



Jaringan Komputer (KP041)

edisi kerjasama
dengan Univ
Kalabahi

Pertemuan 7



2

Review

- Pada pertemuan sebelumnya telah dibahas:
 - Data link Protocols
 - Media Access Control
 - Ethernet
- Pada pertemuan ini akan dibahas:
 - Network layer
 - Karakteristik IPv4



Network layer protocols

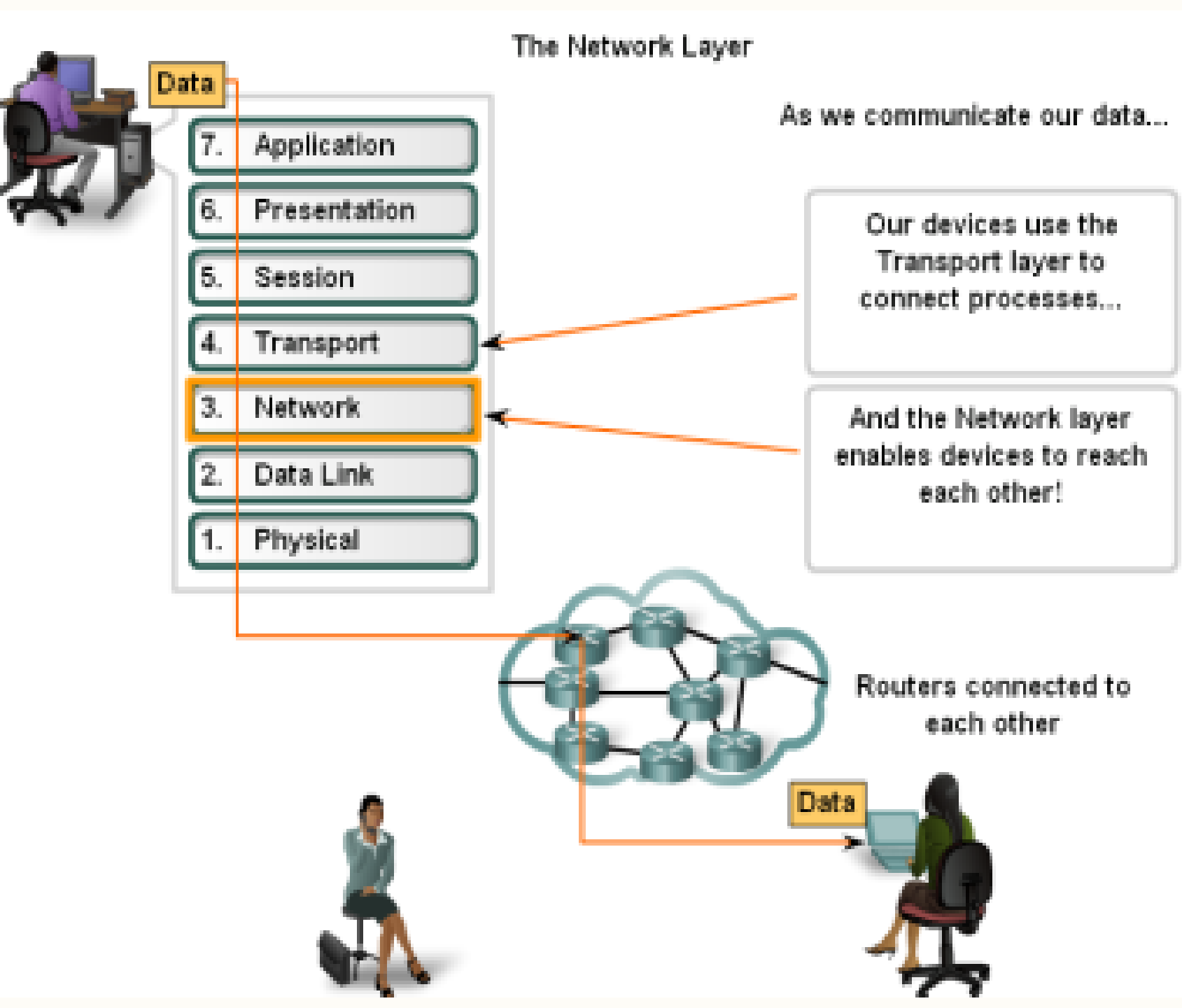


4

Tujuan pembelajaran

1. Mengidentifikasi peran layer network
2. Menganalisa protokol layer network paling umum, yaitu Internet Protocol (IP) dan fiturnya dalam menyediakan layanan connectionless dan best-effort
3. Memahami kelebihan IPv6 terhadap IPv4
4. Memahami dasar rute, next-hop address dan packet forwarding pada host devices dan router





Network layer

- Network layer ada diantara transport layer dan data link layer.

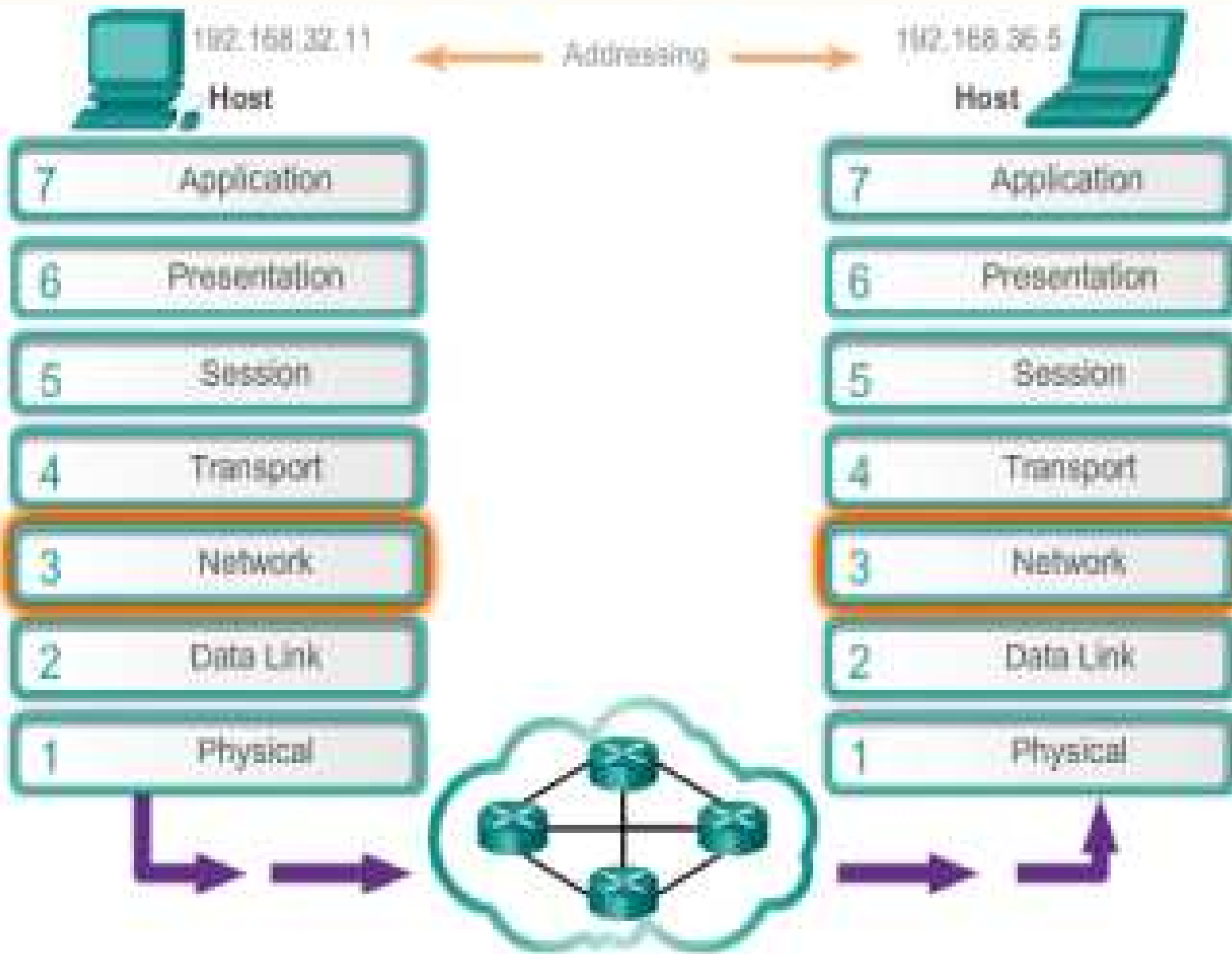


6

Network Layer

- Network layer menyediakan layanan untuk pertukaran data individual pada perangkat yang dikenali dalam jaringan. Untuk mencapai ini ada 4 proses dasar:
 1. Addressing
 2. Encapsulation
 3. Routing
 4. Decapsulation





7

Network Layer

Putar video disamping yang akan mengingatkan ulang proses enkapsulasi dan dekapsulasi

pertemuan06_ver01_NetLayer.mp4



8

Network layer – proses dasar

1. Addressing

Network layer harus menyediakan mekanisme pengalamatan end devices. Jika potongan data individual akan dikirim ke sebuah end device, maka perangkat itu harus memiliki alamat unik.

Pada jaringan IPv4, sebuah perangkat end device yang telah memiliki alamat disebut **host**

2. Encapsulation

Pada enkapsulasi layer 3, segment (PDU layer 4) akan ditambahkan header sehingga menjadi paket (PDU layer 3).

Isi header berupa alamat sumber (source address) dan tujuan (destination address).



9

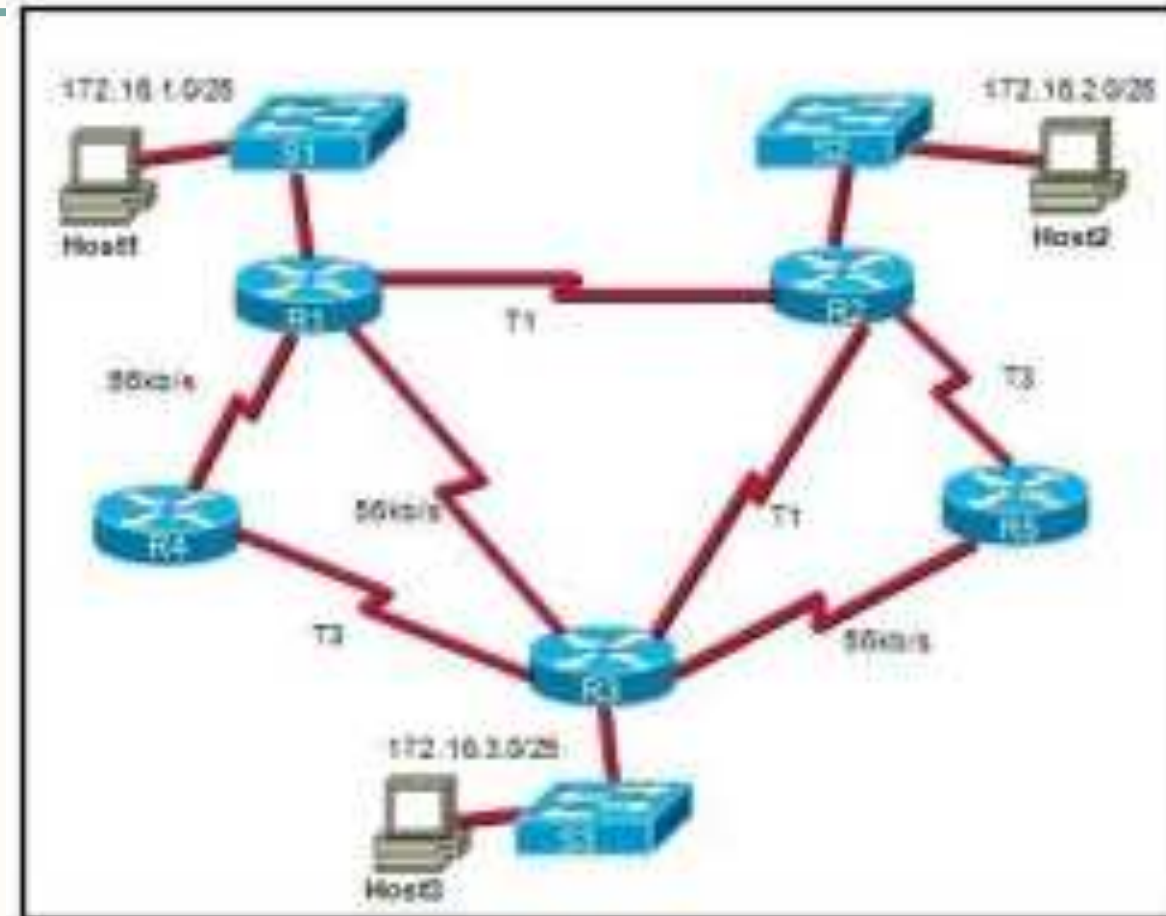
Network layer – proses dasar

3. Routing

Network layer harus menyediakan layanan untuk mengarahkan paket menuju destination host.

source and destination hosts tidak selalu terhubung pada jaringan yang sama, sehingga paket dapat melalui jaringan yang berbeda.

Dalam perjalanannya, paket harus diarahkan oleh intermediary devices yang menghubungkan jaringan yang berbeda.

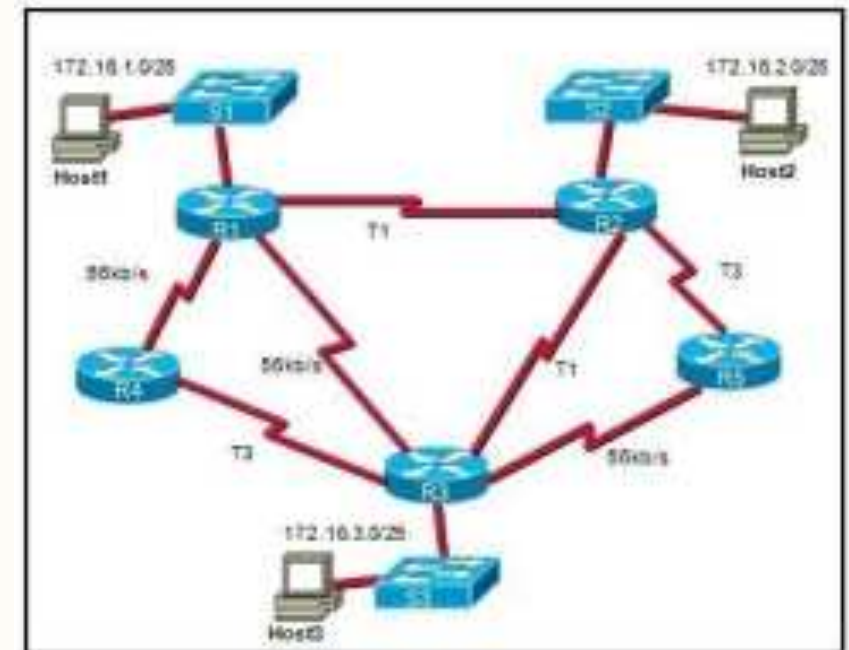


Network layer – proses dasar

3. Routing

Perangkat ini adalah router yang menentukan jalur terbaik untuk mengirim sebuah paket, proses pengarahannya disebut routing.

Dalam perjalanannya, sebuah paket dapat melewati berbagai intermediary device. Setiap rute yang dilalui paket dalam perjalanannya menuju perangkat intermediary berikutnya disebut hop.





Network layer – proses dasar

4. Decapsulation

paket yang tiba pada destination host akan diverifikasi alamat tujuannya, jika benar, maka paket akan di dekapsulasi dan segment akan dikirim ke layer 4

- Tidak seperti layer 4 yang menangani transport data antar proses yang berjalan pada tiap host, layer 3 mendeskripsikan struktur paket dan proses untuk mengirim paket tersebut dari satu host ke host lain **tanpa memperdulikan aplikasi apa yang menggunakan.**
- Hal ini memungkinkan layer network mengirim paket dari berbagai jenis komunikasi antar berbagai host.

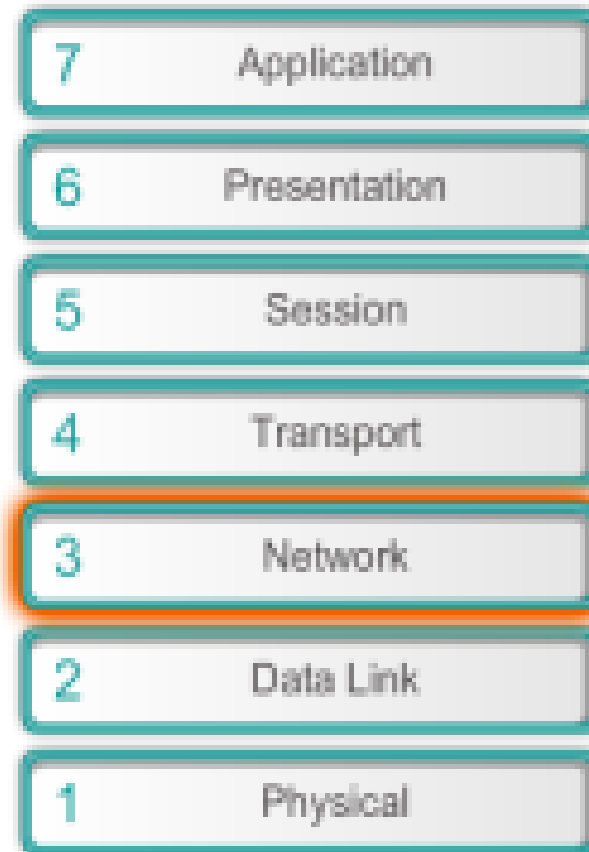


Network layer – protocol overview

– Contoh Protokol yang ada pada layer ini ialah:

1. Internet Protocol version 4 (IPv4)
2. Internet Protocol version 6 (IPv6)
3. Novell Internetwork Packet Exchange (IPX)
4. AppleTalk
5. Connectionless Network Service (CLNS/DECNet)

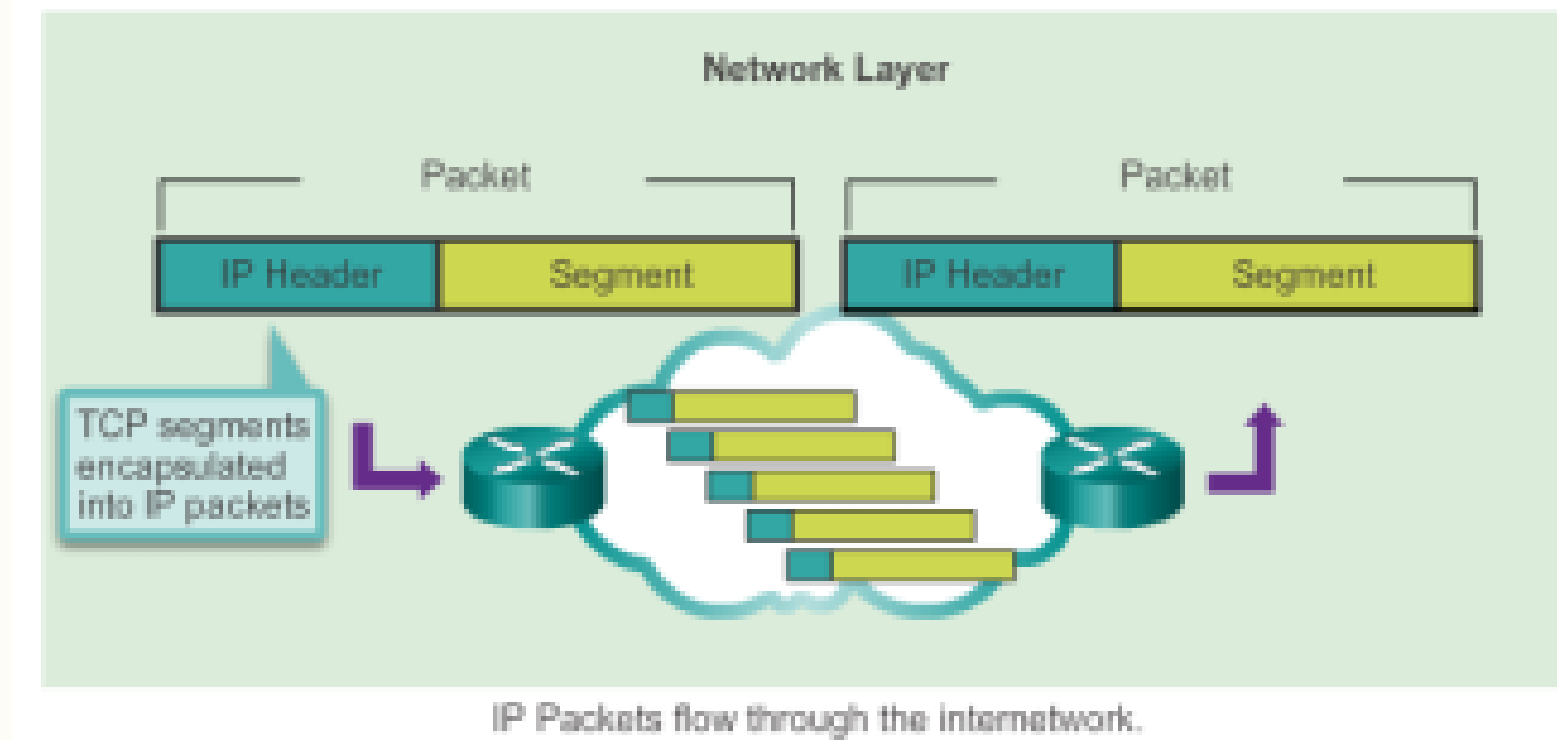
Yang paling luas digunakan ialah IPv4 dan IPv6, sehingga protokol yang lain tidak akan dibahas.



