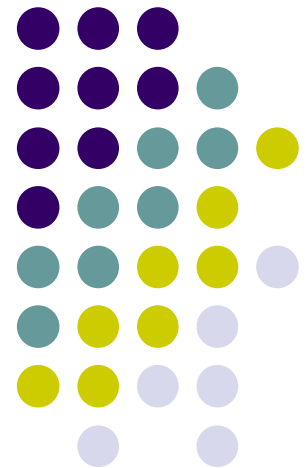
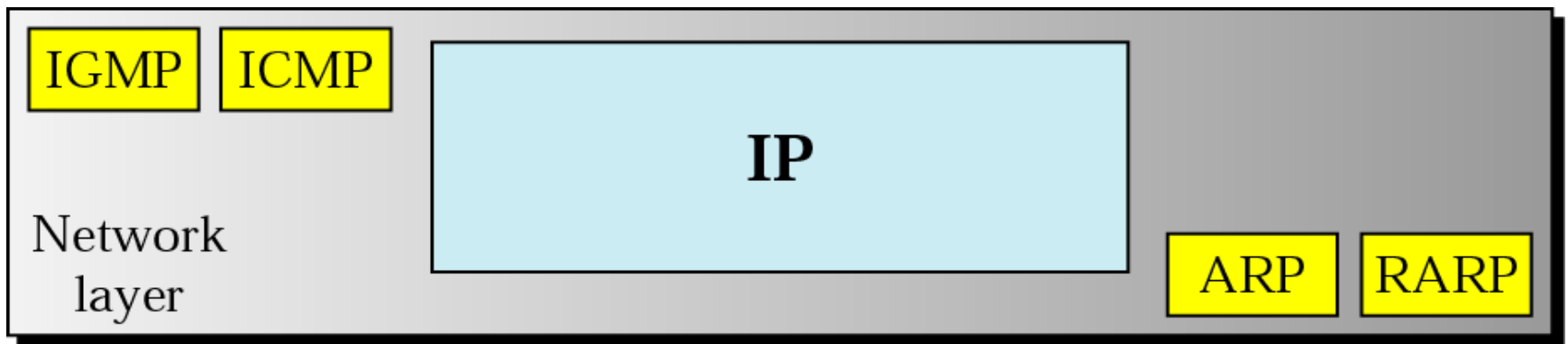
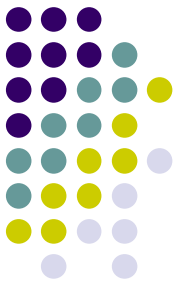


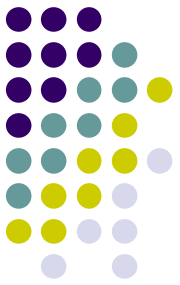
Protokol-protokol lapisan jaringan

Address Resolution Protocol (ARP)
Reverse Address Resolution Protocol (RARP)
Internet Protocol (IP)
Internet Control Message Protocol (ICMP)
Internet Group Management Protocol (IGMP)
Bootstrap Protocol (BOOTP)
Dynamic Host Configuration Protocol (DHCP)



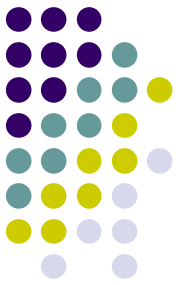
Protokol-protokol Jaringan





Protokol-protokol Jaringan

- Protokol utama dalam lapisan jaringan adalah IP, yang bertanggung jawab untuk *host-to-host delivery* suatu datagram dari sumber ke tujuan. Namun IP membutuhkan layanan dari protokol-protokol lainnya
 - ARP digunakan untuk menemukan MAC (physical) address next hop
 - ICMP digunakan untuk menangani kondisi yang tidak normal selama pengiriman datagram, seperti terjadinya error
 - IGMP digunakan untuk multicasting delivery, satu sumber banyak penerima



ARP

- Dalam pengiriman paket ke host atau router membutuhkan dua tingkat pengalamatan: IP dan MAC.
- Dibutuhkan protokol yang mampu memetakan alamat IP dengan alamat MAC yang sesuai

ARP

mapping: static mapping



Static mapping adalah membuat tabel yang menghubungkan alamat IP dengan alamat MAC.

Tabel ini disimpan di dalam mesin pada jaringan.

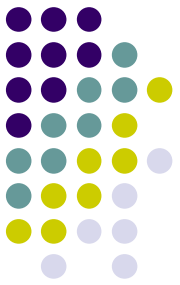
Mesin yang mengetahui alamat IP tetapi tidak mengetahui alamat MAC akan melihat pada tabel ini

Ada beberapa kelemahan dikarenakan perubahan alamat MAC, seperti:

- Pergantian network card pada suatu mesin akan merubah alamat MAC
- Dalam beberapa LAN, seperti LocalTalk (Apple), alamat MAC akan berubah setiap kali mesin dinyalakan
- Mobile computer yang dapat berpindah dari jaringan fisik satu ke lainnya

ARP

mapping: dynamic mapping



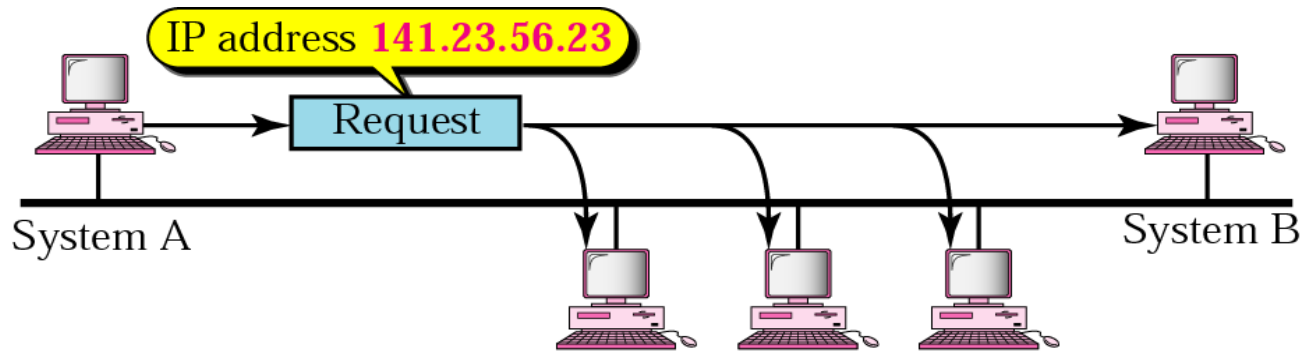
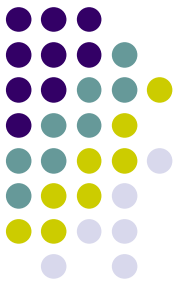
Dalam dynamic mapping setiap kali mesin mengetahui satu dari dua alamat, maka akan menggunakan protokol untuk menemukan yang lainnya

