2. TCP/IP

2.1. TCP dan UDP
2.2. IP Address
2.3. ARP (Address Resolution Protocol)
2.4. RARP (Reverse Address Resolution Protocol)
2.5. DHCP (Dinamic Host Configuration Protocol)
2.6. ICMP (Internet Control Message Protocol)

Pengenalan TCP/IP

Model Referensi DoD (Department of Defense)

Model referensi klasik OSI (Open System Interconnection) mempunyai 7 lapisan (layer) d an merupakan referensi yang sangat lengkap dan sempurna serta mencakup semua tentang networking. Untuk lebih jelas dan detailnya silakan baca buku -buku tentang networking dan TCP/IP.
Disini hanya akan di bahas sedikit tentang referensi model DoD yang merupakan cika l bakal dari TCP/IP

Model DoD membagi network dalam 4 layer. Tabel berikut akan memperlihatkan perbedaan antara model DoD dan OSI.

Model DoD	Model OSI	Layanan/Protokol
Process / Aplication	Aplication Presentation Session	Telnet, FTP, SMTP, HTTP, DNS, TFTP, SNMP, dll
Transport / Logical Protocol	Transport	UDP, TCP
Internet / Physical Protocol	Network	IP, ICMP, ARP, BootP
Network Access / Physical Layer	Data Link Physical	Ethernet, Token Ring , FDDI, Slip, PPP, x25

Network Access / Physical Layer
Bertanggung Jawab mengirim dan menerima data ke dan dari me dia fisik. Media Fisiknya dapat berupa kabel, Serat Optik, Gelombang Radio (Wi reless). Protokol pada layer ini harus mampu menerjemahkan sinyal listrik menjadi data digital yang dimengerti komputer.

Internet / Physical Protocol
Protokol yang berada pada l ayer ini bertanggung jawab dalam proses pengiriman paket (data) ke alamat yang tepat dan tanpa kerusakan.

Transport / Logical Protocol
Protokol ini bertangung jawab untuk mengadakan komunikasi (hubungan) antara dua host (komputer).

Process / Aplication Layer
Pada layer ini terletak semua aplikasi yang mengunakan protokol TCP/IP

2.1. TCP dan UDP

TCP/IP adalah standarad umum yang di pakai untuk mengkoneksikan di antara peralatan jaringan dan juga merupakan dasar dari komunikasi data.

Data biasanya dipecah menjadi beberapa bagian atau paket, paket data di pecah dalam jumlah yang sesuai dengan besaran paket, kemudian dikirim satu persatu hingga selesai.

Pada setiap paket menyertakan Nomor seri / urut (squence number) Pada remote komputer (penerima) mengurutkan kembali paket -paket tersebut dan mengirimkan sinyal ACK (acknowledge) pada setiap paket yang diterima. Bila pada waktu tertentu pengirim tidak menerima sinyal ACK maka pengiriman paket gagal dan harus di ulang kembali.

Ada 2 jenis mekanisme tranport yang paling populer digunakan dalam internet yaitu TCP (Transmission Control Protocol (TCP) dan User Datagram Protocol (UDP).

Bagaimana komputer penerima mengetahui paket yang dikirim untuk program aplikasi apa?. Diantara IP paket selalu berisi potongan informasi di dalam header yang disebut type field. Inilah yang menginformasikan komputer penerima jenis data yang mana , TCP atau UDP yang di kirim. Komputer penerima melakukan pengecekan pada header tersebut apakah data yang dikirim TCP atau UDP dan port mana yang di gunakan, kemudian menentukan program aplikasi mana yang akan memproses data tersebut.

TCP berfungsi untuk mengubah suatu blok data yang besar menjadi segment -segment yang di nomori dan disusun secara berurutan agar penerima dapat menyusun kembali segment-segment tersebut seperti waktu pengiriman. TCP adalah jenis protokol yang Connection Oriented yang memberikan jaminan layanan (bergaransi).

UDP adalah jenis protokol yang Connectionless. UDP bergantung pada lapisan atas untuk mengontrol keutuhan data. Oleh karen penggunaan bandwidth yang efektif, UDP banyak digunakan untuk aplikasi-aplikasi yang tidak peka terhadap ganguan jaringan seperti SNMP, TFTP dan lain sebagainya.

