Pertemuan 4

Pengenalan TCP/IP

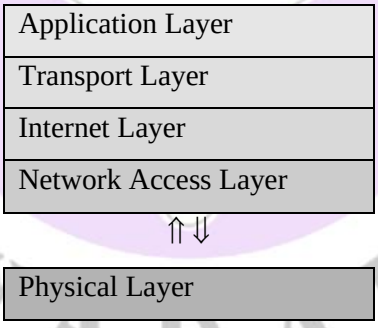
Objektif:

1. Mahasiswa dapat memahami Protokol TCP/IP
2. Mahasiswa dapat mengenal Arsitektur Protokl TCP/IP
3. Mahasiswa dapat mengenal IPv4 dan IPv6
4. Mahasiswa dapat memahami Subnetting

TCP/IP (Transmission Control Protocol/Internet Protocol) adalah sekelompok protocol yang mengatur komunikasi data komputer di Internet. Komputer-komputer yang terhubung ke internet berkomunikasi dengan protocol ini. Karena menggunakan bahasa yang sama, yaitu protocol TCP/IP, perbedaan jenis komputer dan system operasi tidak menjadi masalah. Komputer PC dengan system Operasi Windows dapat berkomunikasi dengan komputer Macintosh atau dengan Sun SPARC yang menjalankan Solaris. Jadi, jika sebuah komputer menggunakan protocol TCP/IP dan terhubung langsung ke Internet, maka komputer tersebutdapat berhubungan dengan komputer di belahan dunia manapun yang juga terhubung ke Internet.

4.1.Arsitektur Protokol TCP/IP

Karena tidak ada perjanjian umum tentang bagaimana melukiskan TCP/IP dengan model layer, biasanya TCP/IP didefinisikan dalam 3-5 level fungsi dalam arsitektur protocol. Kali ini akan digambarkan TCP/IP dalam 4 layer model, yaitu seperti digambarkan dalam diagram di bawah ini :



Jika suatu protocol menerima data dari protocol lain di layer atasnya, maka akan menambahkan informasi tambahan miliknya ke data tersebut, Informasi ini memiliki fungsi yang sesuai dengan fungsi protocol tersebut. Setelah itu, data ini diteruskan lagi ke protocol pada layer di bawahnya. Hal yang sebaliknya terjadi jika suatu protocol menerima data dari protocol lain yang berada pada layer di bawahnya. Jika data ini dianggap valid, protocol akan melepas informasi tambahan

tersebut untuk kemudian meneruskan data itu ke protocol lain yang berada pada layer di atasnya.

a) Network Access Layer

Protokol pada layer ini menyediakan media bagi system untuk mengirimkan data ke device lain yang terhubung secara langsung. Dalam literatur yang digunakan dalam tulisan ini, Network Access Layer merupakan gabungan antara Network, Data Link dan Physical layer. Fungsi Network Access Layer dalam TCP/IP disembunyikan, dan protocol yang lebih umum dikenal (IP, TCP, UDP, dll) digunakan sebagai protocol-level yang lebih tinggi..Fungsi dalam layer ini adalah mengubah IP datagram ke frame yang ditransmisikan oleh network, dan memetakan IP Address ke physical address yang digunakan dalam jaringan. IP Address ini harus diubah ke alamat apapun yang diperlukan untuk physical layer untuk mentransmisikan datagram.

b) Internet Layer

Dalam layer ini terdapat empat buah protocol yaitu :

[1] ARP (Adress Resolution Protocol) → menentukan alamat data link layer untuk IP Address yang telah dikenal.

[2] RARP(Reverse Adress Resolution Protocol) → menentukan Network Address pada saat alamat data link layer di ketahui.

[3] ICMP (Internet Control Message Protocol)→ provides control and messaging capabilities

Salah satu jenis protokol yang biasa digunakan untuk pengecekan dan mengindikasi error pada saat transmisi dalam sebuah jaringan. ICMP disalurkan berbasis “best effort” sehingga bisa mengetahui jika terjadi error (datagram lost). Host (baik device yang mencoba transmisi ataupun device tujuan transmisi tujuan) akan mendeteksi apabila terjadi permasalahan tranmisi, dan membuat “ICMP message” yang akan dikirimkan ke host asal. Contoh penggunaan protokol ICMP yang sering dilakukan misalnya pada saat menjalankan Ping atau Traceroute.

[4] IP (Internet Protocol) → unreliable, connectionless, datagram delivery service

Protokol IP merupakan inti dari protocol TCP/IP. Seluruh data yang berasal dari protocol pada layer di atas IP harus dilewatkan, ialah oleh protocol IP, dan dipancarkan sebagai paket IP, agar sampai ke tujuan. Dalam melakukan pengiriman data, IP memiliki sifat yang dikenal sebagai unreliable, connectionless, datagram delivery service.

