1.4 belong to the same IP subnet.
- To determine the subnets, we can remove all the routers to create islands of isolated networks. Each of these isolated networks is a subnet.

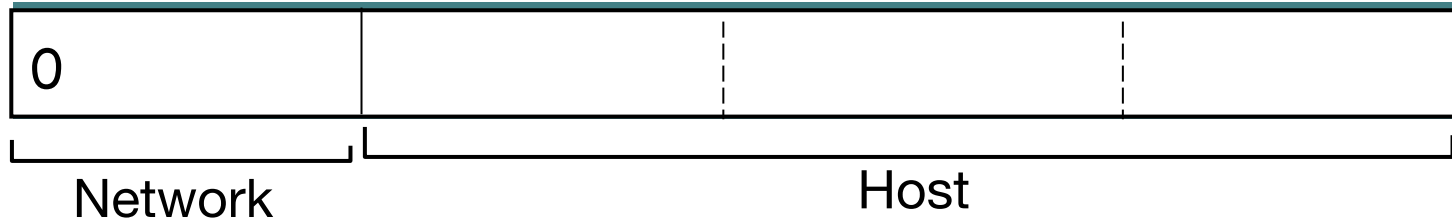
The background features a light gray gradient with decorative elements. Two horizontal teal lines, one above and one below the text, span the width of the slide. On the left side, there are several overlapping teal arcs of varying radii and opacities, creating a dynamic, abstract pattern.

# Classful IP Addressing

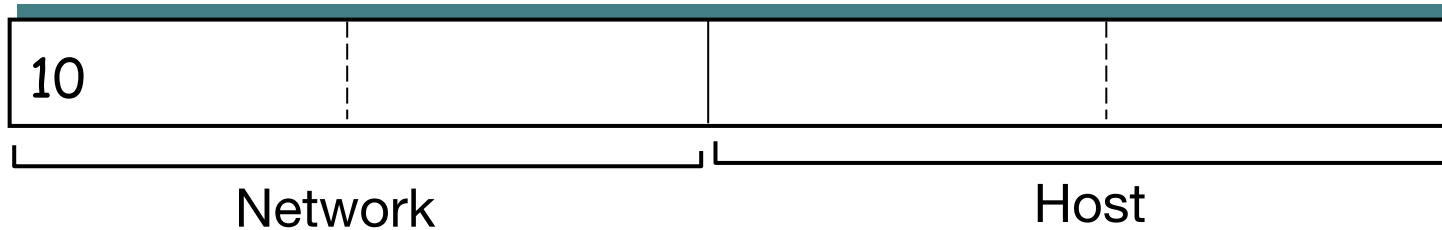
# Classful IP Addressing

Five classes of IP addresses in classful addressing are:

Class A: 0.0.0.0 to 127.255.255.255

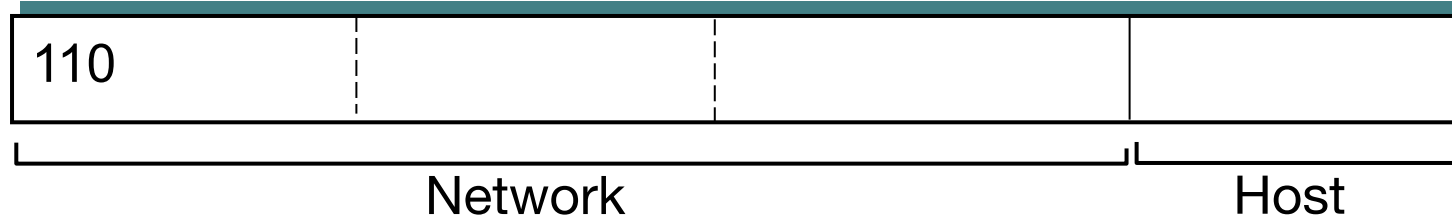


Class B: 128.0.0.0 to 191.255.255.255

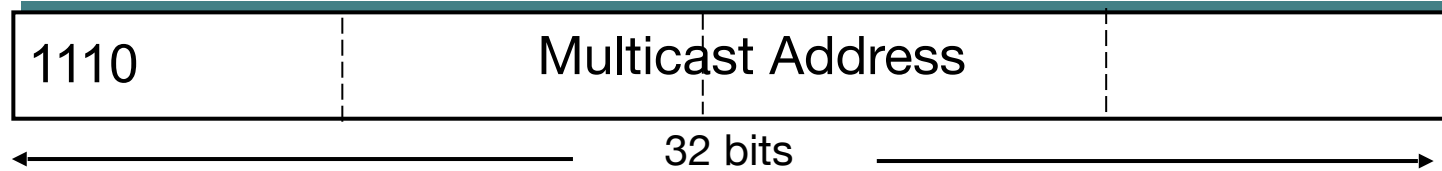


# Classful IP Addressing

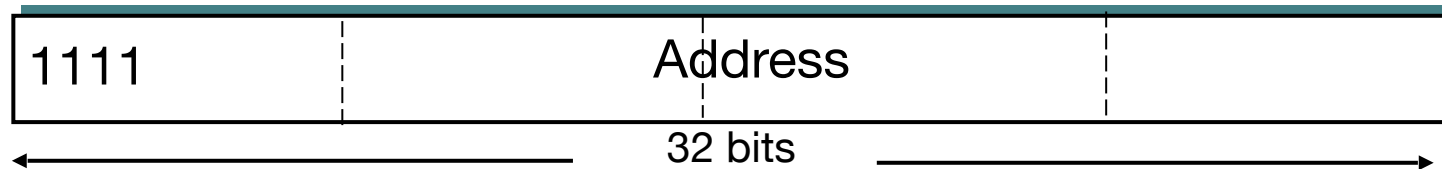
Class C: 192.0.0.0 to 223.255.255.255



Class D: 224.0.0.0 to 239.255.255.255



Class E: 240.0.0.0 to 255.255.255.255



No separation of network and host part for Class D and E.

# Classful IP Addressing

Class	Binary Values of 1 <sup>st</sup> Octet	Decimal Values
A	<b>0000</b> 0000 - <b>0111</b> 1111	0 - 127
B	<b>1000</b> 0000 - <b>1011</b> 1111	128 - 191
C	<b>1100</b> 0000 - <b>1101</b> 1111	192 - 223
D	<b>1110</b> 0000 - <b>1110</b> 1111	224 - 239
E	<b>1111</b> 0000 - <b>1111</b> 1111	240 - 255

Class E is reserved for future use or research.

From the value of the first 4 bits and the first decimal number in the dotted-decimal notation, we could identify the classful address class.

# Classful IP Addressing

Major drawback of classful addressing:

## Inefficient use of address space

- A class B network is allocated enough addresses for 65,534 ( $=2^{16}-2$ ) hosts – too large for many organisations.

## Address space exhaustion

- A class C network is allocated addresses for only 254 ( $=2^8 - 2$ ) hosts – too small for many organisations.

There are only 16,384 ( $=2^{14}$ ) class B addresses for the whole world.

