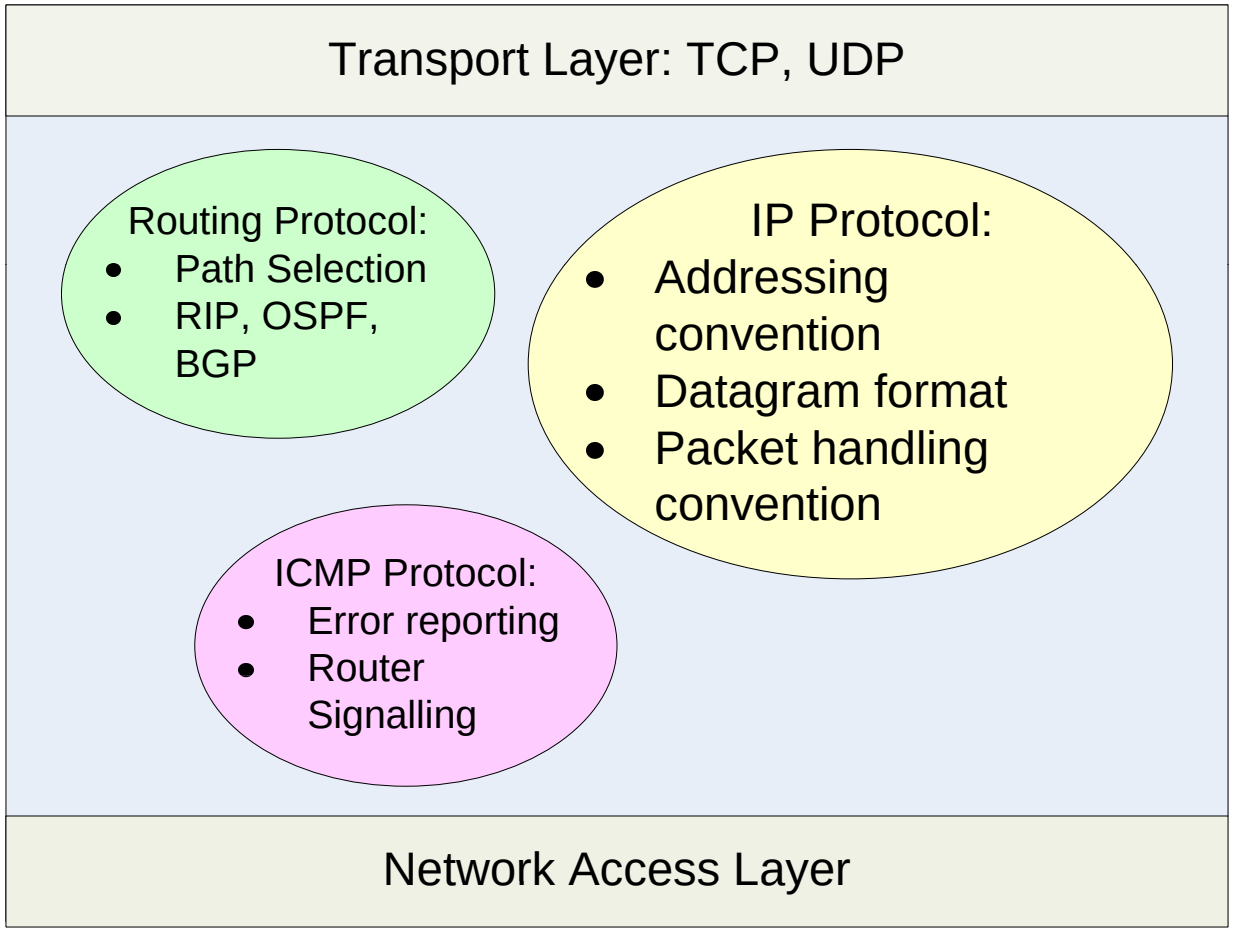
Pertemuan-4.
Internet Layer Protokol

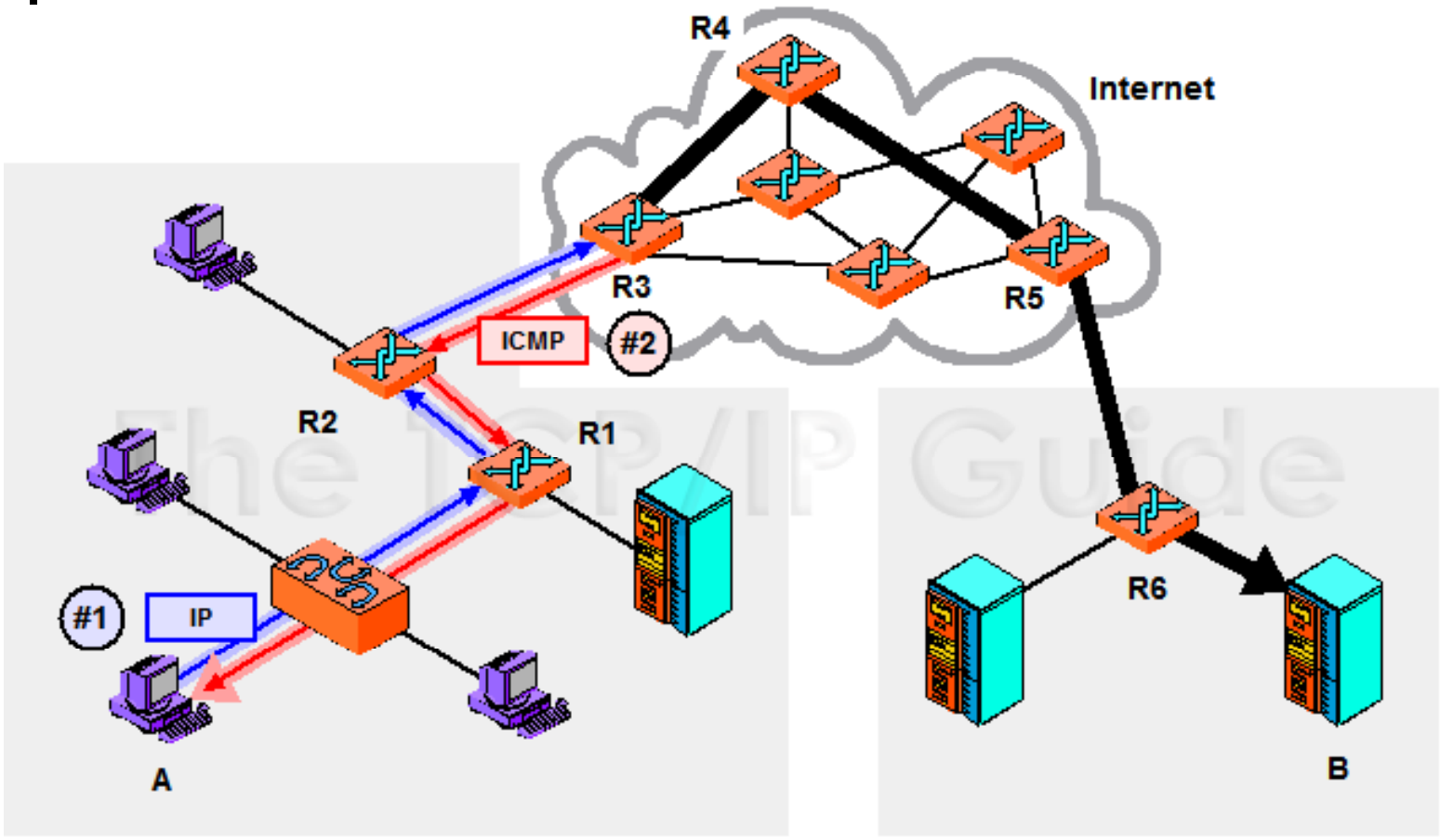
Komponen Internet Layer



ICMP

- ICMP →Internet Control Message Protocol (RFC 792).
- ICMP digunakan oleh host, router, gateway untuk mengirimkan pesan-pesan kesalahan.
- Tugas ICMP adalah mendukung sepenuhnya tugas-tugas protokol IP.
- ICMP tidak menggunakan nomor port seperti pad TCP dan UDP.

