

Kata Pengantar

Puji syukur kami panjatkan kehadiran Allah SWT, atas segala rahmat dan karuniaNya sehingga kami dapat menyelesaikan buku ajar Modul 1 Mikrotik Operating System Jaringan Komputer ini dengan baik. Buku ini dibuat sebagai panduan belajar Jaringan Komputer, khususnya bagi mahasiswa Fakultas Teknologi Informasi, Universitas Kanjuruhan Malang.

Buku ini diharapkan dapat menjadi acuan dan referensi mahasiswa yang sedang menempuh matakuliah Jaringan Komputer. Dengan tersusunnya buku ajar ini juga memudahkan bagi dosen yang mengampu matakuliah ini dalam memberikan perkuliahannya. Selain itu juga menambah perbendaharaan buku ajar yang ada di Fakultas Teknologi Informasi, Universitas Kanjuruhan Malang.

Tiada gading yang tak retak. Penulis menyadari bahwa kesalahan dan kekurangan masih melekat dalam penyusunan buku ajar ini, karena buku ajar ini masih jauh dari sempurna. Oleh karena itu penulis sangat mengharapkan kritik dan saran dari berbagai pihak demi perbaikan buku ajar ini.

Akhir kata, semoga buku ini bermanfaat bagi kami dan para pembaca untuk memberikan tambahan pengetahuan, dan wawasan khususnya dalam bidang Jaringan Komputer.

Malang, 13 Maret 2015

Penulis,

DAFTAR ISI

DAFTAR ISI	2
DAFTAR GAMBAR	3
DAFTAR TABEL	5
BAB 1 KONSEP JARINGAN KOMPUTER	6
A. SEJARAH JARINGAN KOMPUTER	6
BAB 2 PROTOKOL JARINGAN KOMPUTER	10
BAB 3 HARDWARE & SOFTWARE	30
BAB 5 : MODEL REFERENSI OSI	54
BAB 7 : ROUTING	73
BAB 8 MIKROTIK	89

DAFTAR GAMBAR

Gambar 1. Jaringan Komuter Model TSS	10
Gambar 2. Jaringan Komputer Model distibuted	11
Gambar 3. Contoh ethernet address.....	12
Gambar 4. Jaringan dengan media 10Base5.....	14
Gambar 5 Struktur 10Base5	14
Gambar 6. Jaringan dengan media 10Base5.....	14
Gambar 7 Struktur 10Base2.	15
Gambar 8. Jaringan dengan media 10BaseT.	15
Gambar 9. Struktur 10BaseT.....	15
Gambar 10. Struktur 10BaseF	17
Gambar 11. <i>Dua jenis jaringan broadcast. (a) Bus. (b) Ring</i>	21
Gambar 12. Arsitektur MAN DQDB	23
Gambar 13. <i>Hubungan antara host-host dengan subnet</i>	24
Gambar 14. <i>beberapa topologi subnet untuk poin-to-point</i>	24
Gambar 15. <i>Protokol Ethernet</i>	26
Gambar 16. <i>Protokol Token Ring</i>	27
Gambar 17. <i>Protokol FDDI</i>	28
Gambar 18. <i>Aplikasi File Server</i>	30
Gambar 19. <i>Perangkat-perangkat Jaringan</i>	31
Gambar 20. <i>Network Interface Card (NIC)</i>	32
Gambar 21. <i>LocalTalk Card</i>	33
Gambar 22. <i>Switch</i>	33
Gambar 23. <i>Access Point</i>	35
Gambar 24. <i>Kabel Coaxial dan Berbagai Connector</i>	35
Gambar 25. <i>UTP Cross-Over</i>	36
Gambar 26. <i>Fiber Optic</i>	37
Gambar 27. <i>Komunikasi radio</i>	38
Gambar 28. <i>Perangkat Wireless LAN</i>	39
Gambar 29. <i>Komunikasi Satelit dengan VSAT</i>	40
Gambar 30. <i>Topologi Mesh</i>	42

Gambar 31. <i>Topologi Star</i>	43
Gambar 32. <i>Topologi Bus</i>	44
Gambar 33. <i>Topologi Cincin</i>	45
Gambar 34. Topologi Ring	46
Gambar 35. TCP/ IP Layer	47
Gambar 36. <i>Model Referensi OSI</i>	54
Gambar 37. <i>Contoh tentang bagaimana model OSI digunakan</i>	63
Gambar 38. Kelas IP Address	65
Gambar 39. Pembagian Oktet tiap kelas	67
Gambar 40. Perhitungan 2 pangkat N.....	67
Gambar 41. Perubahan topologi distance vector	80
Gambar 42. perubahan topologi distance vector.....	80
Gambar 43. routing loop	81
Gambar 44. masalah: counting to infinity.....	82
Gambar 45. solusi: mendefinisikan nilai maksimum	82
Gambar 46. Solusi: Split Horizon	83
Gambar 47. <i>route poisoning</i>	84
Gambar 48. Tampilan Winbox	92
Gambar 49. Memberi nama pada Mikrotik	92
Gambar 50. Mengganti nama interface.....	93
Gambar 51. Setting IP Address	94
Gambar 52 Setting default route.....	94
Gambar 53. Setting DNS	95
Gambar 54. Setting SRC-NAT Masquerading	96
Gambar 55. DHCP Server Setup	97
Gambar 56. DHCP Client Setup.....	98
Gambar 57. Interface Bridging Setup	99
Gambar 58. Topologi Jaringan RIP	100
Gambar 59. Topologi Jaringan OSPF.....	102

DAFTAR TABEL

Table 1. Daftar vendor terkenal chip ethernet	12
Table 2. Jenis kabel UTP dan aplikasinya	15
Table 3. Faktor-faktor mendesain LAN.....	17
Table 4. Klasifikasi prosesor interkoneksi berdasarkan jarak	19
Table 5. <i>Daftar Protokol</i>	28
Table 6. <i>Daftar kategori Twisted Pair</i>	36
Table 7. <i>Frekuensi Kerja Satelit</i>	40
Table 8. Pemisahan Lapisan atas dan Lapisan bawah pada model OSI.....	56
Table 9. Perhitungan 2 pangkat N	68
Table 10. Network Class	70
Table 11. Range IP Address	71
Table 12. Router dan Switch	74



BAB 1 Konsep Jaringan Komputer

A. SEJARAH JARINGAN KOMPUTER

Perkembangan teknologi komputer meningkat dengan cepat, hal ini terlihat pada era tahun 80-an jaringan komputer masih merupakan teka-teki yang ingin dijawab oleh kalangan akademisi, dan pada tahun 1988 jaringan komputer mulai digunakan di universitas-universitas, perusahaan-perusahaan, sekarang memasuki era milenium ini terutama world wide internet telah menjadi realitas sehari-hari jutaan manusia di muka bumi ini.

Selain itu, perangkat keras dan perangkat lunak jaringan telah benar-benar berubah, di awal perkembangannya hampir seluruh jaringan dibangun dari kabel koaxial, kini banyak telah diantaranya dibangun dari serat optik (*fiber optics*) atau komunikasi tanpa kabel.

Sebelum lebih banyak lagi dijelaskan mengenai jaringan komputer secara teknis, pada bab pendahuluan ini akan diuraikan terlebih dahulu definisi jaringan komputer, manfaat jaringan komputer, dan macam jaringan komputer.

B. DEFINISI JARINGAN KOMPUTER

Dengan berkembangnya teknologi komputer dan komunikasi suatu model komputer tunggal yang melayani seluruh tugas-tugas komputasi suatu organisasi kini telah diganti dengan sekumpulan komputer yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya, sistem seperti ini disebut jaringan komputer (*computer network*).⁽¹⁾

Dalam buku ini kita akan menggunakan istilah jaringan komputer untuk mengartikan suatu himpunan *interkoneksi* sejumlah komputer yang *autonomous*. Dua buah komputer dikatakan terinterkoneksi bila keduanya dapat saling bertukar informasi. Bentuk koneksinya tidak harus melalui kawat tembaga saja melainkan dapat menggunakan serat optik, gelombang mikro, atau satelit komunikasi.

Untuk memahami istilah jaringan komputer sering kali kita dibingungkan dengan sistem terdistribusi (*distributed system*). Kunci perbedaannya adalah bahwa sebuah sistem

terdistribusi, keberadaan sejumlah komputer autonomus bersifat transparan bagi pemakainya. Seseorang dapat memberi perintah untuk mengeksekusi suatu program, dan kemudian program itupun akan berjalan dan tugas untuk memilih prosesor, menemukan dan mengirimkan file ke suatu prosesor dan menyimpan hasilnya di tempat yang tepat merupakan tugas sistem operasi. Dengan kata lain, pengguna sistem terdistribusi tidak akan menyadari terdapatnya banyak prosesor (multiprosesor), alokasi tugas ke prosesor-prosesor, alokasi file ke disk, pemindahan file yang disimpan dan yang diperlukan, serta fungsi-fungsi lainnya dari sistem harus bersifat otomatis.

Pada suatu jaringan komputer, pengguna harus secara eksplisit log ke sebuah mesin, secara eksplisit menyampaikan tugasnya dari jauh, secara eksplisit memindahkan file-file dan menangani sendiri secara umum seluruh manajemen jaringan. Pada sistem terdistribusi, tidak ada yang perlu dilakukan secara eksplisit, semuanya sudah dilakukan secara otomatis oleh sistem tanpa sepengetahuan pemakai.

Dengan demikian sebuah sistem terdistribusi adalah suatu sistem perangkat lunak yang dibuat pada bagian sebuah jaringan komputer. Perangkat lunaklah yang menentukan tingkat keterpaduan dan transparansi jaringan yang bersangkutan. Karena itu perbedaan jaringan dengan sistem terdistribusi lebih terletak pada perangkat lunaknya (khususnya sistem operasi), bukan pada perangkat kerasnya.

C. MANFAAT JARINGAN KOMPUTER

Sebelum membahas kita masalah-masalah teknis lebih mendalam lagi, perlu kiranya diperhatikan hal-hal yang membuat orang tertarik pada jaringan komputer dan untuk apa jaringan ini digunakan. Manfaat jaringan komputer bagi manusia dapat dikelompokkan pada jaringan untuk perusahaan, jaringan untuk umum, dan masalah sosial jaringan.