# Notes: Classful IP Addressing

- When the IP addressing scheme was first designed, the network portions of an IP address were constrained to 8 (Class A), 16 (Class B) and 24 bits (Class C) in length. This is known as Classful Addressing.
- In Classful addressing, a Class A network is identified by its most significant bit being 0, a Class B network is identified by its most significant two bits being 10, while a Class C network is identified by its most significant three bits being 110.
- Class D, which is reserved for multicasting, has its most significant four bits equal to 1110.
- Class E, which is reserved for R&D purpose and future, has its most significant four bits equal to 1111.
- Note that as the first few bits of Class A, B, C, D and E networks are fixed, the range of IP addresses are fixed.
- Note that there is no notion of network part and host part for Class D and Class E IP addresses.

## Notes: Classful IP Addressing

---

- Note also that when the host part consists of  $n$  bits, the theoretical number of IP addresses are  $2^n$ ; however, the usable IP addresses are only  $2^n - 2$  because host part is all zeros refer to the network per se and host part of all ones is the broadcast address for that subnet.
- Classful addressing is rather inefficient and due to IP address shortages, classful IP addressing is replaced by Classless Interdomain Routing (CIDR – pronounced as cider).



## Exercise: Question

Identify the classful IP address classes to which the following IP addresses belong to and then find the network addresses, where applicable:

- a) 136.23.45.122
- b) 202.11.54.43
- c) 67.125.4.200
- d) 233.54.97.210

- a) 136.23.45.122

136 = 10001000 in binary. As the first two bits are '10', this IP address belongs to a Class B network. The class B network is 136.23.0.0.



## Exercise: Answer

b) 202.11.54.43

202 = 11001010 in binary. As the first three bits are '110', this IP address belongs to a Class C network. The class C network is 202.11.54.0.

c) 67.125.4.200

67 = 01000011 in binary. As the first bit is '0', this IP address belongs to a Class A network. The class A network is 67.0.0.0.

d) 233.54.97.210

233 = 11101001 in binary. As the four bits are '1110', this IP address is a Class D IP address. For a Class D network, there is no notion of network address.



The background features a light gray gradient with decorative elements. Two horizontal teal lines, one above and one below the text, span the width of the slide. On the left side, there are several overlapping teal arcs of varying radii and opacities, creating a dynamic, abstract pattern. On the right side, a single large teal arc is visible, also overlapping the horizontal lines.

# Special IP Addresses

# Special IP Addresses

Special IP addresses are reserved for specific purposes and never assigned to host/router interfaces. Some examples are:

Network Addresses	(Directed) Broadcast Addresses	(Limited) Broadcast Address
<ul style="list-style-type: none"><li>• IP addresses with host bits all zeros</li><li>• Denote the prefix of given networks</li><li>• For example, 128.211.0.0/16 denotes the network with prefix 128.211</li><li>• Refers to the network itself and not any interface in the network</li></ul>	<ul style="list-style-type: none"><li>• IP addresses with host bits all ones</li><li>• For sending a copy of datagram to all hosts in an IP network/subnet</li><li>• For example, 199.31.0.255/24 is the broadcast address for network 199.31.0.0/24</li></ul>	<ul style="list-style-type: none"><li>• 255.255.255.255</li><li>• For broadcast on a local physical network during system startup by a computer which does not yet know the network address</li></ul>

# Special IP Addresses

Special IP addresses are reserved for specific purposes and never assigned to host/router interfaces. Some examples are:

## This Computer Address

- 0.0.0.0
- Used as a host's IP address during system startup as the host is yet to know its IP address

## Loopback Address

- 127/8; next 24 (host) bits are irrelevant
- For example, 127.0.0.1 is a loopback address
- For sending datagrams from one application to another application running on the same host during testing

# Special IP Addresses

Prefix	Suffix	Type	Purpose
All 0's	All 0's	This computer	Use during bootstrap
Network	All 0's	Network addresses	Identifying networks
Network	All 1's	Directed broadcast	Broadcast on specific network
All 1's	All 1's	Limited broadcast	Broadcast on local network
127	Any	Loopback	Testing

# New IP Addressing: CIDR

**C**lassless **I**nter**D**omain **R**outing (CIDR) supersedes Classful Addressing. In CIDR, the network portion of an address is of an arbitrary length. The address format is **a.b.c.d/x**, where x is the number of bits in the network portion of the address.

For example, 200.23.16.0/23 represents:



The background features a light gray gradient with decorative teal elements. These include several concentric arcs of varying radii and thicknesses, some of which are semi-transparent, creating a layered effect. Two solid teal horizontal lines run across the width of the image, one positioned above and one below the central text.

# Subnet Addressing (Subnetting)



# Subnet Addressing (Subnetting)

**Subnetting** is the technique used by an organisation (e.g. ISP) to divide its IP address space into several smaller blocks to serve different subnets or clients.

## How?

Several most significant bits in the host part of the IP address are used as the subnet bits.

## Example

If the ISP has an address space, 200.23.16.0/20, how does the ISP divide it into 8 blocks to serve its 8 clients? See the next 2 slides.

# Subnet Addressing (Subnetting)

How does ISP split its IP addresses?

ISP's address space: 200.23.16.0/20

from    11001000 00010111 00010000 00000000  
to      11001000 00010111 00011111 11111111

Client 1's address space: 200.23.16.0/23

from    11001000 00010111 0001**000**0 00000000  
to      11001000 00010111 0001**000**1 11111111

Client 2's address space: 200.23.18.0/23

from    11001000 00010111 0001**001**0 00000000  
to      11001000 00010111 0001**001**1 11111111

# Subnet Addressing (Subnetting)

How does ISP split its IP addresses?

Client 3's address space: 200.23.20.0/23

from    11001000 00010111 0001**010**0 00000000  
to      11001000 00010111 0001**010**1 11111111  
:  
:

Client 8's address space: 200.23.30.0/23


from    11001000 00010111 0001**111**0 00000000  
to      11001000 00010111 0001**111**1 11111111

ISP allocates a portion of its address space to a client.

# Subnet Mask

A subnet mask is used by an organisation's router to extract the network part of its subnets.

The subnet mask for the previous example must be:

11111111 11111111 11111110 00000000  
  
23 bits

Example: A datagram is to be sent to IP address:

11001000 00010111 00010001 01010101

# Subnet Mask

The ISP router will perform an AND operation between the IP address of the datagram and the subnet mask.

11001000 00010111 00010001 01010101

and

11111111 11111111 11111110 00000000

equal to

11001000 00010111 00010000 00000000



This is the 23-bit network part of client (subnet) 1.

# Subnet Mask

Decimal values of an octet in subnet mask:

$$0000\ 0000 = 0_{10}$$

$$1000\ 0000 = 128_{10} \qquad 1111\ 1000 = 248_{10}$$

$$1100\ 0000 = 192_{10} \qquad 1111\ 1100 = 252_{10}$$

$$1110\ 0000 = 224_{10} \qquad 1111\ 1110 = 254_{10}$$

$$1111\ 0000 = 240_{10} \qquad 1111\ 1111 = 255_{10}$$

For example, the subnet mask:

11111111 11111111 11111110 00000000

is 255.255.254.0 in dotted decimal notation.

# Notes: Classless Interdomain Routing

- CIDR generalises the notion of subnet addressing. As with subnet addressing, the 32-bit IP address is divided into two parts and is commonly expressed in the dotted-decimal form a.b.c.d/x, where x indicates the number of bits in the network part of the address. Note that if there are x bits in the network part, there will be 32-x bits in the host part.
- In order to obtain a block of IP addresses for use within an organisation's subnet, a network administrator must first contact its ISP, which would provide addresses from a larger block of addresses that had already been allocated to the ISP.
- For example, the ISP may itself have been allocated the address block 200.23.16.0/20, and decide to divide this address block into 8 equal-sized contiguous address blocks and give one of these address blocks out to 8 clients. How this can be done has been illustrated in the last few slides.