Network Ports

Ports adalah "Pintu Masuk" datagram dan paket data, port yang ada pada komputer sangat banyak sekali mulai dari 0 sampai port 65536.

Port 0 sampai 1024 disediakan untuk layanan yang standart, seperti FTP, Telnet, SSH, Mail, Web dan masih banyak lagi. Port -port ini disebut juga sebagai well know port.

Ketika sebuah paket (TCP atau UDP) datang pada sistem, paket itu meminta dikirimkan ke ports yang sudah ditentukan. Beda port melayani service (program aplikasi) yang berbeda pula. Service email server biasa disebut SMTP (Simple Ma il Transport Protocol) berjalan pada port 25. Jika sebuah koneksi TCP meminta jawaban untuk port 25, maka dapat di katakan koneksi tersebut untuk mail server. Port mengijinkan banyak koneksi diantara banyak mesin (host).
Contoh port yang di pakai TCP dan UDP

TCP Port		UDP Port	
No Port	Aplikasi	No Port	Aplikasi
20, 21	FTP	15	Netstat (Network Status)
23	Telnet	53	DNS
22	SSH	69	TFTP
25	SMTP	137	NetBIOS Name Service
80	HTTP (web)	161	SNMP

2.2. IP address

1. IP Address

IP (Internet Protocol) address (alamat IP) adalah suatu identitas yang unik dari suatu node atau host dalam sua tu Jaringan (network). Format alamat dari IP adalah X.Y.W.Z , masing masing huruf tersebut terdirti dari 8 bit sehingga kalau di tampilkan dalam desimal berupa angka dari 0 -255 (di kenal sebagai bilangan octets) dan di pisahkan oleh notasi titik (dot).

contoh : 192.168.1.1

IP Address	:	192	.168	.1	.1
dalam binari	:	11000000	11001000	00000001	00000001

Aturan penggunaan IP adalah tidak di perbolehkan penggunaan semua nilai 0 atau 1 dalam bentuk binari untuk Network ID maupun Host ID. Angka 255 dal am desimal sama dengan 11111111 dalam binari (angka 1 semua) dan angka 0 dalam desimal sama dengan 00000000 (angka 0 semua) dalam binari. Kelas dari address dan subnet mask , yang memisahkan yang mana bagin dari network id , dan yang mana yang menjadi host id. Sebuah IP Address adalah bilangan binari 32 bit, mengapa 32 bit ? 32 bit di ambil dari 4 * 8 bit (yang mewakili 1 huruf pad format IP di atas).

2. Peng-kelasan IP Address

Ada 5 kelas IP address yang berbeda. Kita dapat menyebutkan IP itu termasuk d i dalam kelas apa dengan memperhatikan 4 bits pertama dari IP address tersebut. Aturan untuk kelas A nilai binari -nya selalu di mulai dengan 0, kelas B dimulai dari 10, kelas C 110, kelas D 1110, dan kelas E 1111.

Kelas A address di mulai dari 0XXX atau 1 sampai 126 desimal
Kelas B address di mulai dari 10XX atau 128 sampai 191 desimal
Kelas C address di mulai dari 110X atau 192 sampai 223 desimal
Kelas D address di mulai dari 1110 atau 224 sampai 239 desimal
Kelas E address di mulai dari 1111 atau 240 sampai 254 desimal

Address yang di mulai dengan 01111111 atau 127 (desimal) digunakan khusus untuk loopback dan internal testing pada local mechine (localhost). Kelas D di gunakan khusus untuk multicasting. Kelas E di gunakan untuk eksperiment. IP-IP itu tidak di pergunakan untuk alamat host (host address).

Pembagian kelas IP secara default yang menjelaskan mana bagian dari Network ID (N) dan Host ID (h) sebagai berikut:
Kelas A : NNNNNNNN.hhhhhhhh.hhhhhhhh.hhh hhhhh
Kelas B : NNNNNNNN.NNNNNNNN.hhhhhhhh.hhhhhhhh
Kelas C : NNNNNNNN.NNNNNNNN.NNNNNNNN.hhhhhhhh

Contoh: 150.150.100.100 adalah IP kelas B secara default Network ID di definisikan oleh 2 oktet pertama (150.150.x.x) dan Host ID di definisikan oleh 2 octet terakhir (x.x.100.100).