1. Jaringan untuk perusahaan/organisasi

Dalam membangun jaringan komputer di perusahaan/ organisasi, ada beberapa keuntungan yang dapat diperoleh dalam hal-hal resource sharing, reliabilitas tinggi, lebih ekonomis, skalabilitas, dan media komunikasi.

Resource sharing bertujuan agar seluruh program, peralatan, khususnya data dapat digunakan oleh setiap orang yang ada pada jaringan tanpa terpengaruh oleh lokasi resource dan pemakai. jadi source sharing adalah suatu usaha untuk menghilangkan kendala jarak.

Dengan menggunakan jaringan komputer akan memberikan **reliabilitas tinggi** yaitu adanya sumber-sumber alternatif pengganti jika terjadi masalah pada salah satu perangkat dalam jaringan, artinya karena perangkat yang digunakan lebih dari satu jika salah satu perangkat mengalami masalah, maka perangkat yang lain dapat menggantikannya.

Komputer yang kecil memiliki rasio harga/kinerja yang lebih baik dibanding dengan komputer besar. Komputer mainframe memiliki kecepatan kurang lebih sepuluh kali lipat kecepatan komputer pribadi, akan tetapi harga mainframe seribu kalinya lebih mahal. Dengan selisih rasio harga/kinerja yang cukup besar ini menyebabkan perancang sistem memilih membangun sistem yang terdiri dari komputer-komputer pribadi dibanding menggunakan mainframe.

Yang dimaksud dengan **skalabilitas** yaitu kemampuan untuk meningkatkan kinerja sistem secara berangsur-angsur sesuai dengan beban pekerjaan dengan hanya menambahkan sejumlah prosesor. Pada komputer mainframe yang tersentralisasi, jika sistem sudah jenuh, maka komputer harus diganti dengan komputer yang mempunyai kemampuan lebih besar. Hal ini membutuhkan biaya yang sangat besar dan dapat menyebabkan gangguan terhadap kontinuitas kerja para pemakai.

Sebuah jaringan komputer mampu bertindak sebagai **media komunikasi** yang baik bagi para pegawai yang terpisah jauh. Dengan menggunakan jaringan, dua orang atau lebih yang tinggal berjauhan akan lebih mudah bekerja sama dalam menyusun laporan.

2. Jaringan untuk umum

Apa yang telah diulas di atas bahwa minat untuk membangun jaringan komputer semata-mata hanya didasarkan pada alasan ekonomi dan teknologi saja. Bila komputer mainframe yang besar dan baik dapat diperoleh dengan harga murah, maka akan banyak perusahaan/organisasi yang menggunakannya.

Jaringan komputer akan memberikan layanan yang berbeda kepada perorangan di rumah-rumah dibandingkan dengan layanan yang diberikan pada perusahaan seperti apa yang telah diulas di atas. Terdapat tiga hal pokok yang menjadi daya tarik jaringan komputer pada perorangan yaitu:

- access ke informasi yang berada di tempat yang jauh
- komunikasi orang-ke-orang
- hiburan interaktif.

Ada bermacam-macam bentuk access ke informasi jarak jauh yang dapat dilakukan, terutama setelah berkembangnya teknologi internet, berita-berita di koran sekarang dapat di download ke komputer kita melalui internet, dan tidak hanya itu sekarang kita dapat melakukan pemesanan suatu produk melalui internet, bisnis yang dikenal dengan istilah *electronic commerce* (e-commerce), ini sekarang sedang berkembang dengan pesat.

Dengan menggunakan internet kita juga dapat melakukan komunikasi orang-ke orang, fasilitas *electronic mail* (e-mail) telah dipakai secara meluas oleh jutaan orang. Komunikasi menggunakan e-mail ini masih mengandung *delay* atau waktu tunda.

Videoconference atau pertemuan maya merupakan teknologi yang memungkinkan terjadinya komunikasi jarak jauh tanpa delay. Pertemuan maya ini dapat pula digunakan untuk keperluan sekolah jarak jauh, memperoleh hasil pemeriksaan medis seorang dokter yang berada di tempat yang jauh, dan sejumlah aplikasi lainnya.

Video on demand merupakan daya tarik ketiga dari jaringan komputer bagi orang per orang dimana kita dapat memilih film atau acara televisi dari negara mana saja dan kemudian ditampilkan di layar monitor kita.

3. Masalah sosial jaringan

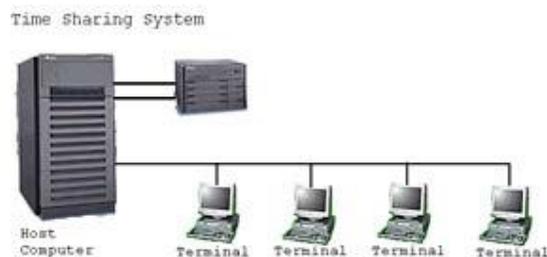
Penggunaan jaringan oleh masyarakat luas akan menyebabkan masalah-masalah sosial, etika, dan politik. Internet telah masuk ke segala penjuru kehidupan masyarakat, semua orang dapat memanfaatkannya tanpa memandang status sosial, usia, jenis kelamin. Penggunaan internet tidak akan menimbulkan masalah selama subyeknya terbatas pada topik-topik teknis, pendidikan atau hobi, hal-hal dalam batas norma-norma kehidupan, tetapi kesulitan mulai muncul bila suatu situs di internet mempunyai topik yang sangat menarik perhatian orang, seperti politik, agama, sex. Gambar-gambar yang dipasang di situs-situs tersebut mungkin akan merupakan sesuatu yang sangat mengganggu bagi sebagian orang. Selain itu, bentuk pesan-pesan tidaklah terbatas hanya pesan tekstual saja. Foto berwarna dengan resolusi tinggi dan bahkan video clip singkatpun sekarang dapat dengan mudah disebar-luaskan melalui jaringan komputer. Sebagian orang dapat bersikap acuh tak acuh, tapi bagi sebagian lainnya pemasangan materi tertentu (misalnya pornografi) merupakan sesuatu yang tidak dapat diterima.



BAB 2 Protokol Jaringan Komputer

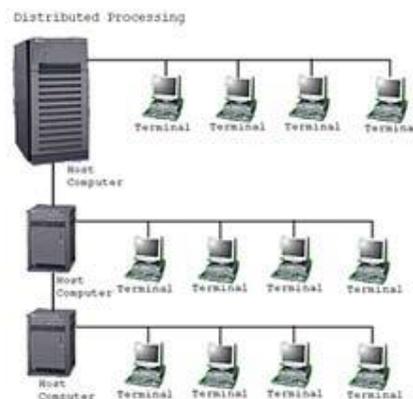
A. SEJARAH PROTOKOL

Sejak memasyarakatnya Internet, cara untuk menghubungkan beberapa komputer baik komputer pribadi (PC) maupun server dengan sebuah jaringan dari jenis LAN (Local Area Network) sampai WAN (Wide Area Network) menjadi sebuah hal yang biasa. Demikian pula dengan konsep "downsizing" maupun "lightsizing" yang bertujuan menekan anggaran belanja khususnya peralatan komputer, maka sebuah jaringan merupakan satu hal yang sangat diperlukan. Konsep jaringan komputer lahir pada tahun 1940-an di Amerika dari sebuah proyek pengembangan komputer MODEL I di laboratorium Bell dan group riset Harvard University yang dipimpin profesor H. Aiken. Pada mulanya proyek tersebut hanyalah ingin memanfaatkan sebuah perangkat komputer yang harus dipakai bersama. Untuk mengerjakan beberapa proses tanpa banyak membuang waktu kosong dibuatlah proses beruntun (Batch Processing), sehingga beberapa program bisa dijalankan dalam sebuah komputer dengan dengan kaidah antrian. Ditahun 1950-an ketika jenis komputer mulai membesar sampai terciptanya super komputer, maka sebuah komputer mesti melayani beberapa terminal. (Lihat Gambar 1.) Untuk itu ditemukan konsep distribusi proses berdasarkan waktu yang dikenal dengan nama TSS (Time Sharing System), maka untuk pertama kali bentuk jaringan (network) komputer diaplikasikan. Pada sistem TSS beberapa terminal terhubung secara seri ke sebuah host komputer. Dalam proses TSS mulai nampak perpaduan teknologi komputer dan teknologi telekomunikasi yang pada awalnya berkembang sendiri-sendiri.



Gambar 1. Jaringan Komputer Model TSS

Memasuki tahun 1970-an, setelah beban pekerjaan bertambah banyak dan harga perangkat komputer besar mulai terasa sangat mahal, maka mulailah digunakan konsep proses distribusi (Distributed Processing). Seperti pada Gambar 2., dalam proses ini beberapa host komputer mengerjakan sebuah pekerjaan besar secara paralel untuk melayani beberapa terminal yang tersambung secara seri disetiap host komputer. Dalam proses distribusi sudah mutlak diperlukan perpaduan yang mendalam antara teknologi komputer dan telekomunikasi, karena selain proses yang harus didistribusikan, semua host komputer wajib melayani terminal-terminalnya dalam satu perintah dari komputer pusat.



Gambar 2. Jaringan Komputer Model distibuted

Selanjutnya ketika harga-harga komputer kecil sudah mulai menurun dan konsep proses distribusi sudah matang, maka penggunaan komputer dan jaringannya sudah mulai beragam dari mulai menangani proses bersama maupun komunikasi antar komputer (Peer to Peer System) saja tanpa melalui komputer pusat. Untuk itu mulailah berkembang teknologi jaringan lokal yang dikenal dengan sebutan LAN. Demikian pula ketika Internet mulai diperkenalkan, maka sebagian besar LAN yang berdiri sendiri mulai berhubungan dan terbentuklah jaringan raksasa WAN.