- Unreliable berarti bahwa Protokol IP tidak menjamin datagram yang dikirim pasti akan sampai ke tempat tujuan. Protokol IP hanya berjanji ia akan melakukan usaaha sebaik-baiknya (best effort delivery service), agar paket yang dikirim tersebut sampai ke tujuan. Jika di perjalanan terjadi hal-hal yang diinginkan (salah satu jalur putus, router down, atau host/network tujuan sedang down), protocol IP hanya memberitahukan ke pengirim paket melalui protocol ICMP, bahwa terjadi masalah dalam pengiriman paket IP ke tujuan. Jika diinginkan keandalan yang lebih baik, keandalan itu harus disediakan oleh protocol yang berada diatas layer IP ini (yaitu TCP dan application layer).
- Connectionless berarti dalam mengirim paket dari tempat asal ke tujuan, pihak pengirim dan penerima paket IP sama sekali tidak mengadakan perjanjian (handshake) terlebih dahulu.
- Datagram delivery service berarti setiap paket data yang dikirim adalah independen terhadap paket data yang lain. Akibatnya jalur yang ditempuh oleh masing-masing paket data IP ke tujuannya bias jadi berbeda satu dengan yang lainnya. Karena jalur yang ditempuh berbeda, kedatangan paket pun bias jadi tidak berurutan. Hal ini dilakukan untuk menjamin tetap sampainya paket IP ke tujuan, walaupun salah satu jalur ke tujuan itu mengalami masalah.

Setiap paket IP membawa data yang terdiri atas :

- *Header Length*, berisi panjang dari header paket IP dalam hitungan 32 bit word.
- *Type of Service*, berisi kualitas service yang dapat mempengaruhi cara pengangan paket IP ini.
- *Total Length of Datagram*, panjang IP datagram dalam ukuran byte.
- *Identification, Flags, dan Fragment Offset*, berisi beberapa data yang berhubungan dengan fragmentasi paket. Paket yang yang dilewatkan melalui berbagai jenis jalur akan mengalami fragmentasi (dipecah menjadi beberapa paket yang lebih kecil) sesuai dengan besar data maksimal yang bias di transmisikan melalui jalur tersebut.
- *Time to Live*, berisi jumlah router/hop maksimal yang boleh dilewati paket IP. Setiap kali melewati satu router, isi dari field ini dikurangi satu. Jika TTL telah habis dan paket tetap belum sampai ke tujuan, paket ini akan dibuang dan router terakhir akan mengirimkan paket ICMP *time exceeded*. Hal ini dilakukan untuklmencegah paket IP terus menerus berada di dalam nerwork.
- *Protocol*, mengandung angka yang mengidentifikasikan protocol layer atas pengguna isi data dari paket IP ini.
- *Header Checksum*, berisi nilai *checksum* yang dihitung dari seluruh field dari header packet IP. Sebelum dikirimkan, protocol IP terlebih dahulu menghitung checksum dari header paket IP tersebut untuk nentinya dihitung kembali di sisi penerima. Jika terjadi perbedaan, maka paket ini dianggap rusak dan dibuang.
- *IP Address* pengirim dan penerima data.
- *Version*, berisi versi dari protocol yang dipakai. Saat ini yang dipakai ialah IP versi 6 dan versi 4.

c) Transport Layer

Transport layer mempunyai dua fungsi , yaitu; mengatur aliran data antara dua host dan reliability.

Pada transport layer terdapat dua buah protocol :

- *TCP* -- a connection-oriented, reliable protocol, byte stream service. Connection Oriented berarti sebelum melakukan pertukaran data, dua aplikasi pengguna TCP harus melakukan hubungan (handshake) terlebih dahulu. Reliable berarti TCP menerapkan proses deteksi kesalahan paket dan retransmisi. Byte Stream Service berarti paket dikirimkan dan sampai ke tujuan secara berurutan.
- *UDP* -- connectionless and unreliable. Walaupun bertanggung jawab untuk mentransmisikan pesan/data, tidak ada software yang menge-cek pengantara setiap segmen yang dilakukan oleh layer ini. Keuntungan penggunaan UDP adalah kecepatannya karena pada UDP tidak ada acknowledgements, sehinggan trafik yang lewat jaringan rendah, dan itu yang membuat UDP lebih cepat daripada TCP.

d) Application Layer

Pada sisi paling atas dari arsitektur protokol TCP/IP adalah Application Layer. Layer ini termasuk seluruh proses yang menggunakan transport layer untuk mengirimkan data. Banyak sekali application protocol yang digunakan saat ini.