Dua protokol yang digunakan untuk melakukan dynamic mapping adalah

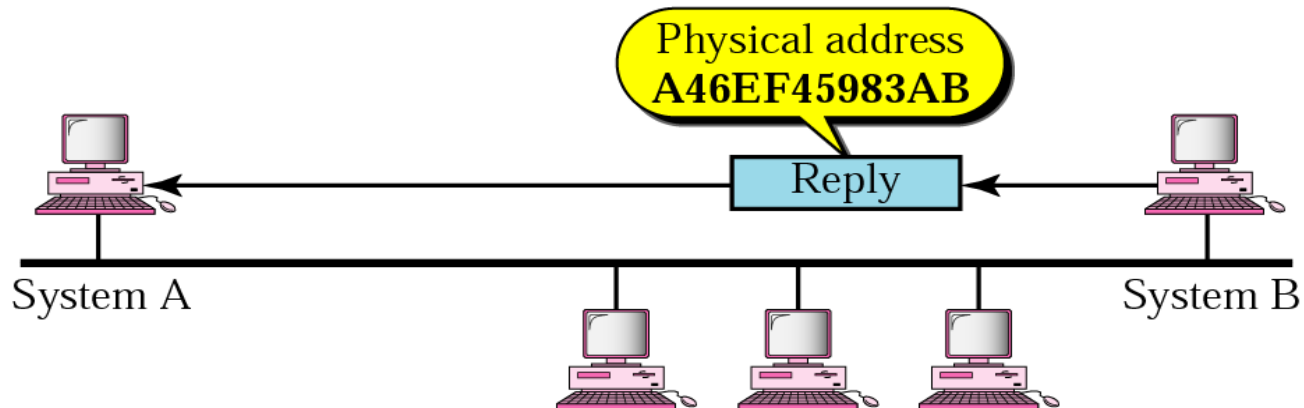
- Address Resolution Protocol (ARP)
 - Reverse Address Resolution Protocol (RARP)
- ARP digunakan untuk memetakan alamat IP ke alamat MAC
 - RARP digunakan untuk memetakan alamat MAC ke alamat IP

ARP

operation



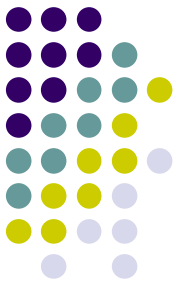
a. ARP request is broadcast



b. ARP reply is unicast

ARP

operation



Dikarenakan pengirim tidak mengetahui alamat fisik (MAC) penerima, ARP request dilakukan secara ***broadcast*** pada jaringan.
ARP reply dilakukan secara ***unicast***

ARP

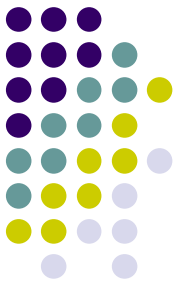
format packet



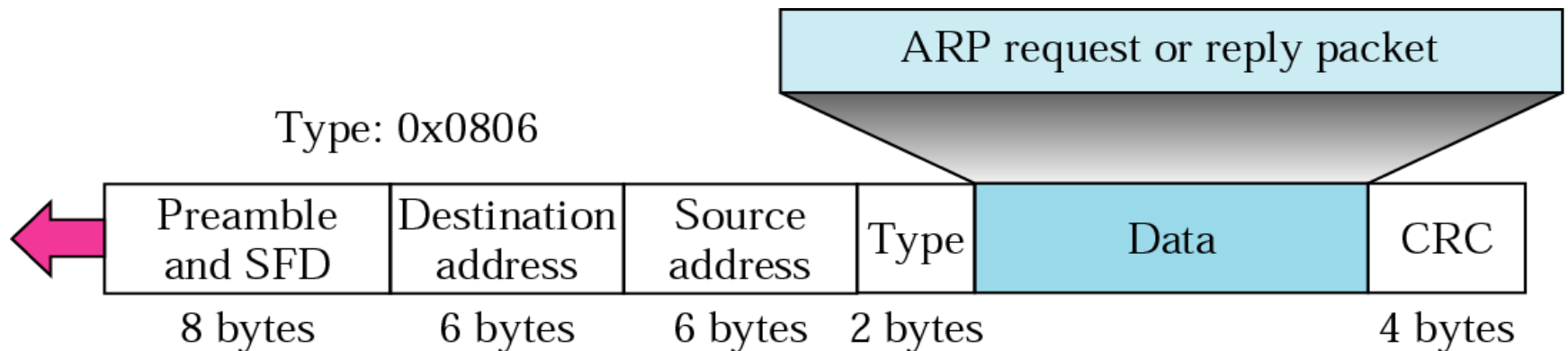
Hardware Type		Protocol Type
Hardware length	Protocol length	Operation Request 1, Reply 2
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled in a request)		
Target protocol address (For example, 4 bytes for IP)		

ARP

encapsulation

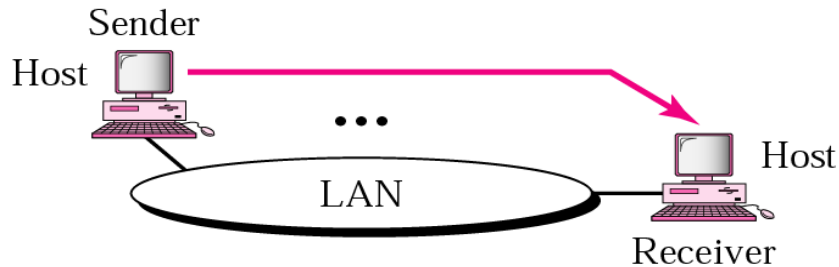


- Paket ARP dienkapsulasi langsung kedalam frame data-link.
- Contoh: paket ARP dienkapsulasi ke dalam frame Ethernet, isi dari tipe mengindikasikan data yang dibawa oleh frame adalah paket ARP