Ilustrasi ICMP



Source: www.tcpipguide.com

Ilustrasi ICMP

Pada contoh di atas dapat dilihat bahwa:

- ICMP dapat melintasi *internetwork*.
- Misalkan host A akan mengirim pesan ke host B melalui protokol IP, tetapi masalah terdeteksi pada Router 3. Selanjutnya Router 3 akan mengirim pesan ICMP balik ke host A sebagai informasi kesalahan (bukan ke Router 2 atau Router 1).

ICMP: Two classes

ICMP dapat digolongkan dalam 2 kelas:

- Pesan kesalahan

  Digunakan sebagai umpan balik kepada divais pengirim apabila terjadi kesalahan (error).

- Pesan informasi

  Digunakan oleh divais-divais untuk bertukar informasi, melakukan pengujian.

ICMP Error Messages

Message Class	Type Value	Message Name	Summary Description of Message Type	Defining RFC Number
ICMPv4 Error Messages	**3**	***Destination Unreachable***	Indicates that a datagram could not be delivered to its destination. The *Code* value provides more information on the nature of the error.	792
	4	***Source Quench***	Lets a congested IP device tell a device that is sending it datagrams to slow down the rate at which it is sending them.	792
	5	***Redirect***	Allows a router to inform a host of a better route to use for sending datagrams.	792

ICMP Error Messages (Cont.)

Message Class	Type Value	Message Name	Summary Description of Message Type	Defining RFC Number
	11	***Time Exceeded***	Sent when a datagram has been discarded prior to delivery due to expiration of its *Time To Live* field.	792
	12	***Parameter Problem***	Indicates a miscellaneous problem (specified by the *Code* value) in delivering a datagram.	792

ICMP Informational Messages

Message Class	Type Value	Message Name	Summary Description of Message Type	Defining RFC Number
ICMPv4 Informational Messages	**0**	***Echo Reply***	Sent in reply to an *Echo (Request)* message; used for testing connectivity.	792
	8	***Echo (Request)***	Sent by a device to test connectivity to another device on the internetwork. The word "Request" sometimes appears in the message name.	792
	9	***Router Advertisement***	Used by routers to tell hosts of their existence and capabilities.	1256
	10	***Router Solicitation***	Used by hosts to prompt any listening routers to send a *Router Advertisement*.	1256

ICMP Informational Messages (Cont.)

Message Class	Type Value	Message Name	Summary Description of Message Type	Defining RFC Number
	13	***Timestamp (Request)***	Sent by a device to request that another send it a timestamp value for propagation time calculation and clock synchronization. The word "Request" sometimes appear in the message name.	792
	14	***Timestamp Reply***	Sent in response to a *Timestamp (Request)* to provide time calculation and clock synchronization information.	792
	15	***Information Request***	Originally used to request configuration information from another device. Now obsolete.	792

Contoh: ICMP

- Program *PING* mengirimkan ICMP type 8 (echo request). Host tujuan akan membalas dengan menggunakan ICMP type 0 (echo reply).
- Program *Traceroute* mengirimkan IP datagram dengan TTL 1, 2, 3 dst. Host tujuan membalas dengan ICMP type 11 (TTL).

ARP

- ARP → Address Resolution Protocol.
- Protokol ini bertugas untuk menemukan hardware address (MAC Address) suatu host dengan alamat IP tertentu.
- Ketika suatu IP paket akan dikirim, maka paket tersebut diteruskan ke layer dibawahnya (Data Link), yang akan memberikan alamat hardware sesuai dengan alamat IP tersebut.

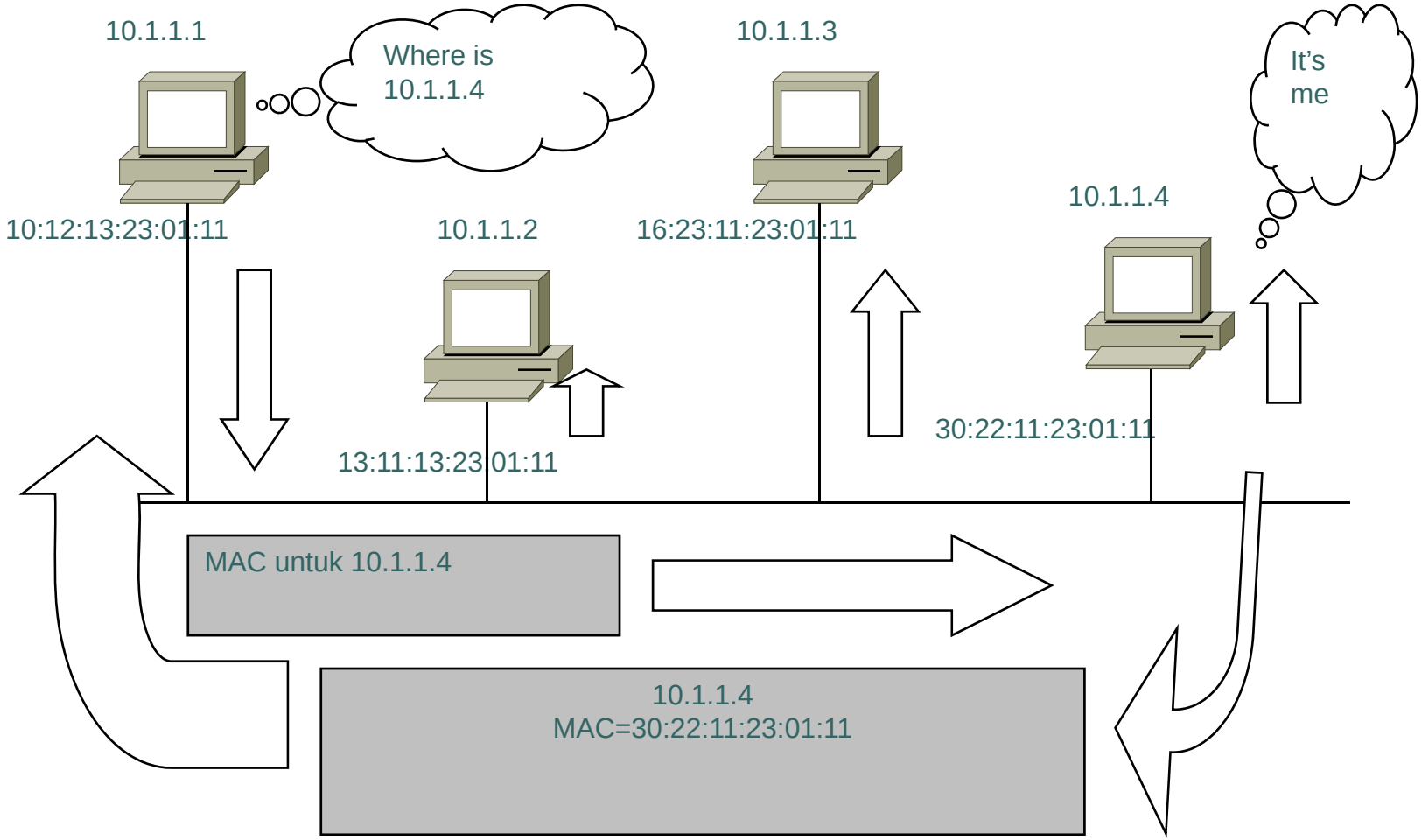
Tabel ARP

- Setiap host menyimpan Tabel ARP dalam cache.
- Tetapi jika hardware address ini tidak ada di dalam cache ARP, maka ARP bertugas untuk mencarinya (Tabel ARP terupdate setiap 15-20mn).