Beberapa diantaranya adalah :

- TELNET, yaitu Network Terminal Protocol, yang menyediakan remote login dalam jaringan
- FTP, File Transfer Protocol, digunakan untuk file transfer
- SMTP, Simple Mail Transfer Protocol, dugunakan untuk mengirimkan electronic mail
- DNS, Domain Name Service, untuk memetakan IP Address ke dalam nama tertentu
- RIP, Routing Information Protocol, protokol routing
- OSPF, Open Shortest Path First, protokol routing

- NFS, Network File System, untuk sharing file terhadap berbagai host dalam jaringan
- HTTP, Hyper Text Transfer Protokol, protokol untuk web browsing.

4.2.Alamat IP

a) IP Address versi 4

Penulisan IP Address versi 4 adalah sebagai berikut:

- Bentuk binner

  IP address merupakan bilangan biner 32 bit yang dipisahkan oleh tanda pemisah berupa tandatitik setiap 8 bitnya. Tiap 8 bit ini disebut sebagai oktet. Bentuk IP address adalah sebagai berikut :

  xxxxxxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx

  setiap simbol "x" dapat digantikan oleh angka 0 dan 1.

- Bentuk dotted decimal

  Notasi IP address dengan bilangan biner tidaklah mudah dibaca. Untuk membuatnya lebih mudah dibaca dan ditulis, IP address sering ditulis sebagai 4 bilangan desimal yang masing-masing dipisahkan oleh sebuah titik. Format ini dikenal dengan nama "dotted-decimal notation" (notasi desimal bertitik). Setiap bilangan desimal tersebut merupakan nilai dari satu oktet IP address. IP address yang ditulis dengan notasi dotted-decimal adalah sebagai berikut : 132.92.121.1

IP Address ini dikelompokkan dalam lima kelas :

- Kelas A

  Format : 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh
  Byte Pertama : 0 – 127 (127 untuk *local loopback*)
  Jumlah : 126 kelas A (0 dan 127 dicadangkan)
  Range IP : 1.xxx.xxx.xxx sampai 126.xxx.xxx.xxx
  Jumlah IP : 16.777.214 IP Address untuk tiap kelas A

- Kelas B

  Format : 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh

Byte Pertama : 128 – 191
Jumlah : 16384 kelas B
Range IP : 128.0.xxx.xxx sampai 191.155.xxx.xxx
Jumlah IP : 65.532 IP Address untuk tiap kelas B

- Kelas C

Format : 110nnnn nnnnnnnn nnnnnnnn hhhhhhhh
Byte Pertama : 192 – 223
Jumlah : 2.097.152 Kelas C
Range IP : 192.0.0.xxx sampai 223.255.255.xxx
Jumlah IP : 254 IP Address untuk tiap kelas C

- Kelas D

Format : 1110mmmm mmmmmmmm mmmmmmmm mmmmmmmm
Bit multicast : 128 bit
Byte Inisial : 224 – 247
Deskripsi : Kelas D adalah ruang alamat multicast (RFC 1112)

- Kelas E

Format : 1111rrrr rrrrrrrr rrrrrrrr rrrrrrrr
Bit cadangan : 28 bit
Byte Inisial : 248 – 255
Deskripsi : Kelas D adalah ruang alamat yang dicadangkan untuk keperluan eksperimental.

Ket : n = network bit, h = host bit, m = multicast bit, r = bit cadangan

b) IP Address versi 6

Internet protokol yang digunakan sekarang untuk komunikasi di internet dikenal dengan IPv4. IPv4 ini telah berumur lebih dari 20 tahun. Suksesor dari IPv4 adalah IPv6. IPv6 menawarkan fitur dan fungsionalitas yang lebih dari IPv4 seperti ruang pengalamatan yang jauh lebih besar, fitur keamanan IPSec, penanganan lalu lintas multimedia di internet, dan lain-lain.

Protokol internet pertama kali dirancang awal tahun 1980-an. Pada saat itu hanya digunakan untuk menghubungkan beberapa node saja dan tidak diprediksikan akan tumbuh secara global seperti sekarang ini. Pada awal tahun 1990-an mulai disadari bahwa internet mulai tumbuh ke seluruh dunia dengan pesat, pada saat itu juga orang-orang mulai menyadari cepat atau lambat alamat

IPv4 yang sebesar 32 bit akan semakin terbatas dan sulit didapatkan padamasa-masa mendatang, selain itu internet sekarang ini mulai melewatkan aplikasi multimedia, sehingga ada beberapa masalah timbul pada traffic internet seperti masalah priority, bottleneck, dan sebagainya.

