

PERCOBAAN II

ROUTING DAN INTERNET PROTOCOL

3.1. Tujuan

- Mengetahui cara kerja routing statis
- Mengetahui cara konfigurasi subneting pada jaringan dengan router
- Mengetahui bagaimana TCP/IP mengidentifikasi jaringan
- Mengetahui bagaimana *netmask* menentukan range IP address
- Mengetahui fungsi kerja *subnetting*

3.2. Peralatan Yang Digunakan

- Perangkat komputer yang menggunakan sistem operasi Linux dan *BSD
- Perangkat komputer disertai perangkat tambahan *keyboard*
- Perangkat jaringan yang menggunakan kabel UTP dengan konektor RC45, NIC, HUB, dan *switch*

3.3. Teori Dasar

Internet adalah inter-network dari banyak jaringan yang terpisah. Jaringan ini dikoneksikan ke jaringan lainnya dengan menggunakan router. Ketika saya berkomunikasi dengan anda, paket-paket dari PC saya berjalan hop demi hop melewati semua jaringan yang didepannya, menuju jaringan anda dan akhirnya ke PC anda. Pada setiap hop, sebuah router meneruskan paket menuju alamat tujuannya. Akan tetapi paket itu sendiri hanya berisi **IP address tujuan** dan tidak **berisi informasi routing apapun**. Ketika sebuah paket tiba pada sebuah router, router memutuskan kemana mengirim paket, router meneruskan paket pada satu atau lebih hop menuju alamat tujuannya, ia memutuskan dimana meneruskannya dengan menggunakan routing table – sekumpulan aturan yang memberitahu router mengenai hop berikutnya untuk penerusan paket ke tujuan tertentu. Pertanyaan di sini adalah:

- Bagaimana router menemukan rute yang ada ke berbagai tujuan?
- Bagaimana semua router dikonfigurasi? Apakah seseorang harus mengkonfigurasikannya secara manual?

- Bagaimana sebuah mesin (host atau router) menemukan router apa yang ada pada jaringannya?

Dalam praktikum ini kita mengasumsikan bahwa router dikonfigurasi secara manual (*static routing*). Untuk jaringan yang lebih besar, diperlukan sesuatu yang lebih kompleks (*dynamic routing*)

Dalam suatu sistem *packet switching*, routing mengacu pada proses pemilihan jalur untuk pengiriman paket, dan router adalah perangkat yang melakukan tugas tersebut. Perutean dalam IP melibatkan baik *gateway* maupun *host* yang ada. Ketika suatu program aplikasi dalam suatu host akan berkomunikasi, protokol TCP/IP akan membangkitkannya dalam bentuk banyak datagram. Host harus membuat keputusan perutean untuk memilih jalur pengiriman.

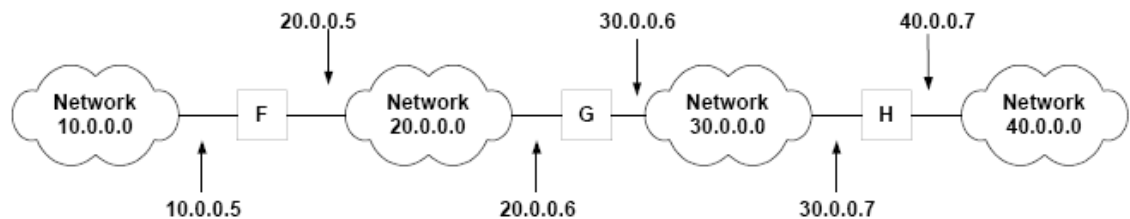
Pengiriman Langsung dan Tidak Langsung

Pengiriman langsung (*direct delivery*) adalah transmisi datagram dari suatu mesin langsung ke mesin lain, dan hal ini dapat terjadi bila keduanya berada dalam satu media transmisi yang terhubung langsung. Sedangkan pengiriman yang tidak langsung mengharuskan suatu datagram untuk melewati gateway. Untuk pengiriman langsung datagram IP, pengirim akan mengenkapsulasi datagram dalam suatu frame fisik, memetakan alamat IP tujuan ke alamat fisik dan menggunakan perangkat keras jaringan untuk pengiriman secara langsung. Identifikasi bahwa tujuan masih berada dalam satu jaringan dapat dilihat di IP address bagian network-nya, jika ditemukan alamat yang sama maka dapat dilakukan pengiriman langsung. Pengiriman tidak langsung terjadi bilamana antar host yang bertukar informasi tidak terletak pada satu jaringan sehingga perlu melalui beberapa gateway hingga gateway terakhir dapat dicapai dan pengiriman langsung dapat dilakukan.