Contoh: Tabel ARP

```
C:\arp -a
Interface: 172.25.82.74 --- 0x2
Internet Address      Physical Address      Type
172.25.82.51          00-90-27-54-3a-47     static
172.25.82.247         00-60-08-3e-1d-2f     dynamic
172.25.82.248         00-60-08-3e-ba-61     dynamic
172.25.82.254         00-a0-c9-fb-33-6e     dynamic
```

Cara Kerja ARP



Cara Kerja ARP

- Teriminal dengan IP 10.1.1.1 (sumber) ingin mengirimkan pesan ke terminal dengan IP 10.1.1.4 (tujuan).
- Terminal sumber mengirim ARP-request secara broadcast.
- Tetapi hanya Terminal tujuan yang dimaksud mengambil ARP-request.
- Teminal tujuan mengirim balik ARP-reply beserta no MAC-address.

Apa yang terjadi jika nomor IP tujuan berada pada network yang berbeda ?

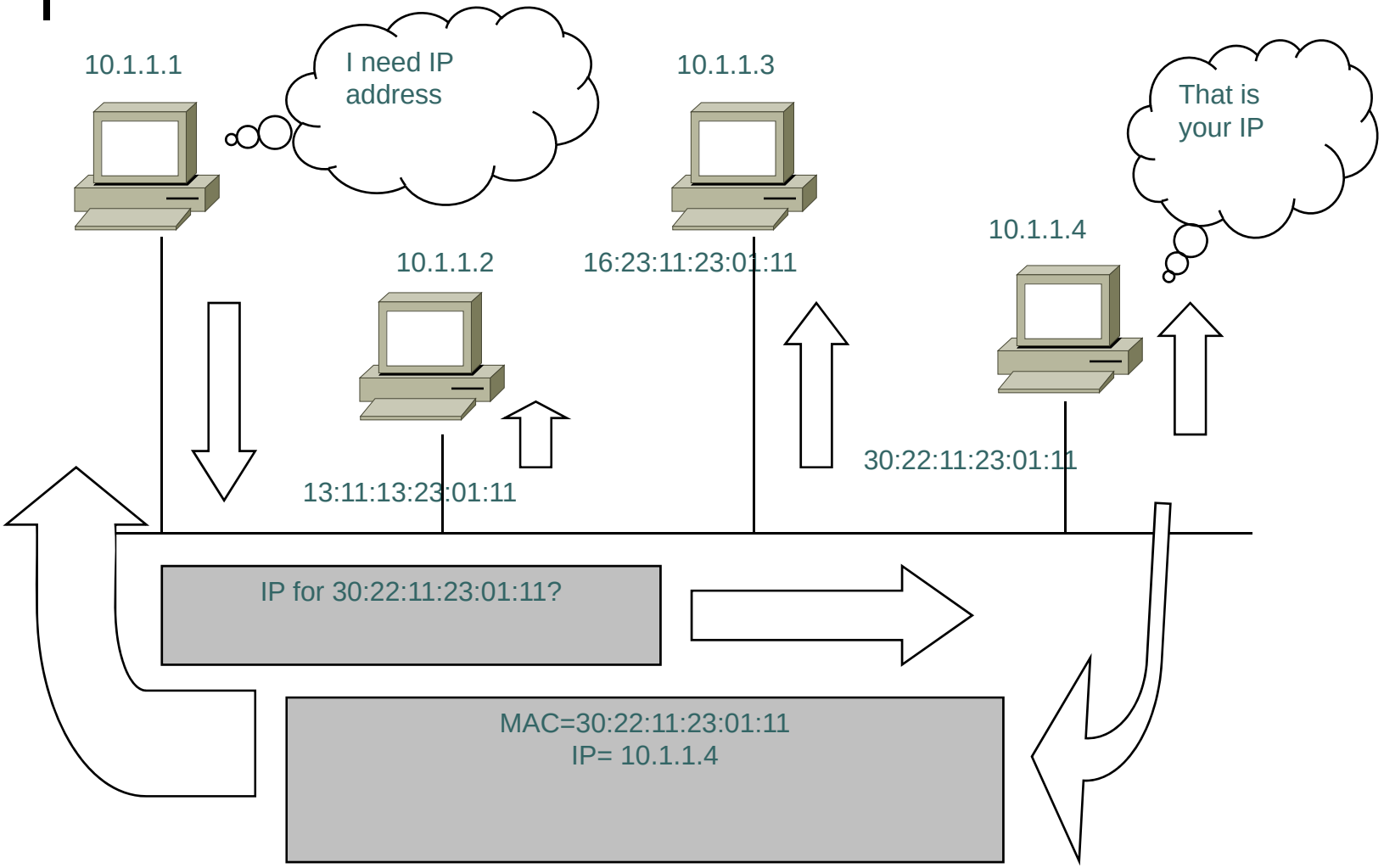
RARP

- RARP →Reverse Address Resolution Protocol
- Merupakan protokol yang bertugas untuk menemukan IP address suatu host yang hanya tahu Hardware address-nya saja (misal pada diskless machine).

Cara Kerja RARP

- Host mengirim paket berikut alamat MAC-nya secara broadcast untuk meminta alamat IP yang sesuai.
- RARP server akan menjawab paket tersebut dengan memberikan nomor IP.
- Contoh: BootP protocol dan Dynamic Host Control Protocol (DHCP).

Cara Kerja RARP

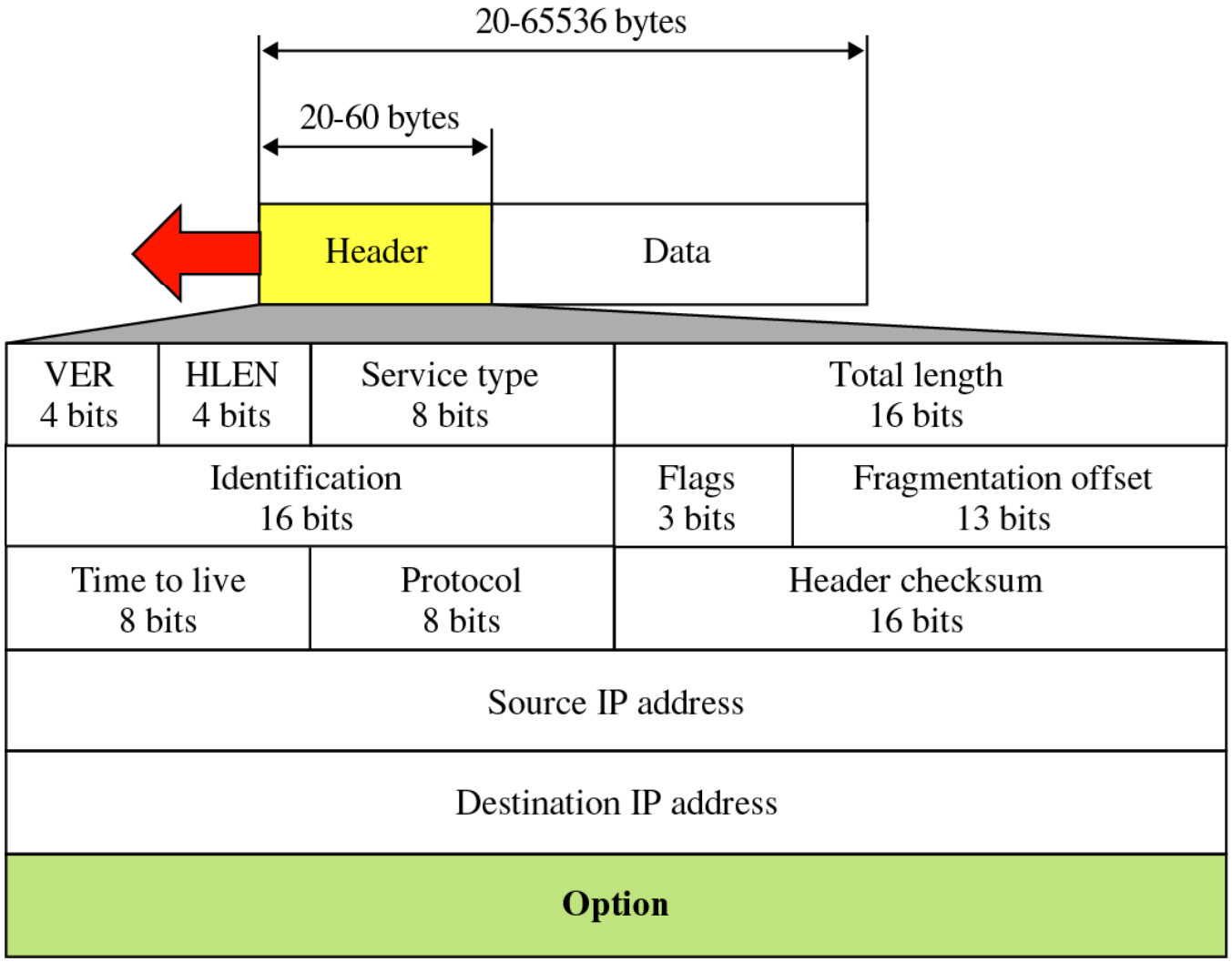


Internet Protocol (IP)

Datagram

- Packet pesan pada Internet Layer disebut juga sebagai *Datagram*.
- IP Datagram mengandung alamat IP sumber dan alamat IP tujuan, masing-masing sebesar 32 bit (i.e., IP Address).
- IP Datagram bergerak melintasi network switching dari satu node (router) ke node berikutnya berdasarkan pemilihan jalur tertentu.