Private IP Address

Ada 3 blok IP Network Address (ID) yang di gunakan khusus untuk jaringan private (lokal). Blok IP tersebut adalah 10.0.0.0/8 (10.0.0.0/255.0.0.0), 172.16.0.0/12 (172.16.0.0/255.240.0.0), dan 192.168.0.0/16 (192.168.0.0/255.255.0.0). IP-IP tersebut dapat digunakan oleh siapa saja untuk jaringan lokal (internal), seperti dalam lab, LAN dalam rumah atau kantor, LAN yang di belakang NAT (network Address Translation) atau proxy server atau juga router. Router di internet tidak akan pernah melewatkan paket (data) yang datang dari IP-IP tersebut. Tentang IP Address tersebut didefinisikan dalam RFC1918.

3. Network, Host dan Subnet

IP address sebenarnya dibagi dalam 2 bagian yaitu Network ID dan Host ID. Network ID yang membedakan antara Network (jaringan),Host ID yang membedakan antara host-host (node) atau komputer.

Agar komputer dapat saling berhubungan maka komputer-komputer tersebut haruslah mempunyai Network ID yang sama dan mempunyai Host ID yang berbeda. Jika Network ID berbeda antara 2 komputer, maka di katakan komputer tersebut tidak berada pada satu jaringan (network) dan tidak dapat berhubungan (kecuali melalui router).

Subnetting adalah suatu metode untuk memperbanyak network ID dari satu network ID, yaitu sebagian host ID dikorbankan untuk di gunakan didalam membuat network ID tambahan.

Subnet pada Jaringan IP digunakan untuk berbagai macam keperluan antara lain: penyatuan kelompok (organisasi), penggunaan media fisik yang berbeda (Ethernet, FDDI, WAN, dsb), Penghematan IP address, keamanan. Sebagian besar penggunaannya adalah untuk mengontrol lalu litas jaringan. Pada Jaringan Ethernet semua host (nodes) dalam satu segment dapat melihat semua packet yang dikirimkan oleh semua ke host (node) lain dalam satu segment. Performa jaringan akan menjadi lambat bila komputer yang terhubung dalam satu segment network (jaringan) semakin banyak (bertambah), hal ini disebabkan karena adanya collisions dan juga adanya retransmissions packet. Sebuah router di gunakan untuk meminimilisasi jumlah trafik diantara segment network yang harus di terima.

Penggunaan subnet mask pada IP Address memungkinkan kita untuk mengetahui Network ID dan Host ID pada IP Address tersebut. Pada Subnet Mask, Network ID mengunakan (diwakili) bit 1 semua, dan Host ID di wakili oleh bit 0 semua. Menghitung Network ID dapat dilakukan dengan menggunakan logika AND antara IP Address dan Subnet Mask.
Cara mendapatkan Subnet dengan rumus = 2^n - 2 (2 pangkat n di kurangi 2, di mana n adalah banyaknya bit mask pada satu kelompok oktet terakhir yang mempunyai nilai binari 1 semua).
Sedangkan untuk mendapatkan Host (IP) persubnet = 2^N - 2 (2 pangkat N di kurangi 2 di mana N adalah sisa bit untuk host ID)
Contoh:

150.150.100.100	IP Address kelas B	10010110.10010110.01100100.01100100
255.255.0.0	Default subnet mask kelas B	11111111.11111111.00000000.00000000
	- AND ----------	
150.150.0.0	Network ID	10010110.10010110.00000000.00000000

Adapun Default dari subnet mask kelas -kelas IP adalah

Kelas A : 255.0.0.0	11111111.00000000.00000000.00000000
Kelas B : 255.255.0.0	11111111.11111111.00000000.00000000
Kelas C : 255.255.255.0	11111111.11111111.11111111.00000000

Persedian IPv4 berkelas (kelas A,B,C) di khawatirkan semakin tidak mencukupi kebutuhan, maka diciptakan beberapa metode lain untuk memperbanyak persedian IP address.

3.1. VLSM (Variable Length Subnet Masks)

Jaringan yang menerapkan ukuran subnet yang berbeda-beda (mengunakan lebih dari satu subnet masks) untuk tiap subnetnya di sebut VLSM.