Table Routing

Suatu algoritma perutean menggunakan tabel perutean yang menyimpan informasi mengenai kemungkinan tujuan yang dapat dicapai & cara pencapaiannya. Host dan gateway merutekan datagram, oleh karena itu keduanya memiliki tabel perutean. Untuk efisiensi tabel routing, tidak semua informasi mengenai kemungkinan tujuan akan disimpan, IP address tidak perlu ditulis lengkap. Biasanya tabel routing terdiri dari pasangan Network & Gateway (N,G) dimana N menunjukkan jaringan tujuan & G merupakan gateway berikutnya untuk sampai di jaringan N. Tabel perutean

akan selalu menunjuk kepada gateway yang dapat ditempuh langsung dalam satu jaringan. Semua gateway yang terdaftar di mesin tabel perutean mesin M harus terletak dalam satu jaringan. Ketika suatu datagram akan meninggalkan mesin source maka perangkat lunak IP akan mencari IP address tujuan dan menggunakan bagian networknya untuk membuat keputusan perutean, pemilihan gateway dan pengiriman secara langsung. Contoh:



Ada 4 jaringan dengan 3 gateway yang menghubungkannya. Bila gateway G memiliki tabel perutean maka isi tabel adalah:

JARINGAN YANG DICAPAI	ALAMAT YANG DILEWATI
20.0.0.0	DELIVER DIRECTLY
30.0.0.0	DELIVER DIRECTLY
10.0.0.0	20.0.0.5
40.0.0.0	30.0.0.7

Ukuran tabel routing tergantung pada jumlah jaringan yang terhubung. Kapasitasnya akan bertambah jika jumlah jaringan yang terhubung bertambah tanpa tergantung pada host yang terhubung. Metode lain untuk menghemat ukuran tabel routing adalah menjadikan masukkan-masukkan tertentu dalam bentuk **default**. Prinsip dari metode ini adalah perangkat lunak IP akan melihat terlebih dahulu isi tabel routing untuk jaringan tujuan, jika tidak ada jalur yang terlihat dalam tabel maka dikirimkan datagram ke default gateway. Metode ini sangat berguna untuk jaringan dengan jumlah alamat lokal tidak terlalu banyak & hanya satu koneksi menuju internet.

Proses Pencarian dalam Tabel Routing

Proses pencarian pada tabel routing ini biasanya mengikuti langkah-langkah dibawah ini :

1. Alamat tujuan datagram di-masking dengan subnet mask host pengirim dan dibandingkan dengan alamat network host pengirim. Jika sama, maka ini adalah routing langsung dan frame langsung dikirimkan ke interface jaringan
2. Jika tujuan datagram tidak terletak dalam satu jaringan, periksa apakah terdapat entri routing yang berupa host dan bandingkan dengan alamat IP tujuan datagram. Jika ada entri yang sama, kirim frame ke router menuju host tersebut.
3. Jika tidak terdapat entri host yang cocok pada tabel routing, gunakan alamat tujuan datagram yang telah di-mask pada langkah 1 untuk mencari kesamaan di tabel routing. Periksa apakah ada network/subnetwork di tabel routing yang sama dengan alamat network tujuan datagram. Jika ada entri yang sama, kirim frame ke router menuju network/subnetwork tersebut.
4. Jika tidak terdapat entri host ataupun entri network/subnetwork yang sesuai dengan tujuan datagram, host mengirimkan frame ke router default dan menyerahkan proses proses routing selanjutnya kepada router default.
5. Jika tidak terdapat rute default di tabel routing, semua host diasumsikan dalam keadaan terhubung langsung. Dengan demikian host pengirim akan mencari alamat fisik host tujuan menggunakan ARP

Membentuk Tabel Routing

Ketika suatu host baru dinyalakan, ia belum memiliki cache ARP yang lengkap. Entri pada cache ARP yang dimilikinya hanya untuk host itu sendiri. Setelah berinteraksi dengan host lain, barulah host tersebut memiliki entri-entri tambahan pada cache ARP. Hal yang sama juga terjadi pada tabel routing di host. Pada saat host baru dinyalakan, host tersebut tidak memiliki informasi di tabel routing kecuali entri untuk jaringan lokalnya. Tabel routing seperti ini kadang-disebut sebagai tabel routing minimal. Dalam kondisi hanya memiliki tabel routing minimal, host belum siap untuk melakukan internetwork karena hanya dapat berkomunikasi dengan host-host yang terletak pada satu jaringan lokal. Langkah pertama untuk mempersiapkan host untuk dapat melakukan fungsi internetwork adalah dengan memberikan entri rute default pada tabel routing. Dari rute default yang dimiliki pengisian tabel routing dapat dilakukan dengan beberapa metode dibawah ini :

a. *Routing Redirect*

Router (dalam hal ini router default) dapat menyatakan bahwa dirinya bukan rute terbaik untuk mencapai host tertentu, melainkan harus melalui router yang lain dalam jaringan lokal berdasarkan tabel routing yang dimilikinya. Jika demikian, maka router tersebut mengirimkan pesan kepada host pengirim datagram menggunakan ICMP redirect dan memberitahukan host pengirim tersebut agar datagram menuju host tertentu dialihkan melalui router lain. Host pengirim menerima pesan ICMP redirect itu dan menambahkan entri host pada tabel routing dengan informasi routing yang baru.

b. *Routing Static*

Metode lain yang dapat dipakai untuk membentuk tabel routing adalah dengan memakai *routing static*. Pada metode ini entri-entri rute di host dan di router dimasukkan secara manual

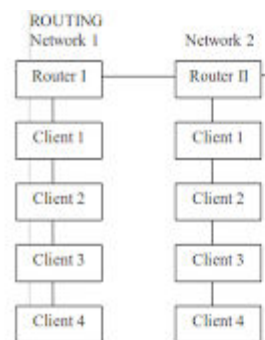
c. *Protocol Routing*

Protocol routing adalah protokol yang digunakan oleh router-router untuk saling bertukar informasi routing. Router-router pada jaringan TCP/IP membentuk tabel routing berdasarkan informasi routing yang dipertukarkan setiap selang waktu tertentu.