Format Datagram



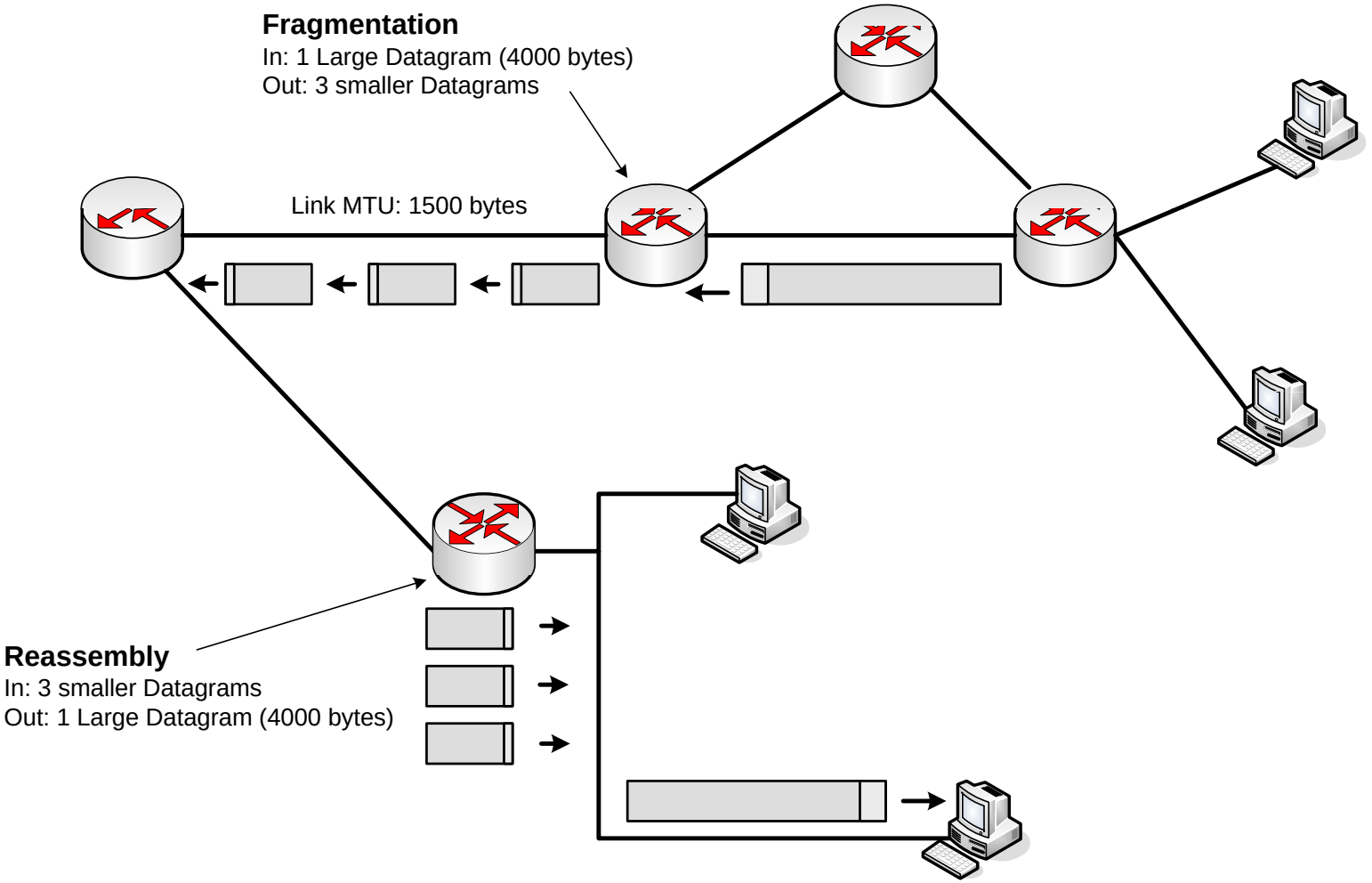
Fragmentasi IP Datagram

- Peralatan memiliki Maximum Transfer Unit (MTU), sehingga packet data yang dilewatkan pada setiap router akan dipotong2 sesuai dengan ukuran MTU.
- Packet data yang terpotong-potong ini disebut sebagai *fragment*.

IP Datagram Reassembly

- Karena adanya proses fragmentasi, maka pada sisi penerima dibutuhkan juga adanya proses *reassembly*.
- Proses reassembly menggunakan field: *identification, flag dan fragmentation* pada IP datagram.

Ilustrasi: Fragmentation and Reassembly



Contoh:

- Sebuah Datagram memiliki ukuran 4000 bytes (lihat Gambar).
- Karena Link MTU hanya 1500 bytes, maka Datagram harus dipotong2 menjadi 3 buah fragment.
- Pada sisi penerima fragment2 tersebut akan dilakukan proses Reassembly menjadi sebuah Datagram.

IP Address

- Dalam jaringan TCP/IP setiap Host ditandai dengan sebuah alamat IP (IP address) logikal yang unik.
- Sebuah IP address pada IPv4 terdiri atas 32 bit angka biner. Sehingga, secara teoritis total IP address yang dapat dibuat adalah: 2^{32}, atau sebanyak 4.294.296 alamat IP.

IP Address (Cont.)

- IP Address terbagi dalam 4 blok, dimana masing-masing blok terdiri atas 8 bit.
- Penulisan IP address dalam bentuk dotted decimal adalah:

  X.X.X.X

- Contoh: 202.155.19.57
- Karena sebuah blok terdiri atas 8 bit, secara desimal nilai X = 0 – 255.

Konversi Biner Desimal

- Biner :

  01110101 10010101 00011101 11101010

- Dotted Decimal : **128.11.3.31**

- Notasi Hexa :