# Subnet Zero and the All-ones Subnet

## Subnet Zero (All-Zeros Subnet)

- If a network address is subnetted, the first subnet obtained after subnetting the network address is called subnet zero.
- In the previous example, 200.23.16.0/23 is Subnet Zero.
- Using subnet zero for addressing was discouraged because of the confusion inherent in having a network and a subnet with indistinguishable addresses.

## The All-Ones Subnet

- When a network address is subnetted, the last subnet obtained is called the all-ones subnet.
- In the previous example, 200.23.30.0/23 is the All-ones subnet.
- Use of the all-ones subnet for addressing has been discouraged in the past because of the confusion inherent in having a network and a subnet with identical broadcast addresses. For example, the broadcast addresses of 200.23.16.0/20 and 200.23.30.0/23 (the all-ones subnet) are the same, which is 200.23.31.255.



# Subnet Zero and the All-ones Subnet

- Network engineers normally calculate the number of usable subnets as  $2^n - 2$  where  $n$  is the number of bits borrowed for subnetting.
- Even though the use of subnet zero and the all-ones subnet have been discouraged, the entire address space including subnet zero and the all-ones subnet have always been usable.
- In this course, normally you will be explicitly told if you should or should not use Subnet Zero and All-Ones subnet. If you are not told, you are free to make your own assumptions.

## Exercise: Question

If a large enterprise is given a class B address 150.23.0.0, how could you divide it into 16 blocks and assign to its 14 departments?

You may not use Subnet Zero and the All-ones subnets. List down the network addresses for the 14 departments. How many hosts could each department support?

What is the subnet mask for the 14 departments?



## Exercise: Answer

As  $2^4 = 16$ ; 4 bits needs to be borrowed from the host part.

<u>First 4 bits of the 3<sup>rd</sup> Byte</u>	<u>Network Address</u>
0000 All zeros subnet (not used)	150.23.0.0
0001 Department 1	150.23.16.0
0010 Department 2	150.23.32.0
0011 Department 3	150.23.48.0
0100 Department 4	150.23.64.0
0101 Department 5	150.23.80.0
0110 Department 6	150.23.96.0
0111 Department 7	150.23.112.0
1000 Department 8	150.23.128.0
1001 Department 9	150.23.144.0
1010 Department 10	150.23.160.0
1011 Department 11	150.23.176.0
1100 Department 12	150.23.192.0
1101 Department 13	150.23.208.0
1110 Department 14	150.23.224.0
1111 All ones subnet (not used)	150.23.240.0



## Exercise: Answer

As there are 12 bits for the host part; hence, number of usable hosts =  $2^{12} - 2 = 4,094$ .

The subnet mask is:

11111111 11111111 11110000 00000000

**OR**

255.255.240.0



## Exercise: Question

Assume that an enterprise network has been assigned a class C network address 192.31.4.0, and the network administrator decided to use 3 bits for subnetting.

- 1) What is the subnet mask for the sub-networks?
- 2) Assume that Subnet Zero and All-ones Subnets cannot be used, what is the maximum number of subnets allowable in the enterprise network? What is the maximum number of hosts allowable in each subnet?
- 3) In the enterprise network, a router has an Ethernet interface with IP address 192.31.4.33. What is the subnet address? What is the IP address range for hosts in this subnet?



## Exercise: Answer

- 1) The subnet mask for subnets is:

11111111.11111111.11111111.11100000 or 255.255.255.224

- 2) The maximum number of subnets is  $2^3 - 2 = 6$ . The maximum number of hosts (including the connecting port of the router) allowable in each subnet is  $2^5 - 2 = 30$ .

- 3)
- |                                  |               |
|----------------------------------|---------------|
| 33 →                             | 00100001      |
| 4 <sup>th</sup> byte of the Mask | 11100000      |
|                                  | -----         |
| Result                           | 00100000 → 32 |

Hence, interface address 192.31.4.33 must be a member of the subnet 192.31.4.32.

IP addresses: 00100001 → 00111110  
(33)                      (62)

As IP address 192.31.4.33 has been assigned to the router interface, the remaining IP addresses that can be assigned to hosts range from 192.31.4.34 to 192.31.4.62.