3.4. Prosedur Percobaan

Aplikasi Routing

Kita akan membuat jaringan router pada komputer berbasis linux sebagai router dan linux sebagai client. Dikondisikan disini ada 13 komputer yg akan dijadikan client dengan OS linux pada setiap jaringan dan sebuah komputer berbasis linux server sebagai router. Ada 2 jaringan akan kita hubungkan sehingga total ada 26 komputer client dan 2 komputer router.



Syarat komputer untuk menjadi router adalah harus mempunyai 2 LAN card. Disini akan ditentukan semua IP untuk router dan client, kalian bisa menggunakan IP lain sesuka kalian.

Konfigurasi IP

Network 1 : Router 1 (Linux)

IP address 1 192.168.0.1 Netmask 255.255.255.192

IP address 2 10.10.10.1 Netmask 255.0.0.0

Client 1

IP address 192.168.0.2 Netmask 255.255.255.192 Gateway 192.168.0.1

Client 2

IP address 192.168.0.3 Netmask 255.255.255.192 Gateway 192.168.0.1

Client 3

IP address 192.168.0.4 Netmask 255.255.255.192 Gateway 192.168.0.1

Client 4

IP address 192.168.0.5 Netmask 255.255.255.192 Gateway 192.168.0.1

Client 5

IP address 192.168.0.6 Netmask 255.255.255.192 Gateway 192.168.0.1

Client 6

IP address 192.168.0.7 Netmask 255.255.255.192 Gateway 192.168.0.1

Client 7

IP address 192.168.0.8 Netmask 255.255.255.192 Gateway 192.168.0.1

Client 8

IP address 192.168.0.9 Netmask 255.255.255.192 Gateway 192.168.0.1

Client 9

IP address 192.168.0.10 Netmask 255.255.255.192 Gateway 192.168.0.1

Network 2 : Router 2 (Linux)

IP address 1 192.168.0.65 Netmask 255.255.255.192

IP address 2 dynamic

Client 1

IP address 192.168.0.66 Netmask 255.255.255.192 Gateway 192.168.0.65

Client 2

IP address 192.168.0.67 Netmask 255.255.255.192 Gateway 192.168.0.65

Client 3

IP address 192.168.0.68 Netmask 255.255.255.192 Gateway 192.168.0.65

Client 4

IP address 192.168.0.69 Netmask 255.255.255.192 Gateway 192.168.0.65

Client 5

IP address 192.168.0.70 Netmask 255.255.255.192 Gateway 192.168.0.65

Client 6

IP address 192.168.0.71 Netmask 255.255.255.192 Gateway 192.168.0.65

Client 7

IP address 192.168.0.72 Netmask 255.255.255.192 Gateway 192.168.0.65

Client 8

IP address 192.168.0.73 Netmask 255.255.255.192 Gateway 192.168.0.65

Client 9

IP address 192.168.0.74 Netmask 255.255.255.192 Gateway 192.168.0.65

Selanjutnya kita akan mengambil contoh pada network 1. Langkah awal tentukan dulu range IP yang akan digunakan, pada network 1 saya gunakan 192.168.0.0/26

1. setting IP pada komputer client (**linux**)

IP address 192.168.0.2 Netmask 255.255.255.192

2. setting IP pada LAN card pertama komputer yg dijadikan router (**linux**)

`ifconfig eth1 192.168.0.1/26` atau `ifconfig eth1 192.168.0.1 netmask 255.255.255.192`

eth disini adalah LAN card, nilainya bisa saja berbeda pada komputer anda, anda bisa mengeceknya dengan mengetikkan `ifconfig`

3. ip yang kita buat pada langkah 2 tadi akan dijadikan gateway pada client. masukan gateway ke komputer client (**linux**)

IP address 192.168.0.2 Netmask 255.255.255.192 Gateway 192.168.0.1

4. setting IP pada LAN card kedua komputer yg dijadikan router, IP ini yang akan digunakan untuk menghubungkan antar router (**linux**)

`ifconfig eth2 10.10.10.1 netmask 255.0.0.0`

Coba Ping antara komputer dalam network 1. Kemudian jelaskan apa yang terjadi ?

Kemudian coba Ping antar komputer pada network 1 dengan komputer pada network 2. Kemudian jelaskan apa yang terjadi ?

5. buat table router pada masing-masing network (**linux**)

route add -net Network Address Tujuan netmask Netmask Network tujuan gw IP Address yg menghubungkan ke router tujuan

mis:

untuk router 1 ingin berkoneksi dengan network 2 maka di router 1 diketikkan

route add -net 192.168.0.64 netmask 255.255.255.192 gw 10.10.10.2

dan di router 2 harus diberi juga tabel routing untuk terhubung ke network 1

route add -net 192.168.0.0 netmask 255.255.255.192 gw 10.10.10.1

Lakukan Ping antara komputer dalam network 1. Kemudian jelaskan apa yang terjadi ?