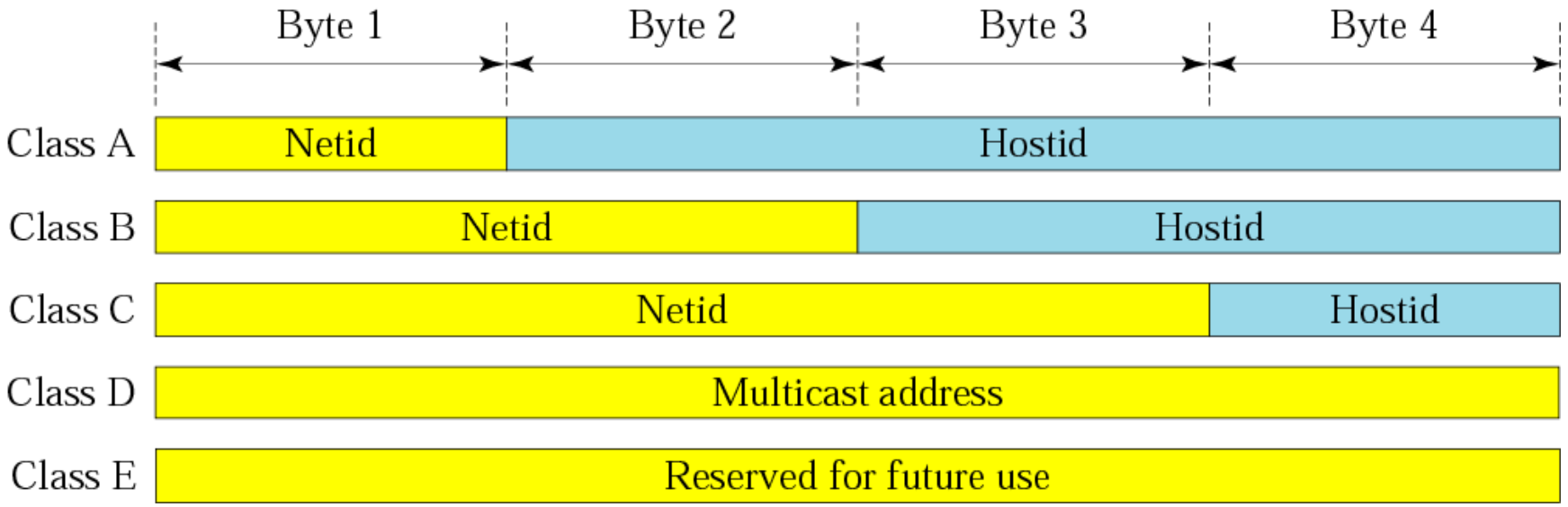
  11000001 10000011 00011011 11111111

  C1 83 1B FF

IP Class

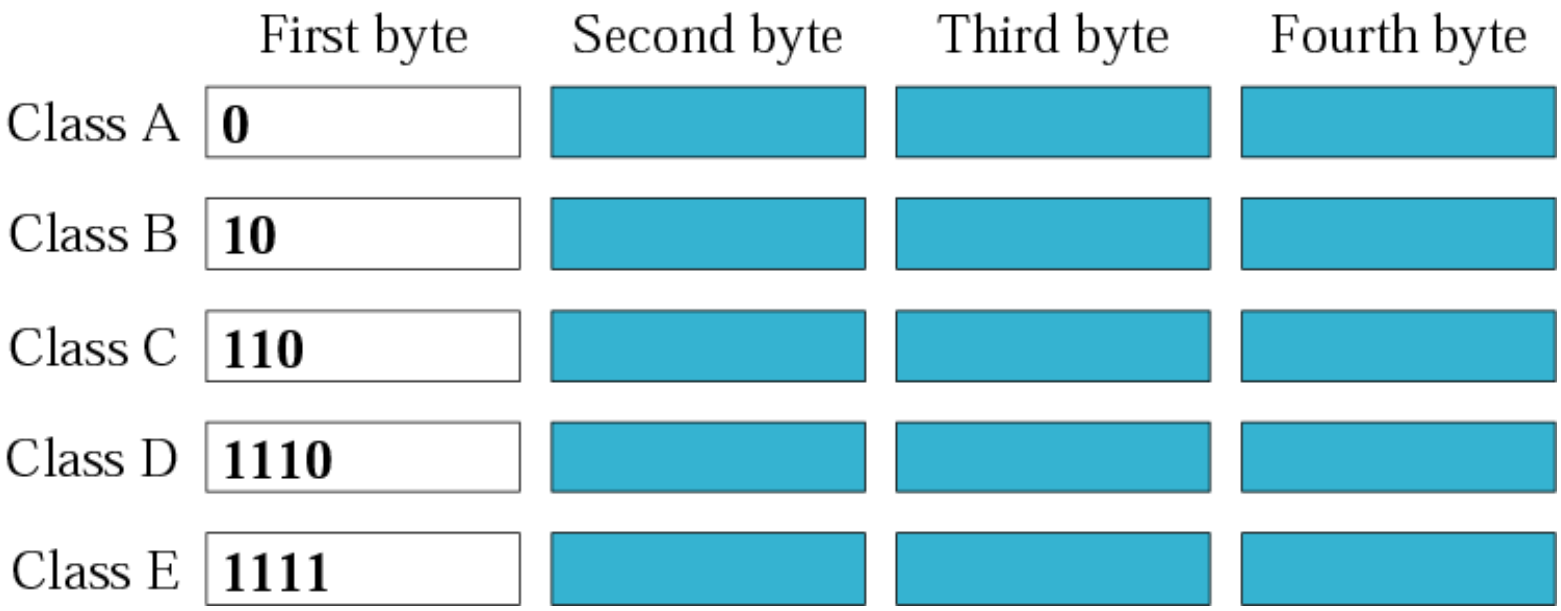
- IP Address terbagi atas 5 kelas (A, B, C, D, E).
- IP address kelas A, B, C digunakan untuk pengalamatan IP publik.
- IP address kelas D, digunakan untuk pengalamatan multicast.
- IP address kelas E, dicadangkan untuk pemakaian masa depan.

Ilustrasi: IP Class (1)

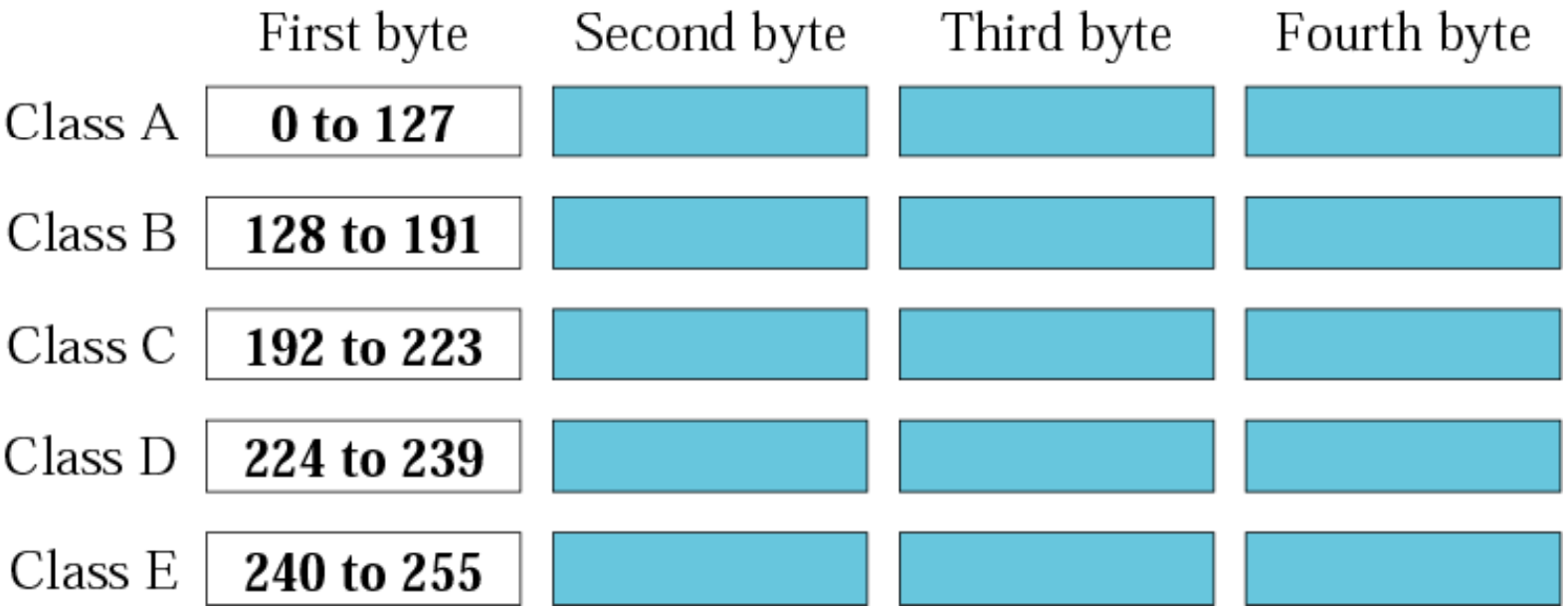


- IP kelas A, B dan C terdiri atas 2 bagian, yaitu *NetId* (identitas sebuah network) dan *HostId* (identitas sebuah host).