B. ETHERNET

Ethernet adalah sistem jaringan yang dibuat dan dipatenkan perusahaan Xerox. Ethernet adalah implementasi metoda CSMA/CD (Carrier Sense Multiple Access with Collision Detection) yang dikembangkan tahun 1960 pada proyek wireless ALOHA di Hawaii University diatas kabel coaxial. Standarisasi sistem ethernet dilakukan sejak tahun 1978 oleh IEEE. (lihat Tabel 2.) Kecepatan transmisi data di ethernet sampai saat ini adalah 10 sampai 100 Mbps. Saat ini yang umum ada dipasaran adalah ethernet berkecepatan 10 Mbps yang

biasa disebut seri 10Base. Ada bermacam-macam jenis 10Base diantaranya adalah: 10Base5, 10Base2, 10BaseT, dan 10BaseF yang akan diterangkan lebih lanjut kemudian. Pada metoda CSMA/CD, sebuah host komputer yang akan mengirim data ke jaringan pertama-tama memastikan bahwa jaringan sedang tidak dipakai untuk transfer dari dan oleh host komputer lainnya. Jika pada tahap pengecekan ditemukan transmisi data lain dan terjadi tabrakan (collision), maka host komputer tersebut diharuskan mengulang permohonan (request) pengiriman pada selang waktu berikutnya yang dilakukan secara acak (random). Dengan demikian maka jaringan efektif bisa digunakan secara bergantian. Untuk menentukan pada posisi mana sebuah host komputer berada, maka tiap-tiap perangkat ethernet diberikan alamat (address) sepanjang 48 bit yang unik (hanya satu di dunia). Informasi alamat disimpan dalam chip yang biasanya nampak pada saat komputer di start dalam urutan angka berbasis 16, seperti pada Gambar 3.

```
NE*000 ethercard probe at 0x300: 00 40 05 61 20 e6  
eth0: NE2000 found at 0x300, using IRQ 9.
```

Gambar 3. Contoh ethernet address

48 bit angka agar mudah dimengerti dikelompokkan masing-masing 8 bit untuk menyetakan bilangan berbasis 16 seperti contoh di atas (00 40 05 61 20 e6), 3 angka didepan adalah kode perusahaan pembuat chip tersebut. Chip diatas dibuat oleh ANI Communications Inc. Contoh vendor terkenal bisa dilihat di Tabel 1 dan informasi lebih lengkap lainnya dapat diperoleh di <http://standards.ieee.org/regauth/oui/index.html>

Table 1. Daftar vendor terkenal chip ethernet

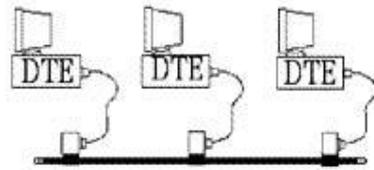
Nomer kode	Nama vendor
00:00:0C	Sisco System
00:00:1B	Novell
00:00:AA	Xerox
00:00:4C	NEC
00:00:74	Ricoh
08:08:08	3COM
08:00:07	Apple Computer
08:00:09	Hewlett Packard
08:00:20	Sun Microsystems
08:00:2B	DEC
08:00:5A	IBM

Dengan berdasarkan address ethernet, maka setiap protokol komunikasi (TCP/IP, IPX, AppleTalk, dll.) berusaha memanfaatkan untuk informasi masing-masing host komputer di jaringan.

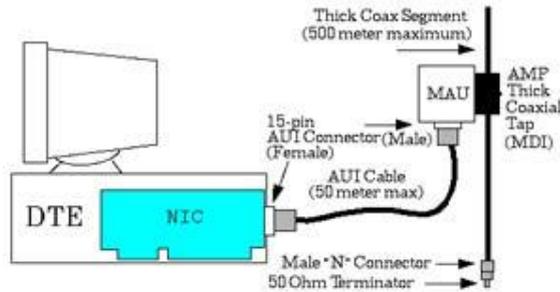
a. 10Base5

Sistem 10Base5 menggunakan kabel coaxial berdiameter 0,5 inch (10 mm) sebagai media penghubung berbentuk bus seperti pada Gambar 4. Biasanya kabelnya berwarna kuning dan pada kedua ujung kebelnya diberi konsentrator sehingga mempunyai resistansi sebesar 50 ohm. Jika menggunakan 10Base5, satu segmen jaringan bisa sepanjang maksimal 500 m, bahkan jika dipasang penghubung (repeater) sebuah jaringan bisa mencapai panjang maksimum 2,5 km.

Seperti pada Gambar 5, antara NIC (Network Interface Card) yang ada di komputer (DTE, Data Terminal Equipment) dengan media transmisi bus (kabel coaxial)-nya diperlukan sebuah transceiver (MAU, Medium Attachment Unit). Antar MAU dibuat jarak minimal 2,5 m, dan setiap segment hanya mampu menampung sebanyak 100 unit. Konektor yang dipakai adalah konektor 15 pin.



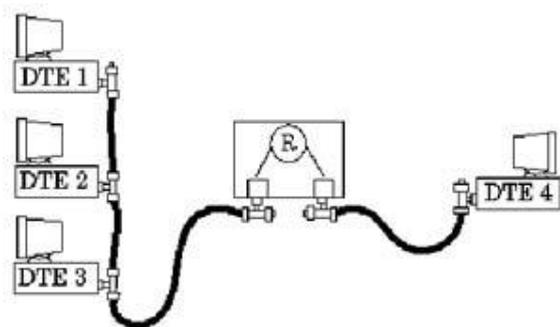
Gambar 4. Jaringan dengan media 10Base5



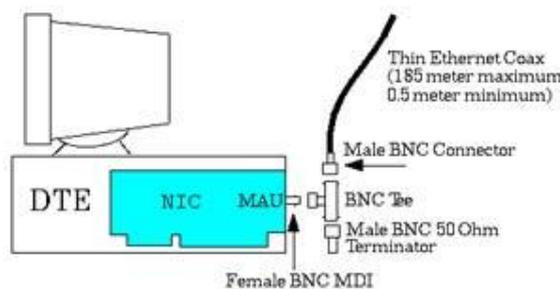
Gambar 5 Struktur 10Base5

b. 10Base2

Seperti pada jaringan 10Base5, 10Base2 mempunyai struktur jaringan berbentuk bus. (Gambar 6). Hanya saja kabel yang digunakan lebih kecil, berdiameter 5 mm dengan jenis twisted pair. Tidak diperlukan MAU karena MAU telah ada didalam NIC-nya sehingga bisa menjadi lebih ekonomis. Karenanya jaringan ini dikenal juga dengan sebutan CheaperNet. Dibandingkan dengan jaringan 10Base5, panjang maksimal sebuah segmennya menjadi lebih pendek, sekitar 185 m, dan bisa disambungkan sampai 5 segmen menjadi sekitar 925 m. Sebuah segmen hanya mampu menampung tidak lebih dari 30 unit komputer saja. Pada jaringan ini pun diperlukan konsentrator yang membuat ujung-ujung media transmisi busnya menjadi beresistansi 50 ohm. Untuk jenis konektor dipakai jenis BNC.



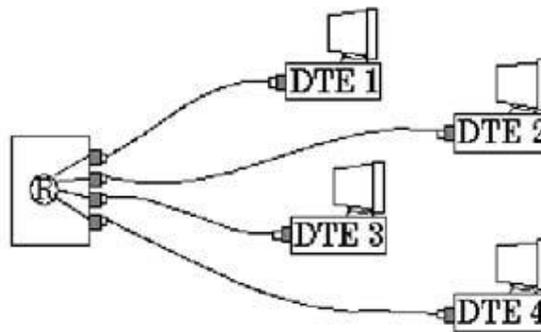
Gambar 6. Jaringan dengan media 10Base5.



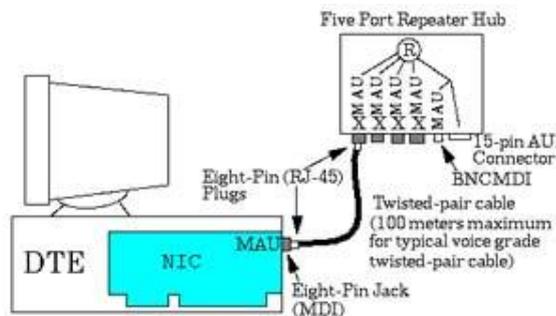
Gambar 7 Struktur 10Base2.

c. 10BaseT

Berbeda dengan 2 jenis jaringan diatas, 10BaseT berstruktur bintang (star) seperti terlihat di Gambar 8. Tidak diperlukan MAU karena sudah termasuk didalam NIC-nya. Sebagai pengganti konsentrator dan repeater diperlukan hub karena jaringan berbentuk star. Panjang sebuah segmen jaringan maksimal 100 m, dan setiap hub bisa dihubungkan untuk memperpanjang jaringan sampai 4 unit sehingga maksimal komputer tersambung bisa mencapai 1024 unit.



Gambar 8. Jaringan dengan media 10BaseT.



Gambar 9. Struktur 10BaseT.

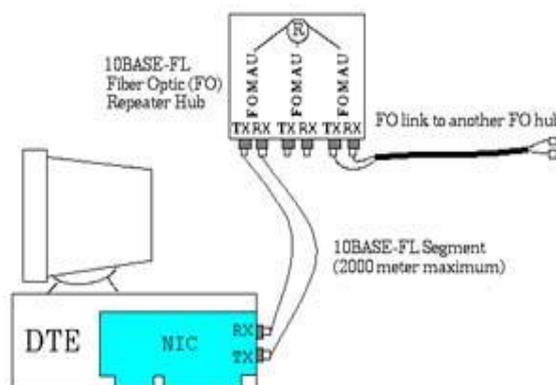
Menggunakan konektor modular jack RJ-45 dan kabel jenis UTP (Unshielded Twisted Pair) seperti kabel telepon di rumah-rumah. Saat ini kabel UTP yang banyak digunakan adalah jenis kategori 5 karena bisa mencapai kecepatan transmisi 100 Mbps. Masing-masing jenis kabel UTP dan kegunaanya bisa dilihat di Table 2.