Kemudian Ping antar komputer pada network 1 dengan komputer pada network 2. Kemudian jelaskan apa yang terjadi ?

Setelah itu lakukan langkah 5 pada semua network. selesailah pekerjaan kita membuat table routing. seluruh cara ini telah dipraktekan dan berhasil

➤ Internet Protocol

- Dasar teori

Dalam melakukan pengiriman data protokol, IP memiliki sifat yang dikenal sebagai *unreliable, connectionless, datagram delivery service*. *Unreliable* atau ketidakhandalan berarti tidak ada jaminan sampainya data di tempat tujuan. *Connectionless* berarti dalam mengirim paket dari tempat asal ke tujuan, tidak diawali dengan perjanjian (*handshake*) antara pengirim & penerima. Sedangkan *datagram delivery service* berarti setiap paket data yang dikirim adalah independen terhadap paket data yang lain. Jalur yang ditempuh antara satu data dengan yang lain bisa berbeda, sehingga kedatangannya pun bisa tidak terurut seperti urutan pengiriman. Dalam mengirim data, protokol IP memiliki format datagram khusus sebagai berikut :

VERSION	HEADER LENGTH	TYPE OF SERVICE	TOTAL LENGTH OF DATAGRAM	
IDENTIFICATION			FLAG	FRAGMENT OFFSET
TIME TO LIVE	PROTOCOL		HEADER CHECKSUM	
SOURCE IP ADDRESS				
DESTINATION IP ADDRESS				
OPTIONS STRICT SOURCE ROUTING, LOOSE SOURCE ROUTING				
DATA				

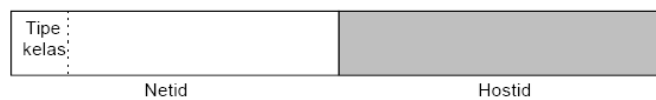
Gambar 2. 1 Format datagram IP

Versi menunjukkan versi protokol yang dipakai, *Header Length* menunjukkan panjang paket header dalam hitungan 32 bit. *Type of Service* menunjukkan kualitas layanan. *Total Length of datagram* menunjukkan total keseluruhan panjang datagram. *Identification, Flags & Fragment Offset* digunakan untuk fragmentasi paket, TTL menunjukkan jumlah hop maksimal yang dilewati paket IP, sedangkan Protokol mengandung angka yang mengidentifikasi protokol layer atasnya. *Header Checksum* berfungsi untuk mengecek kebenaran isi header datagram. *Source & destination IP Address* merupakan alamat pengirim dan penerima datagram. Untuk *byte option* dapat berisi *Strict Source Route*, yaitu daftar lengkap alamat IP dari router yang harus dilalui untuk sampai ke tujuan, dan *Loose Source Route*.

- Pengalamatan

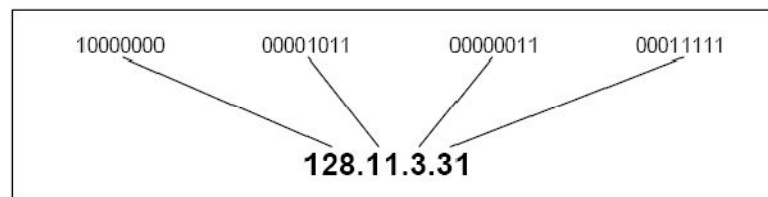
IP address (IPv4) memiliki 32 bit angka yang merupakan *logical address*. IP address bersifat unik, artinya tidak ada *device*, *station*, host atau router yang memiliki IP address yang sama. Tapi setiap host, komputer atau router dapat memiliki lebih dari satu IP address. Setiap alamat IP memiliki makna **netID** dan **hostID**. NetID adalah pada bit-bit terkiri dan hostID adalah bit-bit selain netID (terkanan).

Pembacaan alamat Internet yang merupakan *logical address* lebih mudah dilakukan dengan menyusun IP address dalam bentuk desimal di mana setiap 8 bit diwakili satu bilangan desimal. Masing-masing angka desimal ini dipisahkan oleh tanda titik.



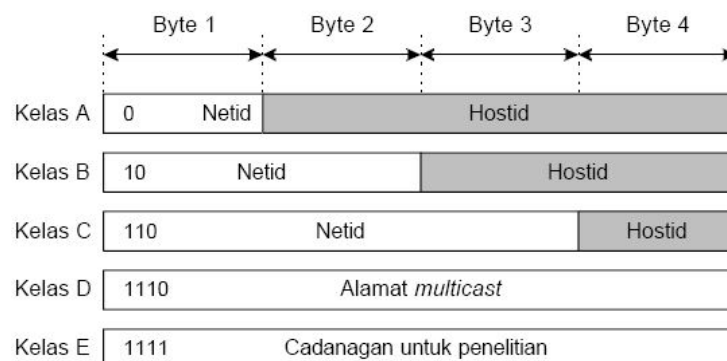
Gambar 2. 2 Alamat Internet

Untuk mempermudah pembacaan, 32 bit alamat internet direpresentasikan dengan notasi desimal.



Gambar 2. 3 Notasi desimal

IP address diklasifikasikan menjadi 5 kelas, yaitu kelas A, kelas B, kelas C, kelas D dan kelas E. Kelas-kelas tersebut didesain untuk kebutuhan jenis-jenis organisasi.