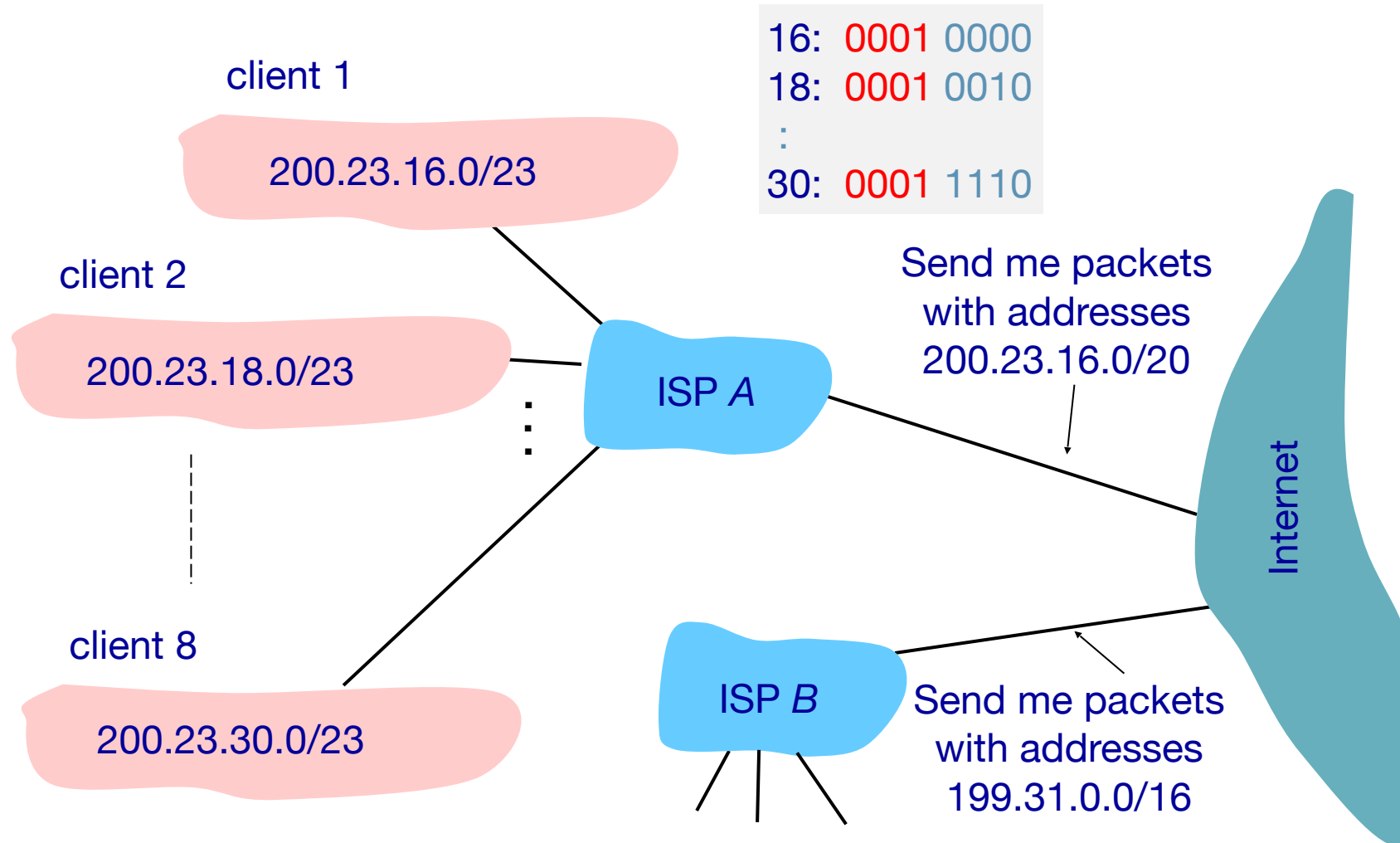


The background features a light gray gradient with decorative elements in various shades of teal. These include several concentric arcs of different radii and thicknesses, as well as a solid horizontal teal band that spans the width of the image, passing behind the central text.

# Route Aggregation/Summarisation

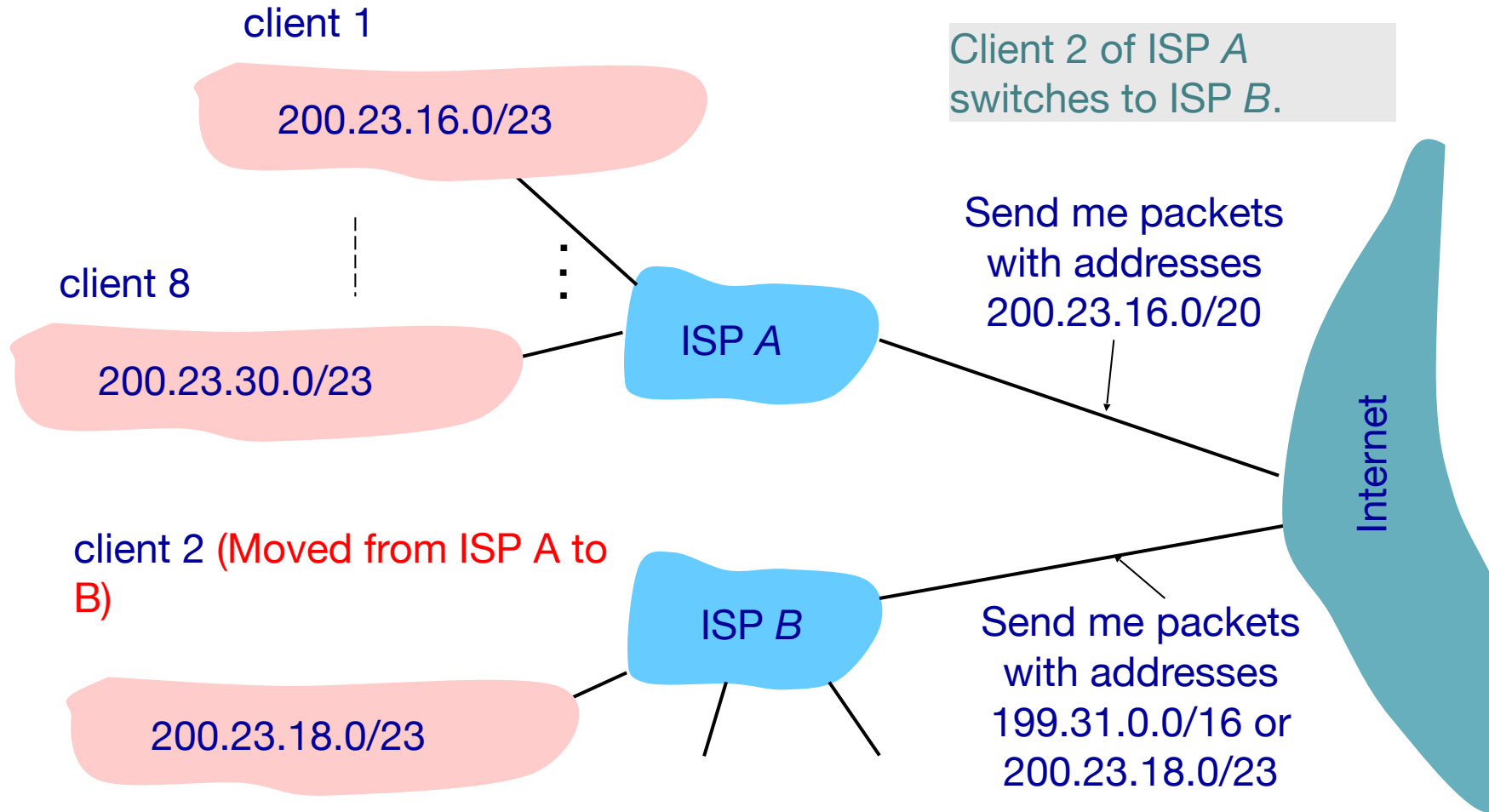
# Route Aggregation/Summarisation

Allows efficient advertisement of routing information.





# Route Aggregation/Summarisation



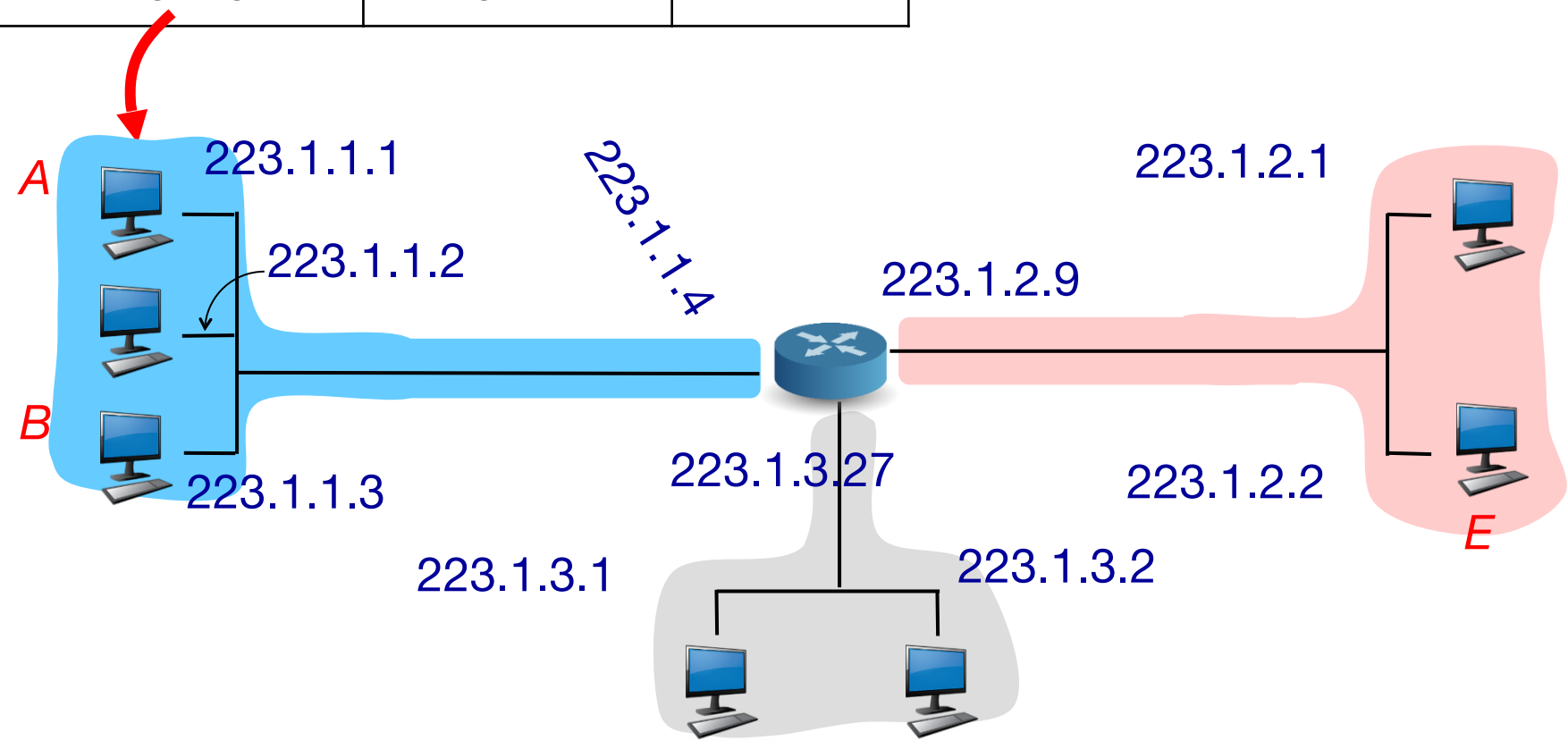
**Longest prefix matching rule** is used when the network address of an IP packet has more than one matches in the routing table.