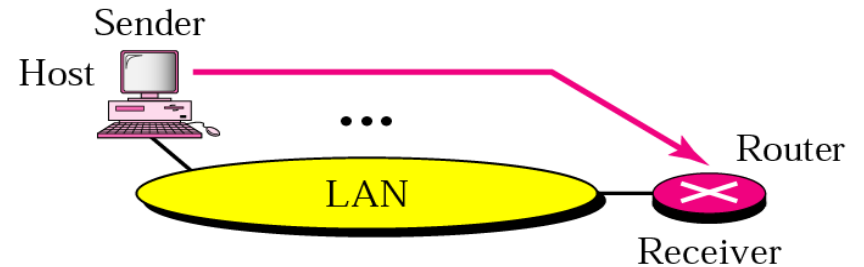


ARP

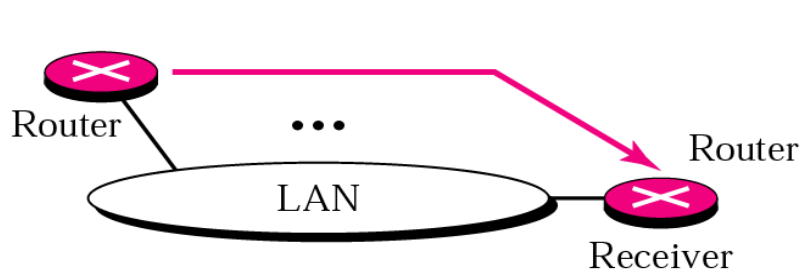
empat kasus berbeda penggunaan ARP



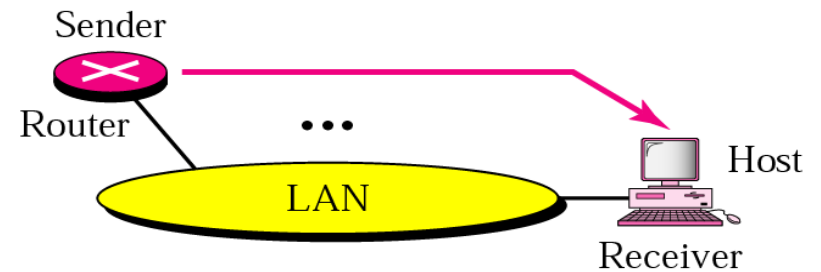
Case 1. A host has a packet to send to another host on the same network.



Case 2. A host wants to send a packet to another host on another network. It must first be delivered to the appropriate router.



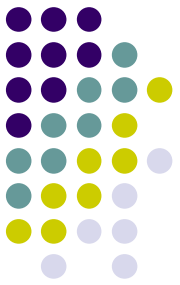
Case 3. A router receives a packet to be sent to a host on another network. It must first be delivered to the appropriate router.



Case 4. A router receives a packet to be sent to a host on the same network.

ARP

empat kasus berbeda penggunaan ARP



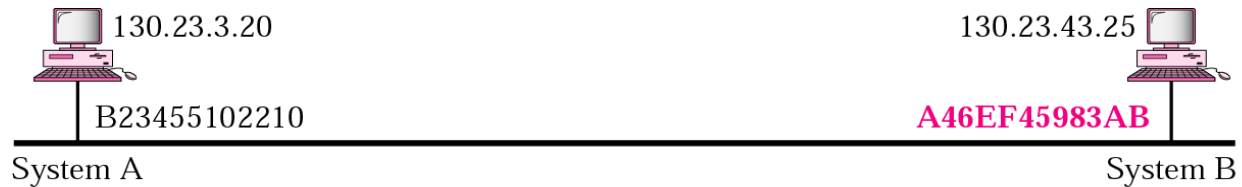
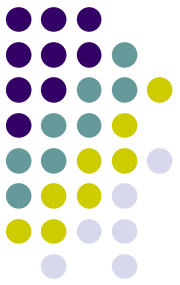
- Pengirim adalah host yang ingin mengirimkan paket ke host lainnya dalam satu jaringan
- Pengirim adalah host yang ingin mengirimkan paket ke host lainnya pada jaringan yang lain. Alamat yang dipetakan adalah alamat IP router
- Pengirim adalah router yang menerima datagram yang ditujukan untuk host pada jaringan lainnya. Alamat IP router berikutnya yang dipetakan
- Pengirim adalah router yang menerima datagram yang ditujukan ke host dalam jaringan yang sama. Alamat IP tujuan dari datagram yang akan dipetakan



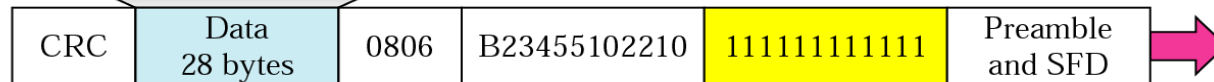
- Suatu host dengan alamat IP 130.23.3.20 dan alamat MAC B23455102210 mempunyai paket yang akan dikirim ke host dengan alamat IP 130.23.43.25 dan alamat MAC A46EF45983AB. Kedua host dalam jaringan Ethernet yang sama. Perhatikan paket ARP request dan reply terenkapsulasi dalam frame Ethernet

ARP

contoh

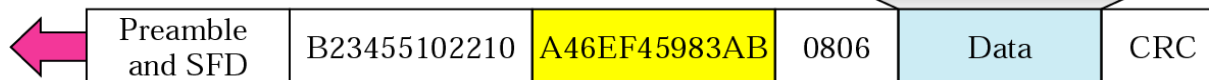


0001		0800
06	04	0001
B23455102210 130.23.3.20 000000000000 130.23.43.25		



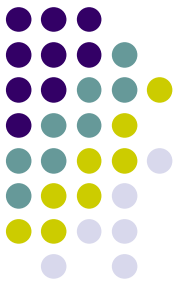
ARP Request (from A to B)