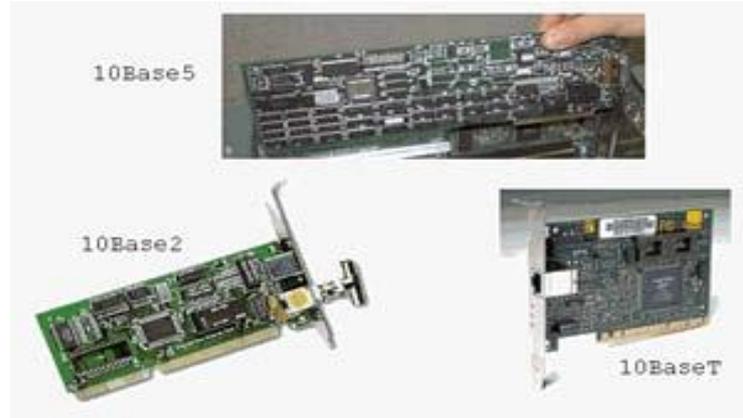
Table 2. Jenis kabel UTP dan aplikasinya.

Kategori	Aplikasi
Category 1	Dipakai untuk komunikasi suara (voice), dan digunakan untuk kabel telepon di rumah-rumah.
Category 2	Terdiri dari 4 pasang kabel twisted pair dan bisa digunakan untuk komunikasi data sampai kecepatan 4 Mbps.
Category 3	Bisa digunakan untuk transmisi data dengan kecepatan sampai 10 Mbps dan digunakan untuk Ethernet dan TokenRing.
Category 4	Sama dengan category 3 tetapi dengan kecepatan transmisi sampai 16 Mbps.
Category 5	Bisa digunakan pada kecepatan transmisi sampai 100 Mbps, biasanya digunakan untuk FastEthernet (100Base) atau network ATM.

d. 10BaseF

Bentuk jaringan 10BaseF sama dengan 10BaseT yakni berbentuk star. Karena menggunakan serat optik (fiber optic) untuk media transmisinya, maka panjang jarak antara NIC dan konsentratornya menjadi lebih panjang sampai 20 kali (2000 m). Demikian pula dengan panjang total jaringannya. Pada 10BaseF, untuk transmisi output (TX) dan input (RX) menggunakan kabel/media yang berbeda.





Gambar 10. Struktur 10BaseF

e. Fast Ethernet (100BaseT series)

Selain jenis NIC yang telah diterangkan di atas, jenis ethernet chip lainnya adalah seri 100Base. Seri 100Base mempunyai beragam jenis berdasarkan metode akses datanya diantaranya adalah: 100Base-T4, 100Base-TX, dan 100Base-FX. Kecepatan transmisi seri 100Base bisa melebihi kecepatan chip pendahulunya (seri 10Base) antara 2-20 kali (20-200 Mbps). Ini dibuat untuk menyaingi jenis LAN berkecepatan tinggi lainnya seperti: FDDI, 100VGAnyLAN dan lain sebagainya.

C. DESAIN JARINGAN

Pada saat kita telah mengetahui perangkat pendukung untuk membangun sebuah jaringan, maka langkah selanjutnya adalah mendesain jaringan sesuai yang kita perlukan. Apakah jaringan yang akan kita bangun akan berbentuk garis lurus (bus), bintang (star), lingkaran (ring), ataukah jaring (mesh) yang paling rumit? Juga apakah kecepatan transmisi jaringan kita merupakan jaringan rendah sampai menengah (beberapa M s/d 20Mbps), jaringan berkecepatan tinggi (ratusan Mbps) atau berkecepatan ultra tinggi (lebih dari 1Gbps)? Demikian pula media apa yang akan kita gunakan, apakah berbentuk jaringan kabel (wireline) atau memanfaatkan gelombang radio (wireless)? Yang terakhir, apakah jaringan kita untuk jaringan utama (backbone LAN) ataukah jaringan biasa (floor LAN) yang tentu saja memerlukan prasarana yang berbeda. Mungkin Tabel 4 bisa dibuat sebagai referensinya.

Table 3. Faktor-faktor mendesain LAN

Jenis LAN	Topologi	Bus	
		Star	
		Ring	Token Ring
			Token Bus
		Mesh	
	Kecepatan	Menengah (beberapa s/d 20 Mbps)	
		Tinggi (100 s/d ratusan Mbps)	
		Ultra (lebih dari 1 Gbps)	
	Media transmisi	Kabel (wireline)	
		Gelombang radio (wireless)	
Tingkatan LAN	Utama (backbone LAN)		
	Biasa (floor LAN)		

Secara fisik, jaringan komputer merupakan komputer yang dihubungkan dengan kabel data. Ada beragam jenis kabel data yang dibuat untuk penggunaan tertentu seperti kabel RG 58 untuk didalam ruangan, dapat juga mempergunakan kabel UTP. Untuk hubungan jaringan komputer antar gedung dapat dipergunakan kabel RG8 atau yang dikenal sebagai kabel backbone. Apabila anda membangun jairngan komputer antar gedung sebaiknya memperhatikan keamanannya dari gangguan petir.

Model penyambungan antara komputer didalam sebuah jaringan komputer juga ada beberapa macam yang secara umum ada 3 buah model yaitu :

1. Model BUS, dimana komputer dan server dihubungkan pada sebuah kabel saja secara berderet. ujung-ujung kabel data diberi komponen elektronik yang disebut terminator, yaitu semacam resistor terbungkus logam dengan nilai tahanan sebesar 50 ohm.
2. Model Star, dalam model ini dipergunakan alat tambahan yang disebut hub sebagai penghubungnya. Hub memiliki lubang konektor sejumlah tertentu, ada yang memiliki 8 buah lubang koneksi (disebut port), 12 port atau 16 port dan 24 port. Kabel data dari masing-masing komputer atau server dihubungkan pada alat ini.
3. Model Token Ring, dalam hubungan komputer model ini, kabel penghubung antar komputer dibuat seperti lingkaran (ring). Komputer yang dihubungkan secara berderet.

D. MACAM JARINGAN KOMPUTER

Dalam mempelajari macam-macam jaringan komputer terdapat dua klasifikasi yang sangat penting yaitu teknologi transmisi dan jarak. Secara garis besar, terdapat dua jenis teknologi transmisi yaitu jaringan broadcast dan jaringan point-to-point

1. Jaringan broadcast

Memiliki saluran komunikasi tunggal yang dipakai bersama-sama oleh semua mesin yang ada pada jaringan.

Pesan-pesan berukuran kecil, disebut paket, yang dikirimkan oleh suatu mesin akan diterima oleh mesin-mesin lainnya. Field alamat pada sebuah paket berisi keterangan tentang kepada siapa paket tersebut ditujukan. Saat menerima paket, mesin akan mengecek field alamat. Bila paket tersebut ditujukan untuk dirinya, maka mesin akan memproses paket itu, bila paket ditujukan untuk mesin lainnya, mesin tersebut akan mengabaikannya.

2. Jaringan point-to-point

Terdiri dari beberapa koneksi pasangan individu dari mesin-mesin. Untuk mengirim paket dari sumber ke suatu tujuan, sebuah paket pada jaringan jenis ini mungkin harus melalui satu atau lebih mesin-mesin perantara. Seringkali harus melalui banyak route yang mungkin berbeda jaraknya. Karena itu algoritma routing memegang peranan penting pada jaringan point-to-point.

Pada umumnya jaringan yang lebih kecil dan terlokalisasi secara geografis cenderung memakai broadcasting, sedangkan jaringan yang lebih besar menggunakan point-to-point.

Kriteria alternatif untuk mengklasifikasikan jaringan adalah didasarkan pada jaraknya. Tabel berikut ini menampilkan klasifikasi sistem multiprosesor berdasarkan ukuran-ukuran fisiknya.

Table 4. Klasifikasi prosesor interkoneksi berdasarkan jarak

Jarak antar prosesor	Prosesor di tempat yang sama	Contoh
0,1 m	Papan rangkaian	Data flow machine
1 m	Sistem	Multicomputer

Jarak antar prosesor	Prosesor di tempat yang sama	Contoh
10 m	Ruangan	Local Area Network
100 m	Gedung	
1 km	Kampus	
10 km	Kota	Metropolitan Area Network
100 km	Negara	Wide area Network
1.000 km	Benua	
10.000 km	Planet	The Internet

Dari tabel di atas terlihat pada bagian paling atas adalah dataflow machine, komputer-komputer yang sangat paralel yang memiliki beberapa unit fungsi yang semuanya bekerja untuk program yang sama. Kemudian multicomputer, sistem yang berkomunikasi dengan cara mengirim pesan-pesannya melalui bus pendek dan sangat cepat. Setelah kelas multicomputer adalah jaringan sejati, komputer-komputer yang berkomunikasi dengan cara bertukar data/pesan melalui kabel yang lebih panjang. Jaringan seperti ini dapat dibagi menjadi local area network (LAN), metropolitan area network (MAN), dan wide area network (WAN). Akhirnya, koneksi antara dua jaringan atau lebih disebut internetwork. Internet merupakan salah satu contoh yang terkenal dari suatu internetwork.

3. Local Area Network

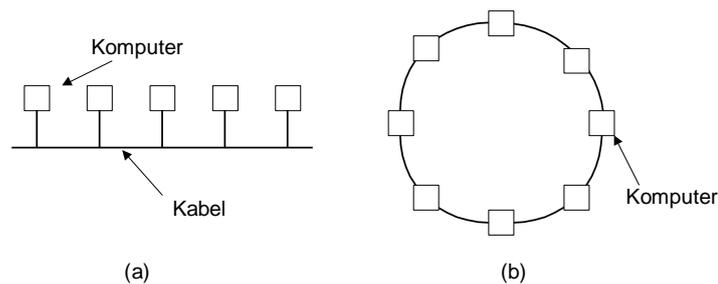
Local Area Network (LAN) merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer.

LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan workstation dalam kantor perusahaan atau pabrik-pabrik untuk memakai bersama resource (misalnya, printer, scanner) dan saling bertukar informasi. LAN dapat dibedakan dari jenis jaringan lainnya berdasarkan tiga karakteristik: ukuran, teknologi transmisi dan topologinya.

LAN mempunyai ukuran yang terbatas, yang berarti bahwa waktu transmisi pada keadaan terburuknya terbatas dan dapat diketahui sebelumnya. Dengan mengetahui

keterbatasannya, menyebabkan adanya kemungkinan untuk menggunakan jenis desain tertentu. Hal ini juga memudahkan manajemen jaringan.