- Internet Protocol version 4 (IPv4)
- Internet Protocol version 6 (IPv6)

Network layer – IPv4

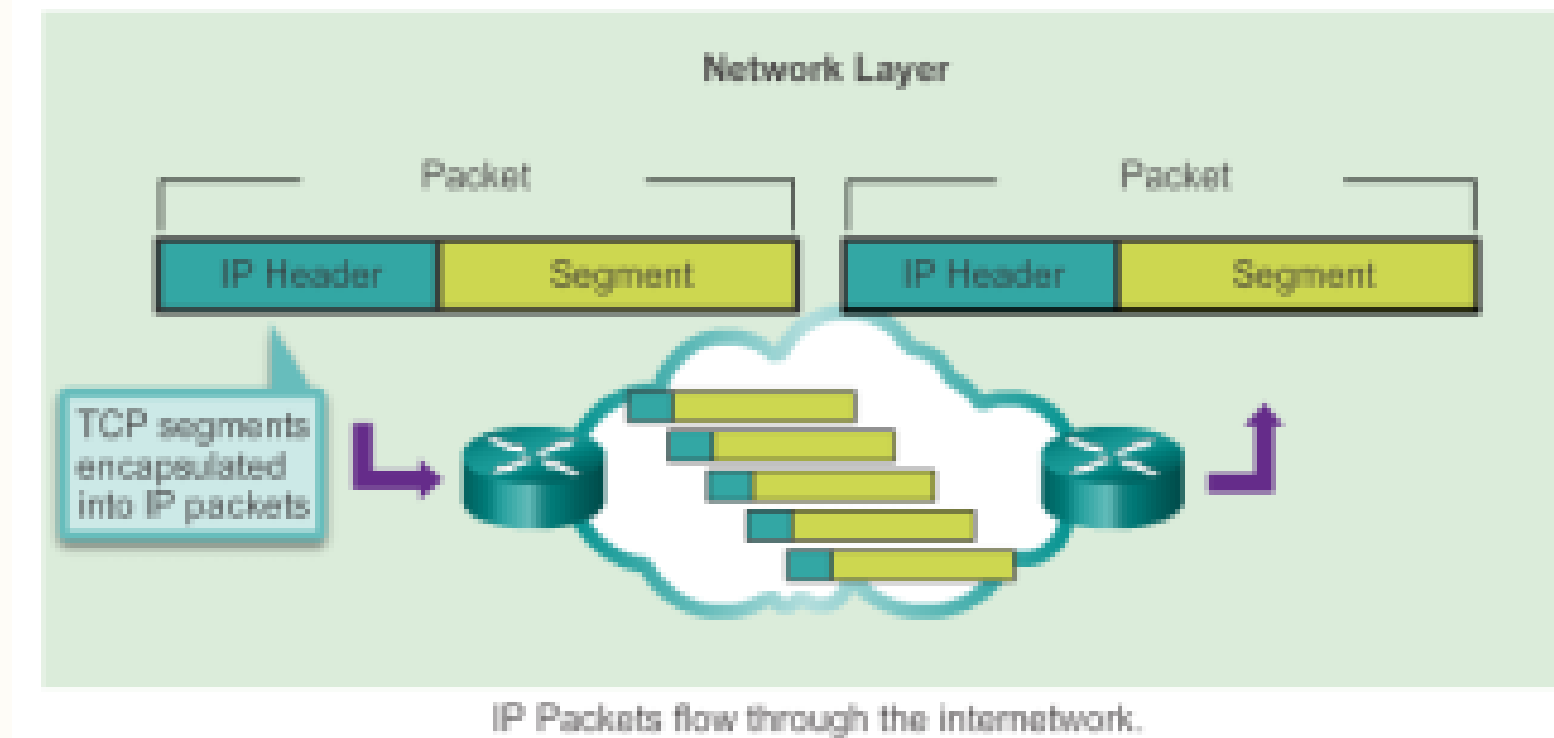
- Internet Protocol di desain sebagai protokol dengan overhead rendah, menyediakan hanya fungsi yang penting untuk mengantarkan paket dari sumber ke tujuan
- Protokol ini tidak melakukan “tracking” dan manajemen flow paket karena akan dilakukan oleh protokol layer lain (pada layer 4).



Network layer – IPv4

– Karakteristik dasar dari IPv4 adalah :

1. Connectionless
Tidak ada koneksi yang dibuka sebelum pengiriman.
2. Best Effort (unreliable)
Tidak ada overhead untuk menjamin pengiriman paket.
3. Media Independent
Bekerja secara independent dari media (tidak terpengaruh jenis media).



IPv4 - Connectionless

- Sifat connectionless pada protokol ini berarti tidak ada sesi pembukaan koneksi yang dibuat sebelum pengiriman.



A letter is sent.

The sender doesn't know:

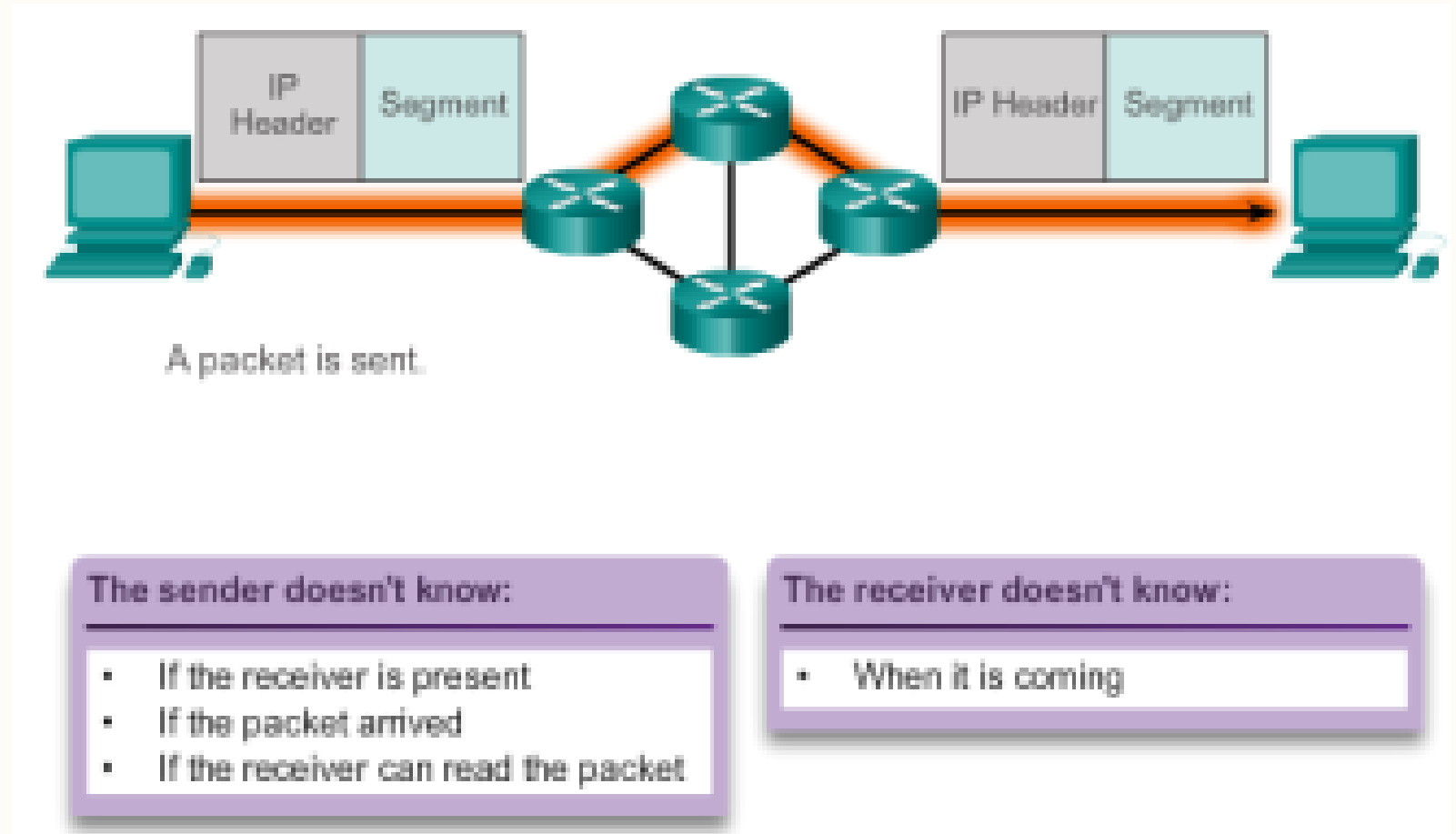
- If the receiver is present
- If the letter arrived
- If the receiver can read the letter

The receiver doesn't know:

- When it is coming

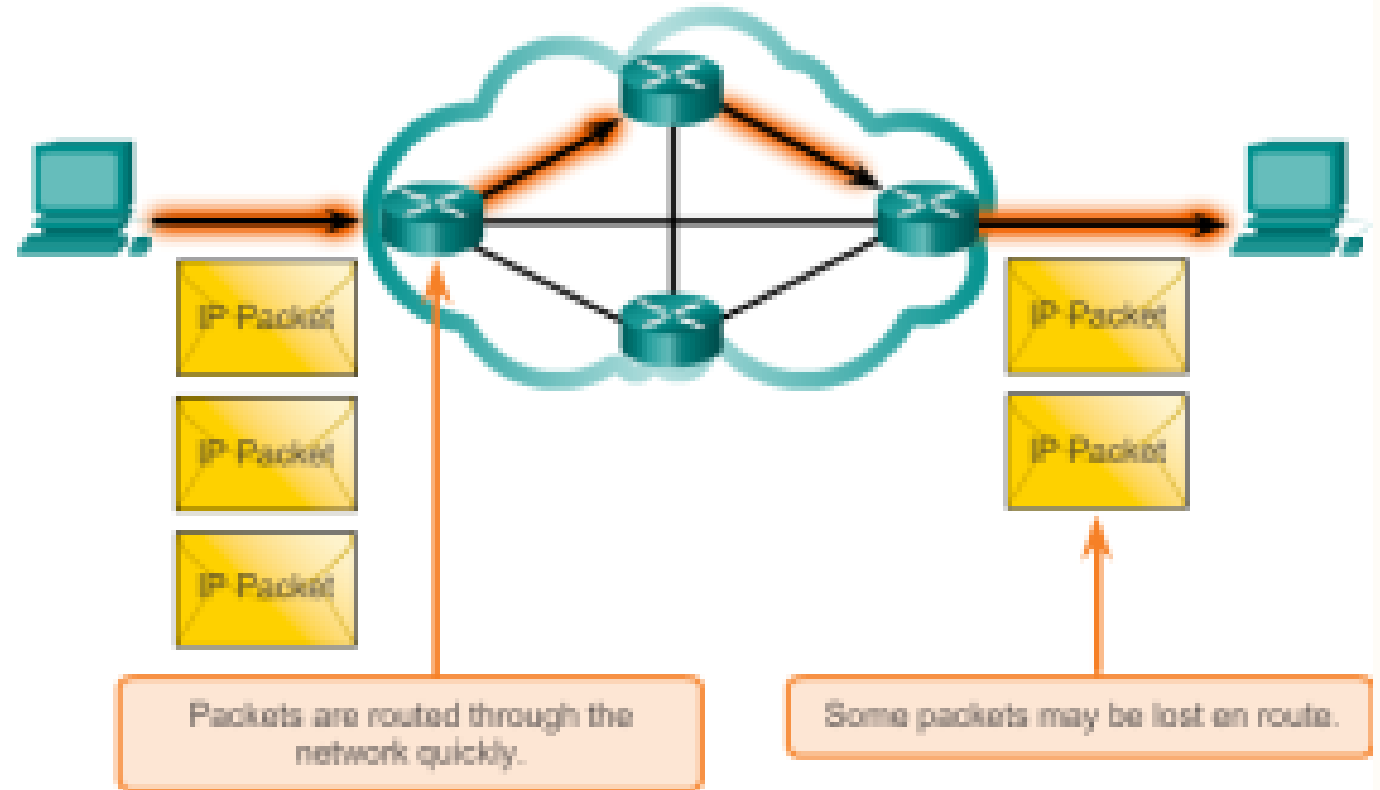
IPv4 - Connectionless

- Overhead rendah, namun si penerima tidak akan mengetahui kapan dan apakah paket akan datang (lihat dari sudut pandang layer 3, karena dari layer 4 dengan protokol TCP, akan dibuat session sebelum pengiriman segment)
- Dapat mengakibatkan tibanya paket dalam urutan yang berbeda, ini harus dikoreksi oleh protokol pada layer di atasnya.



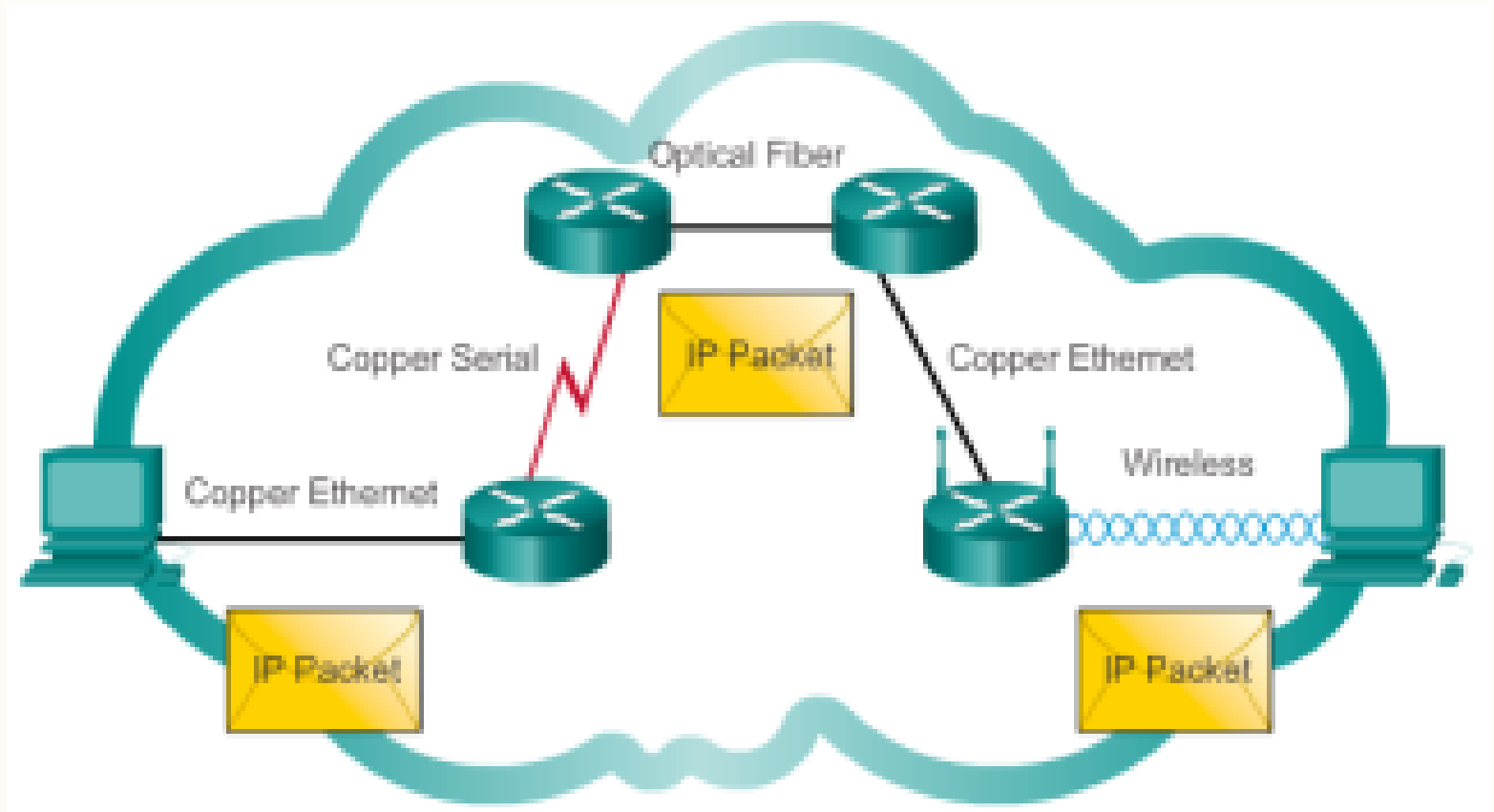
IPv4 – Best effort

- Pengiriman Ip akan menggunakan pendekatan “usaha terbaik” sehingga disebut unreliable.
- “Unreliable” disini dalam konteks bahwa IP tidak memiliki kapabilitas untuk melakukan manajemen dan penanganan paket yang tidak terkirim atau korup.
- Tidak ada ack (acknowledgment / tanda terima) dari pengiriman paket, tidak ada kontrol error dan tidak ada bentuk apapun untuk “tracking” paket, oleh karena itu tidak ada transmisi ulang.
- (kebutuhan reliabilitas ditentukan dari protokol yang digunakan pada layer 4)



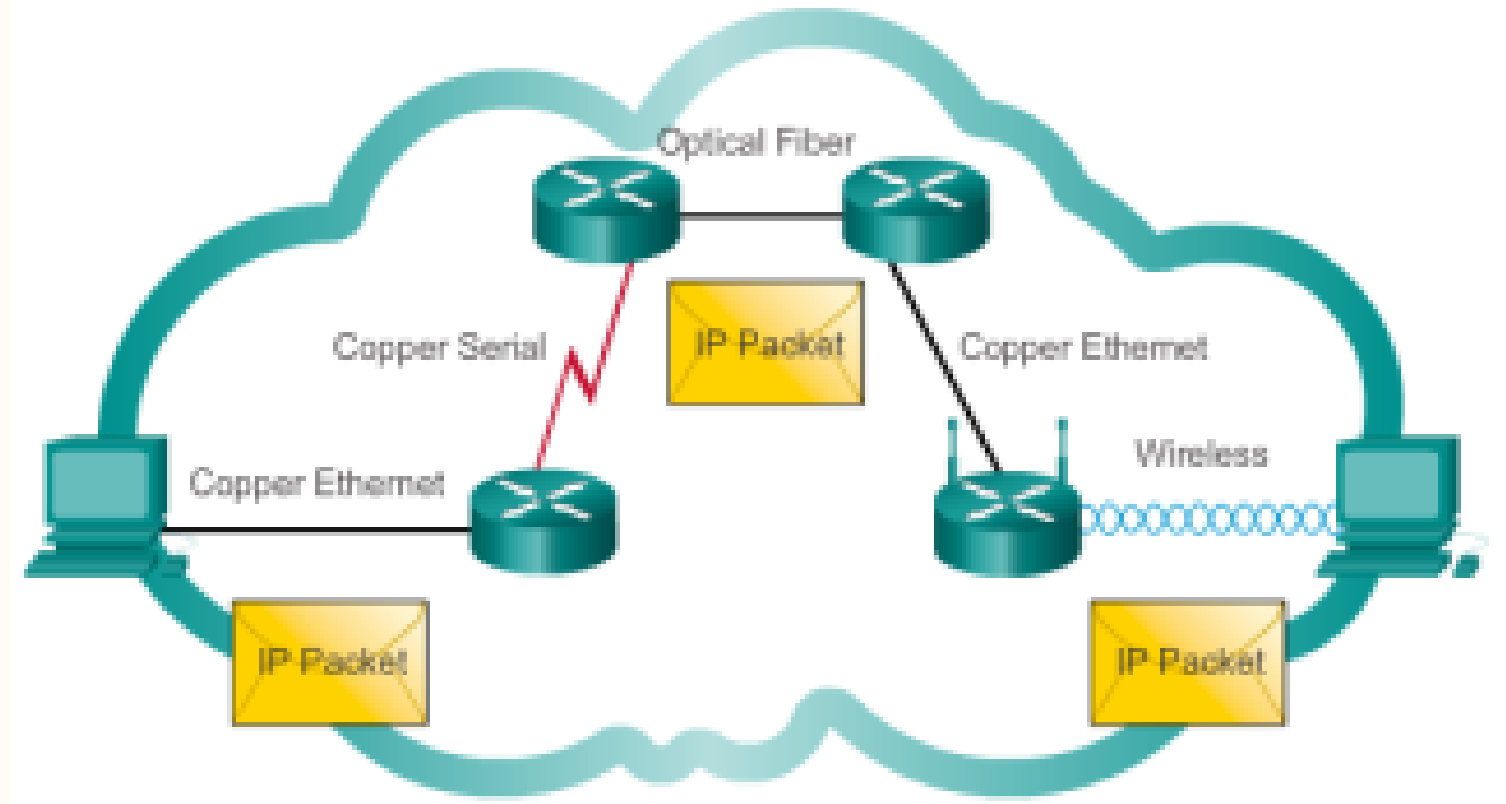
IPv4 – Media independent

- IPv4 juga tidak terbebani dengan karakteristik dari media yang berbeda-beda, fungsi dan format IP tetap sama meskipun media yang digunakan berbeda-beda.
- Hanya ada satu karakteristik utama media yang harus dipertimbangkan layer 3, yaitu ukuran maksimum PDU yang bisa ditransport. Karakteristik ini disebut dengan Maximum Transmission Unit (MTU).