Dengan VLSM memungkinkan dibaginya IP Address secara rekursif sehingga dapat disusun kembali di level paling atas untuk mengurangi jumlah informasi routing. S ecara konsep sebuah network mula -mula dibagi menjdi subnet, kemudian dibagi lagi menjadi sub-subnet, kemudian di bagi lagi menjadi sub -sub-subnet dan seterusnya.

Contoh :

subnet 1.	150.150.0.0/16
sub-subnet 1.1.	150.150.1.0/24, 150.150.2.0/24, 150.150.3.0/24, ...
sub-sub-sbanet 1.1.1	150.150.1.0/27, 150.150.1.32/27, 150.150.1.64/27, ...

3.2. CIDR (Classless Inter-Domain Routing)
Di perkenalkan pada tahun 1992 konsep yang dinamakan Supernetting atau CIDR.
CDIR menghindarkan cara pemberian IP address tradisional yang menggunakan kelas A, B, C. CIDR menggunakan network prefix dengan panjang tertentu. Prefix-length menentukan jumlah bit sebelah kiri yang akan dipergunakan sebagai network ID.

Contoh jika suatu IP address memiliki 18 bit sebagai network ID, Ip address tersebut akan diberikan prefix-length 18 bit atau umumnya di tulis sebagai /18 di belakang ip address tersebut seperti contoh: 150.150.1.1/18

Karena tidak mengenal kelas, CIDR dapt mengalokasikan kelompok IP address dengan lebih efektif.

Contoh, suatu address blok 150.150.16.0/20 dengan tradisional IP address berkelas memberikan 4096 blok /20 dan harus di bagi menjadi 16 blok /24. Setipa yang meminta IP harus menerima blok IP address yang sama karena harus memenuhi peraturan kelas yang telah ditentukan.

Dengan metode CIDR, blok 150.150.16.0/20 dapat si bagi sesukanya tergantung kebutuhan pemakai.

VLSM dan CIDR mempunyai kemiripan, yaitu suatu blok network address dapat di bagi lebih lanjut menjadi sejumlah blok IP address yang lebih kecil.

Perbedan VLSM dan CIDR adalah pembagian blok pada VLSM dilakukan oleh pemilik network address yang memiliki blok network address yang telah di berikan padanya, oleh sebab itu tidak di kenal oleh internet. Sedangkan dengan CIDR, lembaga pemberi IP yang membagikan blok-bok IP address tersebut sehingga dikenal oleh internet.

Umumnya suatu host hanya mengenal IP address berkelas, maka untuk dapat mengunakan metode CIDR maupun VLSM, jaringan harus memenuhi persyaratan-persyaratan tertentu yaitu:

- Routing protokol yang di gunakan harus mempu membawa informasi mengenai network-prefix untuk setiap rute yang disiarkan. Routing protokol RIP versi 1 tidak dapat di gunakan.
- Semua router yang dipergunakan pada jaringan harus mampu mendukung penggunaan metode CIDR atau VLSM dan menggunakan forward algorithm (algoritma penerus) yang sama berdasarkan "longest match".

Contoh lebih lanjut pembagian IP yang lebih kecil
Kita memakai IP kelas B 150.150.25 5.0 dengan Subnet Mask 255.255.255.252. Dengan

subnet mask 255.255.255.252 (11111111.1111111.11111111.11111100) maka kita dapat menghitung :
Subnet yang dapat di peroleh:
oktet terakhir subnet 252 (11111100) maka di dapat 2^6 - 2 = 62 buah subnet mask.
Jumlah Host ID per subnet yang bisa di dapat = 256 -252 = 4 , Kelompok Subnet yang dapat di pakai adalah kelipan angka 4.