Ilustrasi: IP Class (2)



Ilustrasi: IP Class (3)



Class A

- Bit pertama : 0
- Network Address (network-id): 1.0.0.0 s.d 126.0.0.0
- Jumlah alamat jaringan yang mungkin digunakan : 127 alamat (1-126 dapat digunakan sedangkan 127 digunakan untuk reserve)
- Jumlah alamat host yang dapat digunakan : 16.777.216

Class B

- Bit pertama : 10
- Network address (netowork-id): 128.0.0.0 s.d 191.255.0.0
- Jumlah alamat jaringan : 16.384
- Jumlah alamat host : 65.536

Class C

- Bit pertama : 110
- Network address (network-id) : 192.0.0.0 s.d 223.255.255.0
- Jumlah alamat jaringan : 2.097.152
- Jumlah alamat host : 254

Host Address

- Setiap device atau interface harus memiliki host number.
- Total alamat host dalam sebuah network adalah: $2^N - 2$ (Dimana N adalah jumlah bit).
- Pengurangan 2 disini dikarenakan dalam satu alamat jaringan selalu terdapat *network address* dan *broadcast address*.

Netmasking

- Untuk memisahkan antara network-id dan host-id diperlukan sebuah *netmask*.
- Network-id menggunakan mask binary 1, sedangkan host-id menggunakan mask binary 0.
- Network-id dan Host-Id dibedakan dengan cara melakukan operasi **AND** antara IP address dan Netmask.

Netmasking (Cont.)

- Operasi **AND**:

0 **AND** 0 = 0, 0 **AND** 1 = 0,

1 **AND** 0 = 0, 1 **AND** 1 = 1.

- natural netmask:

Kelas A : 11111111.00000000.00000000.00000000
= 255.0.0.0

Kelas B : 11111111.11111111.00000000.00000000
= 255.255.0.0

Kelas C : 11111111.11111111.11111111.00000000
= 255.255.255.0

Contoh

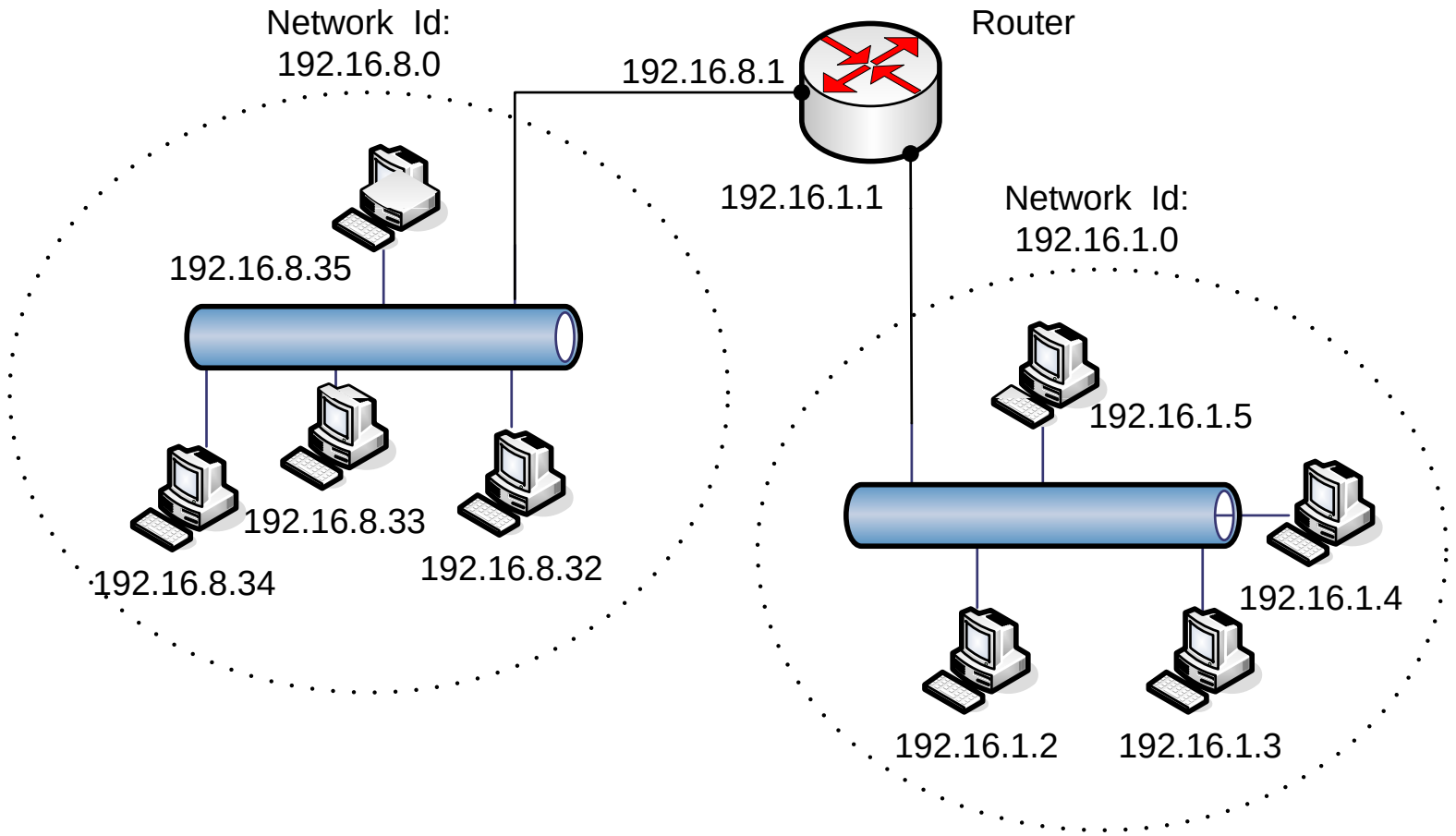
- IP Address : 172.25.88.9 : 10101100.00011001.01011000.00001001
- Netmask : 255.255.255.0 : 11111111.11111111.11111111.00000000

Maka :

- Network-ID : 10101100.00011001.01011000.00000000

  172.25.88.0

Ilustrasi



NetMask : 255.255.255.0

CIDR

- CIDR → Classless Inter-domain Routing. RFC 1591.
- Dengan CIDR, network-prefix pada alamat IP tidak harus 8, 16, dan 24 bit seperti pada kelas A, B, dan C.
- Dengan CIDR, network prefix dituliskan dalam bentuk:

  X.X.X.X/n

  Dimana n adalah jumlah bit pada netmask.