IPv4 – Media independent

- Terdapat komunikasi kontrol antara Data link layer dengan Network layer yang menginformasikan besarnya MTU yang dipakai
- Pada beberapa kasus , sebuah perangkat intermediary (khususnya router) harus membagi sebuah paket besar menjadi paket lebih kecil, proses ini disebut dengan fragmenting the packet atau fragmentation.



20

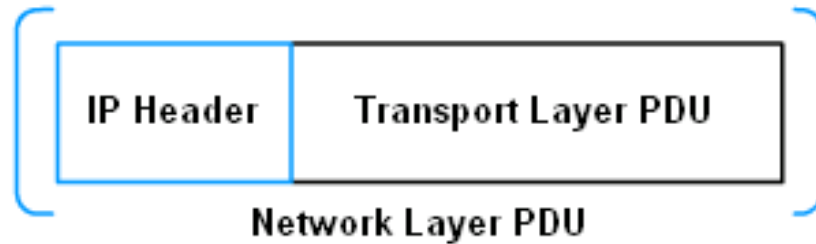
IPv4 Packets - enkapsulasi

Paket IP didapat dari proses
enkapsulasi PDU layer 4

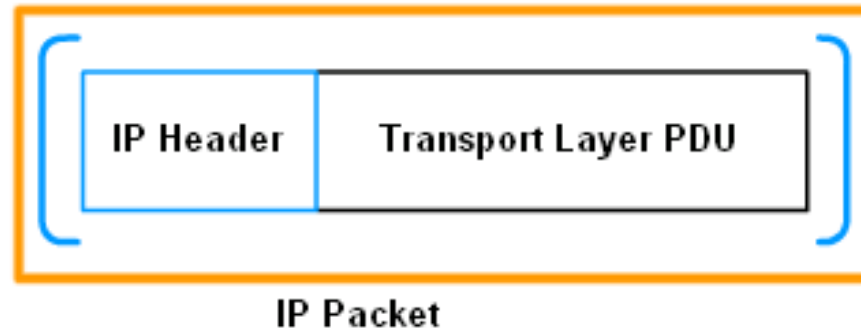
Transport Layer Encapsulation



Network Layer Encapsulation



Network Layer Encapsulation

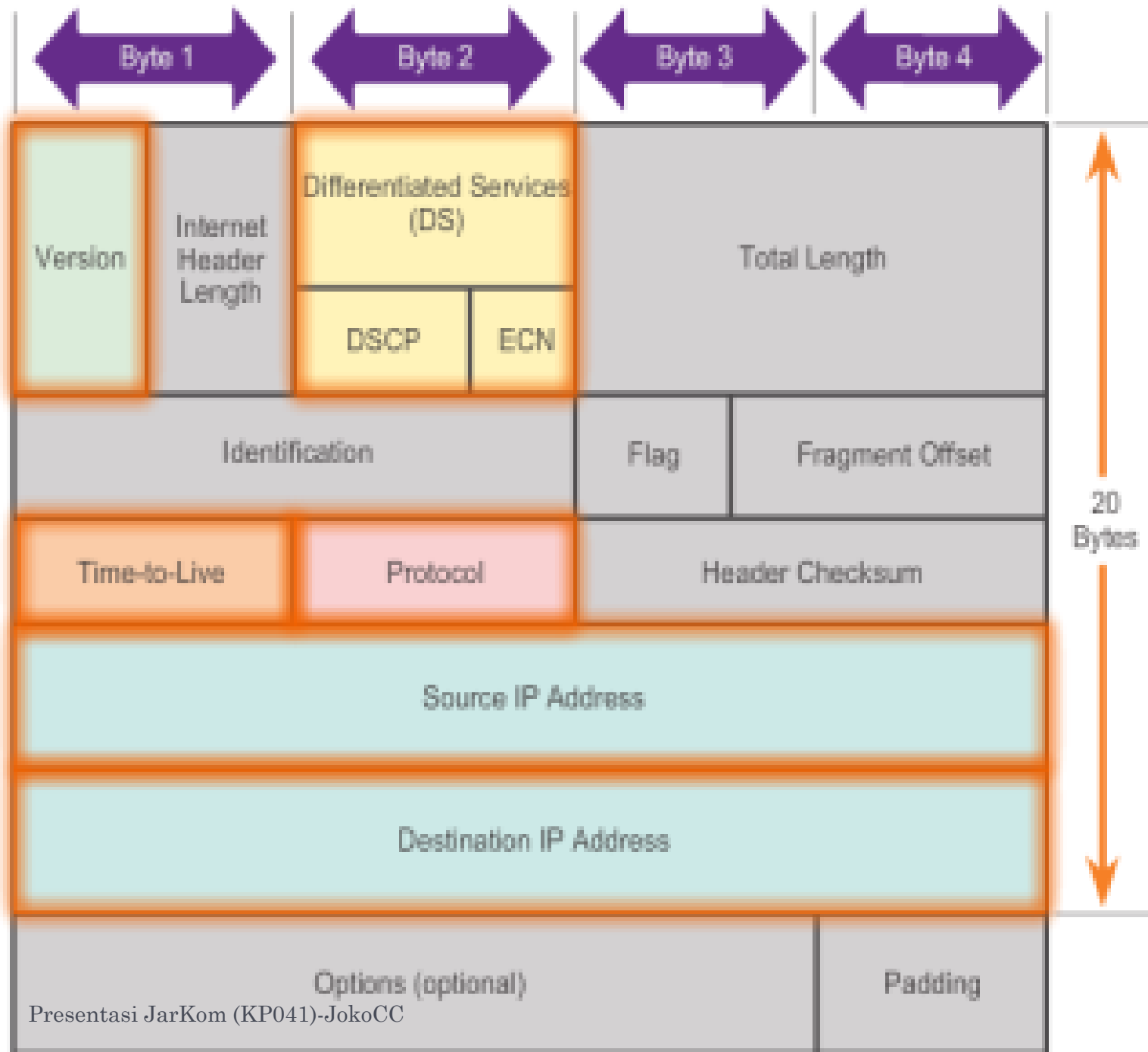




Struktur IPv4

- IPv4 memiliki struktur dasar 2 bagian :
 1. Header
informasi yang ditambahkan oleh protokol IP saat enkapsulasi
 2. Payload
kargo berupa segment atau datagram yang dihasilkan oleh protokol di atasnya





22

IPv4 - header

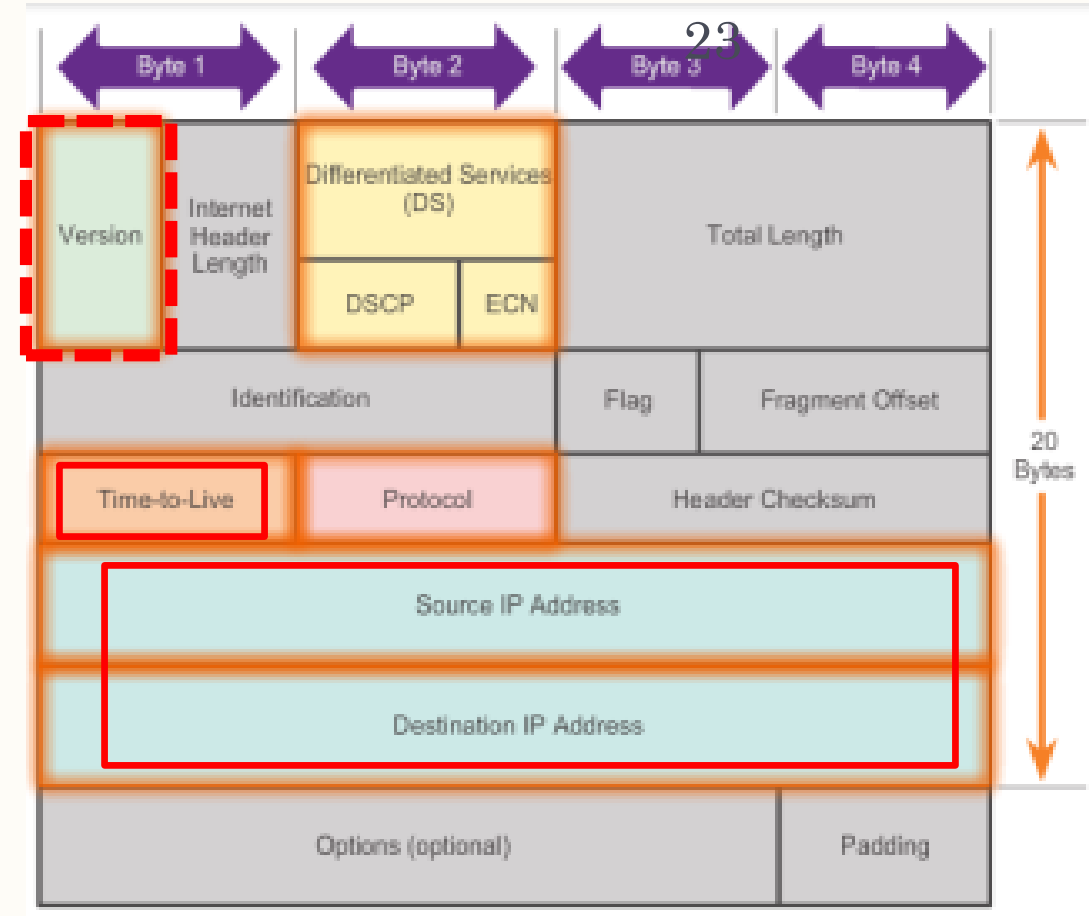
IPv4 - header

- Version
 - Ukuran: 4 bit biner
 - Fungsi : mengidentifikasi versi paket IP
 - Untuk IPv4 nilainya selalu 0100

- IP Destination Address
berisi 32 bit biner alamat tujuan

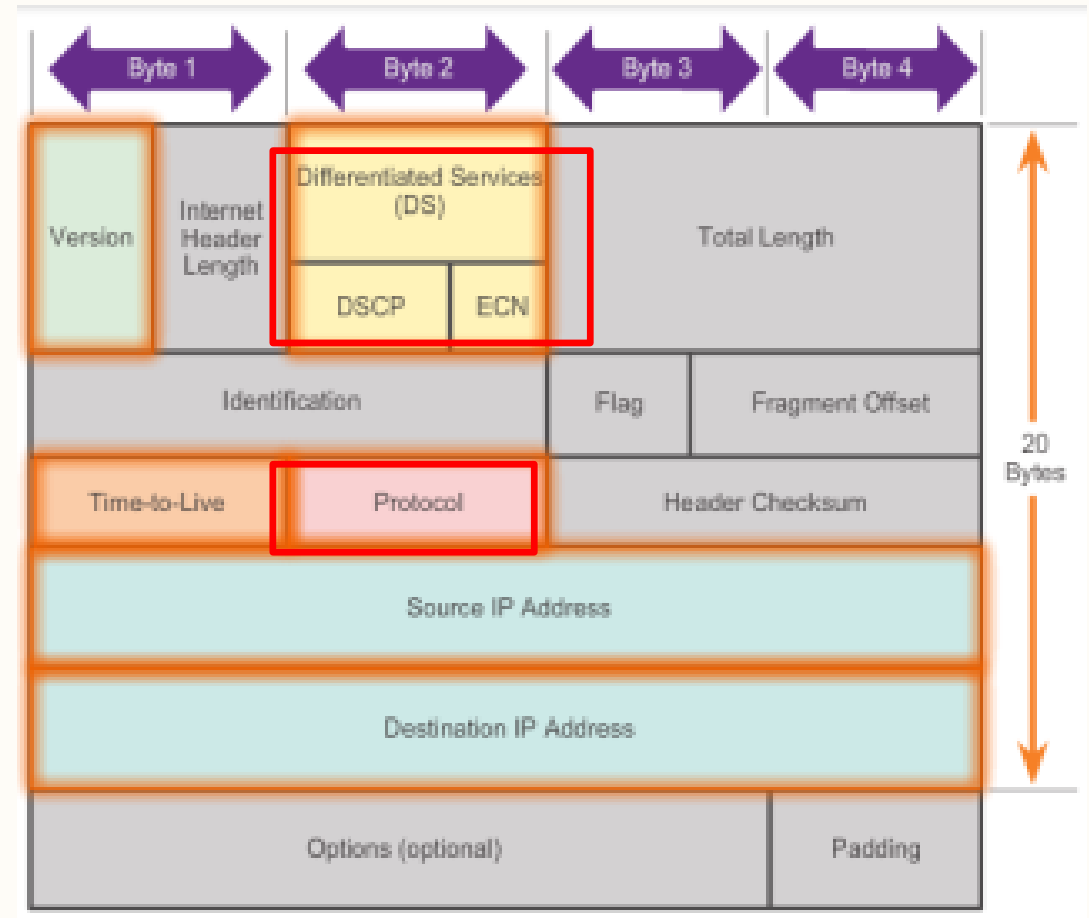
- IP Source Address
berisi 32 bit biner alamat sumber

- Time-to-Live
berisi 8 bit biner yang mengindikasikan “umur” paket. Nilai TTL akan berkurang tiap satu hop, saat nilainya menjadi 0, paket akan dibuang. Mekanisme ini mencegah paket di forward tanpa batas.



IPv4 - header

- ▶ Differentiated Service (DS)
- ▶ Dahulu disebut dengan Type of Service (ToS), sepanjang 8 bit biner:
 - ▶ 6 bit pertama disebut Differentiated Services Code Point (DSCP) yang digunakan oleh mekanisme QoS
 - ▶ 2 bit berikutnya disebut Explicit Congestion Notification (ECN) yang digunakan untuk mencegah paket di drop saat lalu lintas padat.
- ▶ Protocol berisi 8 bit biner yang mengindikasikan jenis data yang dibawa paket. Nilai ini memungkinkan layer network mengirim paket ke protokol layer 4 yang tepat .
Contoh nilainya:
 - ▶ 01 ICMP
 - ▶ 06 TCP
 - ▶ 17 UDP



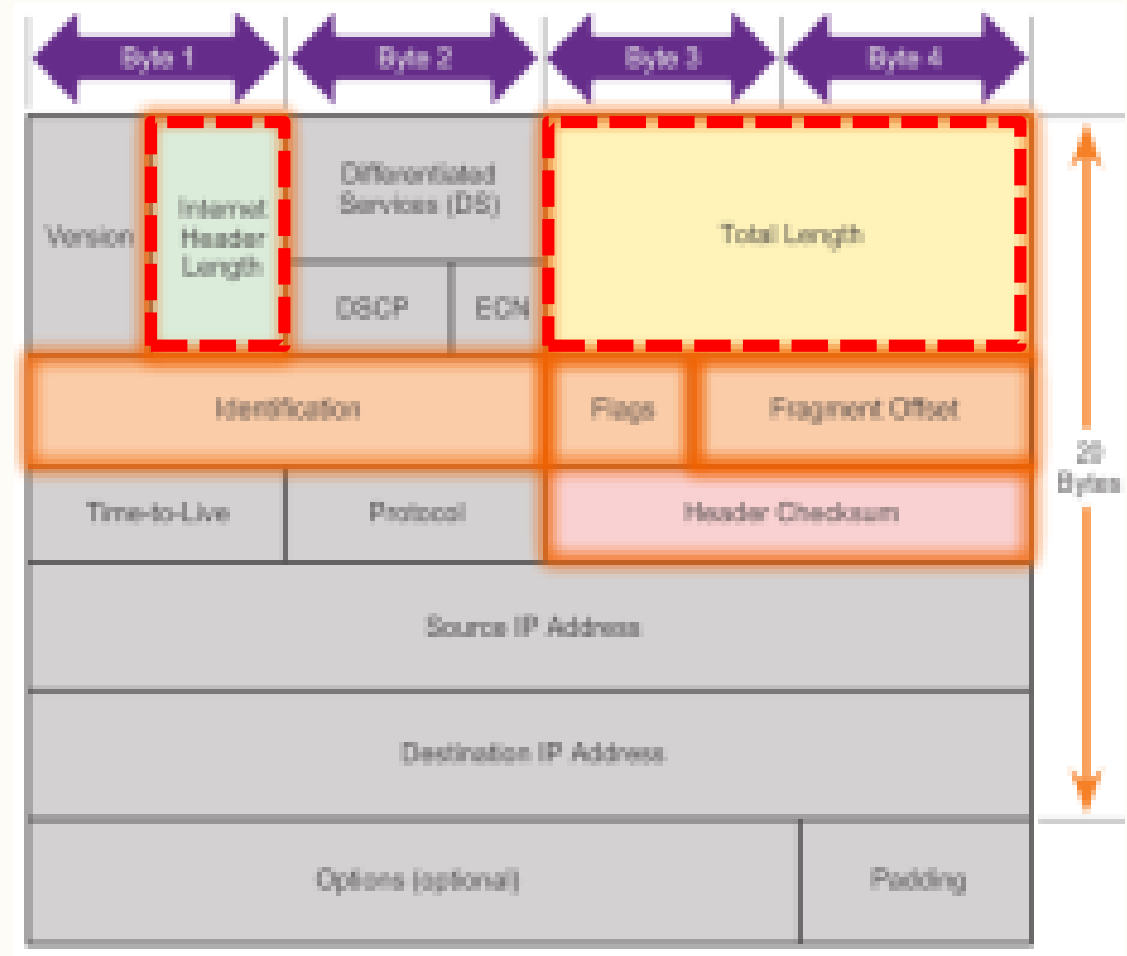
IPv4 - header

Internet Header Length (IHL) –

- Ukuran: 4 bit biner
- Fungsi : menyatakan panjang header paket.
- Satuan yang digunakan adalah word (1 word = 32 bit).
- Nilai minimum adalah 5 (0101) berarti sebesar $5 \times 32 = 160$ bits = 20 bytes
- Nilai maksimum adalah 15 (1111) berarti sebesar $15 \times 32 = 480$ bits = 60 bytes

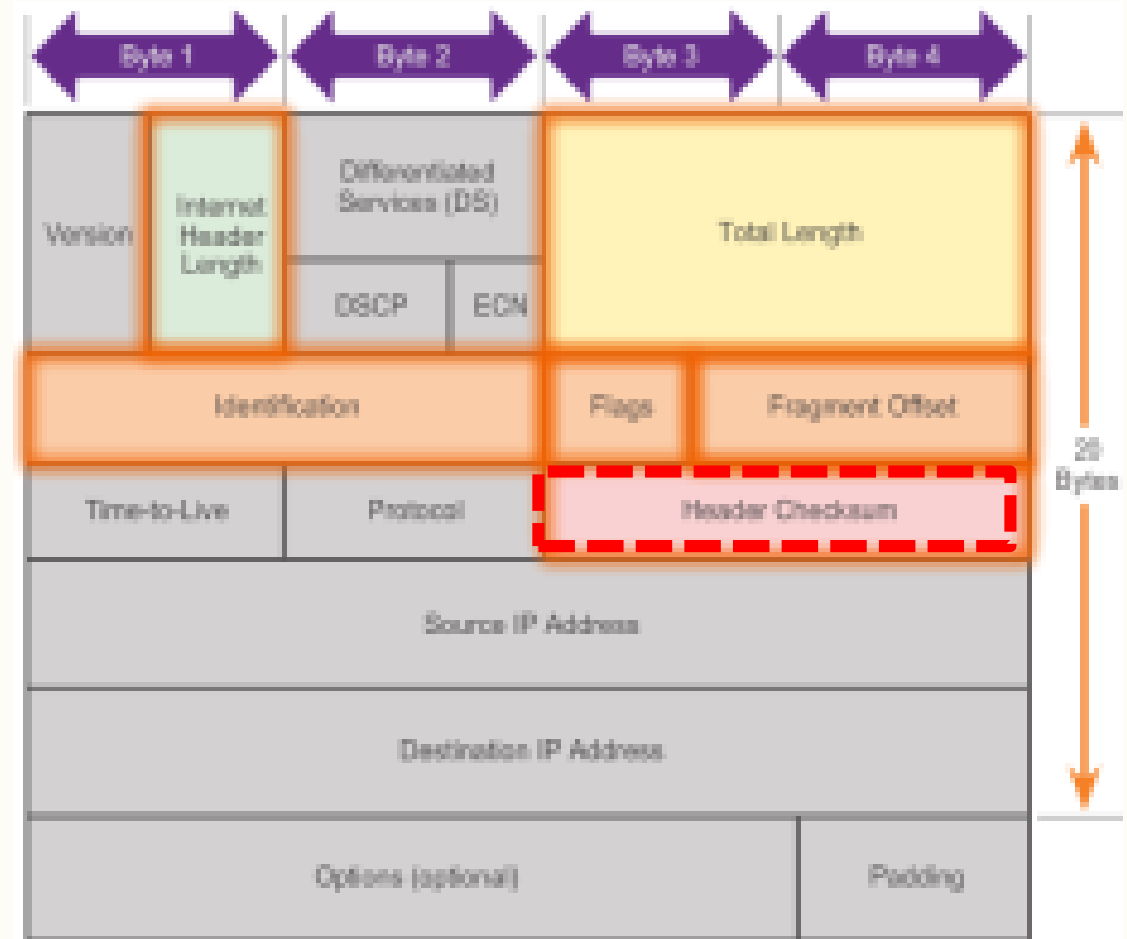
Total Length

- Ukuran: 16 bit biner
- Fungsi : menyatakan panjang keseluruhan paket, termasuk header
- Satuan yang digunakan adalah byte.
- Nilai minimum adalah 20 byte (20-byte header + 0 bytes data)
- Nilai maksimum adalah 65,535 bytes.