150.150.255.4	10010110.10010110.11111111.00000100	IP Address
255.255.255.252	11111111.11111111.11111111.11111100	Subnet Mask
--- AND ----------		
150.150.255.4	10010110.10010110.11111111.00000100	Network ID

Dengan alamat netwotk (Network ID) 150.150.255.4 dan subnet mask 255.255.255.252 maka bisa di dapat 4 ip address dengan hanya 2 IP yang bisa di gunakan. yaitu

150.150.255.4	10010110.10010110.11111111.00000100	Network ID
150.150.255.5	10010110.10010110.11111111.00000101	IP ke 1 yang di dapat
150.150.255.6	10010110.10010110.11111111.00000110	IP ke 2 yang di dapat
150.150.255.7	10010110.10010110.11111111.00000111	Alamat brodcast

3.3. Notasi Prefix

Mungkin ada yang masih bingung tenta ng penulisan IP address, misal IP address 150.150.255.6 dengan subnet mask 255.255.255.252 namun hal ini bisa di persingakat dengan menulis 150.150.255.6/30 hal ini adalah sama saja cuma beda penulisan, angka 30 inilah yang di maksudkan sebagai notasi P refix. Tapi dari dari mana asalnya angka 30 ini. Subnet 255.255.255.252 bila di ubah ke dalam format binari adalah 11111111.11111111.11111111.11111100 banyaknya angka 1 pada subnet tersebut adalah 30. Jadi maksud angka 30 adalah 30 bit.

4. IPv6 (IP version 6)

Sejauh ini IP adres yang di bahas adalah yang disebut IPv4 (IP version 4) yang terdiri atas 32 bit angka binari. Untuk mengatasi permintaan IP address yang makin meningkat, lembaga IANA mengelurkan IPv6 yang terdiri atas 128 bit angka binari.

Dengan menggunakan angka binari empat kali lebih banyak, IPv6 memiliki persediaan IP address yang jauh lebih banyak dibanding IPv4.

Negara yang sangat antusias mengembangkan IPv6 adalah jepang. Karena kalau IPv6 ini sudah sudah di terima secara luas maka perala tan elektronik seperti Microwave, TV, Lemari Es, dan lain sebagainya akan dapat di koneksikan ke internet.
Di Indonesia sendiri baru isp CBN yang akan menerapkan IPv6. Dan menurut kabar terakhir (NICE 2004) indonesia akan menjadi negara yang pertama kali mengimplementasikan IPv6 .

2.3. ARP (Address Resolution Protocol)

ARP adalah protokol yang bertugas mengadakan mapping atau translasi dari IP Addres s (32 bit) yang diketahui ke Hardware Address (MAC Address) (48 bit).
ARP termasuk dalam jenis protokol broa dcast. Suatu host biasanya menyimpan informasi ARP dalam memori yang disebut ARP Cache, yang di gunakan untuk akses yang cepat. Pengunaan ARP Cache ini dengan asumsi pada umumnya relasi dari MAC Address dengan IP Address jarang sekali berubah -ubah.

2.4. RARP (Reverse Address Resolution Protocol)

RARP adalah protokol yang berguna untuk mengadakan translasi MAC Address yang diketahui menjadi IP Address. Pada saat komputer dihidupkan ia akan melakukn broadcast kejaringan, dan menanyakan apakah ada se rver yang dapat memb erikan IP Address untuknya. Paket broadcast tersebut dikirim beserta dengan MAC Address. Server DHCP yang mendengar permintaan tersebut akan menjawab dengan memberikan nomor IP.

2.5. DHCP (Dinamic Host Configuration Protocol)

DHCP server dapat memberikan IP Address secara otomtis ke suatu host (komputer) yang menggunkan prtotokol TCP/IP. DHCP bekerja dengan relasi client -server. DHCP Server menyediakan suatu kelompok Ip Address yang dapat diberikan ke suatu DHCP Client.

Sebenarnya DHCP Server hanya meminjamkan IP Address tersebut untuk suatu periode tertentu. Jika periode tersebut telah dicapai IP Address dapat dipinjamkan ke host yang lain yang memerlukan.

Jika suatu host berada dalam segment jaringan yang berbeda (beda network), harus digunakan DHCP Relay agar host tersebut bisa mendapatkan IP Address.

2.6. ICMP (Internet Control Message Protocol)

ICMP adalah protokol yang berguna untuk membrikan informasi jika terjadi suatu masalh (error) dalam pengiriman data atau dalam jaringan.
Fungsi ICMP antar lain :

- Memberitahukan jika ada paket yang tidak sampai ketujuan.
- Memberitahukan jika memory buffer di Router penuh.
- Redirect paket dari gateway ke host.
- Ping menggunakan ICMP echo untuk memeriksa jaringan atau host.