0002		0800
06	04	0002
A46EF45983AB 130.23.43.25 B23455102210 130.23.3.20		



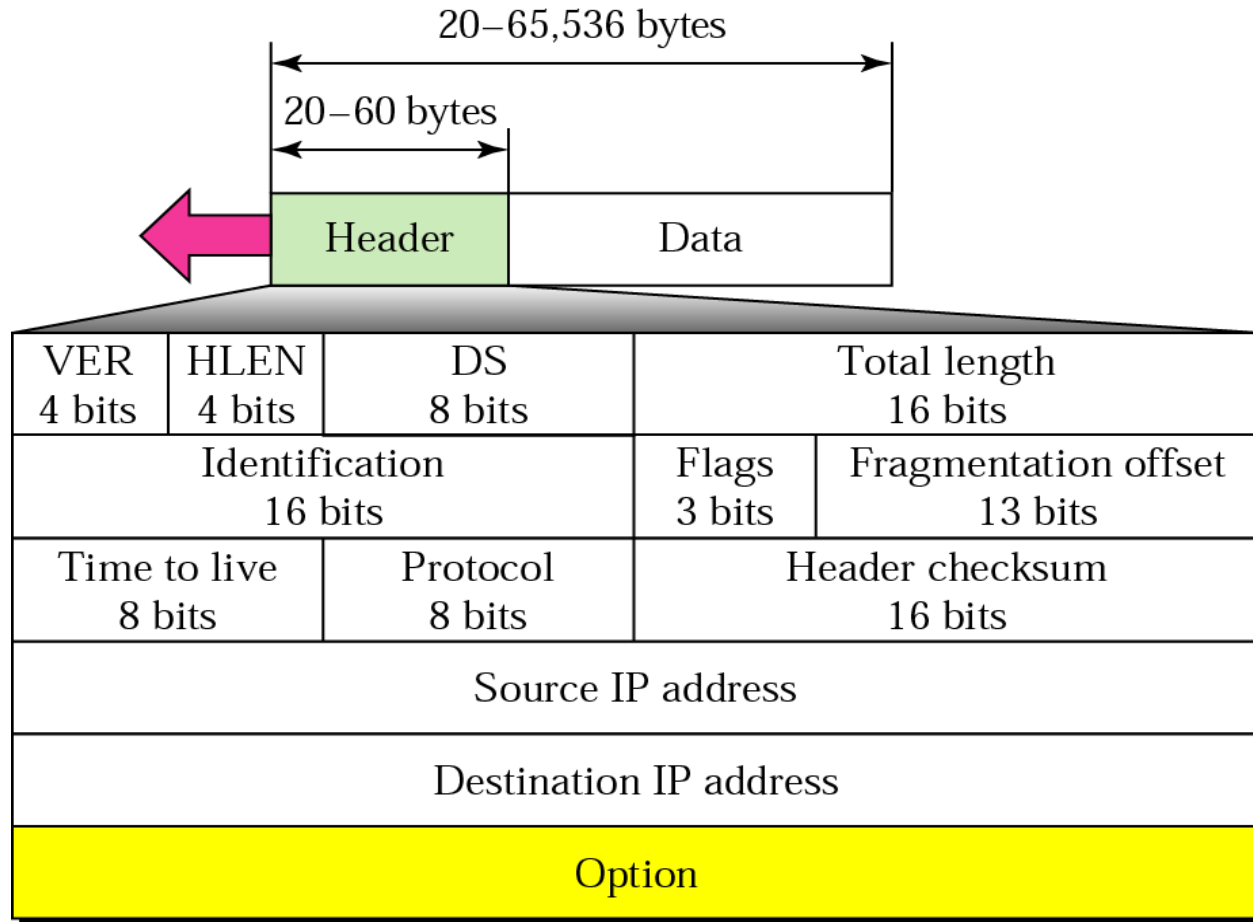
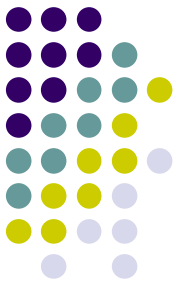
ARP Reply (from B to A)

IP



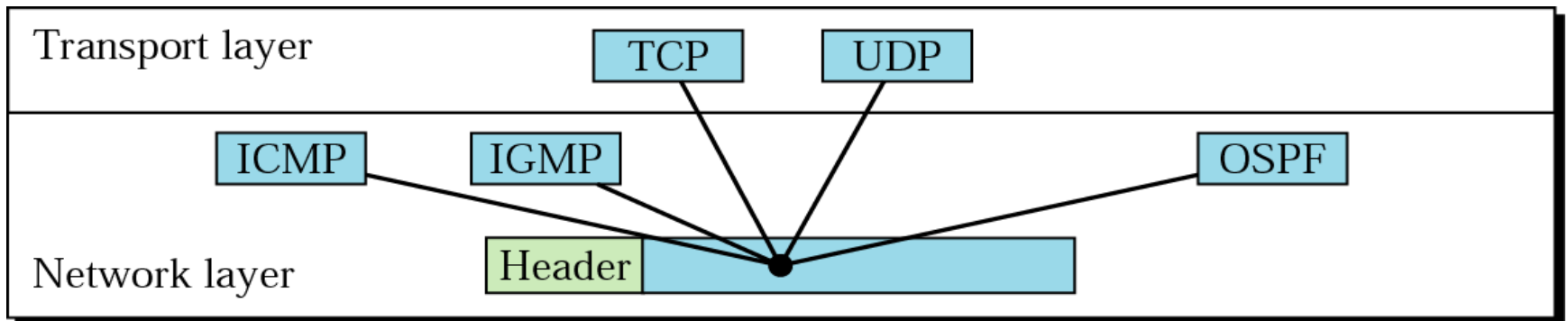
- Adalah protokol datagram connectionless atau unreliable – layanan *best-effort delivery*
- IP hanya menggunakan mekanisme *error detection* dan membuang paket jika terjadi korup