LAN seringkali menggunakan teknologi transmisi kabel tunggal. LAN tradisional beroperasi pada kecepatan mulai 10 sampai 100 Mbps (mega bit/detik) dengan delay rendah (puluhan mikro second) dan mempunyai faktor kesalahan yang kecil. LAN-LAN modern dapat beroperasi pada kecepatan yang lebih tinggi, sampai ratusan megabit/detik.



Gambar 11. Dua jenis jaringan broadcast. (a) Bus. (b) Ring

Terdapat beberapa macam topologi yang dapat digunakan pada LAN broadcast. Gambar 11 menggambarkan dua diantara topologi-topologi yang ada. Pada jaringan bus (yaitu kabel liner), pada suatu saat sebuah mesin bertindak sebagai master dan diijinkan untuk mengirim paket. Mesin-mesin lainnya perlu menahan diri untuk tidak mengirimkan apapun. Maka untuk mencegah terjadinya konflik, ketika dua mesin atau lebih ingin mengirimkan secara bersamaan, maka mekanisme pengatur diperlukan. Mekanisme pengatur dapat berbentuk tersentralisasi atau terdistribusi. IEEE 802.3 yang populer disebut Ethernet merupakan jaringan broadcast bus dengan pengendali terdesentralisasi yang beroperasi pada kecepatan 10 s.d. 100 Mbps. Komputer-komputer pada Ethernet dapat mengirim kapan saja mereka inginkan, bila dua buah paket atau lebih bertabrakan, maka masing-masing komputer cukup menunggu dengan waktu tunggu yang acak sebelum mengulangi lagi pengiriman.

Sistem broadcast yang lain adalah ring, pada topologi ini setiap bit dikirim ke daerah sekitarnya tanpa menunggu paket lengkap diterima. Biasanya setiap bit mengelilingi ring dalam waktu yang dibutuhkan untuk mengirimkan beberapa bit, bahkan seringkali sebelum paket lengkap dikirim seluruhnya. Seperti sistem broadcast lainnya, beberapa aturan harus dipenuhi untuk mengendalikan access simultan ke ring. IEEE 802.5 (token ring) merupakan LAN ring yang populer yang beroperasi pada kecepatan antara 4 s.d 16 Mbps.

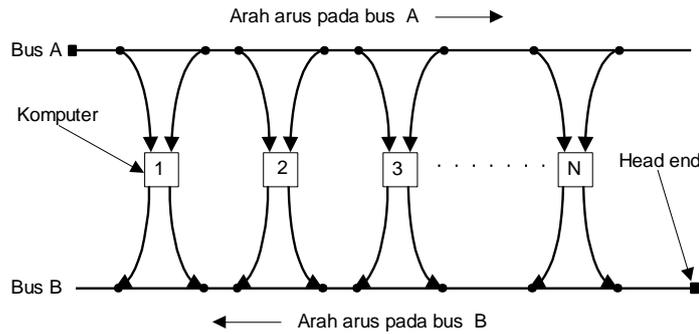
Berdasarkan alokasi channelnya, jaringan broadcast dapat dibagi menjadi dua, yaitu statik dan dinamik. Jenis alokasi statik dapat dibagi berdasarkan waktu interval-interval diskrit dan algoritma round robin, yang memungkinkan setiap mesin untuk melakukan broadcast hanya bila slot waktunya sudah diterima. Alokasi statik sering menyia-nyiakan kapasitas channel bila sebuah mesin tidak punya lagi yang perlu dikerjakan pada saat slot alokasinya diterima. Karena itu sebagian besar sistem cenderung mengalokasi channel-nya secara dinamik (yaitu berdasarkan kebutuhan).

Metoda alokasi dinamik bagi suatu channel dapat tersentralisasi ataupun terdesentralisasi. Pada metoda alokasi channel tersentralisasi terdapat sebuah entity tunggal, misalnya unit bus pengatur, yang menentukan siapa giliran berikutnya. Pengiriman paket ini bisa dilakukan setelah menerima giliran dan membuat keputusan yang berkaitan dengan algoritma internal. Pada metoda alokasi channel terdesentralisasi, tidak terdapat entity sentral, setiap mesin harus dapat menentukan dirinya sendiri kapan bisa atau tidaknya mengirim.

4. Metropolitan Area Network

Metropolitan Area Network (MAN) pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya memakai teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang berdekatan dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. MAN biasanya mampu menunjang data dan suara, dan bahkan dapat berhubungan dengan jaringan televisi kabel. MAN hanya memiliki sebuah atau dua buah kabel dan tidak mempunyai elemen switching, yang berfungsi untuk mengatur paket melalui beberapa output kabel. Adanya elemen switching membuat rancangan menjadi lebih sederhana.

Alasan utama memisahkan MAN sebagai kategori khusus adalah telah ditentukannya standart untuk MAN, dan standart ini sekarang sedang diimplementasikan. Standart tersebut disebut DQDB (Distributed Queue Dual Bus) atau 802.6 menurut standart IEEE. DQDB terdiri dari dua buah kabel unidirectional dimana semua komputer dihubungkan, seperti ditunjukkan pada gambar 1.2. Setiap bus mempunyai sebuah head-end, perangkat untuk memulai aktivitas transmisi. Lalulintas yang menuju komputer yang berada di sebelah kanan pengirim menggunakan bus bagian atas. Lalulintas ke arah kiri menggunakan bus yang berada di bawah.



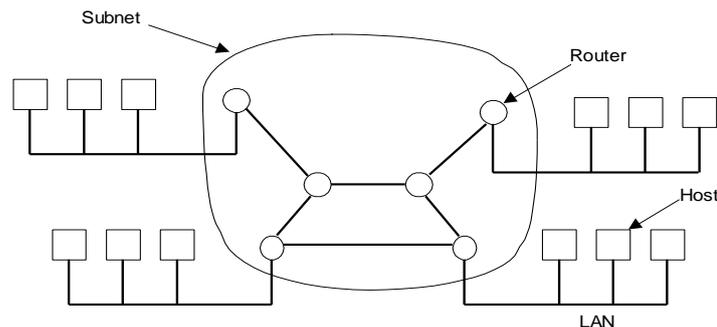
Gambar 12. Arsitektur MAN DQDB

5. Wide Area Network

Wide Area Network (WAN) mencakup daerah geografis yang luas, seringkali mencakup sebuah negara atau benua. WAN terdiri dari kumpulan mesin yang bertujuan untuk menjalankan program-program aplikasi. Kita akan mengikuti penggunaan tradisional dan menyebut mesin-mesin ini sebagai host. Istilah End System kadang-kadang juga digunakan dalam literatur. Host dihubungkan dengan sebuah subnet komunikasi, atau cukup disebut subnet. Tugas subnet adalah membawa pesan dari host ke host lainnya, seperti halnya sistem telepon yang membawa isi pembicaraan dari pembicara ke pendengar. Dengan memisahkan aspek komunikasi murni sebuah jaringan (subnet) dari aspek-aspek aplikasi (host), rancangan jaringan lengkap menjadi jauh lebih sederhana.

Pada sebagian besar WAN, subnet terdiri dari dua komponen, yaitu kabel transmisi dan elemen switching. Kabel transmisi (disebut juga sirkuit, channel, atau trunk) memindahkan bit-bit dari satu mesin ke mesin lainnya.

Element switching adalah komputer khusus yang dipakai untuk menghubungkan dua kabel transmisi atau lebih. Saat data sampai ke kabel penerima, element switching harus memilih kabel pengirim untuk meneruskan pesan-pesan tersebut. Sayangnya tidak ada terminologi standart dalam menamakan komputer seperti ini. Namanya sangat bervariasi disebut paket switching node, intermidiate system, data switching exchange dan sebagainya.

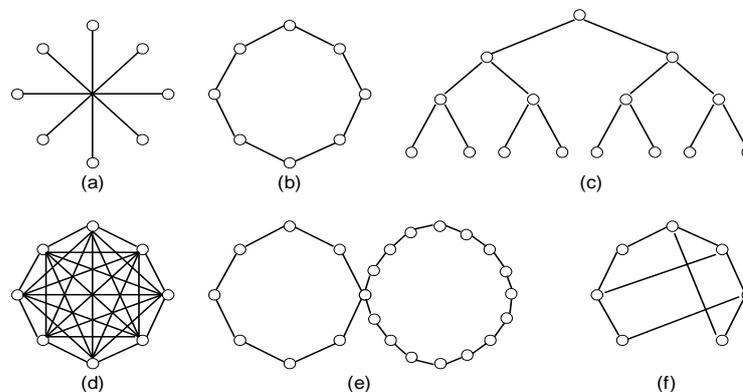


Gambar 13. Hubungan antara host-host dengan subnet

Sebagai istilah generik bagi komputer switching, kita akan menggunakan istilah router. Tapi perlu diketahui terlebih dahulu bahwa tidak ada konsensus dalam penggunaan terminologi ini. Dalam model ini, seperti ditunjukkan oleh gambar 1.4 setiap host dihubungkan ke LAN tempat dimana terdapat sebuah router, walaupun dalam beberapa keadaan tertentu sebuah host dapat dihubungkan langsung ke sebuah router. Kumpulan saluran komunikasi dan router (tapi bukan host) akan membentuk subnet.

Istilah subnet sangat penting, tadinya subnet berarti kumpulan kumpulan router-router dan saluran-saluran komunikasi yang memindahkan paket dari host host tujuan. Akan tetapi, beberapa tahun kemudian subnet mendapatkan arti lainnya sehubungan dengan pengalaman jaringan.

Pada sebagian besar WAN, jaringan terdiri dari sejumlah banyak kabel atau saluran telepon yang menghubungkan sepasang router. Bila dua router yang tidak mengandung kabel yang sama akan melakukan komunikasi, keduanya harus berkomunikasi secara tak langsung melalui router lainnya. ketika sebuah paket dikirimkan dari sebuah router ke router lainnya melalui router perantara atau lebih, maka paket akan diterima router dalam keadaan lengkap, disimpan sampai saluran output menjadi bebas, dan kemudian baru diteruskan.