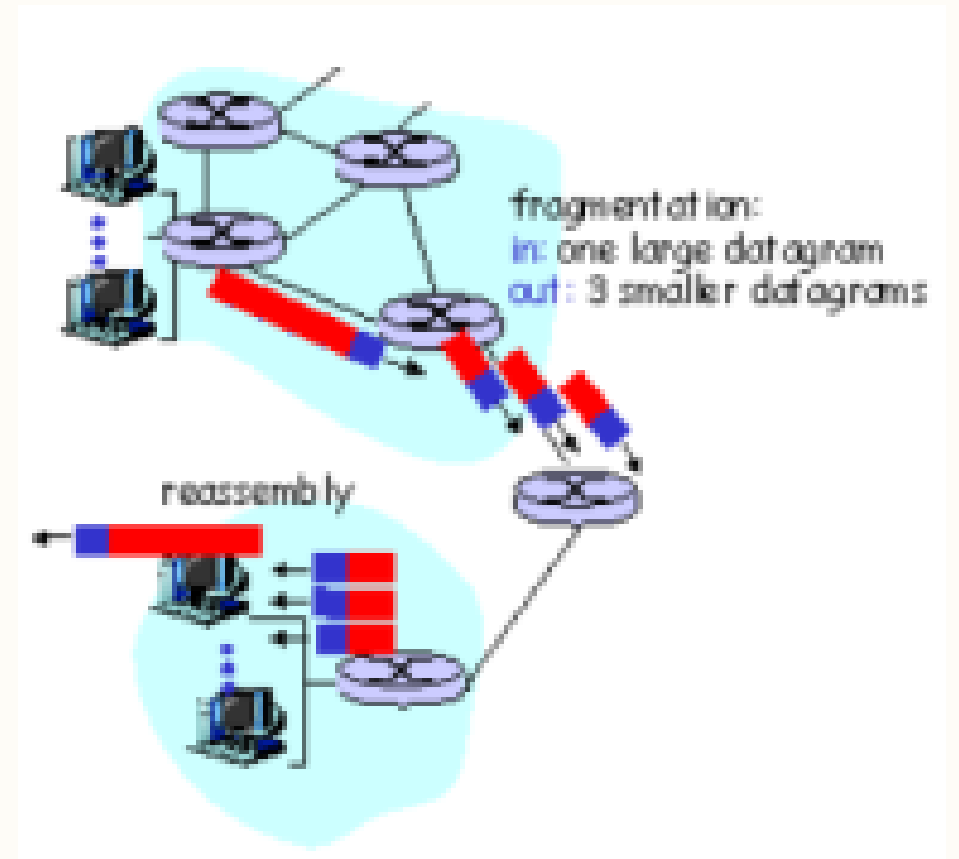
IPv4 - header

- Header Checksum
 - Ukuran :16-bit
 - Fungsi : untuk melakukan check error dari header IP
 - Nilai checksum dihitung oleh pengirim dan diletakkan disini, saat diterima, maka penerima akan melakukan proses checksum lagi dan membandingkan nilainya, jika sama maka paket dianggap valid, jika berbeda maka paket dianggap rusak dan akan dibuang



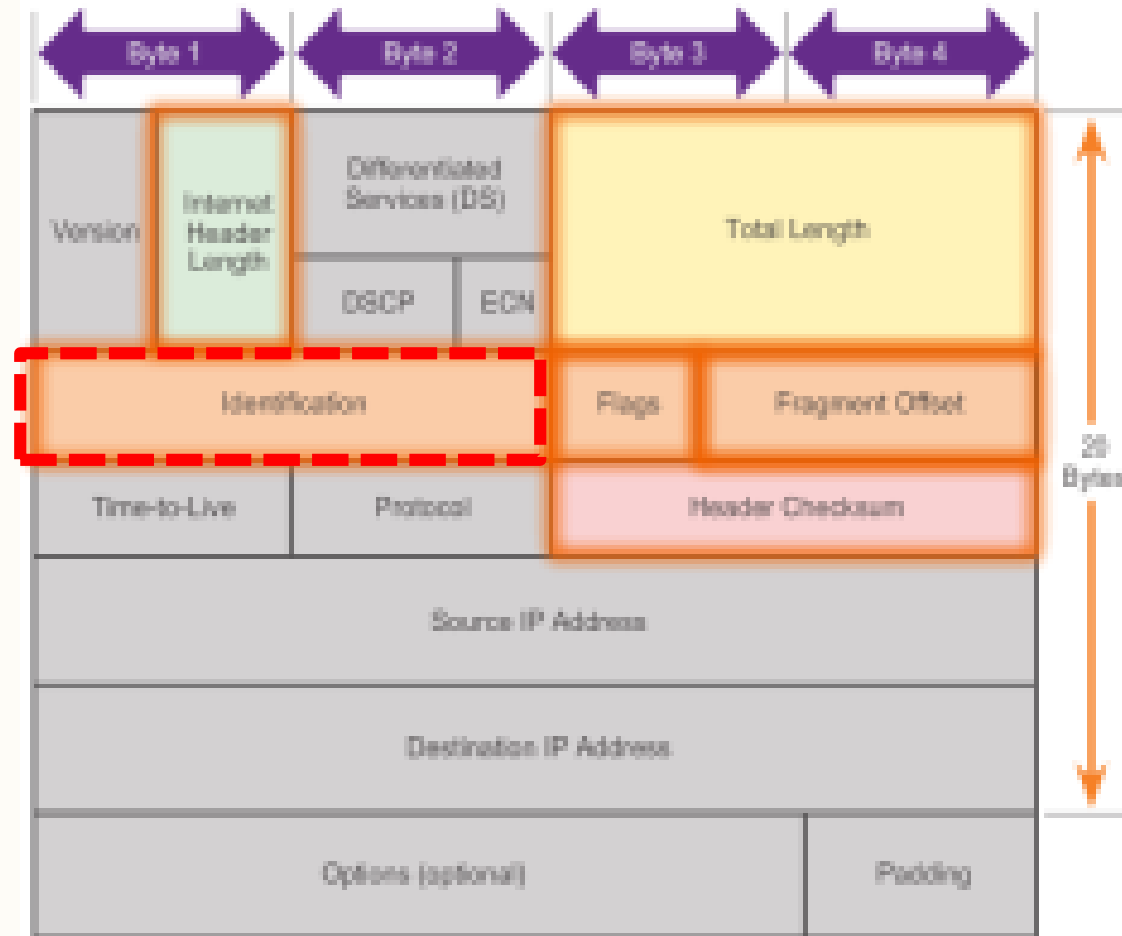
IPv4 - header

- Dalam perjalanan sebuah paket, dapat melalui media yang berbeda-beda kapasitasnya.
- Saat sebuah paket yang diterima router harus dikirim melalui media yang memiliki bandwidth rendah (lebih rendah dari MTU-Maximum Transmission Unit paket), maka paket itu harus difragmentasi



IPv4 - header

- Identification
- Ukuran :16-bit
- Fungsi : untuk mengidentifikasi secara unik sebuah fragment dari paket IP original

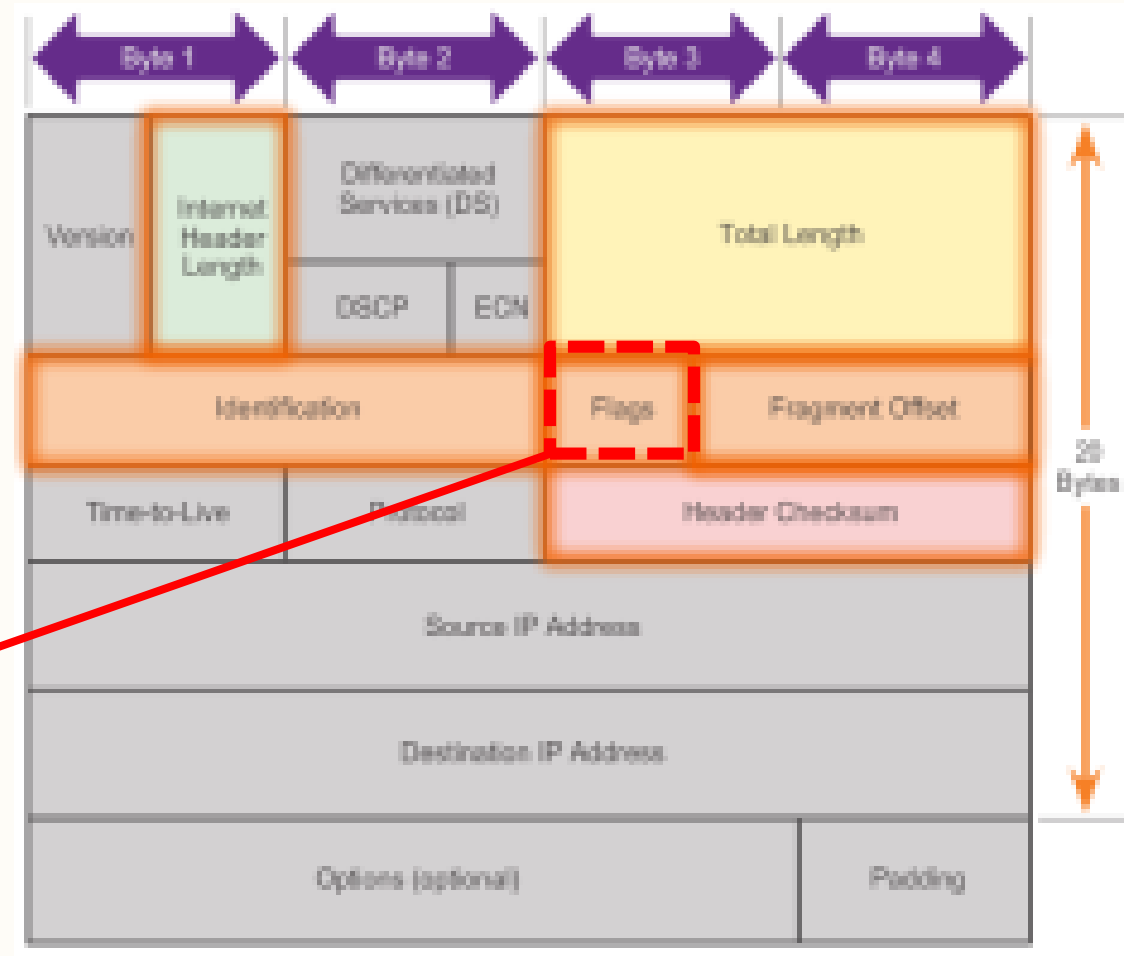


IPv4 - header

- Flags
 - Ukuran :3-bit
 - Fungsi : untuk mengidentifikasi bagaimana sebuah paket terfragmentasi, sehingga membantu router penerima untuk merekonstruksi paket fragment menjadi paket utuh

Terdiri dari 3 bit

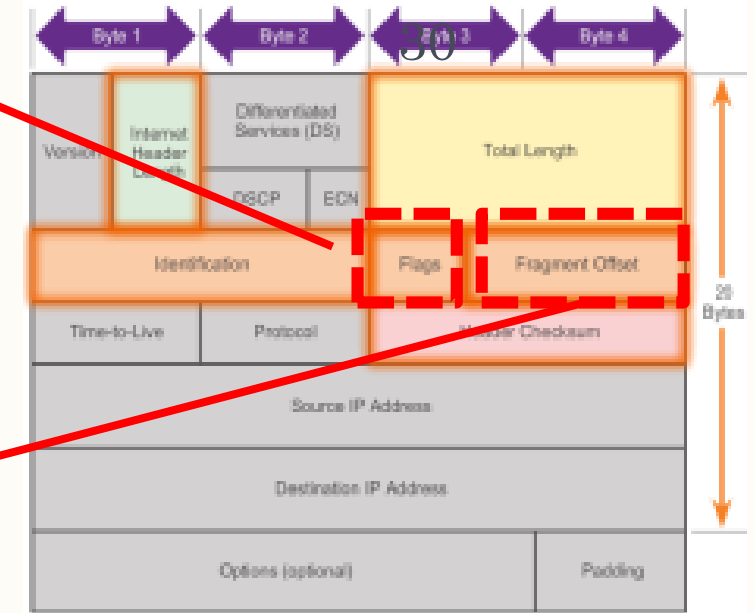
Reserved	DF	MF
Harus 0	0 atau 1	0 atau 1



Flag terdiri dari 3 bit

IPv4 - header

Reserved	DF	MF
Harus 0	0 atau 1	0 atau 1



DF (don't Fragment) (1 bit) merupakan kode untuk mencegah fragmentasi (nilai=1). Jika router harus melakukan fragmentasi, namun nilai DF =1 maka paket akan dibuang

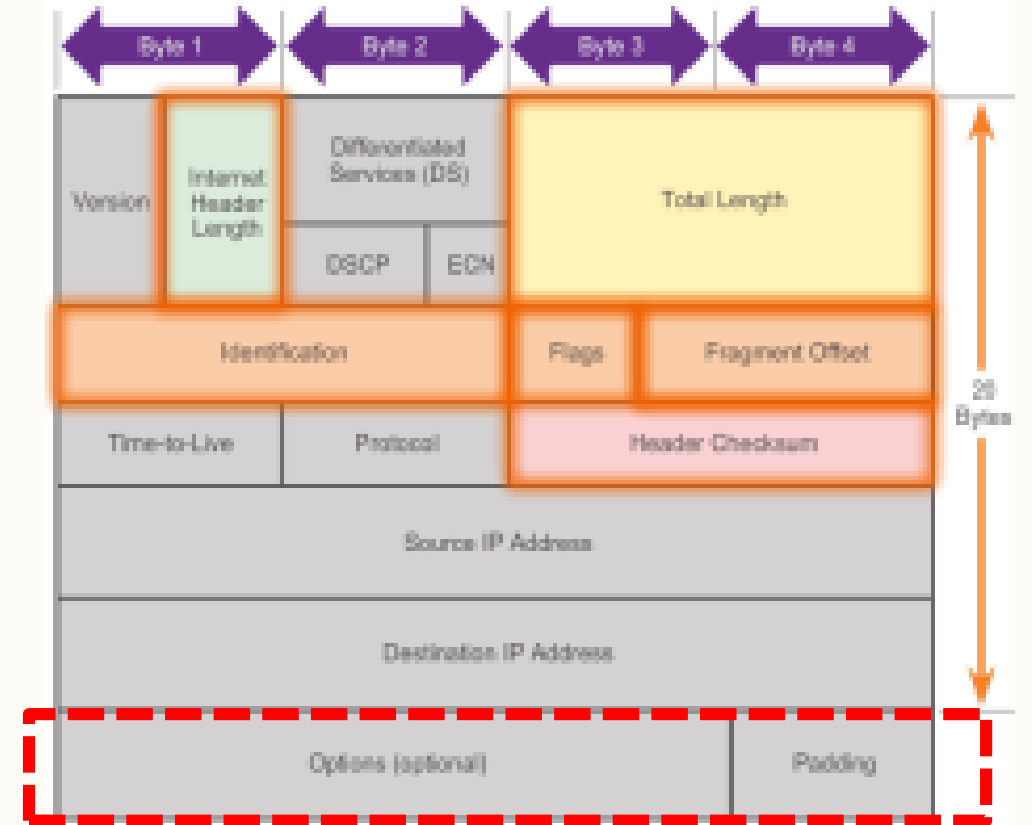
MF (More Fragment Offset) (1 bit) merupakan kode yang menyatakan ada tidaknya fragmentasi, atau penanda akhir fragment.

Fragment Offset (13 bit) merupakan nilai yang berisi nomor urut fragmentasi, digunakan dengan More fragment offset (MF)

MF	Fragment offset	artinya
0	0	Tidak ada fragmentasi
1	Selain 0	Potongan fragment
0	Selain 0	Potongan fragment terakhir

IPv4 - header

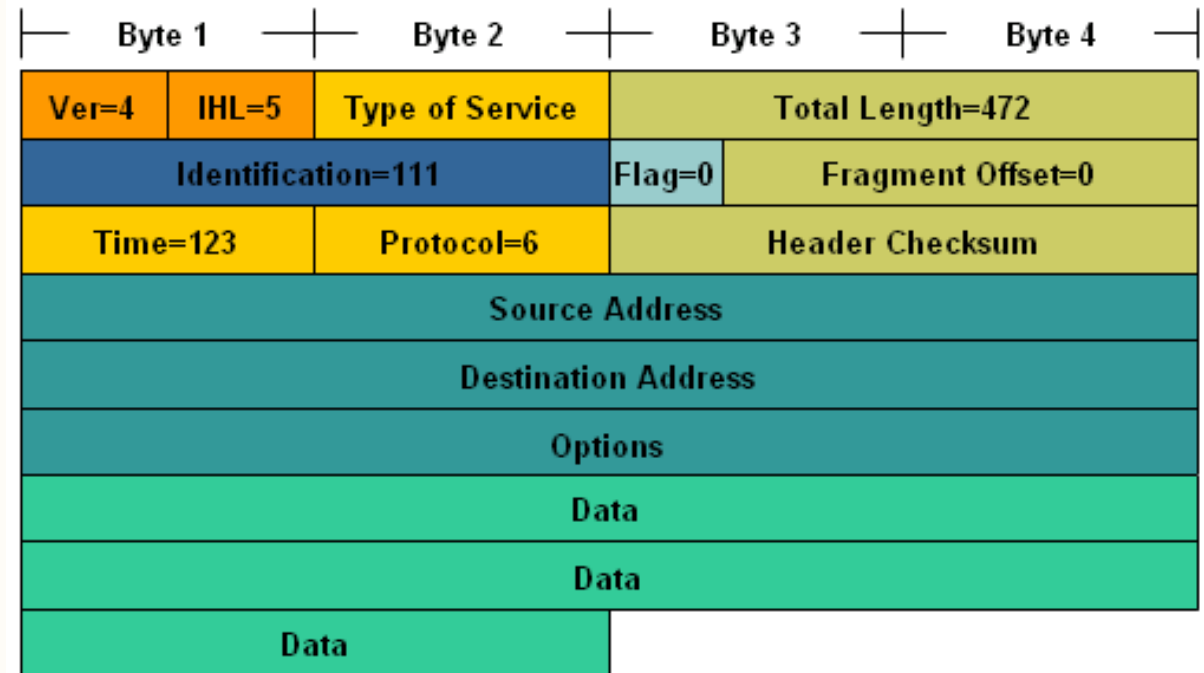
- Options dan padding
- Jarang digunakan dan diluar dari bahasan materi ini.
- Daftar lengkap dapat dilihat di :
<http://www.iana.org/assignments/protocol-numbers>



IPv4 – contoh header paket yg umum

32

- Ver=4 ;Versi 4
- IHL = 5; ukuran header dalam 32 bit words (4 bytes). Header ini berukuran 5*4 = 20 bytes, nilai minimum yang valid.
- Total Length = 472; ukuran paket (header and data) is 472 bytes.
- Identification = 111; nomor identifier asli (diperlukan jika ada fragmentasi).
- Flag = 0; berarti paket boleh di fragmentasi jika diperlukan
- Fragment Offset = 0; menandakan bahwa saat ini paket tidak terfragmentasi (tidak ada nomor offset).



- ▶ Time to Live = 123; menyatakan jumlah hop sisa umur paket (berkurang setiap kali bertemu router).
- ▶ Protocol = 6; menyatakan bahwa isi paket berisi segment TCP.