Contoh Notasi CIDR

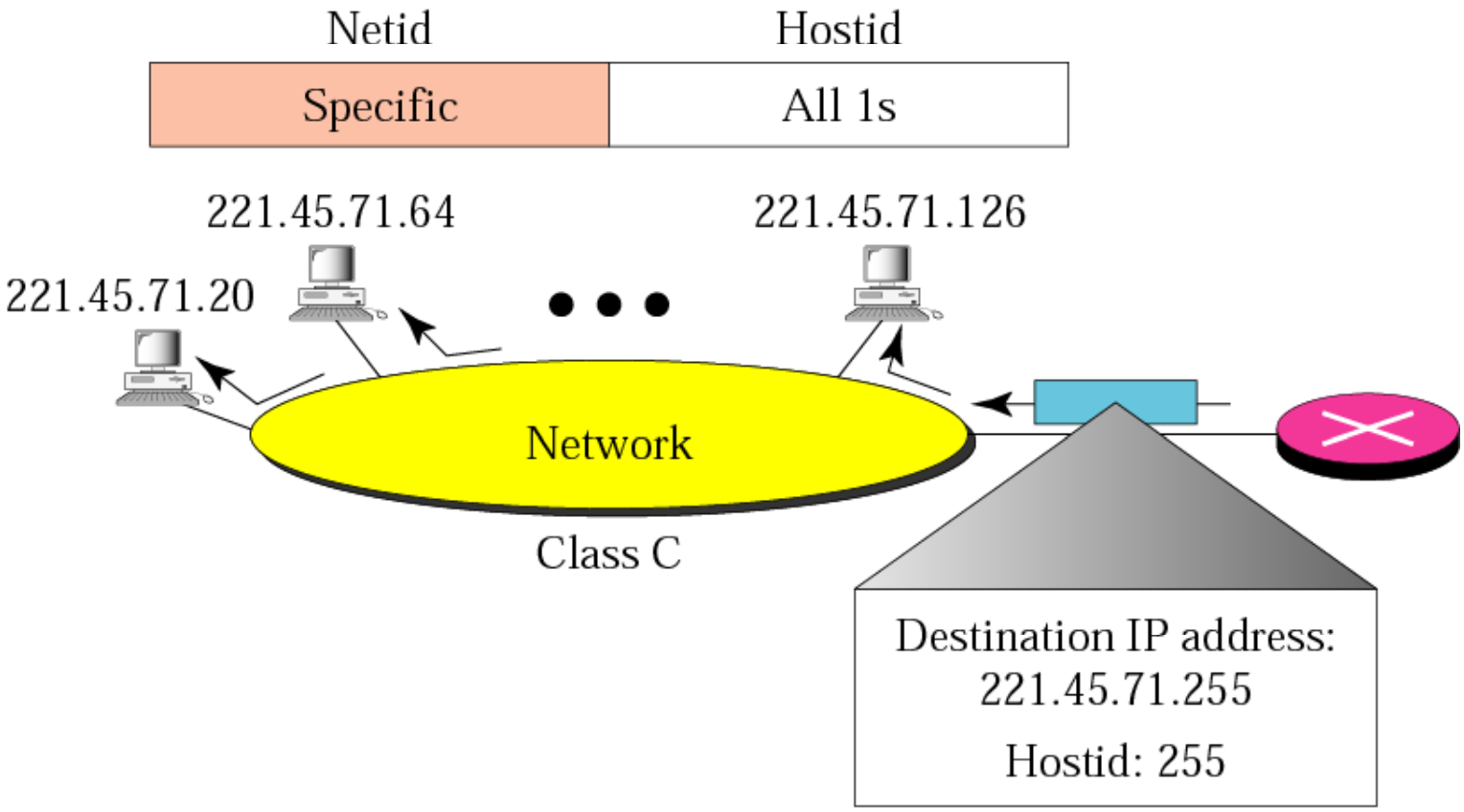
- IP Address : 172.25.88.9 : 10101100.00011001.01011000.00001001
- Netmask : 255.255.255.224 : 11111111.11111111.11111111.11100000
- Notasi CIDR:

172.25.88.9/27

Alamat Khusus: Direct Broadcast Address

- *Direct Broadcast Address* digunakan oleh router untuk mengirimkan pesan ke semua terminal yang berada pada jaringan local.
- *Direct Broadcast address* dilakukan dengan membuat bit pada host-id bernilai 1 semua.
- Misalnya, mengirimkan pesan menuju ke alamat 221.45.71.1, 220.45.71.2 s.d 221.45.71.254, cukup diarahkan ke alamat 221.45.71.255.

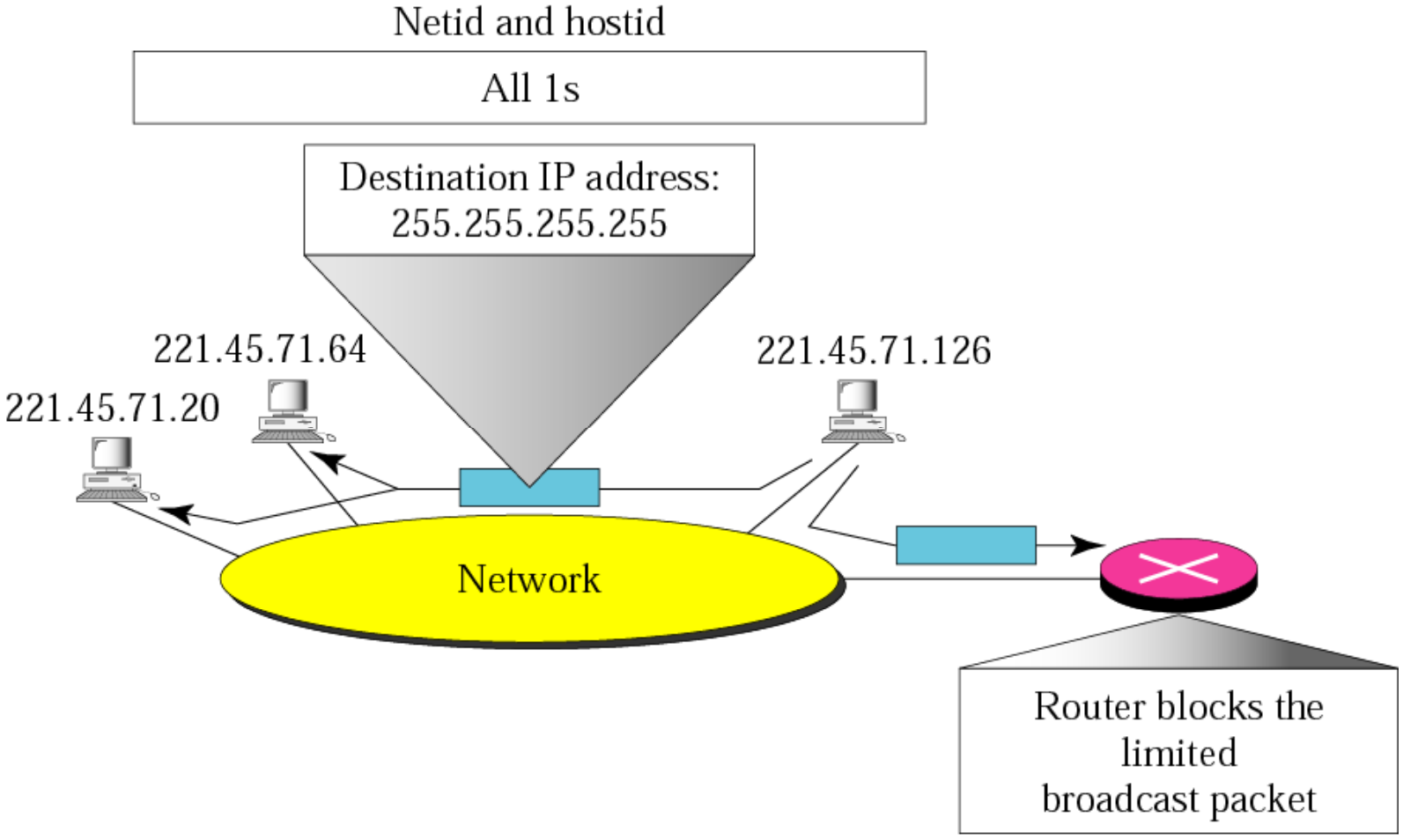
Ilustrasi Direct Broadcast Address



Alamat Khusus: Local Broadcast Address

- *Local Broadcast Address* adalah alamat broadcast untuk network yang aktif saat ini. Packet akan dikirimkan ke setiap host pada network tersebut.
- Router melakukan blocking sedemikian sehingga broadcast ini hanya akan terkirim ke semua host pada network bersangkutan.
- Local Broadcast Address: 255.255.255.255