IP datagram



IP

multiplexing



IP

contoh perhitungan checksum



4	5	0	28	
1			0	0
4	17	0		
10.12.14.5				
12.6.7.9				

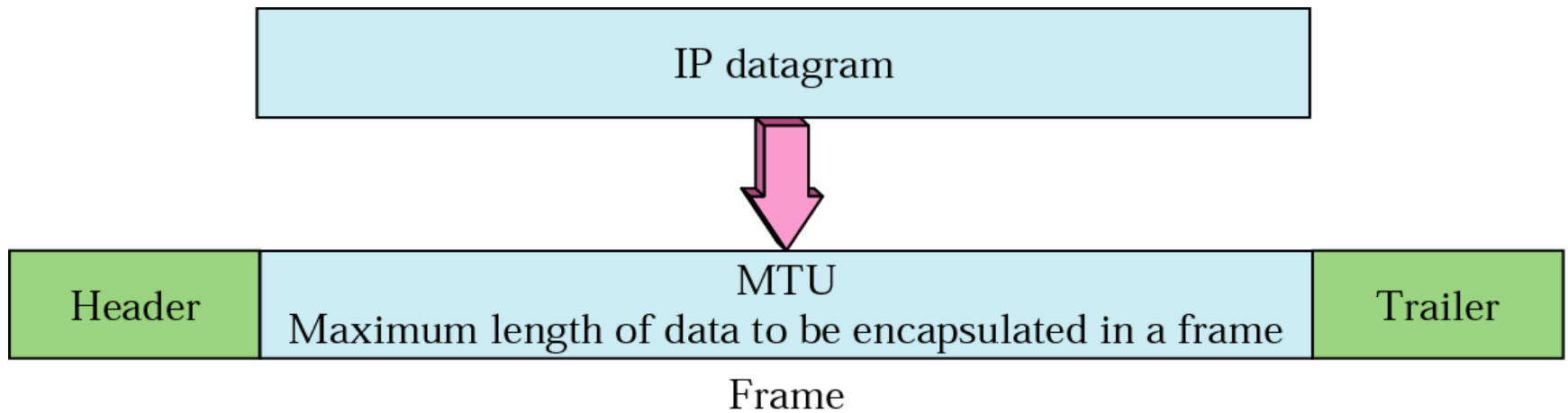
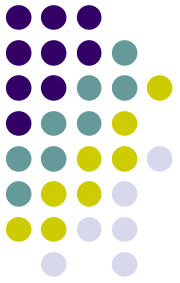
4, 5, and 0	→	0100010100000000
28	→	00000000000011100
1	→	00000000000000001
0 and 0	→	00000000000000000
4 and 17	→	00000100000010001
0	→	00000000000000000
10.12	→	00001010000001100
14.5	→	00001110000000101
12.6	→	00001100000000110
7.9	→	00000111000001001
		<hr/>
Sum	→	0111010001001110
Checksum	→	1000101110110001

IP

contoh perhitungan checksum



- Pengirim akan mengirimkan 4 frame masing-masing 8 bit: 10110011, 10101011, 01011010, 11010101. Carilah checksum dan finalsum! Apakah terdapat error saat pengiriman data?

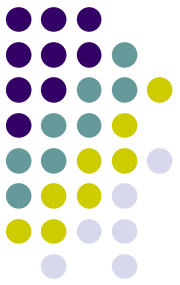


ICMP



- IP tidak punya mekanisme pelaporan-kesalahan atau pembetulan-kesalahan
 - Apa yg terjadi jika terjadi kesalahan?
 - Apa yg terjadi jika datagram dibuang oleh router karena tidak ditemukannya alamat tujuan?
 - Apa yg terjadi jika *time-to-live* bernilai 0?
 - Apa yg terjadi jika seluruh fragment harus dibuang karena penerima tidak menerima secara lengkap seluruh fragmen dalam waktu tertentu?
- IP juga tidak punya mekanisme pengelolaan host dan query
 - Host kadang membutuhkan informasi apakah host atau router sedang hidup atau mati
 - Kadang network manager butuh informasi dari host atau router yang lain

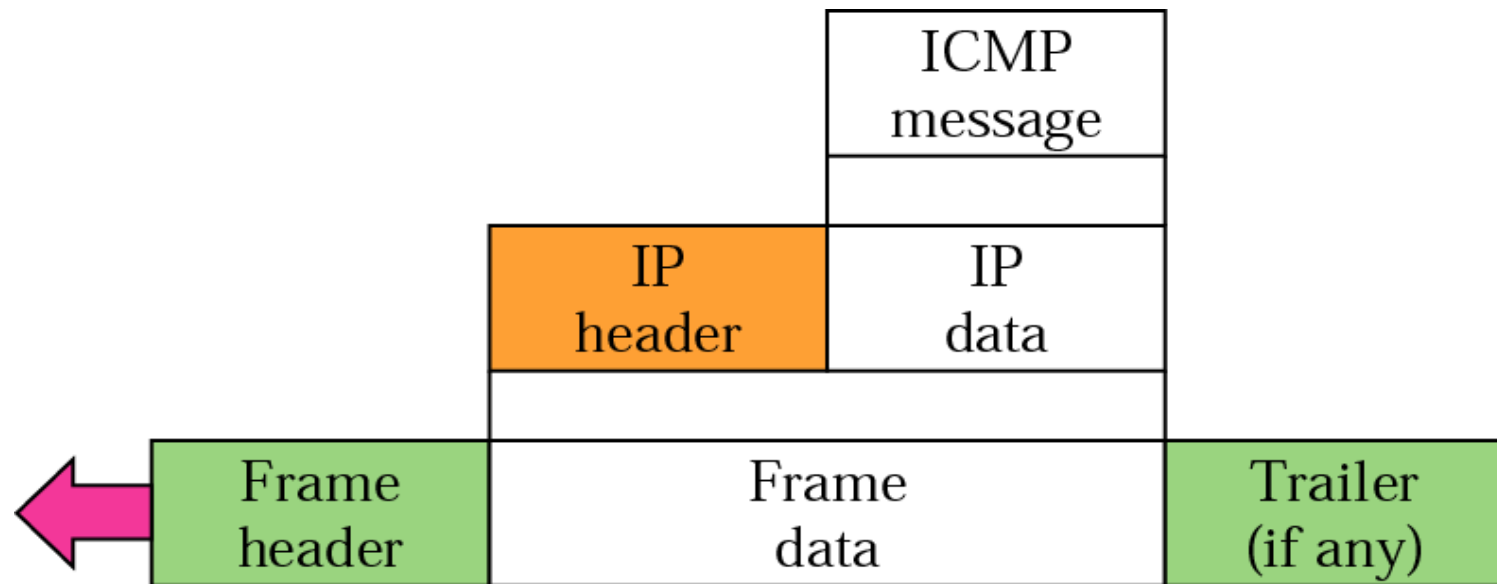
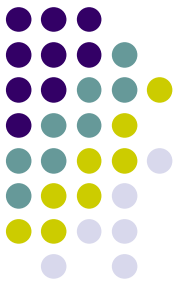
ICMP