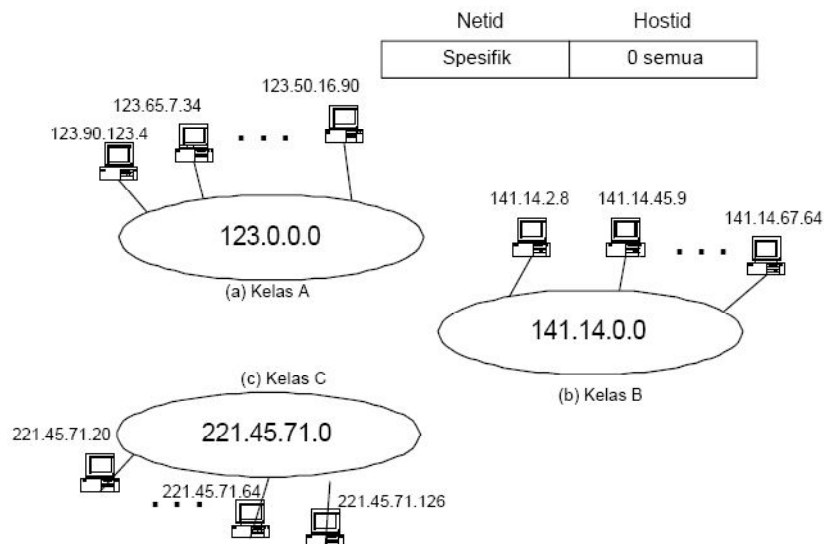
Secara keseluruhan penentuan kelas dapat dilihat gambar berikut:

	Mulai	Hingga
Kelas A	0 . 0 . 0 . 0	127.255.255.255
	Netid Hostid	Netid Hostid
Kelas B	128 . 0 . 0 . 0	191.255.255.255
	Netid Hostid	Netid Hostid
Kelas C	192 . 0 . 0 . 0	223.255.255.255
	Netid Hostid	Netid Hostid
Kelas D	224 . 0 . 0 . 0	239.255.255.255
	Alamat Multicast	Alamat Multicast
Kelas E	24 . 0 . 0 . 0	255.255.255.255
	Cadangan	Cadangan

Gambar 2. 4 Kelas-kelas dengan menggunakan notasi desimal

- Network Address

Dalam kelas A, B dan C, sebuah alamat dengan hostID yang bernilai 0 semua tidak diperuntukkan kepada host manapun. Alamat demikian dicadangkan untuk mendefinisikan alamat jaringan. Namun perlu diingat bahwa netID berbeda dengan alamat jaringan (*network address*), karena netID adalah bagian dari IP address, sedangkan *network address* adalah sebuah alamat di mana hosted-nya di set 0 semua. Tambahan juga, alamat jaringan atau *network address* ini tidak dapat digunakan sebagai alamat asal dan tujuan dalam sebuah paket IP.



Gambar 2. 5 Contoh alamat jaringan/network address

- Direct Broadcast Address

Dalam kelas A, B dan C, jika hostid semuanya di-set 1, alamat tersebut disebut sebagai *direct broadcast address*. Alamat ini digunakan oleh router untuk mengirim sebuah paket ke seluruh host dalam jaringan tertentu/khusus, sehingga seluruh host pada jaringan tertentu tersebut menerima paket dengan alamat ini.

- Loopback Address

Alamat IP yang dimulai dengan desimal 127 digunakan sebagai *loopback address*. Alamat ini digunakan untuk menguji perangkat lunak pada komputer atau host.

- Alamat Privat

Jika suatu organisasi ingin membangun jaringan komputer dan tidak membutuhkan terkoneksi pada jaringan internet, ada 3 pilihan untuk pembuatan alamat-alamat IP nya :

1. Menggunakan sebuah alamat yang unik tanpa menghubungkan ke internet. Hal ini akan sangat menguntungkan apabila di kemudian hari organisasi tersebut berniat untuk menghubungkan jaringan private-nya ke internet, maka tidak akan timbul masalah lagi. Kelas A dan B sudah tidak memungkinkan lagi karena sudah dimiliki oleh organisasi yang terhubung ke internet.
2. Menggunakan sembarang alamat IP dari kelas A, B dan C. Namun ini akan sangat menyulitkan apabila organisasi tersebut berniat terhubung ke internet.
3. Pilihan 1 dan 2 masih memiliki masalah, maka otoritas pencatatan alamat internet telah mencadangkan *range* alamat-alamat tertentu dari kelas A, B dan C yang bisa digunakan oleh organisasi manapun sebagai jaringan private. Tentu saja, di dalam internet alamat khusus ini tidak akan dikenal dan diabaikan. Singkat kata, alamat ini adalah unik bagi jaringan lokalnya namun tidak unik bagi jaringan global.

Tabel 2.1 Alamat yang dicadangkan untuk jaringan private

Kelas A	10.0.0.0-10.255.255.255
Kelas B	172.16.0.0-172.31.255.255
Kelas C	192.168.0.0-192.168.255.255

- Netmask

Komputer dapat mengetahui alamat tujuan pada suatu network dengan menggunakan mekanisme AND antara IP address kita dengan netmask. Bila alamat tujuan tersebut berada pada range kita, maka kita dapat berhubungan dengannya tanpa menggunakan router, dan juga sebaliknya.