## Notes: Route Aggregation/Summarisation

- In this example, ISP A sub-allocated the block of addresses 200.23.16.0/20 to 8 clients. When it advertises these network addresses to the rest of the world, it can choose to do route aggregation, which is also known as route summarisation. Route aggregation will cut down on the number of routes advertised from 8 to one in this case. In addition, the routers in the Internet do not have to maintain 8 separate entries but just one single entry. This is much more efficient.
- Assume that Client 2 subsequently decided to change the ISP from A to B and is allowed to carry over the block of IP addresses. Note that ISP A could still advertise the aggregate route 200.23.16.0/20 while ISP will advertise the route 200.23.18.0/23. Note also that 200.23.18.0/23 is part of 200.23.16.0/20. These two routes will appear in the routing tables of some routers. When an IP packet is received by a router and if the destination IP address matches more than one routes, the router will choose the route with the longest prefix match.

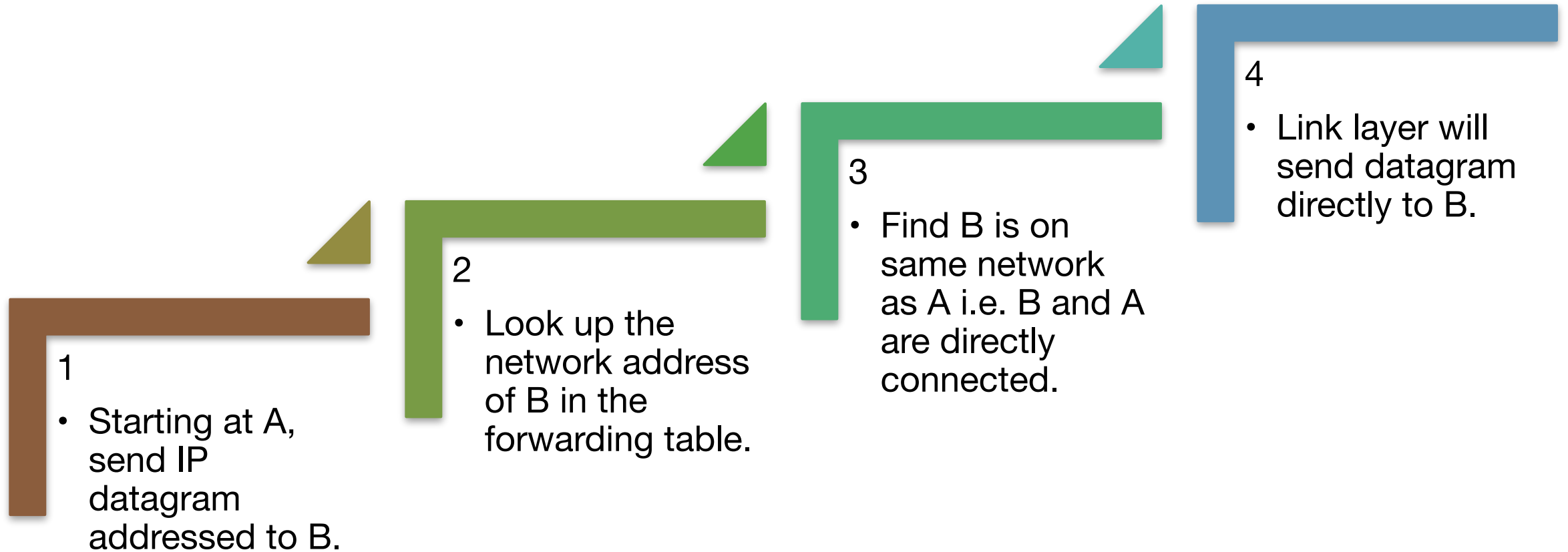
# Forwarding Table in a Host

Destination Net.	Next Router	Nhops
223.1.1		1
223.1.2	223.1.1.4	2
223.1.3	223.1.1.4	2