- ICMP dirancang untuk memberikan kompensasi atas kedua permasalahan tersebut
- ICMP sendiri adalah protokol lapisan jaringan
- Pesan ICMP tidak langsung dienkapsulasi ke lapisan data-link, tetapi dienkapsulasi didalam datagram IP sebelum dibawa ke lapisan data-link
- Nilai dari isi protokol pada paket IP adalah 1 menandakan data datagram IP adalah ICMP

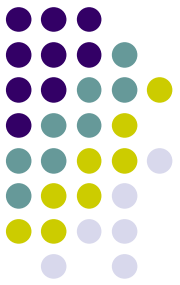
ICMP

ICMP encapsulation



ICMP

Tipe dari pesan ICMP



- Pesan ICMP dibagi dalam dua katagori:
 - *Error-reporting messages*
 - *Query messages*

ICMP

Tipe dari pesan ICMP: error reporting



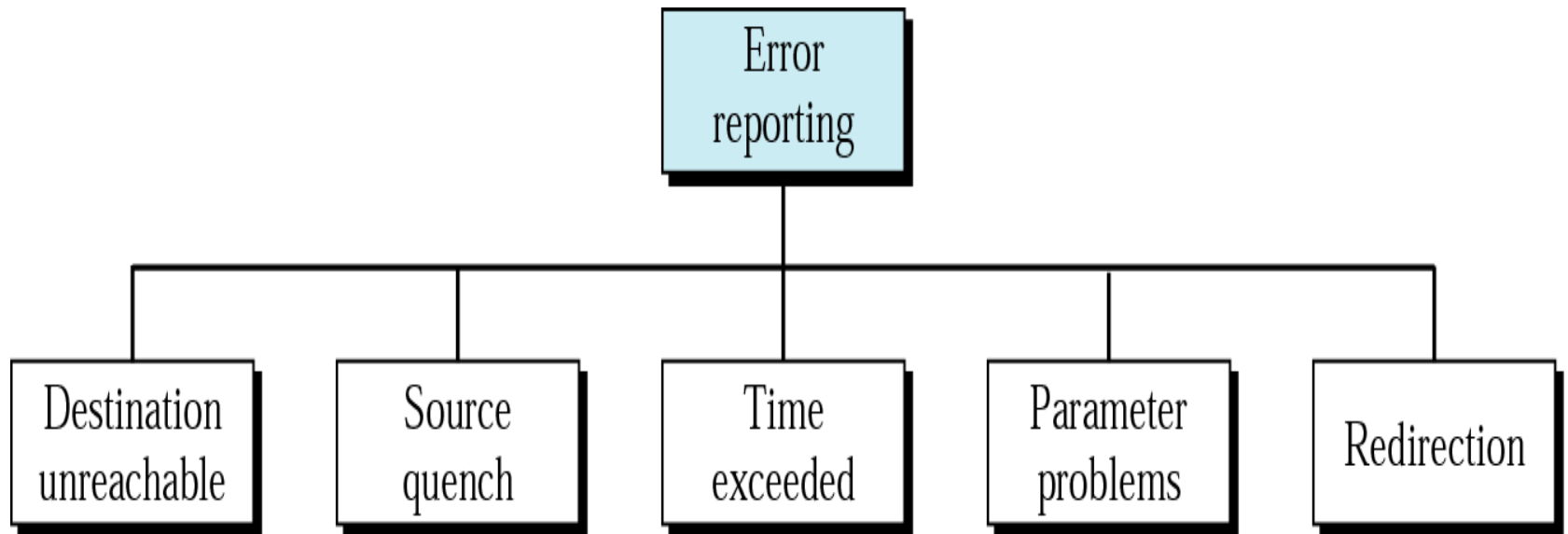
- Tanggung jawab utamanya adalah melaporkan kesalahan.
- ICMP tidak melakukan pembetulan kesalahan
- Pesan kesalahan (*error-reporting message*) selalu dikirim ke sumber aslinya, karena hanya ada informasi alamat IP sumber dan tujuan dalam datagram

ICMP

Tipe dari pesan ICMP: error reporting



Lima tipe pesan kesalahan



ICMP

Tipe dari pesan ICMP: error reporting



- Destination Unreachable

Ketika host atau router tidak dapat merutekan datagram ke tujuan maka datagram akan dibuang dan selanjutnya mengirimkan kembali pesan ***destination unreachable*** ke sumber aslinya

- Source Quench

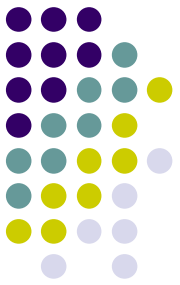
IP tidak mempunyai mekanisme *flow control* dan *congestion control*, ***source-quench message*** dalam ICMP dirancang untuk memberikan sejenis *flow control* dan *congestion control* kepada IP

Pesan ini mempunyai dua kegunaan :

- menginformasikan kepada sumber bahwa datagram telah *discarded*.
- Memperingatkan kepada sumber bahwa ada *congestion* disuatu tempat dalam jalur yg dilalui dan sumber harus memperlambat (*quench*) proses pengiriman

ICMP

Tipe dari pesan ICMP: error reporting



- Time Exceeded

Pesan ***Time-exceeded*** dibangkitkan dalam dua kasus

- router menerima datagram yang nilai TTL (time to live) nya berisi 0 (nol) . Datagram dibuang dan selanjutnya pesan *time-exceeded* harus dikirimkan ke sumber aslinya
- *Time-exceeded* dibangkitkan ketika seluruh fragmen yang membentuk pesan tidak sampai ke penerima dalam waktu tertentu

ICMP

Tipe dari pesan ICMP: error reporting



- Parameter Problem

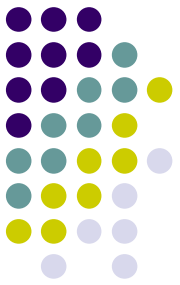
Keragu-raguan terhadap bagian header dari datagram yang melintas di Internet akan menimbulkan masalah serius. Jika host atau router menemukan *ambiguous* atau suatu nilai dari field datagram hilang, datagram akan dibuang dan dikirimkan pesan ***parameter-problem*** ke sumber aslinya

- Redirection

Pesan yang dikirimkan oleh router kepada host untuk membarui tabel routing suatu host