- Masking

Masking adalah suatu proses ekstraksi alamat jaringan fisik dari sebuah IP address. Secara internal TCP/IP menggunakan biner AND untuk memutuskan *route* mana yang digunakan oleh paket, atau memutuskan sebuah *address* ada pada *range* yang mana.

IP address 212.140.133.181

Netmask 255.255.248.0

Network 212.140.128.0

Binary :

1101 0100 1000 1100 1000 0101 1011 0101

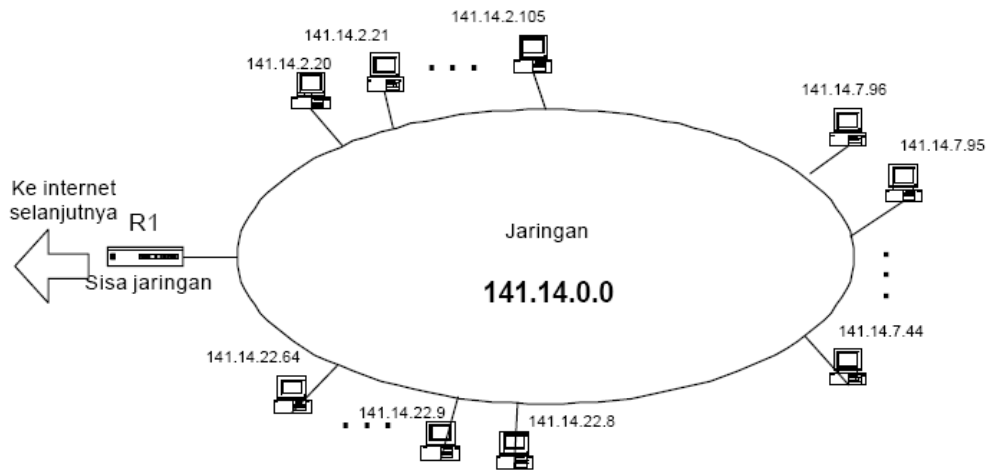
1111 1111 1111 1111 1111 1000 0000 0000

----- AND

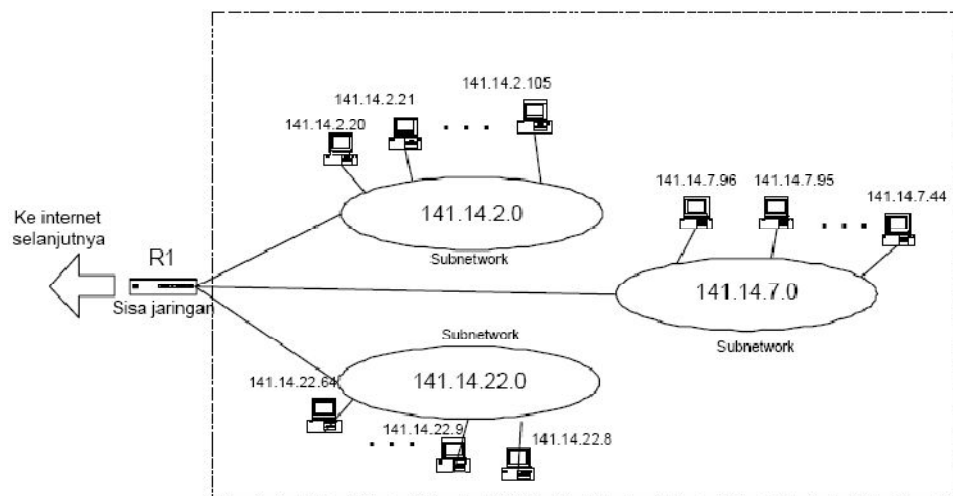
1101 0100 1000 1100 1000 0000 0000 0000

- Subnetting

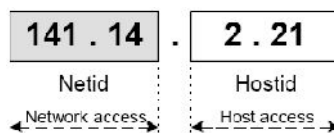
Subnetting merupakan teknik memecah network menjadi subnetwork yang lebih kecil. Subnetting hanya dapat dilakukan pada kelas A, B dan C. Bila kita perhatikan, IP address terdiri dari netID dan hostID. Jadi jika kita menuju suatu host artinya kita mencari netIDnya baru mencari hostIDnya. Mekanisme tersebut terjadi dengan melalui 2 level hierarki. Namun bila sudah mendapatkan netID dari organisasi dan ingin membuat organisasi tersebut menjadi sub kelompok, maka perlu dilakukan pemecahan network dengan teknik subnetting.