Gambar 14. beberapa topologi subnet untuk poin-to-point .

Subnet yang mengandung prinsip seperti ini disebut subnet point-to-point, store-and-forward, atau packet-switched. Hampir semua WAN (kecuali yang menggunakan satelit) memiliki subnet store-and-forward.

Di dalam menggunakan subnet point-to-point, masalah rancangan yang penting adalah pemilihan jenis topologi interkoneksi router. Gambar 1.5 menjelaskan beberapa kemungkinan topologi. LAN biasanya berbentuk topologi simetris, sebaliknya WAN umumnya bertopologi tak menentu.

6. Jaringan Tanpa Kabel

Komputer mobile seperti komputer notebook dan personal digital assistant (PDA), merupakan cabang industri komputer yang paling cepat pertumbuhannya. Banyak pemilik jenis komputer tersebut yang sebenarnya telah memiliki mesin-mesin desktop yang terpasang pada LAN atau WAN tetapi karena koneksi kabel tidaklah mungkin dibuat di dalam mobil atau pesawat terbang, maka banyak yang tertarik untuk memiliki komputer dengan jaringan tanpa kabel ini.

Jaringan tanpa kabel mempunyai berbagai manfaat, yang telah umum dikenal adalah kantor portable. Orang yang sedang dalam perjalanan seringkali ingin menggunakan peralatan elektronik portable-nya untuk mengirim atau menerima telepon, fax, e-mail, membaca fail jarak jauh login ke mesin jarak jauh, dan sebagainya dan juga ingin melakukan hal-hal tersebut dimana saja, darat, laut, udara. Jaringan tanpa kabel sangat bermanfaat untuk mengatasi masalah-masalah di atas.

Walaupun jaringan tanpa kabel dan sistem komputasi yang dapat berpindah-pindah sering kali berkaitan erat, sebenarnya tidaklah sama, seperti yang tampak pada tabel 1.2. Komputer portabel kadang-kadang menggunakan kabel juga, yaitu disaat seseorang yang sedang dalam perjalanan menyambungkan komputer portable-nya ke jack telepon di sebuah hotel, maka kita mempunyai mobilitas yang bukan jaringan tanpa kabel. Sebaliknya, ada juga komputer-komputer yang menggunakan jaringan tanpa kabel tetapi bukan portabel, hal ini dapat terjadi disaat komputer-komputer tersebut terhubung pada LAN yang menggunakan fasilitas komunikasi wireless (radio).

Meskipun jaringan tanpa kabel ini cukup mudah untuk di pasang, tetapi jaringan macam ini memiliki banyak kekurangan. Biasanya jaringan tanpa kabel mempunyai kemampuan 1-2 Mbps, yang mana jauh lebih rendah dibandingkan dengan jaringan berkabel. Laju kesalahan juga sering kali lebih besar, dan transmisi dari komputer yang berbeda dapat mengganggu satu sama lain.

E. Protokol

Protokol adalah aturan-aturan main yang mengatur komunikasi diantara beberapa komputer di dalam sebuah jaringan, aturan itu termasuk didalamnya petunjuk yang berlaku

bagi cara-cara atau metode mengakses sebuah jaringan, topologi fisik, tipe-tipe kabel dan kecepatan transfer data.

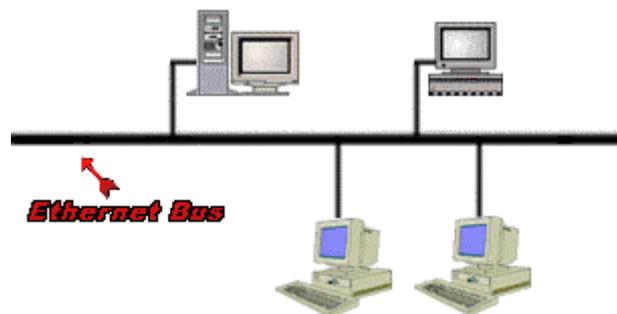
Protokol-Protokol yang dikenal adalah sebagai berikut :

1. Ethernet
2. Local Talk
3. Token Ring
4. FDDI
5. ATM

Ethernet

Protocol Ethernet sejauh ini adalah yang paling banyak digunakan, Ethernet menggunakan metode akses yang disebut CSMA/CD (Carrier Sense Multiple Access/Collision Detection). Sistem ini menjelaskan bahwa setiap komputer memperhatikan ke dalam kabel dari network sebelum mengirimkan sesuatu ke dalamnya. Jika dalam jaringan tidak ada aktifitas atau bersih komputer akan mentransmisikan data, jika ada transmisi lain di dalam kabel, komputer akan menunggu dan akan mencoba kembali transmisi jika jaringan telah bersih. kadangkala dua buah komputer melakukan transmisi pada saat yang sama, ketika hal ini terjadi, masing-masing komputer akan mundur dan akan menunggu kesempatan secara acak untuk mentransmisikan data kembali. metode ini dikenal dengan koalisi, dan tidak akan berpengaruh pada kecepatan transmisi dari network.

Protokol Ethernet dapat digunakan untuk pada model jaringan Garis lurus , Bintang, atau Pohon . Data dapat ditransmisikan melewati kabel twisted pair, koaksial, ataupun kabel fiber optic pada kecepatan 10 Mbps.



Gambar 15. Protokol Ethernet

LocalTalk

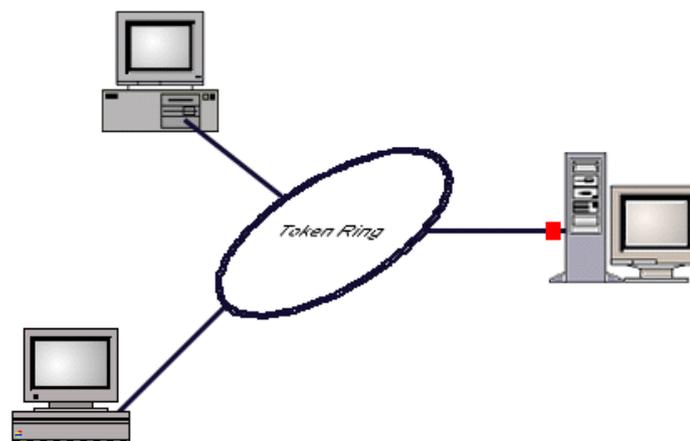
LocalTalk adalah sebuah protokol network yang di kembangkan oleh Apple Computer, Inc. untuk mesin-mesin komputer Macintosh . Metode yang digunakan oleh LocalTalk adalah CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Hampir sama dengan CSMA/CD.. Adapter LocalTalk dan cable twisted pair khusus dapat digunakan untuk menghubungkan beberapa computer melewati port serial. Sistem Operasi Macintosh memungkinkan koneksi secara jaringan peer-to-peer tanpa membutuhkan tambahan aplikasi khusus.

Protokol LocalTalk dapat digunakan untuk model jaringan Garis Lurus , Bintang , ataupun model Pohon dengan menggunakan kabel twisted pair . Kekurangan yang paling mencolok yaitu kecepatan transmisinya. Kecepatan transmisinya hanya 230 Kbps.

Token Ring

Protokol Token di kembangkan oleh IBM pada pertengahan tahun 1980. Metode Aksesnya melalui lewatnya sebuah token dalam sebuah lingkaran seperti Cincin . Dalam lingkaran token, komputer-komputer dihubungkan satu dengan yang lainnya seperti sebuah cincin. Sebuah Sinyal token bergerak berputar dalam sebuah lingkaran (cincin) dalam sebuah jaringan dan bergerak dari sebuah

komputer-menuju ke komputer berikutnya, jika pada persinggahan di salah satu komputer ternyata ada data yang ingin ditransmisikan, token akan mengangkutnya ke tempat dimana data itu ingin ditujukan, token bergerak terus untuk saling mengkoneksikan diantara masing-masing komputer.

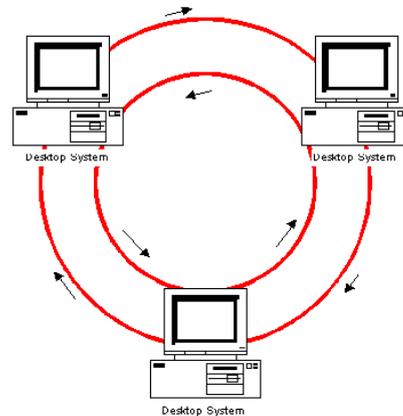


Gambar 16. Protokol Token Ring

Protokol Token Ring membutuhkan model jaringan Bintang dengan menggunakan kabel twisted pair atau kabel fiber optic . Dan dapat melakukan kecepatan transmisi 4 Mbps atau 16 Mbps. Sejalan dengan perkembangan Ethernet, penggunaan Token Ring makin berkurang sampai sekarang.

FDDI

Fiber Distributed Data Interface (FDDI) adalah sebuah Protokol jaringan yang menghubungkan antara dua atau lebih jaringan bahkan pada jarak yang jauh . Metode aksesnyayang digunakan oleh FDDI adalah model token . FDDI menggunakan dua buah topologi ring secara fisik. Proses transmisi biasanya menggunakan satu buah ring, namun jika ada masalah ditemukan akan secara otomatis menggunakan ring yang kedua.



FDDI - all stations functioning

Gambar 17. Protokol FDDI

Sebuah keuntungan dari FDDI adalah kecepatan dengan menggunakan fiber optic cable pada kecepatan 100 Mbps.

ATM

ATM adalah singkatan dari Asynchronous Transfer Mode (ATM) yaitu sebuah protokol jaringan yang mentransmisikan pada kecepatan 155 Mbps atau lebih . ATM mentarnsmisikan data kedalam satu paket dimana pada protokol yang lain mentransfer pada besar-kecilnya paket. ATM mendukung variasi media seperti video, CD-audio, dan gambar. ATM bekerja pada model topologi Bintang dengan menggunakan Kabel fiber optic ataupun kabel twisted pair . ATM pada umumnya digunakan untuk menghubungkan dua atau lebih LAN . dia juga banyak dipakai oleh Internet Service Providers (ISP) untuk meningkatkan kecepatan akses Internet untuk klien mereka.