ICMP

Tipe dari pesan ICMP: query



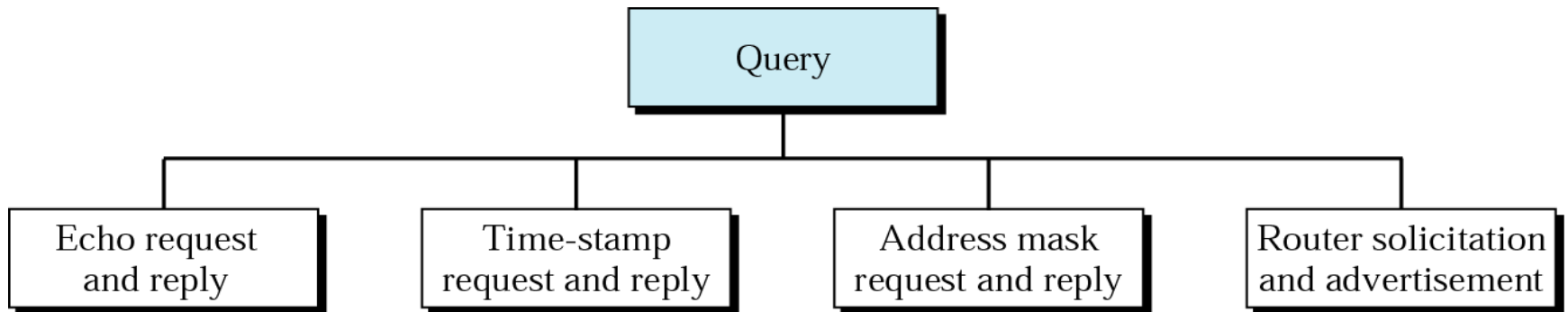
- ICMP dapat mendiagnosa beberapa masalah jaringan
- Hal ini diwujudkan melalui ***query message***
- Dalam tipe pesan ICMP ini, suatu node mengirimkan pesan yang akan dijawab menggunakan format tertentu oleh node tujuan

ICMP

Tipe dari pesan ICMP: query

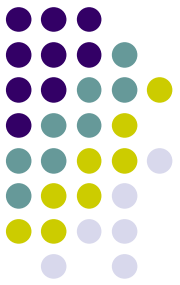


Query messages



ICMP

Tipe dari pesan ICMP: query



- Echo Request and Reply

Pesan ini dirancang untuk keperluan diagnosa.

Kombinasi antara pesan *echo-request* dan *echo-reply* menentukan apakah dua sistem (host atau router) dapat berkomunikasi satu sama lain

- Time-stamp Request and Reply

Dua mesin (host atau router) dapat menggunakan pesan *time-stamp* dan *time-stamp-reply* untuk menentukan waktu *round-trip* yang diperlukan datagram IP untuk berjalan diantara keduanya.

ICMP

Tipe dari pesan ICMP: query



- Address Mask Request and Reply

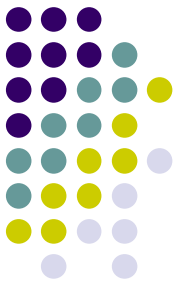
Alamat IP suatu host memuat alamat jaringan, alamat subnet, dan identitas host. Untuk dapat mengetahui bagian-bagian tersebut, host dapat mengirimkan pesan **address mask request** ke router. Selanjutnya router mengirim mask kedalam pesan **address mask reply**.

- Router Solicitation and Advertisement

Pesan *router solicitation* digunakan oleh host untuk meminta informasi routing kepada router. Router yang menerima pesan ini akan menjawab dengan pesan *router advertisement*. Router juga dapat secara periodik mengirimkan pesan *router advertisement* meskipun tidak ada host yang mengirimkan pesan *router solicitation*. Pesan *router advertisement* tidak hanya berisi informasi router tertentu tetapi seluruh router dalam jaringan.

IGMP

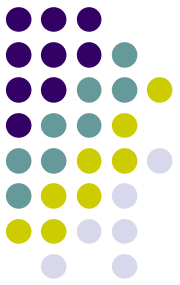
(Internet Group Management Protocol)



- Merupakan standart IP multicast yang digunakan untuk membangun keanggotaan host pada network.

IGMP

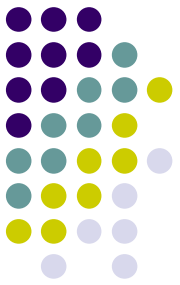
Cara Pengiriman Data



- Unicast
- Broadcast
- Anycast
- Multicast

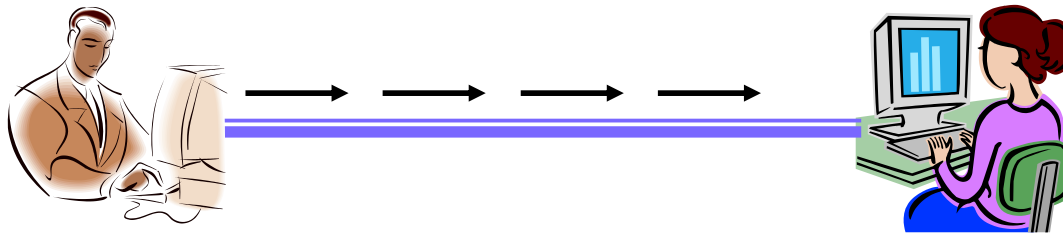
IGMP

Cara Pengiriman Data: Unicast



Data dikirim dari 1 host ke 1 host.