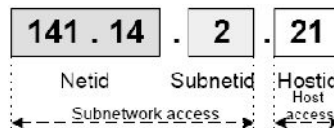
Gambar 2. 6 Jaringan dengan 2 tingkat hierarki (tanpa subnetting)



Gambar 2. 7 Jaringan dengan 3 tingkat hierarki (dengan subnetting)



Tanpa subnetting



Dengan subnetting

Gambar 2. 8 Alamat-alamat dalam jaringan dengan atau tanpa subnetting

- CIDR

CIDR adalah suatu teknik yang berbeda dengan arsitektur kelas dalam membagi network ID dan host ID. CIDR merubah kategori tersebut dengan network prefiks. Prefiks ini panjangnya tidak hanya 8 16 dan 24 (netmask kelas A standart adalah 255.0.0.0 atau bisa disebut /8, kelas B 255.255.0.0 atau bisa disebut /16, dan kelas C 255.255.255.0 atau bisa disebut /24). Prefiks menandakan banyak bit 1 dalam netmask, yang merupakan batas netID). CIDR membolehkan suatu IP kelas A 10.100.100.63 dengan netmask 255.255.255.0 (bisa ditulis 10.100.100.63/24), atau juga 172.17.100.130/27

- VLSM

VLSM adalah digunakannya subnet mask yang berbeda-beda pada sebuah network. VLSM menciptakan efisiensi penggunaan IP dan juga solusi dari keterbatasan IP pada suatu subnetwork.

ARP - Bagaimana mesin saya menemukan alamat ethernet mesin anda?

Saya tahu IP address anda, tetapi memerlukan alamat ethernet anda supaya saya dapat mengirim paket pada anda. TCP/IP memecahkan masalah ini dengan menggunakan ARP - *address resolution protocol*. Saya mem-broadcast, bertanya siapa yang mempunyai IP adress a.b.c.d (IP address anda). Anda menjawab dengan memberitahu saya alamat ethernet. Kita kemudian dapat berkomunikasi. Secara lengkap inilah yang terjadi:

- Saya mengirim sebuah broadcast ethernet, berisi paket permintaan ARP kepada payload/data field. Paket ARP berisi IP address yang MAC address-nya saya perlukan - katakanlah 10.9.8.7 (alamat IP address anda). Tcpcmdump menunjukkan sebagai "arp who has 10.9.8.7 tell 10.9.8.8". Sembari mengirimkan paket pertanyaan, mesin saya juga mengirimkan MAC addressnya.
- Semua mesin pada network ini menerima paket ini, mengekstrak paket ARP , dan melihat IP address yang ada di dalamnya. Jika alamat tidak cocok dengan IP address mesin tersebut, maka paket ditolak.
- Mesin 10.9.8.7 menjawab ke mesin saya (10.9.8.8) dengan paket ARP yang diminta, berisi MAC address dari .7 (Mesin anda tidak membroadcast jawaban karena hanya .8 yang meminta). Tcpcmdump memperlihatkan sebagai "arp-reply 10.9.8.7 is at a.b.c.d.e.f"

- .8 (mesin saya) sekarang tahu MAC address dari .29, dan dapat berkomunikasi dengan bebas.

Mekanisme di atas berlaku untuk komunikasi dalam satu network, karena ketika IP address tujuan berada diluar range network (yang ditentukan oleh mekanisme AND antara IP address dan netmask), maka paket akan dikirimkan ke router (*default gateway*). Begitu pula komunikasi antara router- router yang berhubungan, hingga sampai ke gateway host tujuan. Mekanisme ARP akan digunakan kembali pada gateway host tujuan.

Netmask dalam Desimal	Pre fix	Jumlah IP Address Tersedia	Netmask dalam Hexa	Netmask dalam Binary
255.255.255.255	/32	1	ff.ff.ff.ff	11111111 . 11111111 . 11111111 . 11111111
255.255.255.254	/31	2	ff.ff.ff.fe	11111111 . 11111111 . 11111111 . 11111110
255.255.255.252	/30	4	ff.ff.ff.fc	11111111 . 11111111 . 11111111 . 11111100
255.255.255.248	/29	8	ff.ff.ff.f8	11111111 . 11111111 . 11111111 . 11111000
255.255.255.240	/28	16	ff.ff.ff.f0	11111111 . 11111111 . 11111111 . 11110000
255.255.255.224	/27	32	ff.ff.ff.e0	11111111 . 11111111 . 11111111 . 11100000
255.255.255.192	/26	64	ff.ff.ff.c0	11111111 . 11111111 . 11111111 . 11000000
255.255.255.128	/25	128	ff.ff.ff.80	11111111 . 11111111 . 11111111 . 10000000
255.255.255.0	/24	256	ff.ff.ff.0	11111111 . 11111111 . 11111111 . 00000000
255.255.254.0	/23	512	ff.ff.fe.0	11111111 . 11111111 . 11111110 . 00000000
255.255.252.0	/22	1.024	ff.ff.fc.0	11111111 . 11111111 . 11111100 . 00000000
255.255.248.0	/21	2.048	ff.ff.f8.0	11111111 . 11111111 . 11111000 . 00000000
255.255.240.0	/20	4.096	ff.ff.f0.0	11111111 . 11111111 . 11110000 . 00000000
255.255.224.0	/19	8.192	ff.ff.e0.0	11111111 . 11111111 . 11100000 . 00000000
255.255.192.0	/18	16.384	ff.ff.c0.0	11111111 . 11111111 . 11000000 . 00000000
255.255.128.0	/17	32.768	ff.ff.80.0	11111111 . 11111111 . 10000000 . 00000000
255.255.0.0	/16	65.536	ff.ff.0.0	11111111 . 11111111 . 00000000 . 00000000
255.254.0.0	/15	131.072	ff.fe.0.0	11111111 . 11111110 . 00000000 . 00000000
255.252.0.0	/14	262.144	ff.fc.0.0	11111111 . 11111100 . 00000000 . 00000000
255.248.0.0	/13	524.288	ff.f8.0.0	11111111 . 11111000 . 00000000 . 00000000
255.240.0.0	/12	1.048.576	ff.f0.0.0	11111111 . 11110000 . 00000000 . 00000000
255.224.0.0	/11	2.097.152	ff.e0.0.0	11111111 . 11100000 . 00000000 . 00000000
255.192.0.0	/10	4.194.304	ff.c0.0.0	11111111 . 11000000 . 00000000 . 00000000
255.128.0.0	/9	8.388.608	ff.80.0.0	11111111 . 10000000 . 00000000 . 00000000
255.0.0.0	/8	16.777.216	ff.0.0.0	11111111 . 00000000 . 00000000 . 00000000
254.0.0.0	/7	33.554.432	fe.0.0.0	11111110 . 00000000 . 00000000 . 00000000
252.0.0.0	/6	67.108.864	fc.0.0.0	11111100 . 00000000 . 00000000 . 00000000
248.0.0.0	/5	134.217.728	f8.0.0.0	11111000 . 00000000 . 00000000 . 00000000
240.0.0.0	/4	268.435.456	f0.0.0.0	11110000 . 00000000 . 00000000 . 00000000
224.0.0.0	/3	536.870.912	e0.0.0.0	11100000 . 00000000 . 00000000 . 00000000
192.0.0.0	/2	1.073.741.824	c0.0.0.0	11000000 . 00000000 . 00000000 . 00000000
128.0.0.0	/1	2.147.483.648	80.0.0.0	10000000 . 00000000 . 00000000 . 00000000
0.0.0.0	/0	4.294.967.296	0.0.0.0	00000000 . 00000000 . 00000000 . 00000000