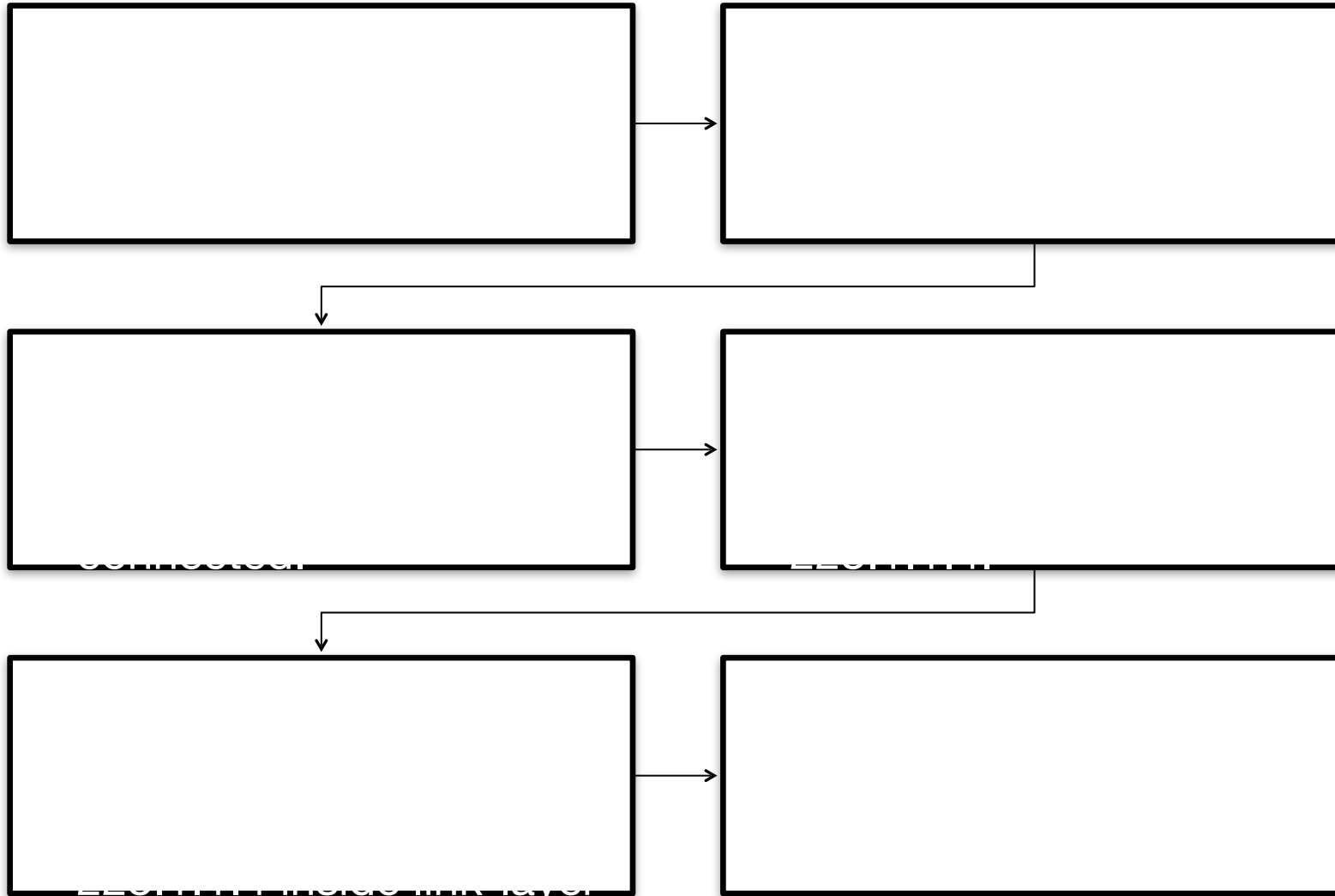
# Forwarding Table in a Host

Routing a datagram from source to destination in the same IP network:



# Forwarding Table in a Host

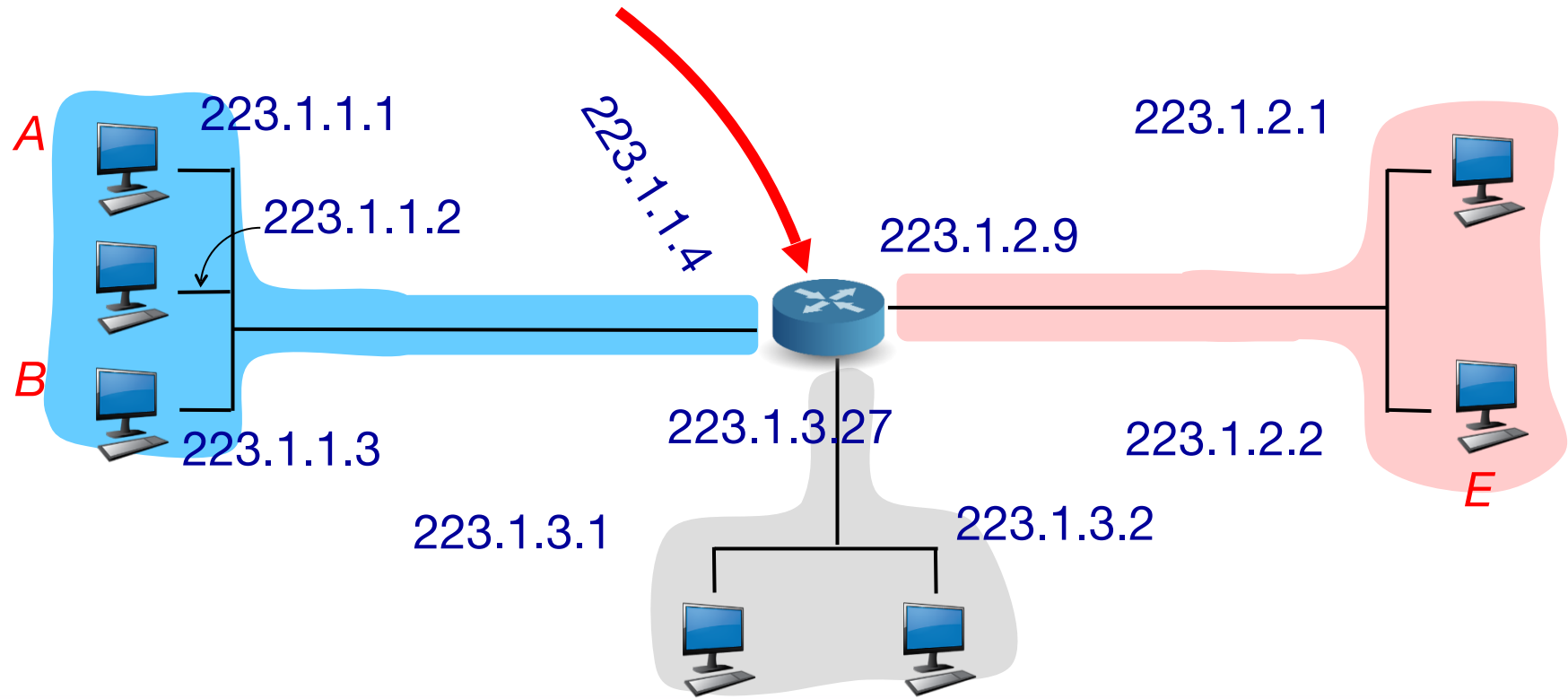
Routing a datagram from source to destination in different IP networks:



frame.