ilustrasi



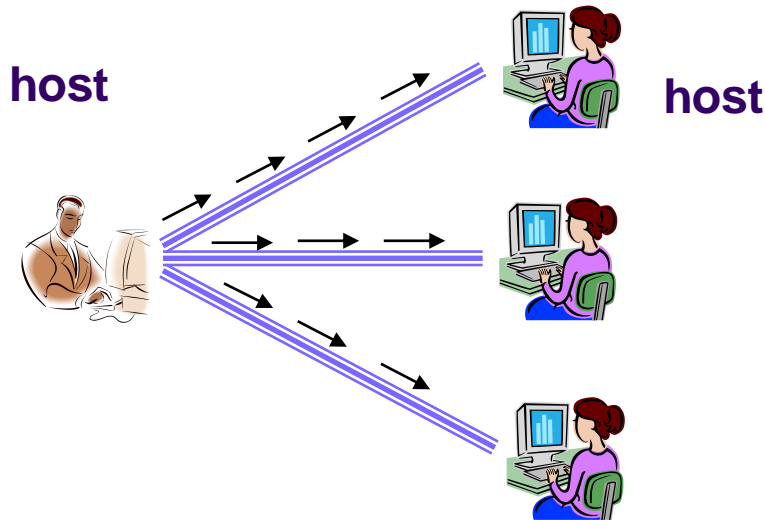
IGMP

Cara Pengiriman Data: Broadcast



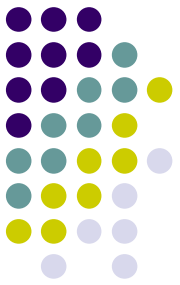
Data dikirim dari 1 host langsung disebar ke banyak host.

ilustrasi



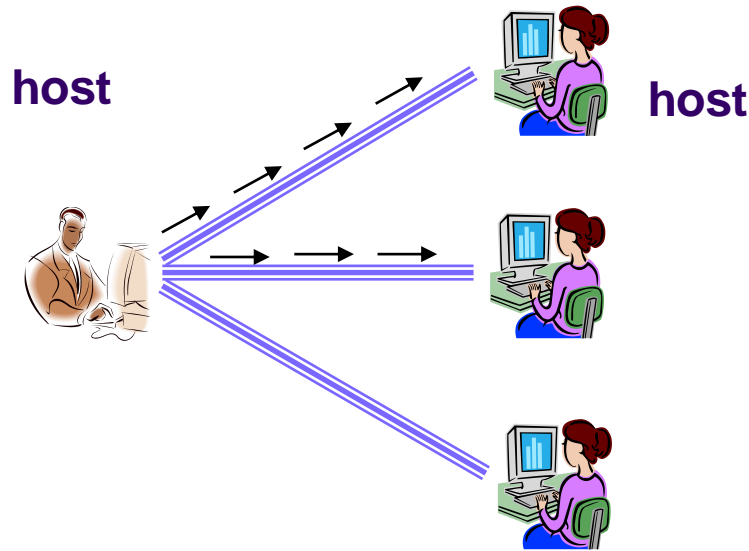
IGMP

Cara Pengiriman Data: AnyCast



Data dikirim dari 1 host langsung disebar ke host tertentu saja.

ilustrasi



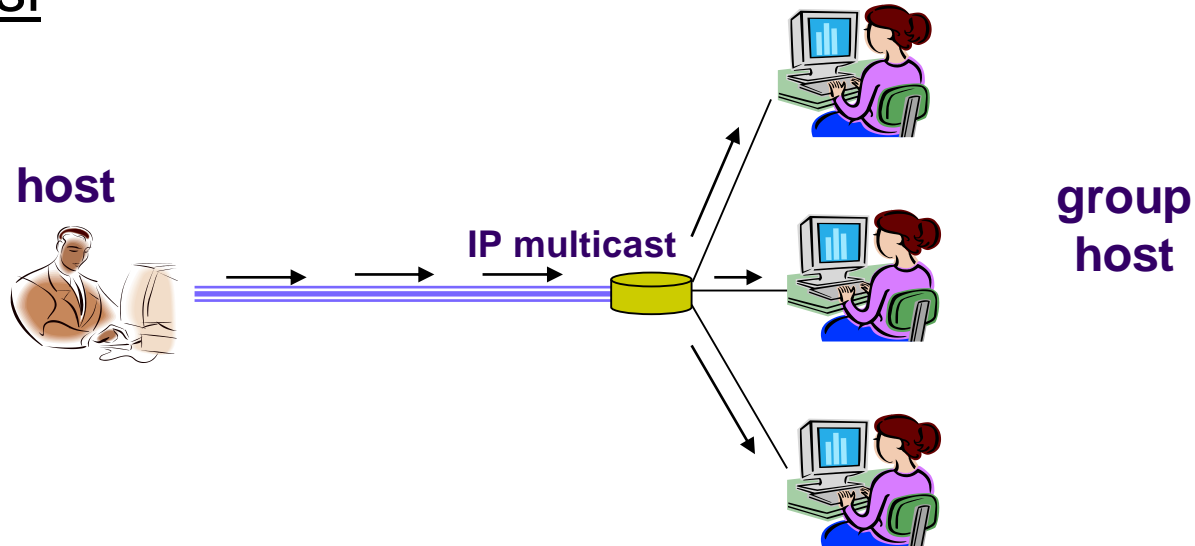
IGMP

Cara Pengiriman Data: MultiCast

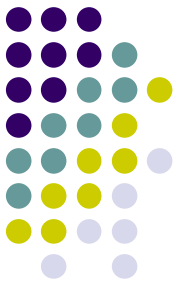


Data dikirim dari 1 host langsung disebar ke dalam group host.

ilustrasi



BOOTP (Bootstrap Protocol)



- Protokol yang digunakan untuk proses boot dari dikless workstation.
- Bootp dapat digunakan pada jaringan jika server dan client tsb terdapat pada LAN yang sama.

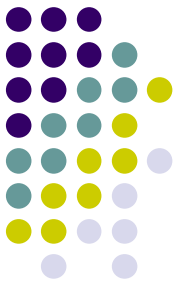
DHCP

(Dynamic Host Configuration Protocol)



- Protokol Standart yang digunakan untuk membagi alamat IP secara otomatis.
- DHCP berbasis pada server DHCP dan Client DHCP.
- Satu server DHCP dapat melayani pemberian alamat pada beberapa jaringan. Scope adalah range alamat IP yang dipakai oleh client.
- Pemasangan server DHCP pada PC yang menjalankan Windows NT Server.
- Sistem Operasi yang berfungsi sebagai client DHCP: Seluruh versi Windows NT, Windows 95, MS DOS workgroup connection 3.0

Tugas



- **Kerjakan secara individu**
- Buatlah tabel perbandingan antara BOOTP dan DHCP !
- Apa kelebihan dan kekurangan masing” protocol tersebut?
- Jelaskan cara kerja BOOTP dan DHCP !
- Kumpulkan dengan format:
Golongan_Nama_TugasMinggu5.pdf
- Deadline pengumpulan hari **Jum’at, 22 September 2023** jam **23.55**