Catatan :

- a) Anda tidak harus mengingat netmask ini - lihat sesuai yang anda butuhkan.
- b) Baris- baris tabel dengan fill berbeda adalah default netmask untuk class jaringan A,B, dan C
- c) Range sering ditulis sebagai IP address yang diikuti dengan dengan “/” dan prefik (prefik sendiri dapat diartikan banyaknya bit 1 pada netmask), yakni jumlah bit pada network part.

Sebagai contoh 192.168.63.128/25

Ini berarti : Net id : 192.168.63.128 255.255.255.0

Range : 192.168.63.128 - 192.168.63.255

Jumlah alamat IP tersedia : 128

Sering disebut “CIDR notation” untuk netmask atau IP address range.

- d) “/32” menentukan IP address tunggal. Sebagai contoh 10.100.100.5/32 berarti ini adalah mesin tunggal - range dengan panjang 1. Anda tidak akan pernah menggunakannya ketika anda mengkonfigurasi IP address dan subnetmask dari sebuah mesin pada LAN, tapi anda akan melihatnya dalam tabel routing dan sejenisnya.
- e) “/0” atau mask 0.0.0.0 menentukan internet keseluruhan - setiap IP address yang mungkin - karena ia memberikan network part yang sama dari 0.0.0.0 ketika digabungkan pada sembarang IP address. Anda akan melihat hal ini dalam praktik pada tabel-tabel routing. (Pada beberapa konteks, “0.0.0.0” mungkin ditulis sebagai word default untuk menentukan bahwa ini berarti “setiap address”.)
0-bit pada mask berkaitan dengan host part dari address. Yang menentukan ukuran jaringan

Tugas Pendahuluan

1. Tuliskan pada layer mana IP address bekerja! Jelaskan jawaban anda?

2. Ubah angka angka berikut ke dalam bentuk binary dan hexa!

a. 172.17.68.131 :

b. 192.168.17.200 :

3. Jelaskan mekanisme yang terjadi ketika sebuah node (komputer) dalam suatu jaringan berhubungan dengan node lain dalam jaringan berbeda!

4. Jelaskan dan sebutkan apa yang dimaksud dengan Router!

5. Jelaskan perbedaan Dedicated router dan OS router, berikan contoh!

2.4. Prosedur Percobaan

1. Buat topologi jaringan yang akan anda gunakan dalam praktikum!
2. Login ke komputer bersistem operasi *Bsd.
3. Memahami teori IP addressing

Dua buah node dengan IP address berikut :

Node a 172.16.17.30/20

Node b 172.16.28.15/20

Amati dan simpulkan!

4. Implementasi IP Address

- a) Konfigurasi setiap node sehingga terhubung satu sama lain

Tuliskan IP address anda serta netmask yang digunakan. Tulis juga IP address serta netmask tetangga-tetangga anda.

- b) Implementasikan IP address dan netmask tersebut di masing-masing node
Tuliskan apa yang anda lakukan

- c) Jalankan tcpdump

```
# tcpdump -n -e -t
```

- d) Ubah IP address salah satu node, samakan dengan salah satu IP address node yang lain, kemudian lakukan hal-hal berikut ini:

- Perhatikan paket apa yang anda lihat pada jaringan!

- Apa yang terjadi bila anda melakukan ping dari node tersebut? Tuliskan juga apa yang terjadi ketika anda melakukan ping dari node lain!

- Ubah IP address node tersebut ke nilai sebenarnya