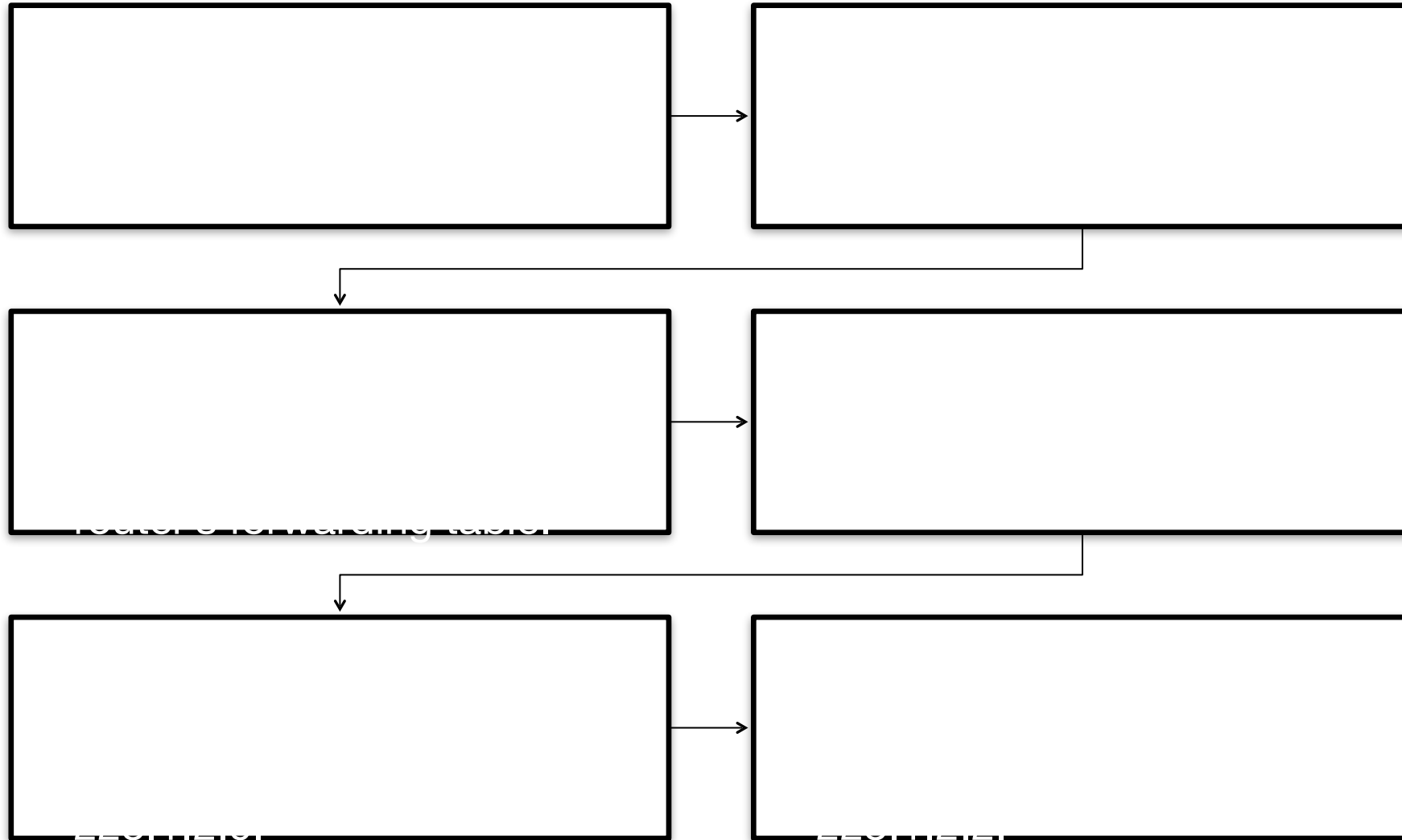
# Forwarding Table in a Router

Destination Net.	Next Router	Nhops	Interface
223.1.1	-	1	223.1.1.4
223.1.2	-	1	223.1.2.9
223.1.3	-	1	223.1.3.27



# Forwarding Table in a Router

Routing a datagram from source to destination in different IP networks:



The background features a light gray gradient with several decorative elements: two horizontal teal lines, one above and one below the text, and several overlapping teal arcs of varying radii and opacities that create a sense of motion or layers.

# Dynamic Host Configuration Protocol (DHCP)



# Dynamic Host Configuration Protocol (DHCP)

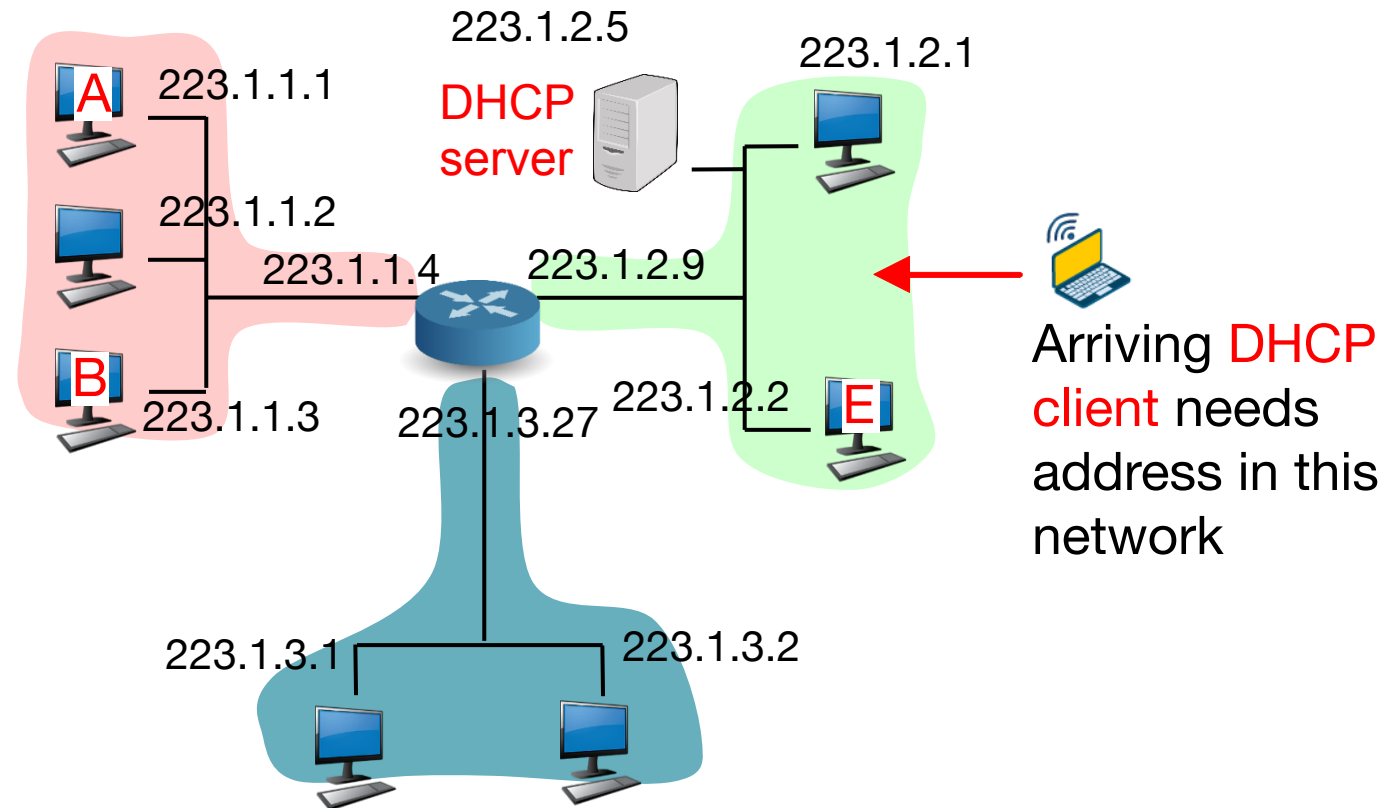
## DHCP Goals

- 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; i.e. “on”)
- Support for mobile users who want to join network (more shortly)