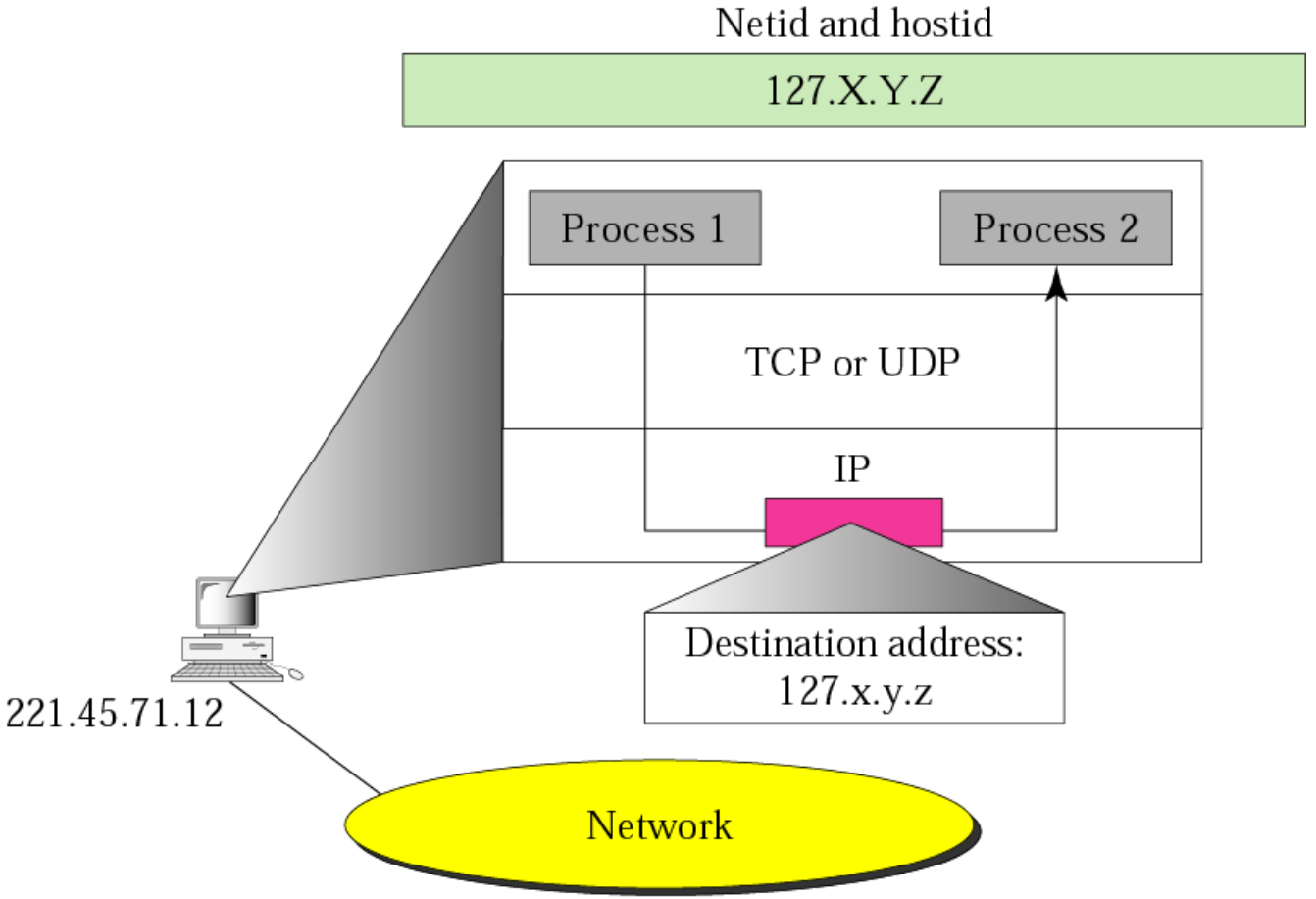
Ilustrasi Local Broadcast Address



Alamat Khusus: LoopBack Address

- IP address dengan alamat IP byte pertama adalah 127, kemudian 3 byte yang lain diisi sembarang adalah alamat loopback.
- Sehingga alamat IP 127.x.x.x tidak dapat digunakan untuk mengalamati host dalam jaringan.
- Contoh: 127.0.0.1

Ilustrasi LoopBack Address



A packet with a loopback address
will not reach the network.

Alamat Khusus: Private IP Address

- International Assigned Numbers Authority (IANA) mengelompokkan alamat IP-Address yang dinyatakan “Private” adalah kelompok IP yang hanya untuk digunakan di kalangan sendiri dan tidak berlaku di Internet.

Class A : 10.0.0.0 – 10.255.255.255 (1 network)

Class B : 172.16.0.0 – 172.31.255.255 (16 network)

Class C : 192.168.0.0 – 192.168.255.255 (256 network)

Multicast

- *Multicast* adalah proses pengiriman packet dari sebuah terminal ke beberapa (sekelompok) terminal (bandingkan dengan broadcast).
- Sekelompok terminal ini disebut sebagai *group management*, yang mana setiap terminal bersifat dinamis (dapat bergabung atau meninggalkan group dengan mudah).
- Administrasi group management diatur oleh IGMP (Internet Group Management Protocol)

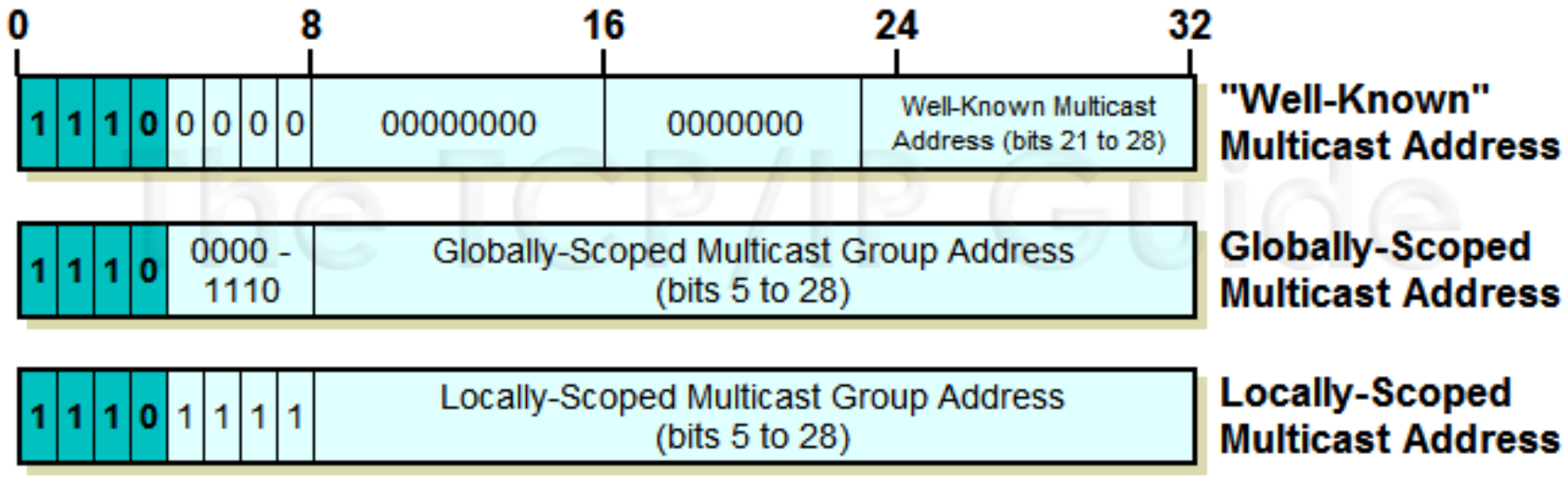
Multicast Addressing

- Multicast menggunakan alamat Kelas D yang dapat diidentifikasi dengan 4 bit pertama ‘1110’.
- Multicast address memiliki range:

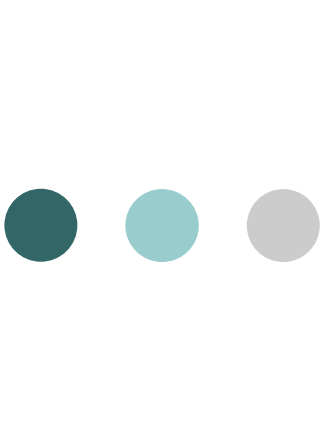
  224.0.0.0 - 239.255.255.255

- ***Pengalamatan ini menunjuk pada pengalamatan sebuah group terminal (bukan sebuah terminal).***

Multicast Addressing



Source: www.tcpipguide.com



The End