33 Latihan

– Cocokkan index istilah sebelah kiri dengan no penjelasan sebelah kanan

Index	istilah	No	penjelasan
A	Version	1	Mengidentifikasi prioritas dari setiap paket
B	Differentiated Services	2	Sering disebut juga sebagai hop-count
C	Time to Live	3	Mengidentifikasi alamat pengirim
D	Protocol	4	Nilai maksimum yang didukung adalah 65535 bersatuan byte
E	Source IP address	5	Selalu di set dengan nilai 0100 untuk IPv4
F	Destination IP address	6	Untuk melakukan cek error IP header
G	Total Length	7	Mengidentifikasi alamat penerima
H	Internet Header Length	8	Mengidentifikasi protokol yang digunakan di layer atas.
I	Header Checksum	9	Menyatakan ukuran header

Index istilah	No penjelasan
A	?
...	?
I	?

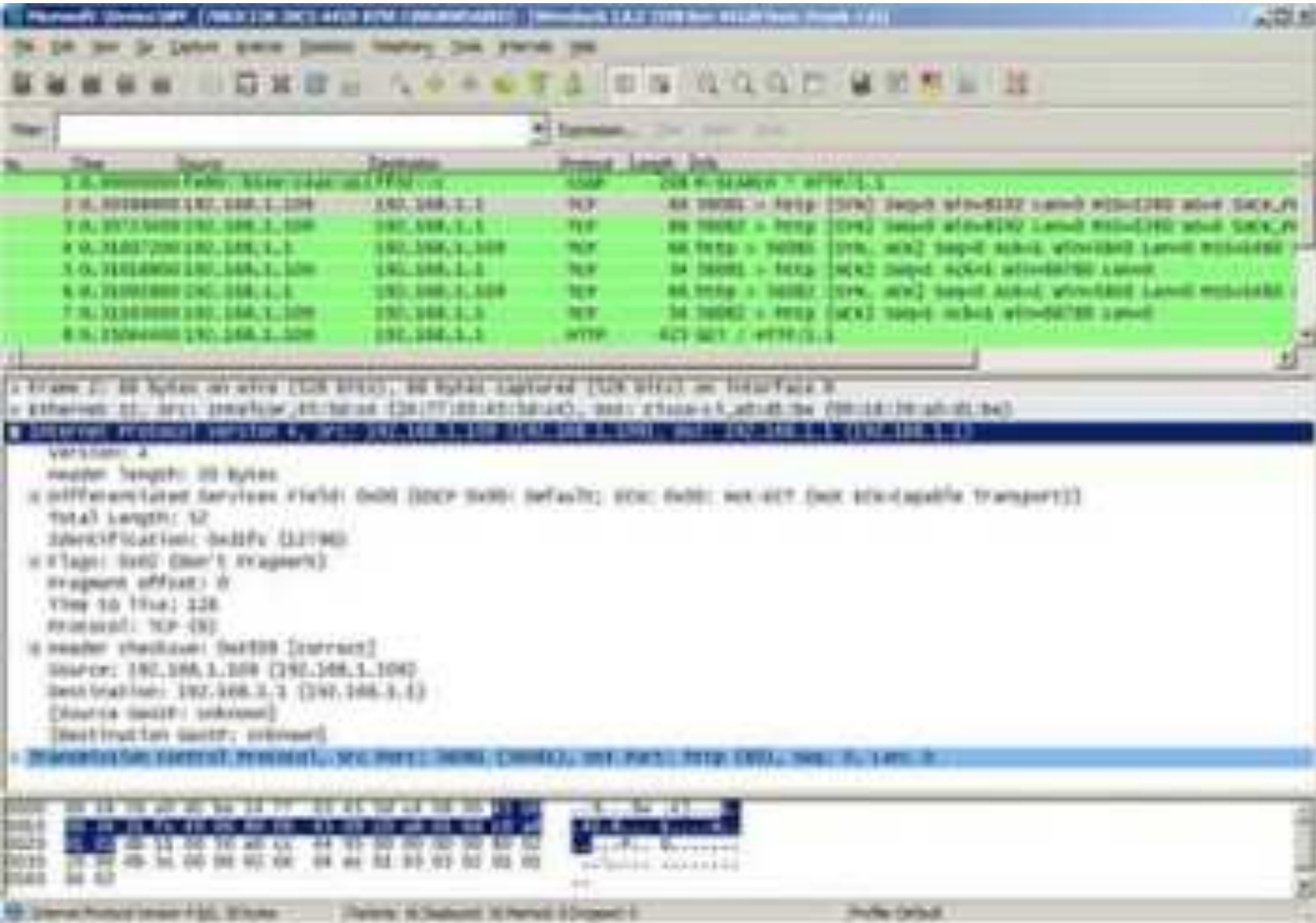


34

Mendapatkan paket IPv4

Untuk mendapatkan contoh (sample) dari IPv4, dapat digunakan software capture paket, salah satunya adalah wireshark

Dosen dapat mendemonstrasikan jika diperlukan





Peragaan

- Jika dimungkinkan, dosen akan menggunakan software wireshark untuk mendemonstrasikan cara capture paket, dan melihat informasi yang ditampilkan pada paket sederhana seperti paket ping.



Batasan IPv4

- IPv4 tidak didesain untuk jumlah penggunaan seperti saat ini. Untuk mempertahankan menggunakan IPv4 telah dilakukan beberapa update seperti penggunaan Variable Length Subnet Mask(VLSM) dan Network Address Translation (NAT).
- Namun, meskipun dengan update tersebut, IPv4 masih mengalami 3 masalah utama:
 1. Habisnya IPv4
 2. Ekspansi routing table Internet
 3. Hilangnya konektivitas end-to-end



1. Habisnya IPv4

IANA Unallocated Address Pool Exhaustion:
03-Feb-2011

Projected RIR Address Pool Exhaustion Dates:

RIR	Projected Exhaustion Date
APNIC:	19-Apr-2011 (actual)
RIFE NCC:	14-Sep-2012 (actual)
LACNIC:	10-Jun-2014 (actual)
ARIN:	24-Sep-2015 (actual)
AFRINIC:	20-Jun-2018

- IPv4 memiliki kapasitas terbatas yang bisa dikombinasikan dari 32 bit biner.
- Meskipun secara teoritis mendukung 4.294.967.296 kombinasi IP, namun dalam desainnya diperlukan blok alamat tertentu tidak dapat digunakan, sehingga hanya dapat digunakan kurang dari nilai tersebut, sekitar 3,7 Miliar
- Pembagian IPv4 public (yang bisa digunakan di internet) diatur oleh IANA (Internet Assigned Number Authority), yang kemudian mendelegasikan kembali ke region-region di dunia.
- IANA sudah habis mendelegasikan blok alamat kepada region, dan hanya tersisa satu region yang masih memiliki sedikit IPv4 public untuk disewakan.



2. Ekspansi routing table Internet

- Routing table digunakan oleh router untuk mengambil keputusan routing yang terbaik.
- Setiap routing table berisi informasi alamat network IP yang bisa dihubungi oleh router tersebut.
- Seiring dengan jumlah server (node) yang terhubung ke internet semakin banyak, maka jumlah rute network pada routing table semakin besar
- Semakin besar routing table maka semakin membebani memori dan sumber daya pada internet router yang pada akhirnya menurunkan kinerja

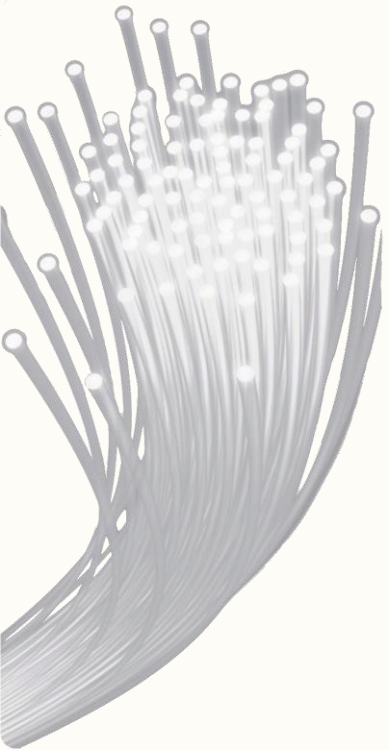




3. Hilangnya konektivitas end-to-end

- Penggunaan NAT untuk memperpanjang penggunaan IPv4 sudah menjadi standar yang berlaku saat ini.
- NAT memungkinkan perangkat untuk berbagi sebuah IPv4 public dan terhubung ke internet.
- Namun karena sebuah IP public digunakan secara berbagi, maka alamat IP internal terselubung
- Hal ini akan menjadi masalah untuk teknologi yang memerlukan end-to-end connectivity (IP sumber dan IP tujuan akhir harus diketahui) seperti game, dan peer-to-peer





IPv6



IPv6

-
- Di awal 1990an, Internet Engineering Task Force (IETF) mulai merasa risau terkait keterbatasan IPv4 an mulai mencoba mencari teknologi pengganti.
 - Hal ini mendorong perkembangan IPv6
 - IPv6 mengatasi permasalahan yang ada di IPv4 dan lebih cocok untuk kebutuhan jaringan masa depan.



IPv6

– Peningkatan pada IPv6 termasuk :

1. Jumlah alokasi alamat yang lebih besar dengan menggunakan kombinasi 128 bit biner, IPv6 secara teoritis dapat menyediakan 340 Undecillion alamat

IPv6 menyediakan kombinasi 340,282,366,920,938,463,463,374,607,431,768,211,456, yang kira-kira sebanyak jumlah butir pasir di bumi.

Number Name	Scientific Notation	Number of Zeros
1 Thousand	10 ³	1,000
1 Million	10 ⁶	1,000,000
1 Billion	10 ⁹	1,000,000,000
1 Trillion	10 ¹²	1,000,000,000,000
1 Quadrillion	10 ¹⁵	1,000,000,000,000,000
1 Quintillion	10 ¹⁸	1,000,000,000,000,000,000
1 Sextillion	10 ²¹	1,000,000,000,000,000,000,000
1 Septillion	10 ²⁴	1,000,000,000,000,000,000,000,000
1 Octillion	10 ²⁷	1,000,000,000,000,000,000,000,000,000
1 Nonillion	10 ³⁰	1,000,000,000,000,000,000,000,000,000,000
1 Decillion	10 ³³	1,000,000,000,000,000,000,000,000,000,000,000
1 Undecillion	10 ³⁶	1,000,000,000,000,000,000,000,000,000,000,000,000

Legend

 There are 4 billion IPv4 addresses

 There are 340 undecillion IPv6 addresses



IPv6

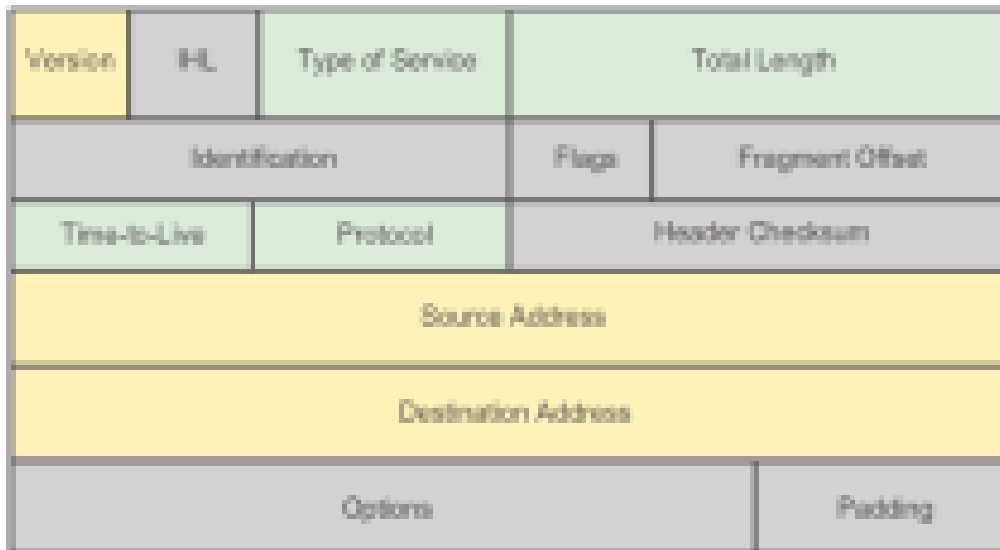
- Peningkatan pada IPv6 termasuk :
 2. Peningkatan packet handling
header pada IPv6 lebih sederhana dan mempermudah pekerjaan router
 3. Menghilangkan kebutuhan NAT
memecahkan masalah end-to-end connectivity






Struktur header IPv4 vs IPv6

- Mari kita bandingkan struktur header IPv4 dengan IPv6

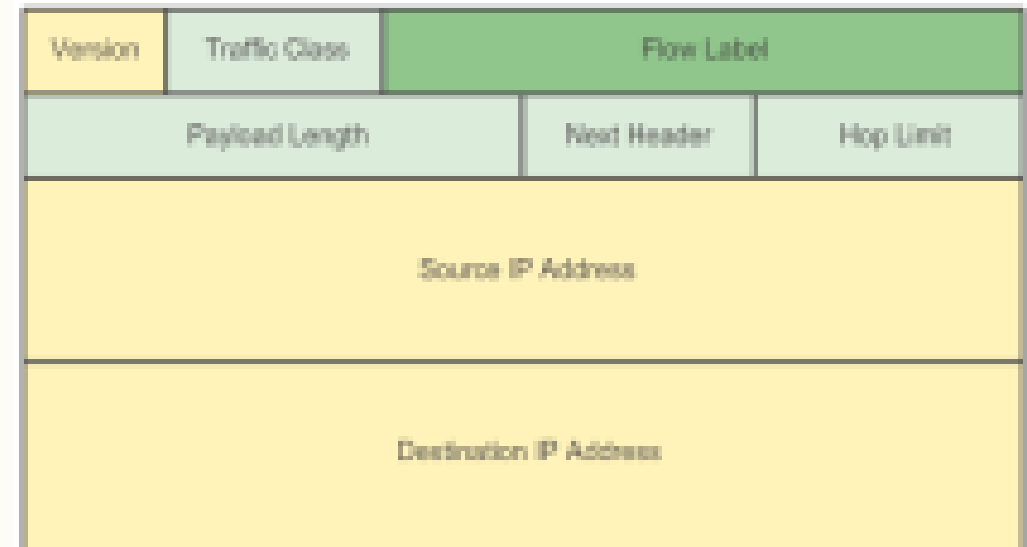
IPv4 Header



Legend

-  - Field names kept from IPv4 to IPv6
-  - Name and position changed in IPv6
-  - Fields not kept in IPv6

IPv6 Header



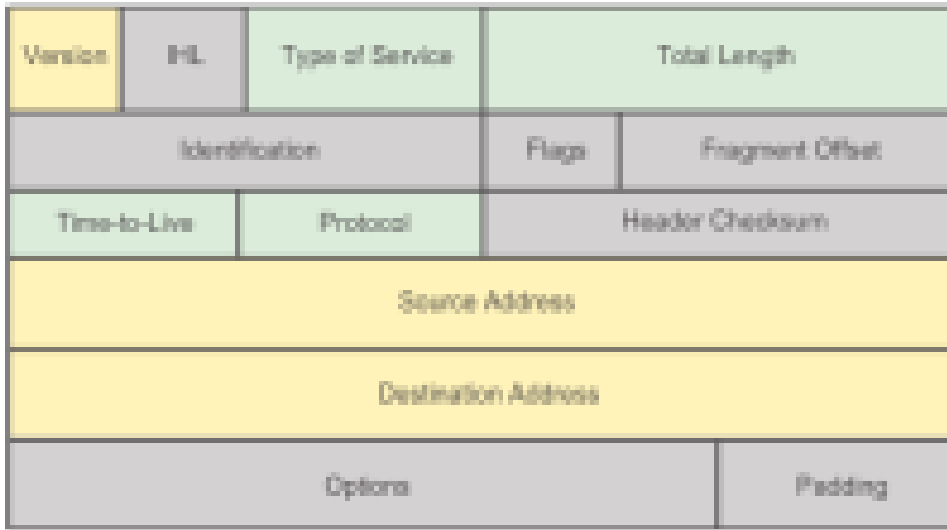
Legend

-  - Field names kept from IPv4 to IPv6
-  - Name and position changed in IPv6
-  - New field in IPv6

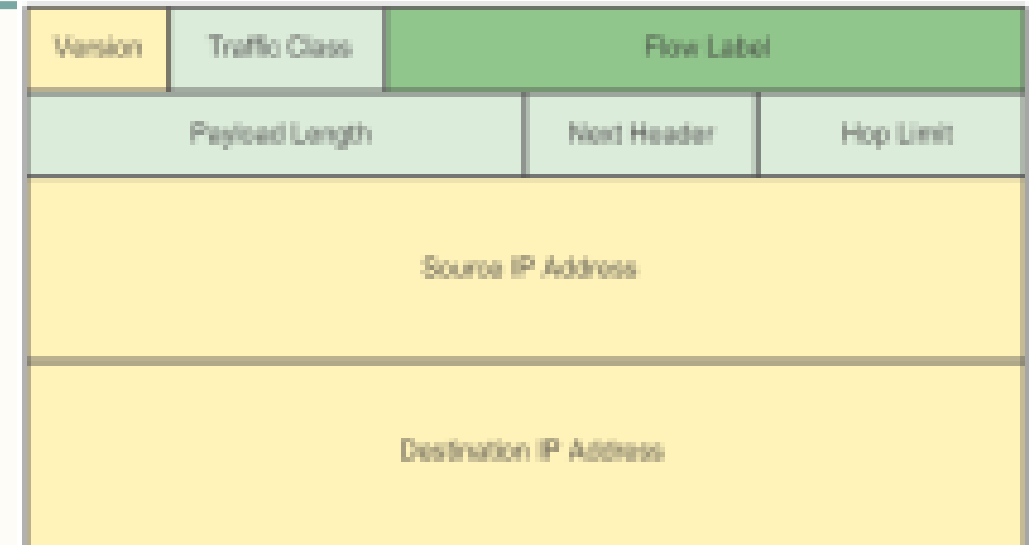


Struktur header IPv4 vs IPv6

IPv4 Header



IPv6 Header



Struktur	IPv4	IPv6
Ukuran minimum	20 octet	40 octet
Ukuran maksimum	60 octet (jika option digunakan)	40 octet
Header fields	12 (diluar option dan padding)	8

Presentasi:





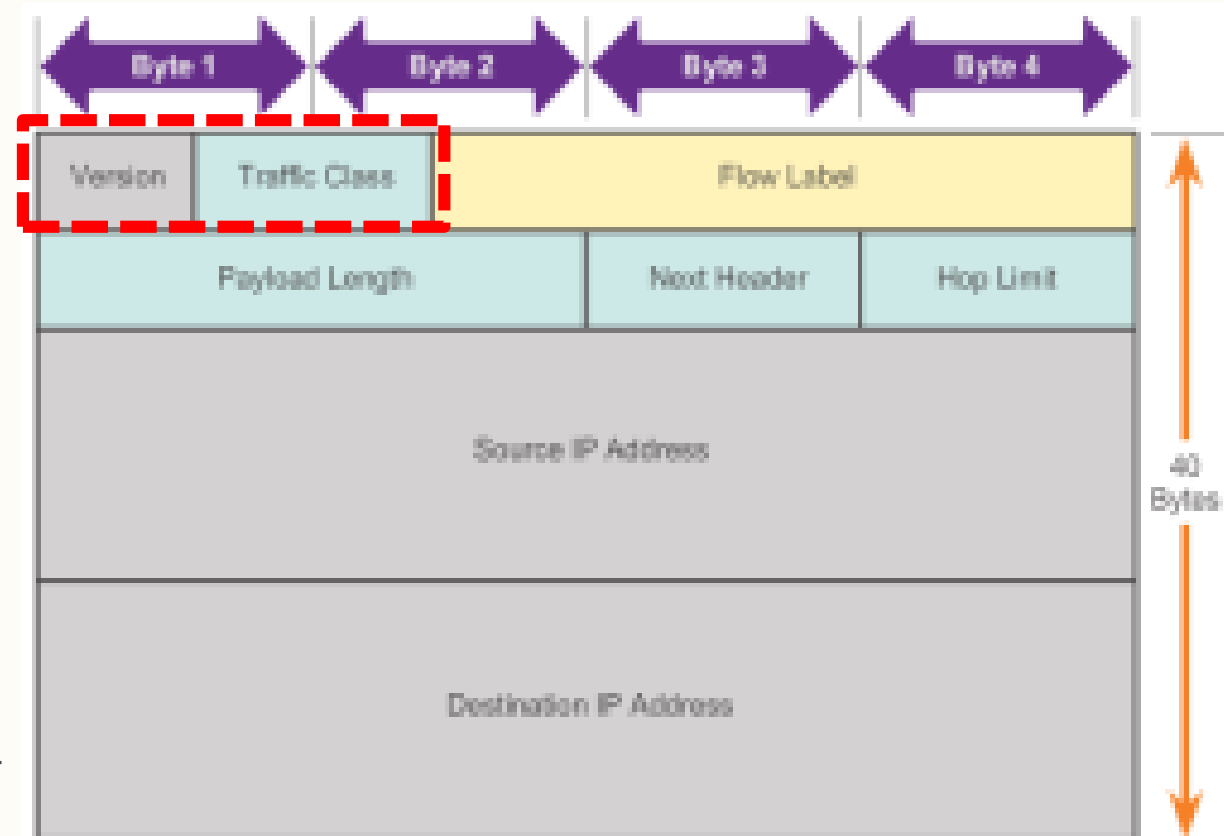
Keunggulan IPv6 dibanding IPv4

- Berikut adalah beberapa keunggulan dari header IPv6 yang lebih sederhana :
 1. Efisiensi routing yang lebih baik untuk performansi dan forwarding-rate scalability
 2. Tidak diperlukan untuk proses checksums (mengurangi beban tugas penerima)
 3. Mekanisme ekstensi header yang lebih sederhana
 4. Flow label memungkinkan pengenalan paket berbasis flow (aliran group) sehingga tidak perlu ada dekapsulasi untuk membaca isi paket dalam menentukan berbagai macam flow data → QoS