Table 5. Daftar Protokol

Protokol yang di pakai	Kabel yang digunakan	Kecepatan Transfer	Topology Fisik
Ethernet	Twisted Pair, Coaxial, Fiber	10 Mbps	Linear Bus, Star, Tree
Fast Ethernet	Twisted Pair, Fiber	100 Mbps	Star
LocalTalk	Twisted Pair	0.23 Mbps	Linear Bus or Star
Token Ring	Twisted Pair	4 Mbps - 16 Mbps	Star-Wired Ring
FDDI	Fiber	100 Mbps	Dual ring
ATM	Twisted Pair, Fiber	155-2488 Mbps	Linear Bus, Star, Tree

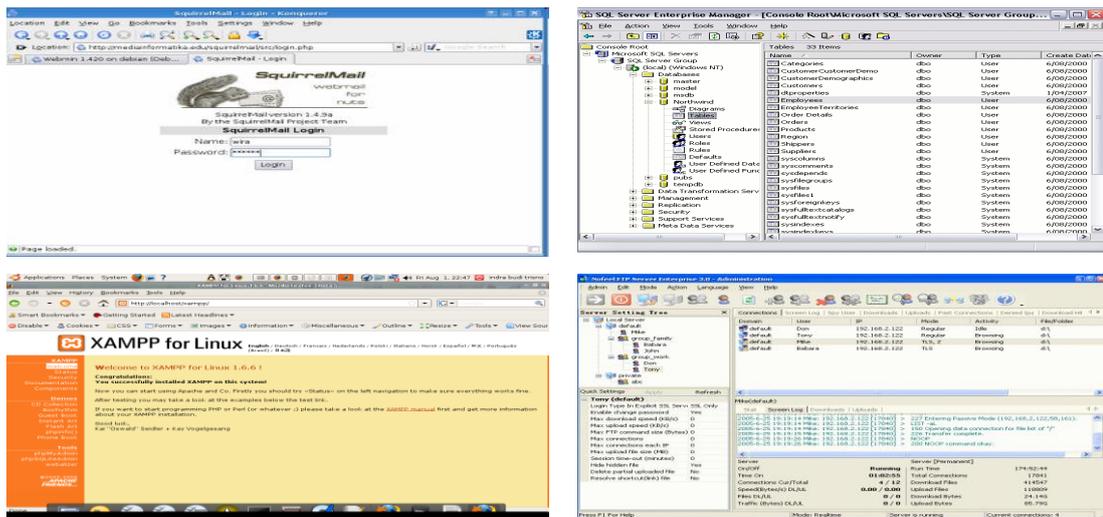


BAB 3 Hardware & Software

A. PERANGKAT LUNAK YANG DIPERLUKAN

File Server

Sebuah file server bertugas mengontrol komunikasi dan informasi diantara node/komponen dalam suatu jaringan. Sebagai contoh mengelola pengiriman file database atau pengolah kata dari workstation atau salah satu node, ke node yang lain, atau menerima email pada saat yang bersamaan dengan tugas yang lain. Terlihat bahwa tugas file server sangat kompleks, dia juga harus menyimpan informasi dan membaginya secara cepat.



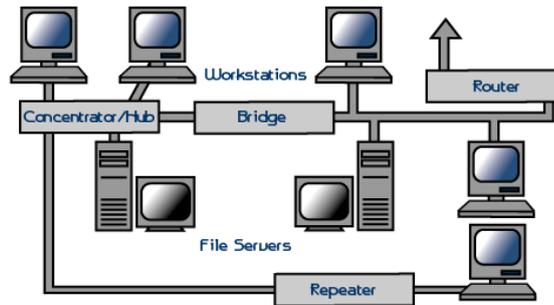
Gambar 18. Aplikasi File Server

Workstations

Keseluruhan komputer yang terhubung ke file server dalam jaringan disebut sebagai workstation. Sebuah workstation harus memiliki perangkat lunak yang mendukung jaringan, mulai dari Sistem Operasi sampe aplikasi pendukung lainnya. Saat ini hampir semua sistem operasi pasti mendukung jaringan komputer, begitupun juga aplikasi-aplikasi lain.

B. PERANGKAT KERAS YANG DIPERLUKAN

Perangkat keras yang dibutuhkan untuk membangun sebuah jaringan komputer yaitu : Komputer, Card Network, Hub, dan segala sesuatu yang berhubungan dengan koneksi jaringan seperti: Printer, CDROM, Scanner, Bridges, Router dan lainnya yang dibutuhkan untuk process transformasi data didalam jaringan.



Gambar 19. Perangkat-perangkat Jaringan

a. Network Interface Cards (NIC) atau Kartu Jaringan

Kartu Jaringan (NIC) merupakan perangkat yang menyediakan media untuk menghubungkan antara komputer, kebanyakan kartu jaringan adalah kartu inernal, yaitu kartu jaringan yang di pasang pada slot ekspansi di dalam komputer. Beberapa komputer seperti komputer MAC, menggunakan sebuah kotak khusus yang ditancapkan ke port serial atau SCSI port komputernya. Pada komputer notebook ada slot untuk kartu jaringan yang biasa disebut PCMCIA slot. Kartu jaringan yang banyak terpakai saat ini adalah : kartu jaringan Ethernet, LocalTalk konektor, dan kartu jaringan Token Ring. Yang saat ini populer digunakan adalah Ethernet, lalu diikuti oleh Token Ring, dan LocalTalk,

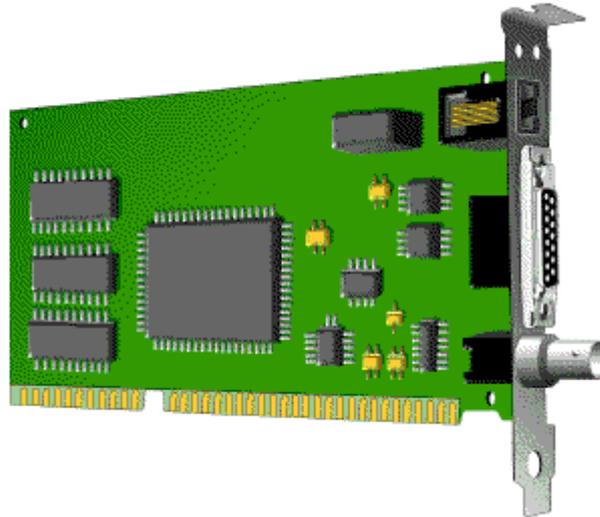
Ethernet biasanya dibeli terpisah dengan komputer, kecuali seperti komputer Macintosh yang sudah mengikutkan kartu jaringan ethernet didalamnya. kartu Jaringan ethernet umumnya telah menyediakan port koneksi untuk kabel Koaksial ataupun kabel twisted pair, jika didesain untuk kabel koaksial konenektorya adalah BNC, dan apabila didesain untuk kabel twisted pair maka akan punya konektor RJ-45. Beberapa kartu jaringan ethernet kadang juga punya konektor AUI. Semua itu di koneksikan dengan koaksial, twisted pair, ataupun dengan kabel fiber optik



Gambar 20. Network Interface Card (NIC)

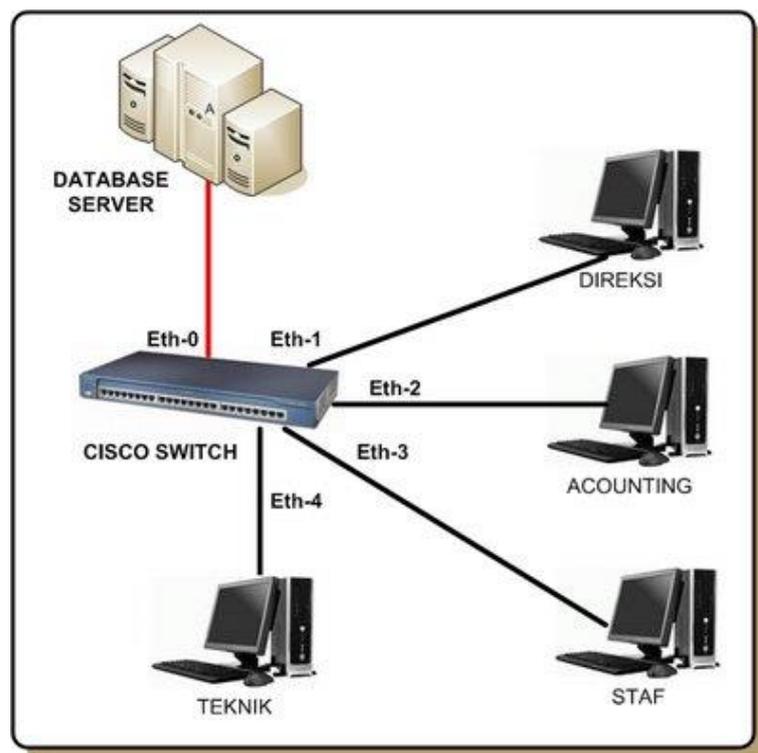
b. LocalTalk Connectors/Konektor LocalTalk

LocalTalk adalah kartu jaringan buat komputer macintosh, ini menggunakan sebuah kotak adapter khusus dan kabel yang terpasang ke Port untuk printer. Kekurangan dari LocalTalk dibandingkan Ethernet adalah kecepatan laju transfer datanya, Ethernet bi Jaringan komputer bukanlah sesuatu yang baru saat ini. Hampir di setiap perusahaan terdapat jaringan komputer untuk memperlancar arus informasi di dalam perudahaan tersebut. Internet yang mulai populer saat ini adalah suatu jaringan komputer raksasa yang merupakan jaringan jaringan komputer yang terhubung dan dapat saling berinteraksi. Hal ini dapat terjadi karena adanya perkembangan teknologi jaringan yang sangat pesat, sehingga dalam beberapa tahun saja jumlah pengguna jaringan komputer yang tergabung dalam Internet berlipat ganda. asanya dapat sampai 10 Mbps, sedangkan LocalTalk hanya dapat beroperasi pada kecepatan 230 Kbps atau setara dengan 0.23 Mps