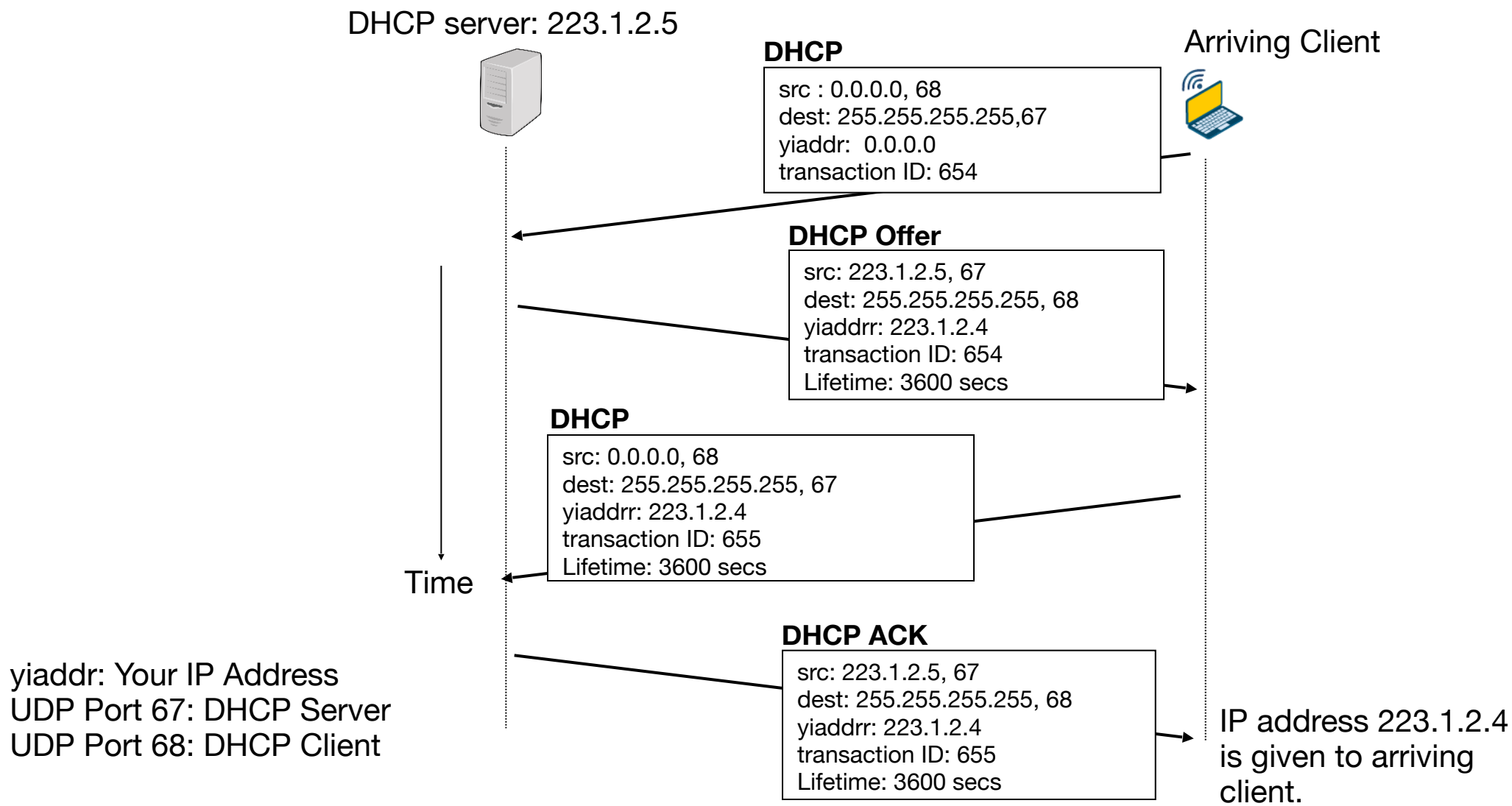
## DHCP Overview

- Host broadcasts “DHCP discover” message
- DHCP server responds with “DHCP offer” message
- Host requests IP address: “DHCP request” message
- DHCP server sends address: “DHCP ack” message

# DHCP Client-Server Scenario



# DHCP Client-Server Scenario



# Notes: DHCP

- Though host addresses can be configured manually, it is not very productive; in most organisations, this is done using DHCP, which allows a host to obtain an IP address automatically.
- In addition to host IP address assignment, DHCP also allows a host to learn additional information, such as its subnet mask, the address of its first-hop router (often called the default gateway), and the address of its local Domain Name System (DNS) server.
- In the simplest case, each subnet will have a DHCP server. For a newly arriving host, the DHCP is a four-step process, as illustrated on the previous slide. The four steps are:

DHCP server discovery:  
This is done using a DHCP discover message, which a client sends within a UDP packet to port 67.

1

The UDP packet is encapsulated in an IP datagram with the broadcast destination address of 255.255.255.255 and a “this host” source IP address of 0.0.0.0.

2

The DHCP client passes the IP datagram to the link layer.

3

The link layer then broadcasts this frame to all nodes attached to the subnet.

4

## Notes: DHCP

- DHCP Server Offer(s): A DHCP server receiving a DHCP discover message responds to the client with a DHCP offer message that is broadcast to all nodes on the subnet, again using the IP broadcast address of 255.255.255.255. Each server offer message contains the transaction ID of the received discover message, the proposed IP address for the client, the network mask, and an IP address lease time – the amount of time for which the IP address will be valid.
- DHCP request: The newly arriving client will choose from among one or more server offers and respond to its selected offer with a DHCP request message, echoing back the configuration parameters.
- DHCP ACK: The server responds to the DHCP request message with a DHCP ACK message, confirming the requested parameters.
- Once the client receives the DHCP ACK, the interaction is complete and the client can use the DHCP-allocated IP address for the lease duration. Note that DHCP also provides a mechanism that allows a client to renew its lease.

The background features a light teal color with several overlapping, curved bands of a slightly darker shade of teal. A solid horizontal line of the same darker teal color runs across the middle of the image, passing behind the text.

# Summary

# Summary

---

Key points discussed in this topic:

- Network layer is present in every host and router. It is responsible for host-to-host communications. It does so by transporting segments receiving from the Transport Layer of a host as IP packets to another host across the network.
- A datagram is a basic transfer unit associated with a packet-switched network. Datagrams are typically structured in header and payload sections.
- When an IP datagram is received by a router and its size is bigger than the MTU of the outgoing link, the IP datagram will need to be fragmented into two or more smaller IP datagrams. These IP datagram fragments will only be reassembled at the destination host.
- The Binary Numbering System is the most fundamental numbering system in all digital and computer based systems and binary numbers follow the same set of rules as the decimal numbering system. But unlike the decimal system which uses powers of ten, the binary numbering system works on powers of two.

# Summary

---

Key points discussed in this topic (cont'd):

- An Interface is the connection point between host/router and physical link. An IP address is a 32-bit identifier for an interface that is written in dotted-decimal notation. An IP address consists of 2 parts; Network part or prefix (high order bits) and Host part or suffix (low order bits).
- When the IP addressing scheme was first designed, the network portions of an IP address were constrained to 8 (Class A), 16 (Class B) and 24 bits (Class C) in length. This is known as Classful Addressing.
- Special IP addresses are reserved for specific purposes and never assigned to host/router interfaces.
- Subnetting is the technique used by an organisation (e.g. ISP) to divide its IP address space into several smaller blocks to serve its subnets (e.g. clients).



# Summary

---

Key points discussed in this topic (cont'd):

- **C**lassless **I**nter**D**omain **R**outing (CIDR) supersedes Classful Addressing. In CIDR, the network portion of an address is of an arbitrary length. The address format is **a.b.c.d/x**, where x is the number of bits in the network portion of the address.
- Route aggregation or summarisation cuts down the number of routes advertised. In addition, the routers in the Internet do not have to maintain separate entries but just one single entry.
- DHCP allows a host to obtain an IP address automatically. In addition to host IP address assignment, DHCP also allows a host to learn additional information, such as its subnet mask, the address of its first-hop router (often called the default gateway), and the address of its local DNS.