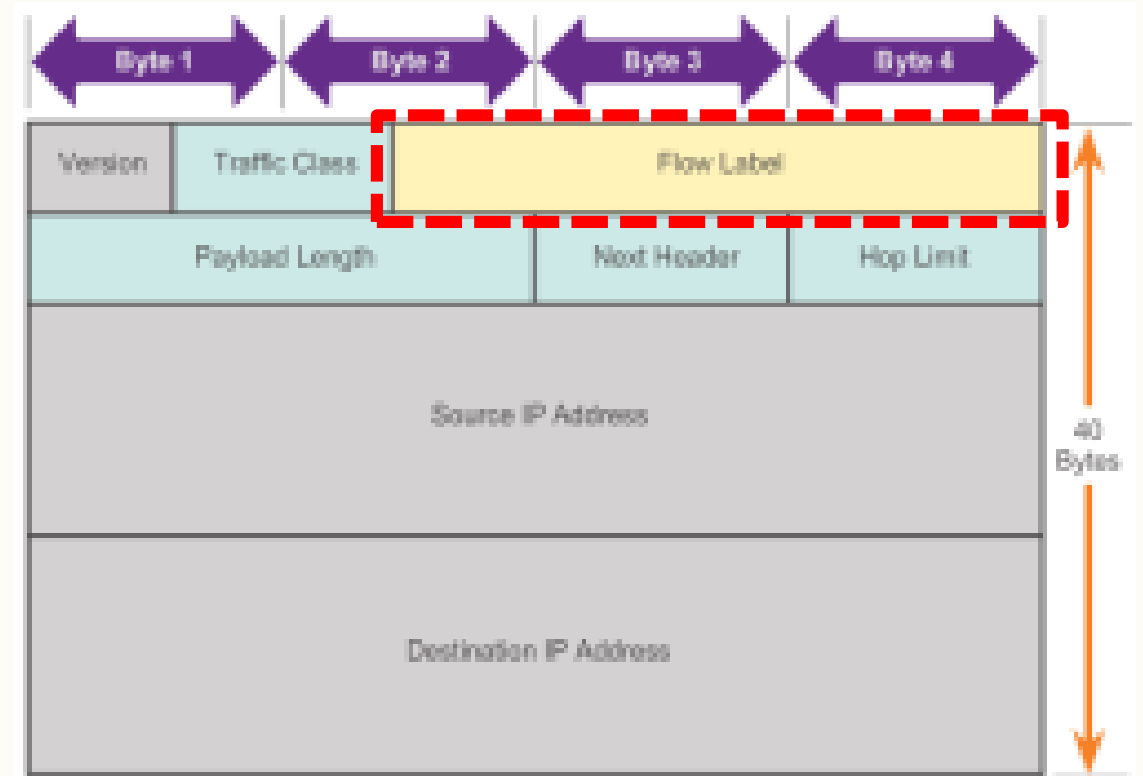
Struktur IPv6

- Version
 - Ukuran : 4 bit biner
 - Fungsi: mengidentifikasi versi dari paket IP
 - Nilai untuk IPV6 selalu 0110
- Traffic Class
 - Ukuran: 8 bit biner
 - Fungsi : sama dengan field Differentiated Services (DS) pada IPv4



Struktur IPv6

- Flow Label
 - Ukuran : 20 bit biner
 - Fungsi: menampung nilai label yang digunakan untuk mengidentifikasi kelompok flow dari paket tersebut.
 - Paket yang tidak termasuk dalam sebuah flow akan memiliki nilai 0
 - Paket dengan flow label (selain nol) dan ip address sumber yang sama akan diarahkan oleh router IPv6 menggunakan sumber daya yang sama (rute yang sama)
 - Dengan rute yang sama, maka paket tidak perlu diurutkan ulang
 - Manajemen flow membutuhkan informasi tambahan yang diatur dengan control protocol seperti the RSVP (Resource reSerVation Protocol). (diluar cakupan materi ini

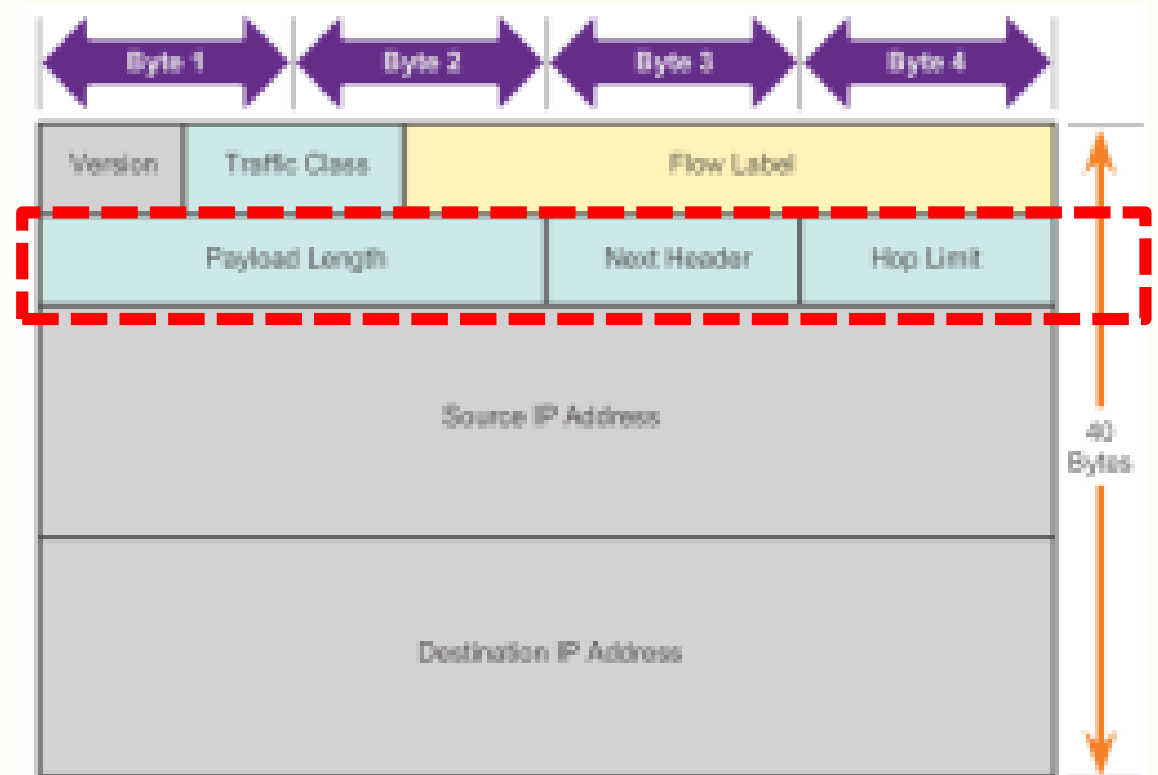


Struktur IPv6

- Payload Length
 - Ukuran : 16 bit biner
 - Fungsi: menampung besar (ukuran) paket tersebut.
 - Satuan dalam byte

- Next Header
 - Ukuran : 8 bit biner
 - Fungsi : mengidentifikasi tipe protokol yang ada pada payload, juga digunakan jika ada tambahan (extension header)

- Hop Limit
 - Ukuran : 8 bit biner
 - Fungsi : menyatakan umur maksimum sebuah paket. Berkurang setiap bertemu satu router.

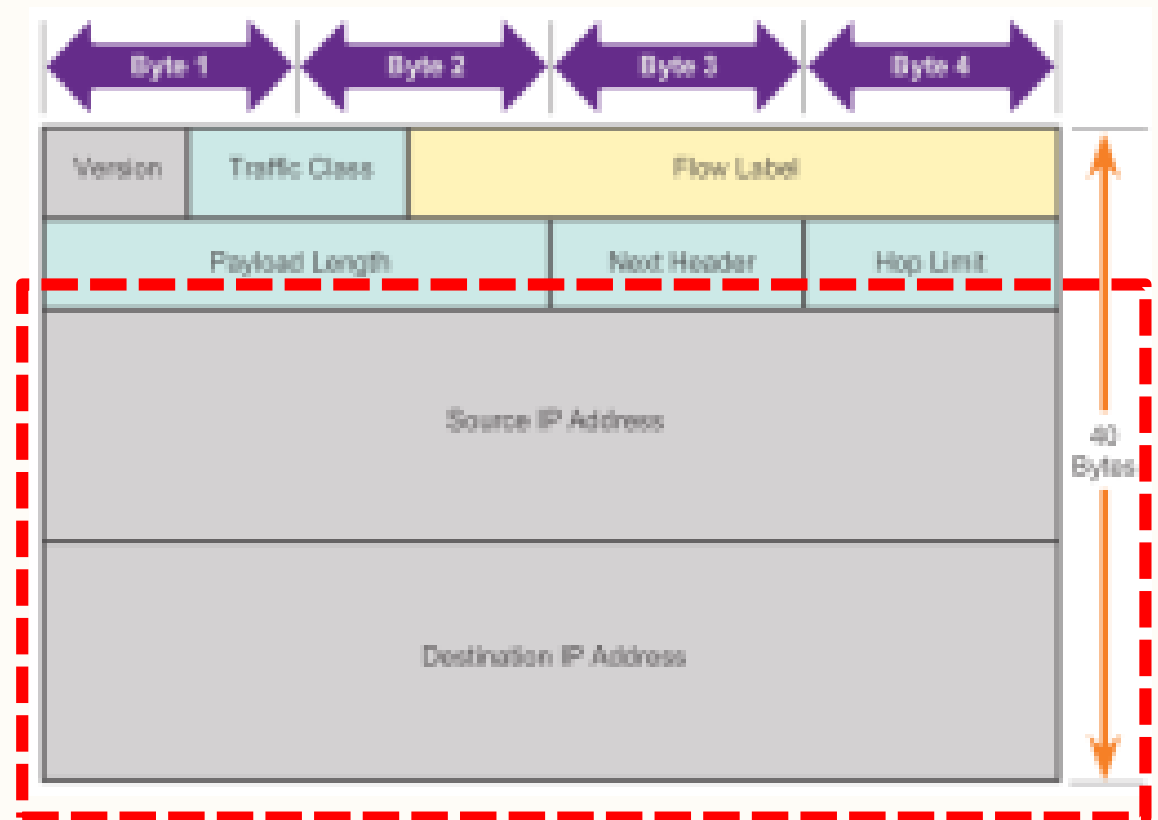


Struktur IPv6

- Source IP address
 - Ukuran : 128 bit biner
 - Fungsi: identifier alamat pengirim

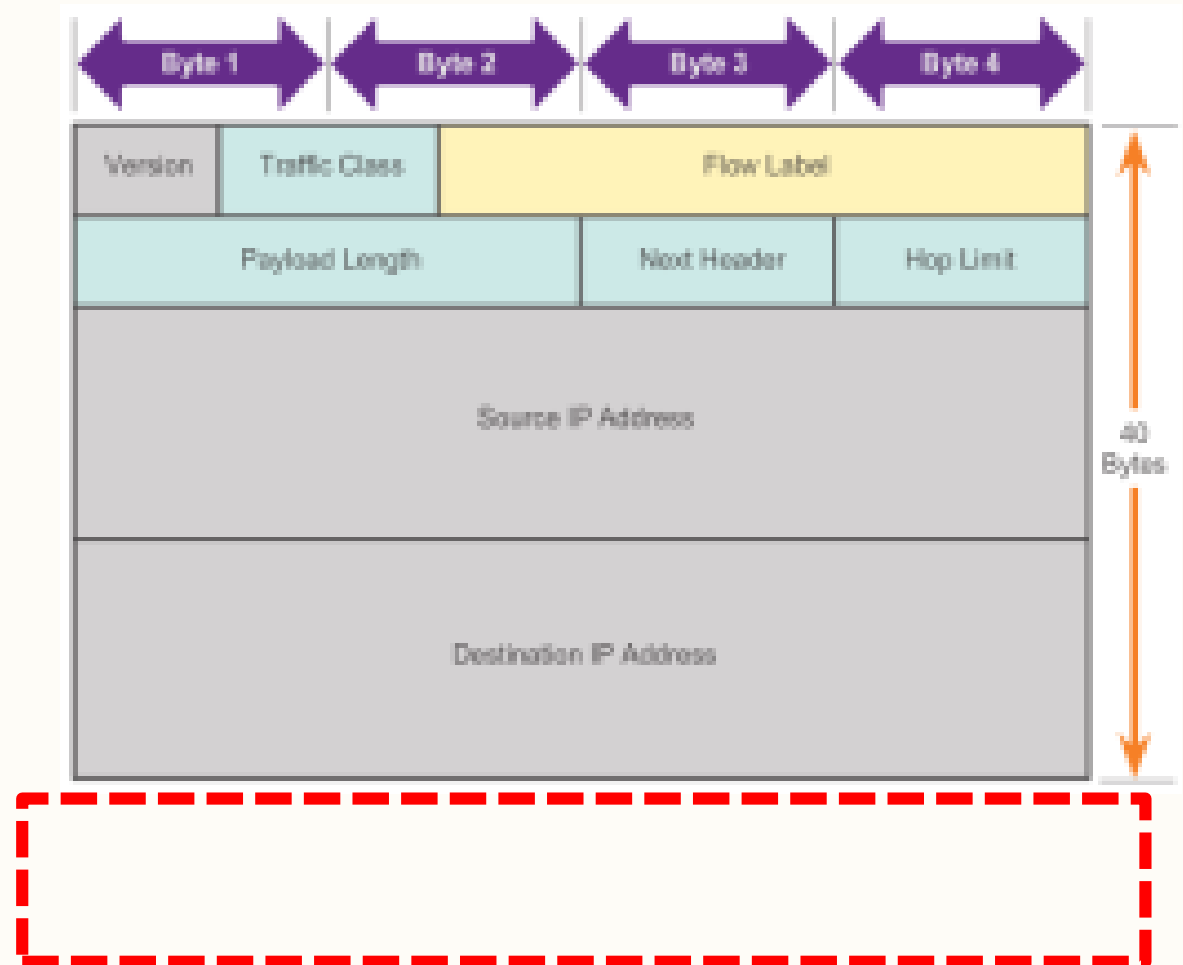
- Destination IP address
 - Ukuran : 128 bit biner
 - Fungsi: identifier alamat penerima

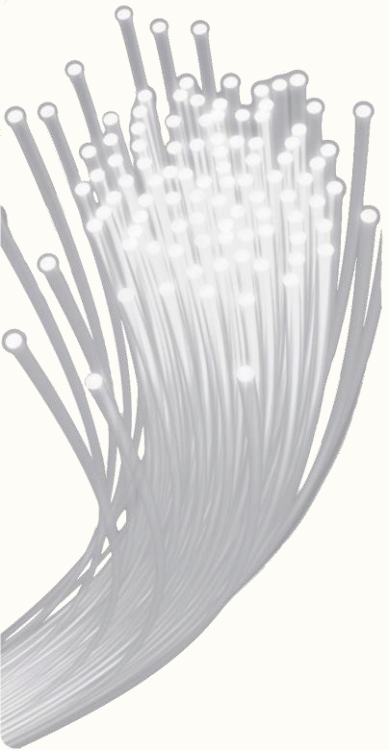
- Untuk konsumsi manusia, alamat sumber dan tujuan pada IPv6 dapat ditampilkan dalam hexadesimal



Struktur IPv6

- Selain field header standar tersebut, sebuah paket IPv6 dapat diberikan extension header (EH) yang diletakkan antara header standar dengan payload.
- EH dapat digunakan pada fragmentasi, keamanan, dll

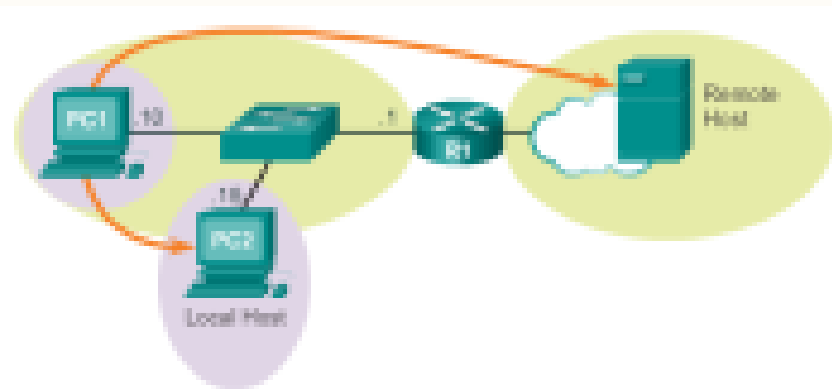




Routing

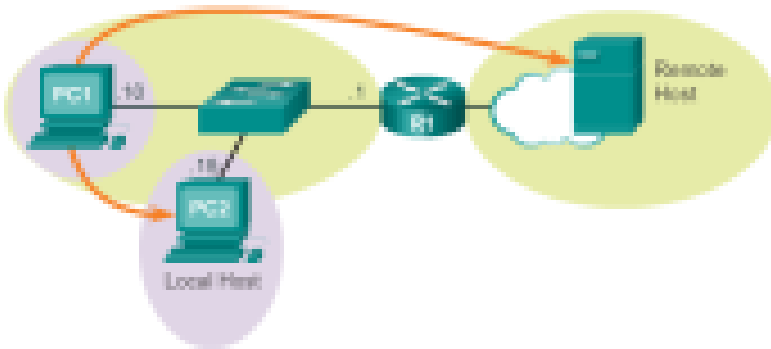
Routing- Host forwarding decision

- Peran dari network layer adalah memungkinkan proses mengarahkan paket dalam perjalanannya dari sumber ke tujuan.
- Sebuah host dapat mengirimkan paket ke :
 1. Dirinya sendiri
ini disebut juga loopback address
pada IPv4 tersedia network 127.0.0.0/8 untuk keperluan loopback
 2. Local host
host pada network yang sama dengan host pengirim
 3. Remote host
host yang berada pada network yang berbeda dari host pengirim



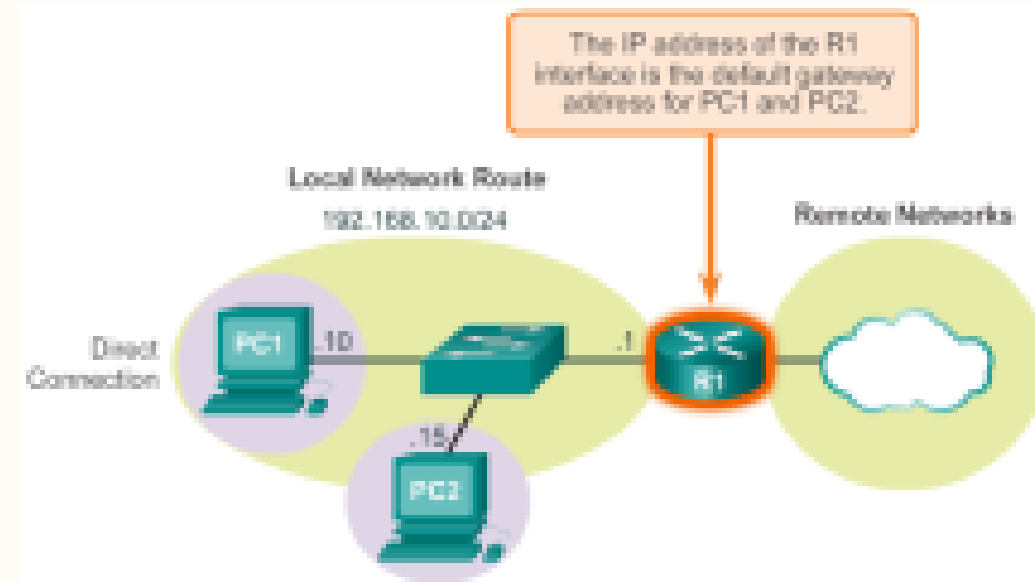
Routing- Host forwarding decision

- Penentuan apakah sebuah paket dikirim ke local host atau remote host berdasarkan alamat IP dan subnet mask dari perangkat tujuan.
- Pada network kecil, umumnya semua perangkat terhubung ke sebuah switch, atau Access Point yang sama, dan memiliki alamat network yang sama, dalam kondisi ini tidak diperlukan router
- Jika perlu menghubungi host pada network lain, maka diperlukan router sebagai penjembaran antar network (atau antar media).
- Router yang terhubung pada local network akan disebut sebagai default gateway bagi perangkat end-devices yang memanfaatkan layanan router tersebut.