Solusi untuk mengatasi keterbatasan alamat IPv4 ini adalah penggunaan NAT (Network Address Translation) dan CIDR (classes interdomain routing). Kedua digunakan dalam rangka penggunaan alamat IP secara hemat dan efisien.Namun solusi seperti NAT tidaklah menyelesaikan persoalan secara utuh. Ada beberapa hambatan muncul bila menggunakan NAT, seperti kesulitan pada aplikasi VoIP, kesulitan pada aplikasi IPSec, lalu lintas Muticastyang tidak dapat melewati NAT, dan NAT itu sendiri sebagai single failure boxdimana bila mesin penyedia NAT rusak maka semua koneksi client dengan internet menjadi terputus.

Alasan utama untuk mulai beralih ke IPv6 adalah terbatasnya ruang pengalamatan. Pada masa sekarang ini bukan komputer saja yang terhubung ke internet namun peralatan sehari-hari seperti telepon seluler, PDA, home appliances, dan sebagainya juga terhubungkan ke internet, dapat dibayangkan seberapa banyak alamat IP yang dibutuhkan untuk menghubungkan semua itu ke internet.

Diperkirakan pada 1 sampai 7 tahun kedepan merupakan masa transisi dari IPv4 ke IPv6. Secara eksplisit berdasarkan kesepakatan IETF memang tidak ada tanggal pasti kapan umur IPv4 akan berakhir, namun masatransisi dari IPv4 ke IPv6 merupakan proses yang bertahap dan selama transisi harus ada jaminan bahwa proses tersebut tidak mengganggu aktifitas internet.

Penulisan IP Address versi 6

Yang menarik dari IPv6 adalah penjang alamat sebesar 128 bit. Notasi alamat IPv6 ditulis dalam hexadesimal yang dipisahkan dengan karakter ":". Contohnya sebagai berikut:

- 3ffe:0501:008:1234:0260:97ff:fe40:efab
- ff02:0000:0000:0000:0000:0000:0000:0001

Angka nol didepan dapat diabaikan sehingga penulisan menjadi:

- 3ffe:501:8:1234:260:97ff:fe40:efab

- fe02:0:0:0:0:0:0:1

Angka nol yang berurutan dapat digantikan dengan karakter"::", sehingga penulisan menjadi:

- fe02::1

Alamat IPv6 yang mempunyai panjang 128 bit dalam hexadesimal tentunya sulit dihapalkan karena itu alamat numerik jarang digunakan, lebih mudah menggunakan hostname, untuk itu DNS masih memegang peranan penting.

Alamat IPv6 sendiri terbagi atas beberapa macam, berdasarkan RFC 3513 :

- Unspecified dengan notasi ::/128
- Loopback dengan notasi ::1/128
- Multicast dengan notasi ff00::/8
- Link local unicast dengan notasi FE80::/8
- Site local unicast dengan notasi FEC0::/8

4.3.Subnetting

Subnetting adalah sebuah teknik yang mengizinkan para administrator jaringan untuk memanfaatkan 32 bit IP address yang tersedia dengan lebih efisien.Teknik subnetting membuat skala jaringan lebih luas dan tidak dibatas oleh kelas-kelas IP (IP Classes) A, B, dan C yang sudah diatur. Dengan subnetting, dibuat network dengan batasan host yang lebih realistis sesuai kebutuhan. Subnetting menyediakan cara yang lebih fleksibel untuk menentukan bagian mana dari sebuah 32 bit IP adddress yang mewakili netword ID dan bagian mana yang mewakili host ID.

Dengan kelas-kelas IP address standar, hanya 3 kemungkinan network ID yang tersedia; 8 bit untuk kelas A, 16 bit untuk kelas B, dan 24 bit untuk kelas C. Subnetting mengizinkan pengguna memilih angka bit acak (arbitrary number) untuk digunakan sebagai network ID.

Dua alasan utama melakukan subnetting:

- Mengalokasikan IP address yang terbatas supaya lebih efisien. Jika internet terbatas oleh alamat-alamat di kelas A, B, dan C, tiap network akan memliki

254, 65.000, atau 16 juta IP address untuk host devicenya. Walaupun terdapat banyak network dengan jumlah host lebih dari 254, namun hanya sedikit network yang memiliki host sebanyak 65.000 atau 16 juta. Dan network yang memiliki lebih dari 254 device akan membutuhkan alokasi kelas B dan mungkin akan menghamburkan percuma sekitar 10 ribuan IP address.