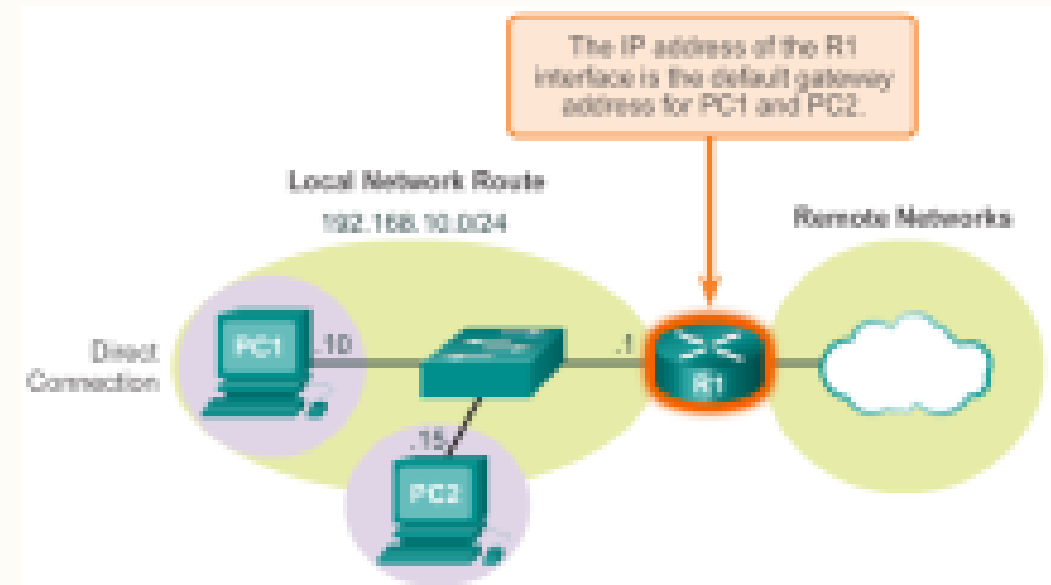
Routing-how hosts route

- Alamat IP dari interface R1 yang mengarah ke local network berfungsi sebagai default gateway bagi hosts yang ada pada network tersebut.
- Jika PC1 mengirimkan paket ke PC2, maka tidak memerlukan default gateway.
- Jika ada host yang ingin mengirimkan paket keluar dari network nya, maka default gateway diperlukan.
- Ini karena host tidak menyimpan informasi routing selain dari local network yang terhubung



Routing-how hosts route

- host tetap harus memiliki mekanisme untuk mengetahui apakah paket yang akan dikirim perlu melalui gateway atau tidak.
- Setiap host akan mempertahankan routing local table yang digunakan untuk menjamin paket dikirimkan dengan benar.





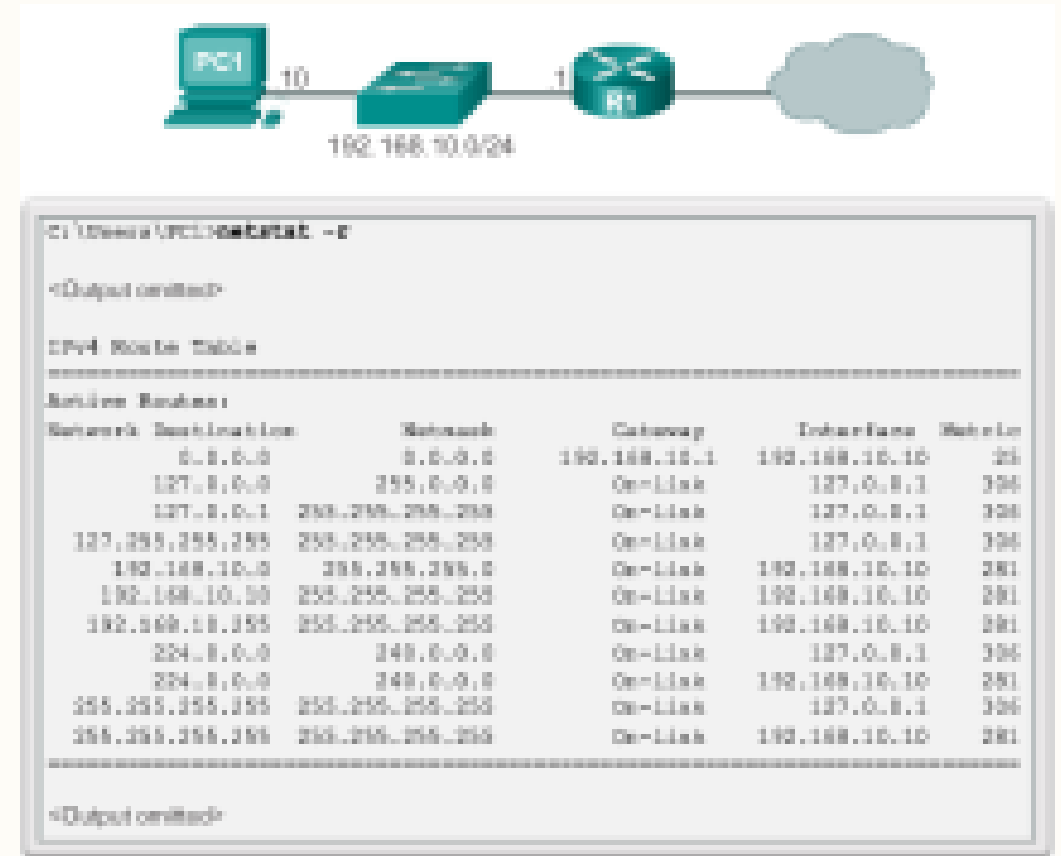
1. Direct connection

- Local routing table host umumnya berisi:
 1. Direct connection
Adalah rute ke interface loopback
 2. Local network route
Network local yang secara otomatis diisi ke routing table saat host terhubung
 3. Local default route
adalah alamat IP dari gateway (router yang terhubung jaringan luar), informasinya bisa didapatkan secara manual (dientry user), atau dari protokol DHCP.



Melihat routing table

- Pada PC dengan sistem operasi Windows, dapat digunakan perintah
- “netstat -r”
- Terdiri dari 3 bagian
 1. Interface list
daftar MAC address dan nomor interface
 2. IPv4 route table
routing table protokol IPv4
 3. IPv6 route table
routing table protokol IPv6 (jika aktif)





Informasi pada routing table HOST

-
- Setiap routing table pada umumnya memiliki informasi berikut:
 1. Network destination
alamat network tujuan
 2. Netmask
nilai subnet mask dari network tujuan
 3. Gateway
alamat ip gateway untuk mengirimkan paket, jika network adalah local (terhubung langsung) maka akan bertuliskan “on-link”
 4. Interface
daftar alamat interface fisik yang digunakan
 5. Metric
biaya untuk setiap rute, dan digunakan untuk menentukan rute terbaik (jika tersedia lebih dari satu rute untuk network tujuan yang sama)



Informasi pada routing table HOST

- Berikut adalah contoh pembahasan output routing table host
- 0.0.0.0 adalah rute local default, semua paket yang tidak memenuhi alamat lain yang terdaftar akan melalui rute ini, tercantum alamat ip gateway
- 127.0.0.0 – 127.255.255.255 adalah alamat loopback

```
C:\Users\PC1> netstat -r

<Output omitted>

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway           Interface         Metric
-----
0.0.0.0                    0.0.0.0          192.168.10.1      192.168.10.10     25
127.0.0.0                  255.0.0.0        On-link           127.0.0.1         306
127.0.0.1                  255.255.255.255 On-link           127.0.0.1         306
127.255.255.255           255.255.255.255 On-link           127.0.0.1         306
192.168.10.0              255.255.255.0    On-link           192.168.10.10     281
192.168.10.10             255.255.255.255 On-link           192.168.10.10     281
192.168.10.255           255.255.255.255 On-link           192.168.10.10     281
224.0.0.0                 240.0.0.0        On-link           127.0.0.1         306
224.0.0.0                 240.0.0.0        On-link           192.168.10.10     281
255.255.255.255           255.255.255.255 On-link           127.0.0.1         306
255.255.255.255           255.255.255.255 On-link           192.168.10.10     281
=====

<Output omitted>
```

Informasi pada routing table HOST

- 192.168.10.0 – 192.168.10.255
adalah network local yang terhubung langsung
- 192.168.10.0
alamat network
- 192.168.10.10
alamat host itu sendiri
- 192.168.10.255
alamat broadcast network
- 224.0.0.0
untuk pengalamatan multicast
- 255.255.255.255 (ada 2)
 - Alamat broadcast untul loopback
 - Alamat broadcast untuk local net

```
C:\Users\PC1> netstat -r

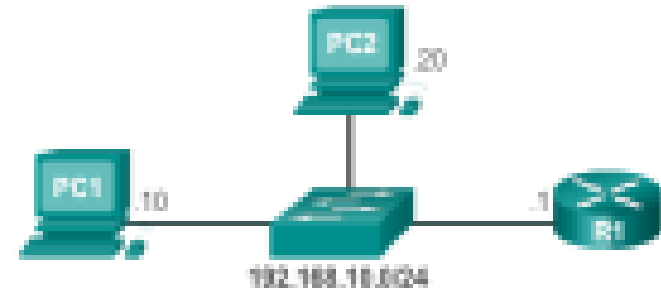
<Output omitted>

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
-----
0.0.0.0                    0.0.0.0          192.168.10.1    192.168.10.10    25
127.0.0.0                  255.0.0.0        On-link         127.0.0.1        306
127.0.0.1                  255.255.255.255 On-link         127.0.0.1        306
127.255.255.255           255.255.255.255 On-link         127.0.0.1        306
192.168.10.0               255.255.255.0    On-link         192.168.10.10    281
192.168.10.10              255.255.255.255 On-link         192.168.10.10    281
192.168.10.255             255.255.255.255 On-link         192.168.10.10    281
224.0.0.0                  240.0.0.0        On-link         127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link         192.168.10.10    281
255.255.255.255            255.255.255.255 On-link         127.0.0.1        306
255.255.255.255            255.255.255.255 On-link         192.168.10.10    281
=====

<Output omitted>
```

How a host routes

- Sebagai contoh, jika PC 1 ingin mengirim paket pada 192.168.10.20
1. Mencari ke routing table
 2. Ditemukan bahwa 192.168.10.0 adalah sejangaran “On link”
 3. PC1 akan mengirim paket menggunakan local interface 192.168.10.10



```
C:\Users\PC1> netstat -r
```

```
<Output omitted>
```

```
IPv4 Route Table
```

```
=====
```

```
Active Routes:
```

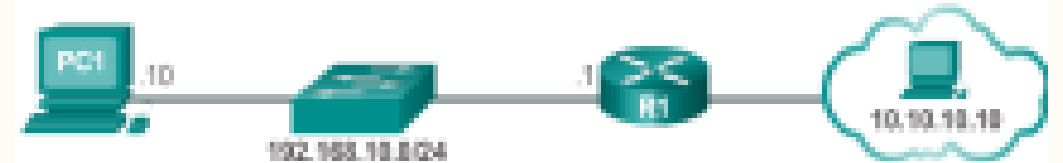
Network	Destination	Network	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.10.1	192.168.10.10	25
	127.0.0.0	255.0.0.0	On-Link	127.0.0.1	306
	127.0.0.1	255.255.255.255	On-Link	127.0.0.1	306
	127.255.255.255	255.255.255.255	On-Link	127.0.0.1	306
	192.168.10.0	255.255.255.0	On-Link	192.168.10.10	281
	192.168.10.10	255.255.255.255	On-Link	192.168.10.10	281
	192.168.10.255	255.255.255.255	On-Link	192.168.10.10	281
	224.0.0.0	240.0.0.0	On-Link	127.0.0.1	306
	224.0.0.0	240.0.0.0	On-Link	192.168.10.10	281
	255.255.255.255	255.255.255.255	On-Link	127.0.0.1	306
	255.255.255.255	255.255.255.255	On-Link	192.168.10.10	281

```
<Output omitted>
```



How a host routes

- Sebagai contoh, jika PC 1 ingin mengirim paket ke 10.10.10.10
 1. Mencari ke routing table
 2. Tidak ditemukan kecocokan
 3. Default route (0.0.0.0) digunakan, dengan tujuan 192.168.10.1
 4. PC1 akan mengirim paket menggunakan local interface 192.168.10.10 dengan menyertakan informasi gateway pada paket



```
C:\Users\PC1> netstat -r
<Output omitted>
IP: Route Table
=====
Active Routes:
Network Destination        Network      Gateway         Interface      Metric
0.0.0.0                    0.0.0.0     192.168.10.1   192.168.10.10   30
127.0.0.0                  127.0.0.0   127.0.0.1     127.0.0.1       306
127.0.0.1                  127.0.0.1   127.0.0.1     127.0.0.1       306
192.168.10.0                192.168.10.0 192.168.10.1 192.168.10.10   300
192.168.10.10              192.168.10.10 192.168.10.1 192.168.10.10   300
192.168.10.255             192.168.10.255 192.168.10.1 192.168.10.10   300
224.0.0.0                  224.0.0.0   224.0.0.0     224.0.0.0       306
255.255.255.255           255.255.255.255 255.255.255.255 255.255.255.255 306
255.255.255.255           255.255.255.255 255.255.255.255 255.255.255.255 306
<Output omitted>
```



Routing table host IPv6

- Pada routing table IPv6, informasi berikut tersedia :
1. If
adalah interface number dapat berupa Ethernet atau wifi, atau Bluetooth
 2. Metric
biaya tiap rute
 3. Network Destination
daftar jaringan yang dapat dihubungi
 4. Gateway
Daftar alamat yang digunakan local host untuk memforward paket, On link menunjukkan terhubung langsung

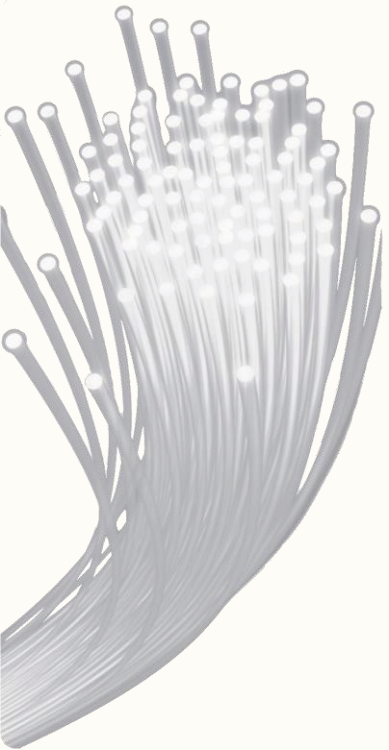
```
fe80::2c30:3071:e718:a926/128
2001:db8:9c38:953c:2c30:3071:e718:a926/128
```

```
C:\Users\PC1> netstat -r
<Output omitted>

IPv6 Route Table
-----
Active Routes:
  If Metric Network Destination      Gateway
  --  -  -  -  -  -
  14     58  ::0
  1     306  ::1/128
  14     58  2001::/32
  14     306  2001:0:9d38:953c:2c30:3071:e718:a926/128
                                           On-link
  15     281  fe80::/64
  14     306  fe80::/64
  14     306  fe80::2c30:3071:e718:a926/128
                                           On-link
  15     281  fe80::b1ae:ca4a:a117:271d/128
                                           On-link
  1     306  ::0::/8
  14     306  ::0::/8
  15     281  ::0::/8
-----
<Output omitted>
```



Activity - Identify Elements of a Host Routing Table Entry

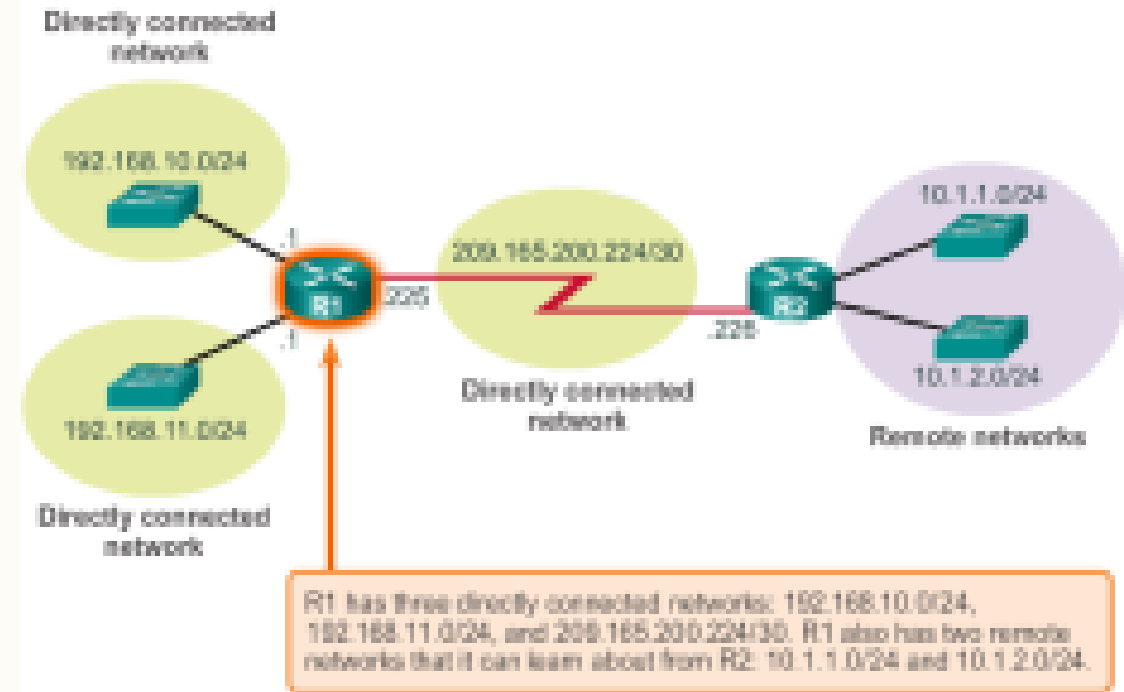


```
C:\Documents and Settings\ciaco>netstat -r
Route Table
-----
<Output omitted>
      A           B           C           D           E
-----
Active Routes:
Network Destination    Netmask          Gateway          Interface        Metric
0.0.0.0                0.0.0.0          192.168.1.1     192.168.1.100    20
127.0.0.0              255.0.0.0        127.0.0.1       127.0.0.1        1
192.168.1.0            255.255.255.0   192.168.1.100   192.168.1.100    20
192.168.1.100         255.255.255.255 127.0.0.1       127.0.0.1        20
```

	A	B	C	D	E
1. The physical interface IP address used to send the packet to the gateway.					
2. The route cost - lower numbers are best.					
3. The reachable networks available.					
4. The network address is found in this column.					
5. Used to determine the network portion of an IP address.					
6. The IP address of the device that can send the packet beyond the local network.					