- Alasan kedua adalah, walaupun sebuah organisasi memiliki ribuan host device, mengoperasikan semua device tersebut di dalam network ID yang sama akan memperlambat network. Cara TCP/IP bekerja mengatur agar semua komputer dengan network ID yang sama harus berada di physical network yang sama juga. Physical network memiliki domain broadcast yang sama, yang berarti sebuah medium network harus membawa semua traffic untuk network. Karena alasan kinerja, network biasanya disegmentasikan ke dalam domain broadcast yang lebih kecil – bahkan lebih kecil – dari Class C address.

Penghitungan subnetting bisa dilakukan dengan dua cara, cara binary yang relatif lambat dan cara khusus yang lebih cepat. Pada hakekatnya semua pertanyaan tentang subnetting akan berkisar di empat masalah: Jumlah Subnet, Jumlah Host per Subnet, Blok Subnet, dan Alamat Host- Broadcast.

Penulisan IP address umumnya adalah dengan 192.168.1.2. Namun adakalanya ditulis dengan 192.168.1.2/24, artinya bahwa IP address 192.168.1.2 dengan subnet mask 255.255.255.0. /24 diambil dari penghitungan bahwa 24 bit subnet mask diselubung dengan binari 1.

Atau dengan kata lain, subnet masknya adalah: 11111111.11111111.11111111.00000000 (255.255.255.0). Konsep ini yang disebut dengan CIDR (Classless Inter-Domain Routing) yang diperkenalkan pertama kali tahun 1992 oleh IEFT.

Subnet Mask yang bisa digunakan untuk melakukan subnetting dapat dilihat pada tabel di bawah:

Tabel Subnetting

Subnet Mask	Nilai CIDR
255.128.0.0	/9
255.192.0.0	/10
255.224.0.0	/11
255.240.0.0	/12
255.248.0.0	/13
255.252.0.0	/14
255.254.0.0	/15
255.255.0.0	/16
255.255.128.0	/17
255.255.192.0	/18
255.255.224.0	/19

Subnet Mask	Nilai CIDR
255.255.240.0	/20
255.255.248.0	/21
255.255.252.0	/22
255.255.254.0	/23
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

Subnetting Pada IP Address Class C

Subnetting seperti apa yang terjadi dengan sebuah NETWORK ADDRESS **192.168.1.0/26**

Analisa: 192.168.1.0 berarti kelas C dengan Subnet Mask /26 berarti 11111111.11111111.11111111.11000000 (255.255.255.192).

Penghitungan: Seperti sudah disebutkan sebelumnya semua pertanyaan tentang subnetting akan berpusat di 4 hal, jumlah subnet, jumlah host per subnet, blok subnet, alamat host dan broadcast yang valid. Jadi diselesaikan dengan urutan seperti itu:

1. **Jumlah Subnet** = 2^x, dimana x adalah banyaknya binari 1 pada oktet terakhir subnet mask (2 oktet terakhir untuk kelas B, dan 3 oktet terakhir untuk kelas A). Jadi Jumlah Subnet adalah $2^2 = 4$ subnet
2. **Jumlah Host per Subnet** = $2^y - 2$, dimana y adalah adalah kebalikan dari x yaitu banyaknya binari 0 pada oktet terakhir subnet. Jadi jumlah host per subnet adalah $2^6 - 2 = 62$ host

3. **Blok Subnet** = 256 – 192 (nilai oktet terakhir subnet mask) = 64. Subnet berikutnya adalah 64 + 64 = 128, dan 128+64=192. Jadi subnet lengkapnya adalah **0, 64, 128, 192**.
4. Sebagai catatan, host pertama adalah 1 angka setelah subnet, dan broadcast adalah 1 angka sebelum subnet berikutnya.

Tabel 2.2. Hasil Subnet Kelas C

Subnet	192.168.1.**0**	192.168.1.**64**	192.168.1.**128**	192.168.1.**192**
Host Pertama	192.168.1.**1**	192.168.1.**65**	192.168.1.**129**	192.168.1.**193**
Host Terakhir	192.168.1.**62**	192.168.1.**126**	192.168.1.**190**	192.168.1.**254**
Broadcast	192.168.1.**63**	192.168.1.**127**	192.168.1.**191**	192.168.1.**255**

Setelah menyelesaikan subnetting untuk IP address Class C. Selanjutnya untuk subnet mask yang lain, dengan konsep dan teknik yang sama. Subnet mask yang bisa digunakan untuk subnetting class C adalah seperti di bawah.

Tabel 2.3. Tabel Subnet Kelas C

Subnet Mask	Nilai CIDR
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30