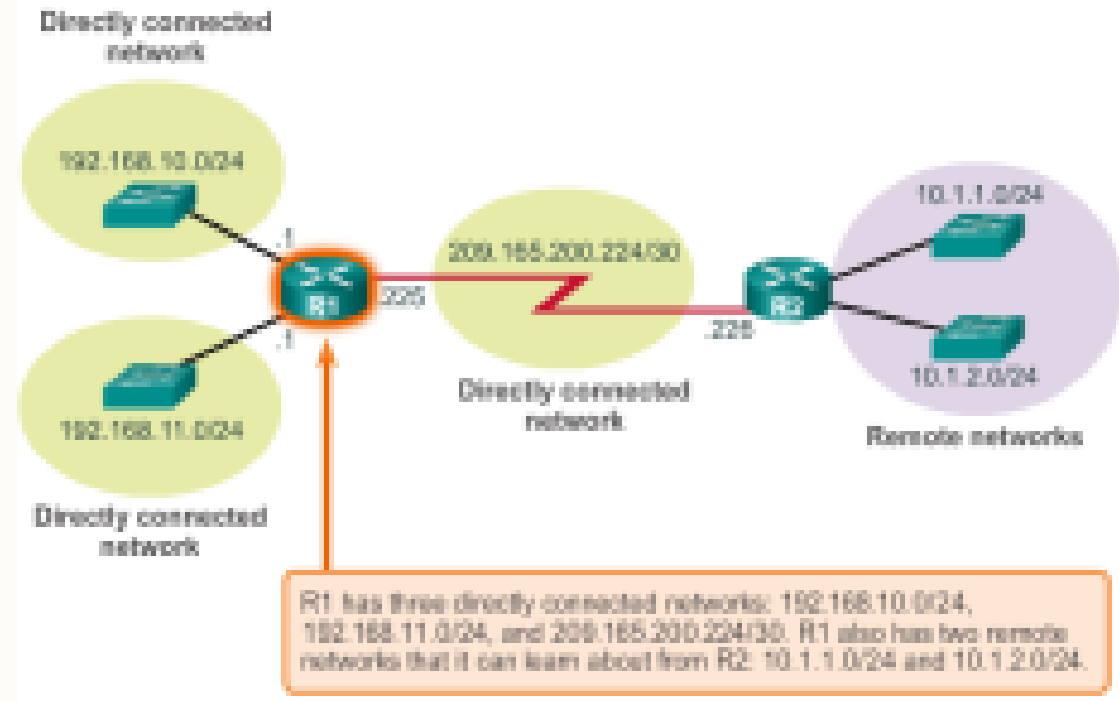
Router Packet Forwarding Decision

- Saat sebuah host mengirimkan paket ke host lain, dia akan menggunakan routing table untuk menentukan kemana paket akan dikirim. Jika network tujuan adalah remote network, maka paket diforward ke perangkat gateway.
- Apa yang terjadi saat paket dikirim ke perangkat gateway? Router akan mencari routing table nya untuk menentukan kemana paket akan di forward

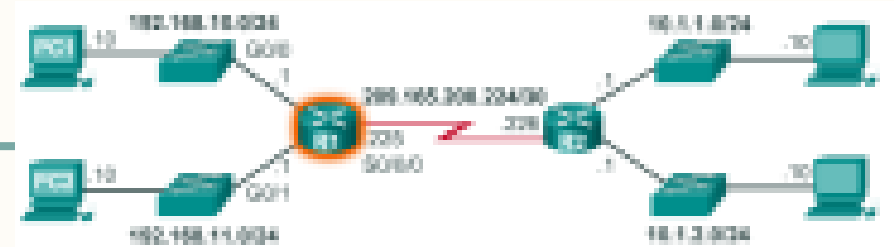


Router Packet Forwarding Decision

- Routing table pada router akan menyimpan informasi terkait:
 1. Jaringan terhubung langsung rute ini berasal dari interface router yang aktif dan terhubung, setiap ip interface adalah bagian dari sebuah jaringan terhubung langsung
 2. Jaringan Remote rute ini adalah berasal dari jaringan yang tidak terhubung langsung (misalnya terhubung di router tetangga). Rute pada kategori ini dapat dimasukkan secara manual atau secara dinamis menggunakan routing protocol



IPv4 Router Routing Table



- Sebuah routing table pada router memiliki informasi:
 1. Destination network
 2. Metric biaya sebuah jalur
 3. Gateway pintu keluar untuk forward paket
- Pada router cisco, perintah untuk menampilkan routing table ipv4 adalah :
- “show ip route”

```

R1#show ip route
Codes: C - local, I - Internet, E - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF area inter
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, I - IGP
       S - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, Ia - IS-IS
           area 0
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

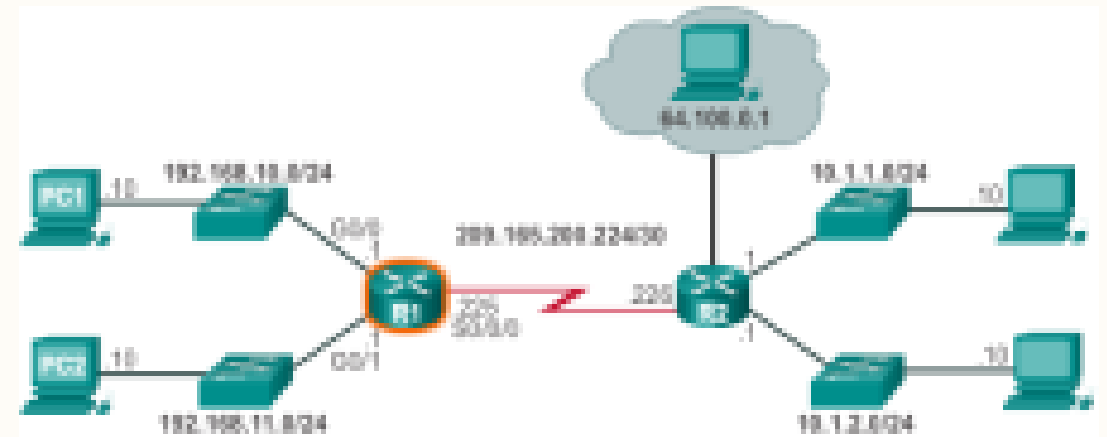
Gateway of last resort is not set

10.0.0.0 is variably subnetted, 2 subnets, 2 masks
O    10.1.1.0/24 [10/178112] via 209.149.108.128, 00:00:00,
Serial0/0/0
O    10.1.2.0/24 [10/178112] via 209.149.108.128, 00:00:00,
Serial0/0/0
192.168.16.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.16.0/24 is directly connected, GigabitEthernet0/1
L    192.168.16.1/32 is directly connected, GigabitEthernet0/1
192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.11.0/24 is directly connected, GigabitEthernet0/1
L    192.168.11.1/32 is directly connected, GigabitEthernet0/1
209.149.108.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.149.108.0/24 is directly connected, Serial0/0/0
L    209.149.108.128/32 is directly connected, Serial0/0/0
R1#
    
```



Directly Connected Routing Table Entries

- Dua baris rute otomatis dibuat saat sebuah interface router dikonfigurasi dengan ip address dan subnet mask.
- Pada routing table router, kita dapat melihat informasi jaringan terhubung langsung dengan memilah tiap baris menjadi 3 bagian:
 1. Bagian A adalah informasi bagaimana router mengetahui rute tersebut
 2. Bagian B adalah alamat network tujuan dan bagaimana terhubung
 3. Bagian C adalah pintu keluar untuk mencapai jaringan tersebut



A	B	C
C	192.168.10.0/24 is directly connected,	GigabitEthernet0/0
S	192.168.10.1/32 is directly connected,	GigabitEthernet0/0

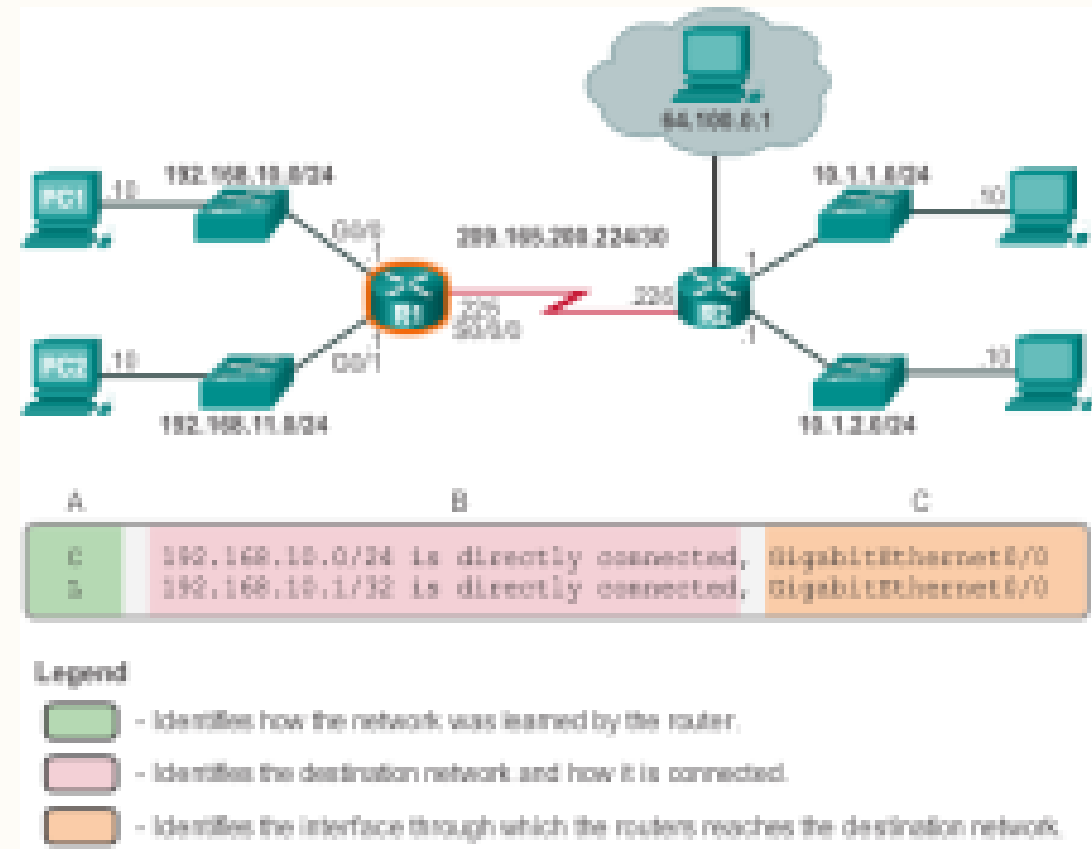
Legend

- Identifies how the network was learned by the router.
- Identifies the destination network and how it is connected.
- Identifies the interface through which the routers reaches the destination network.



Directly Connected Routing Table Entries

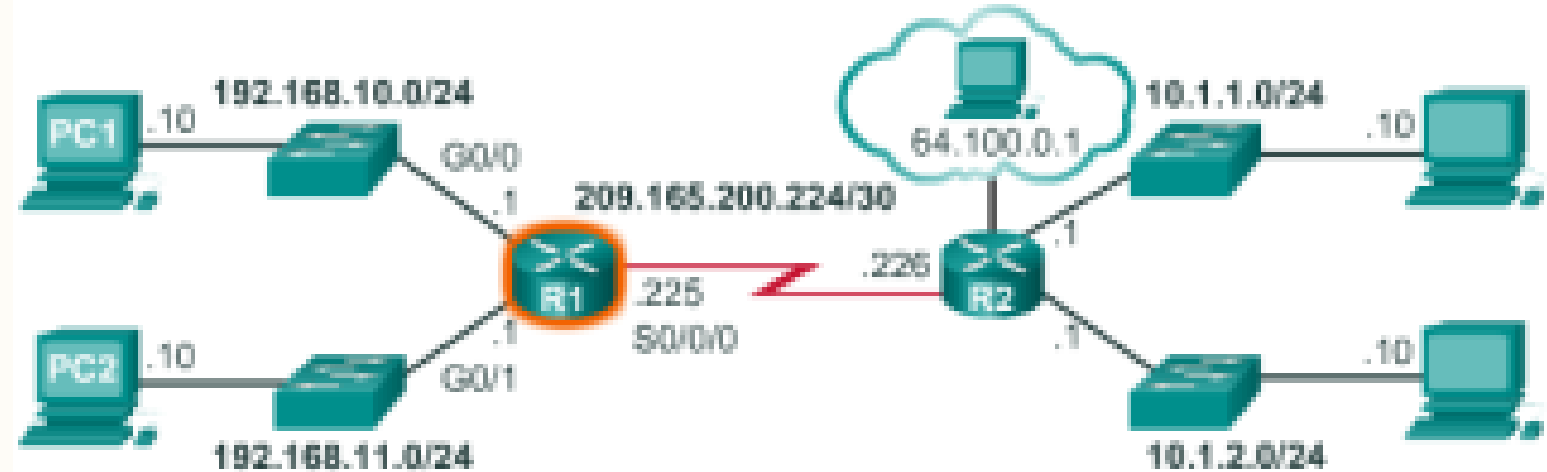
- Kode C artinya jaringan terhubung langsung
- Kode L artinya alamat IP interface itu sendiri
- Baik kode C maupun L akan dinyatakan terhubung langsung pada kolom B
- Pada kolom C akan tertera nama interface yang terhubung ke rute tersebut.



Remote Network Routing Table Entries

73





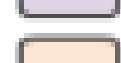


- Untuk memahami rute jaringan remote pada routing table router, kita akan membaginya menjadi 7 kolom:



```
D 10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
```

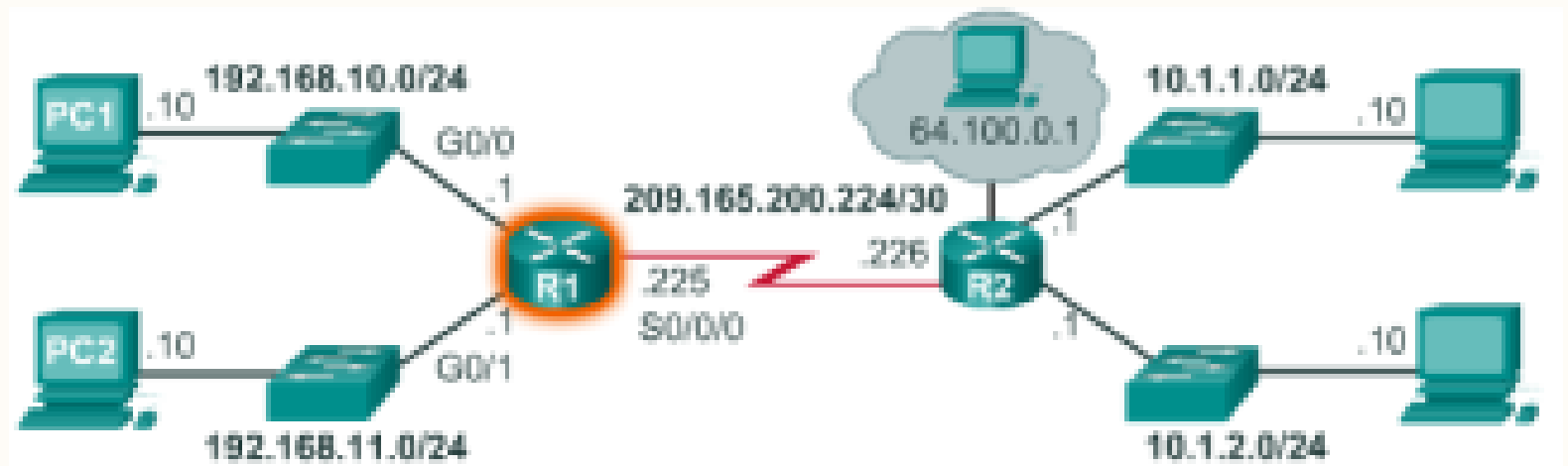
Route source
 Destination network
 Administrative distance
 Metric
 Next-hop
 Route timestamp
 Outgoing interface

Legend

-  Mengidentifikasi sumber info
-  Mengidentifikasi alamat network tujuan
-  Mengidentifikasi biaya administrative
-  Mengidentifikasi metric (biaya) rute tersebut
-  Mengidentifikasi nexthop IP address
-  Mengidentifikasi waktu yang berlalu sejak kabar terakhir
-  Mengidentifikasi nama interface keluar

Next hop address

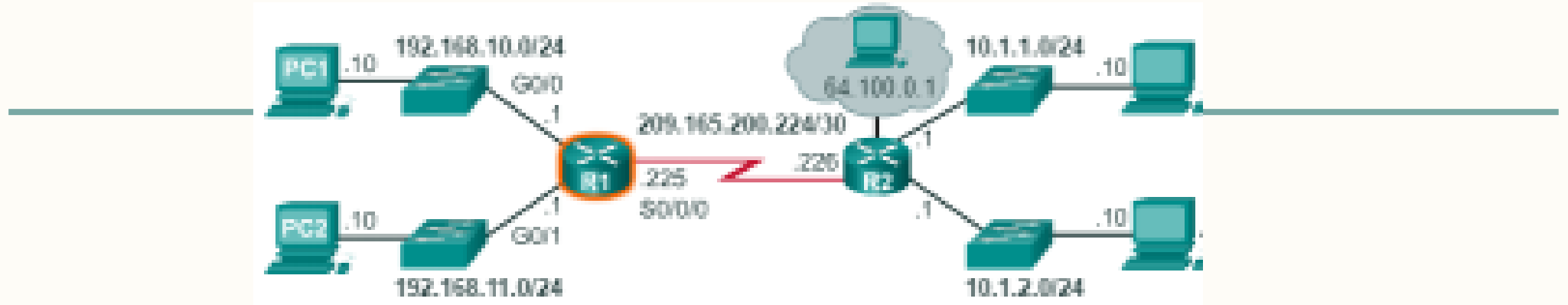
- Next hop address adalah alamat ip dari perangkat berikutnya yang akan memproses paket tersebut



```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D    10.1.1.0/24 [90/2170112] via 209.145.200.226, 00:00:05,
    Serial10/0/0
D    10.1.2.0/24 [90/2170112] via 209.145.200.226, 00:00:05,
    Serial10/0/0
```



Sample Router IPv4 Routing Table



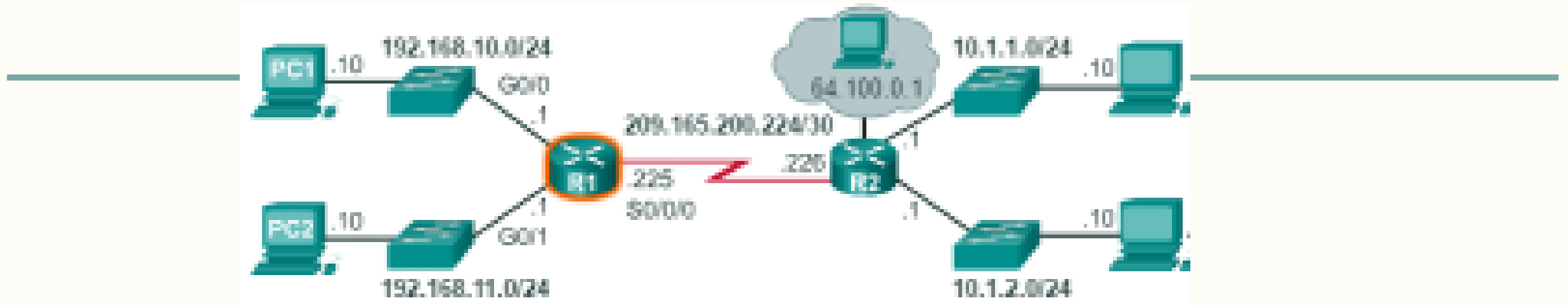
```

D    10.1.1.0/24 [90/2170112] via 209.165.200.226, 01:13:55,
      Serial0/0/0
D    10.1.2.0/24 [90/2170112] via 209.165.200.226, 01:13:55,
      Serial0/0/0
    192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C    192.168.10.0/24 is directly connected, GigabitEthernet0/0
L    192.168.10.1/32 is directly connected, GigabitEthernet0/0
    192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C    192.168.11.0/24 is directly connected, GigabitEthernet0/1
L    192.168.11.1/32 is directly connected, GigabitEthernet0/1
    209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C    209.165.200.224/30 is directly connected, Serial0/0/0
L    209.165.200.225/32 is directly connected, Serial0/0/0
  
```





Sample Router IPv4 Routing Table

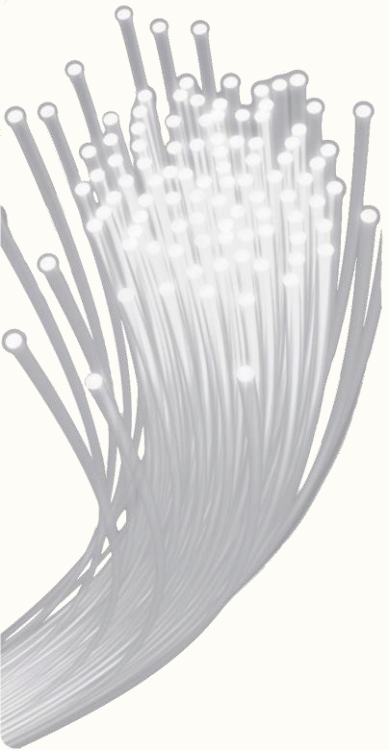


```

192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C    192.168.10.0/24 is directly connected, GigabitEthernet0/0
L    192.168.10.1/32 is directly connected, GigabitEthernet0/0
192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C    192.168.11.0/24 is directly connected, GigabitEthernet0/1
L    192.168.11.1/32 is directly connected, GigabitEthernet0/1
209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C    209.165.200.224/30 is directly connected, Serial0/0/0
L    209.165.200.225/32 is directly connected, Serial0/0/0
S*  0.0.0.0/0 [1/0] via 209.165.200.226

```







Kesimpulan

- Pada pertemuan ini telah kita bahas tentang:
 - Network layer
 - Karakteristik IPv4
- Pada pertemuan mendatang akan dilaksanakan UTS





Akhir pertemuan 7

- Terima kasih
- Materi ini bisa di-download melalui link yang tersedia di :
- <https://sites.google.com/site/jokocc>