Gambar 21. LocalTalk Card

c. Hub/ Switch/ Konsentrator



Gambar 22. Switch

Sebuah Konsentrator/ Hub adalah sebuah perangkat yang menyatukan kabel-kabel network dari tiap-tiap workstation, server atau perangkat lain. Dalam topologi Bintang, kabel twisted pair datang dari sebuah workstation masuk kedalam hub. Hub mempunyai banyak slot concentrator yang mana dapat dipasang menurut nomor port dari card yang dituju. Ciri-ciri yang dimiliki Konsentrator adalah:

- o Biasanya terdiri dari 8, 12, atau 24 port RJ-45

- Digunakan pada topologi Bintang/ Star
- Biasanya di jual dengan aplikasi khusus yaitu aplikasi yang mengatur manajemen port tersebut.
- Biasanya disebut hub

d. Access Point

Suatu wireless access point adalah perangkat jaringan wireless yang menghubungkan client wireless (seperti komputer yang dilengkapi dengan adapter USB wireless atau laptop yang dilengkapi dengan adapter ExpressCard wireless) dengan jaringan yang menggunakan kabel – yang biasanya juga bisa koneksi terhadap internet melaluinya. Seperti halnya dengan sebuah bridge, wireless access point mempunyai sedikitnya dua koneksi jaringan dan sebagai jembatan agar bisa saling bertukar traffic antar keduanya. Koneksi pertama adalah interface wireless yang umumnya berupa on-board radio atau wireless card didalamnya. Interface jaringan kedua bisa berupa Ethernet, modem dial-up, atau bahkan bisa berupa adapter wireless lainnya. Bahkan sekarang ini sudah banyak wireless access point mempunyai lebih dari satu Ethernet port yang mana bisa menyederhanakan pembuatan segment jaringan.

Beberapa jenis wireless access point juga bisa mengendalikan apa yang bisa dikirimkan kepada clients dari jaringan kabel local, melalui rule-2 firewall sederhana. Hampir fungsional utilitynya bisa diakses lewat web interface dengan koneksi ke address defaultnya (jika belum diubah).

Beberapa fitur yang membedakan mereka sebut saja berikut ini:

- Bridging langsung kepada jaringan kabel
- Mendukung fitur NAT dan juga layanan DHCP
- Dual-band radio frequency 2.4 GHz dan 5 GHz.
- Konektor external antenna
- Power outout radio yang lebih besar (kebanyakan beroperasi pada 30mW, sementara beberapa juga ada yang beroperasi pada power 1000mW atau lebih.
- Perbaikan system security seperti WPA / WPA2 dan tagged VLANs



Gambar 23. Access Point

e. Media Transmisi

1. Coaxial

Kabel data yang menggunakan material tembaga dimana terdapat 2 bagian yaitu, **Kabel inti ditengah** dan **Kabel serabut** disisi samping dengan dipisahkan oleh suatu isolator. Kabel ini menggunakan konektor **Bayonet Nut Connector (BNC)**.



Gambar 24. Kabel Coaxial dan Berbagai Connector

2. Twisted Pair

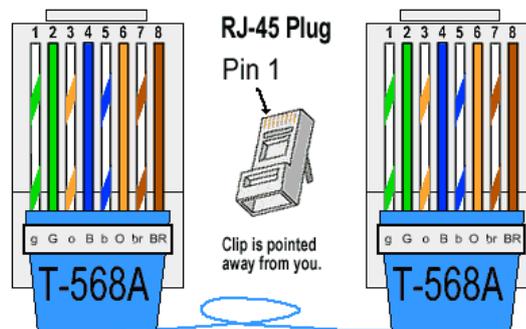
Kabel berpilin (Twisted Pair), menggunakan kabel berpasangan dimana tujuannya untuk menghilangkan efek crosstalk. Banyak digunakan untuk jaringan LAN, dikarenakan mampu mengirimkan bandwidth dengan jumlah yang besar.

Kabel ini menggunakan konektor seri Registered Jack (RJ), dan tergantung dari jenis kategorinya. Untuk kategori 2 menggunakan RJ11 sedangkan untuk kategori 5 keatas menggunakan RJ45.

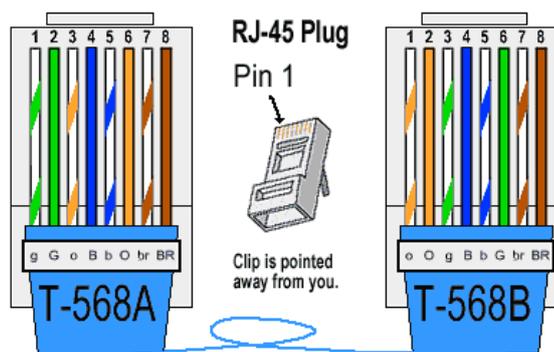
Table 6. Daftar kategori Twisted Pair

Kategori	Data Rate Maksimum	Penggunaan
CAT 1	1 Mbps (1 MHz)	Analog Voice, ISDN
CAT 2	4 Mbps	Token Ring
CAT 3	16 Mbps	Voice dan Data 10BaseT
CAT 4	20 Mbps	16 Mbps Token Ring
CAT 5	100 Mbps 1000 Mbps	ATM
CAT 5E	1000 Mbps	Ethernet
CAT 6	Mecapai 400 MHz	Superfast Broadband
CAT 6E	Mencapai 500 MHz	10GbaseT
CAT 7	Mencapai 1.2 GHz	Full Montion Video Taleradiology

Untuk pemasangan kabelnya mengikuti aturan TIA/EIA-586-A/B, apabila kedua ujung menggunakan aturan yang sama, kabel tersebut disebut Straight-Through, sedangkan bila berbeda disebut Cross-Over.



Gambar 3.8 UTP Straight-Through



Gambar 25. UTP Cross-Over

3. Fiber Optic

Jenis kabel yang satu ini tidak menggunakan tembaga (cooper), melainkan serat optik. Dimana sinyal yang dialirkan berupa berkas cahaya. Mampu mengirimkan bandwidth lebih banyak. Banyak digunakan untuk komunikasi antar Backbone, LAN dengan kecepatan tinggi.

Jika Anda melihat dekat pada serat optik tunggal, Anda akan melihat bahwa ia memiliki bagian-bagian berikut:

- Core – tipis pusat kaca serat mana cahaya perjalanan
- Kelongsong – bahan Luar optik yang mengelilingi inti yang mencerminkan kembali cahaya ke dalam inti
- Buffer lapisan – lapisan plastik yang melindungi serat dari kerusakan dan kelembaban

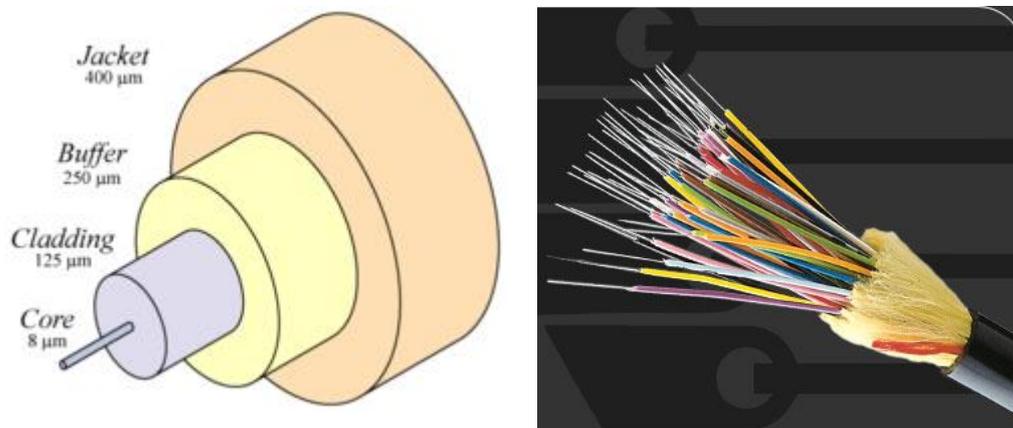
Ratusan atau ribuan serat optik ini disusun dalam bundel dalam kabel optik. Bundel dilindungi dengan menutup luar kabel, yang disebut jaket.

Serat optik datang dalam dua jenis:

1. Single-mode fibers
2. Multi-mode fibers

Single-mode fibers memiliki core kecil (sekitar $3,5 \times 10^{-4}$ inci atau 9 mikron diameter) dan mengirimkan sinar laser inframerah (panjang gelombang = 1.300 sampai 1.550 nanometer). Multi-mode serat memiliki core lebih besar (sekitar $2,5 \times 10^{-3}$ inchi atau 62,5 mikron diameter) dan memancarkan sinar inframerah (panjang gelombang = 850 untuk 1.300 nm) dari dioda pemancar cahaya (LED).

Beberapa serat optik dapat dibuat dari plastik. Serat ini memiliki inti besar (0,04 inci atau 1 mm diameter) dan mengirimkan lampu merah tampak (panjang gelombang = 650 nm) dari LED.

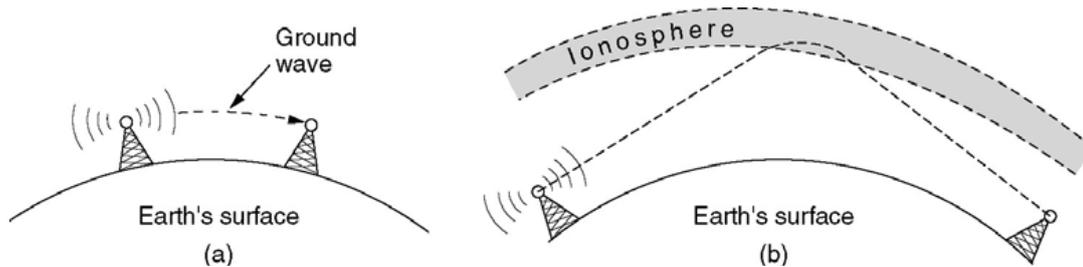


Gambar 26. Fiber Optic

4. Transmisi Radio

Perkembangan teknologi komunikasi radio sangat pesat, penggunaan wireless-LAN sudah semakin populer. Untuk mengirimkan data menggunakan komunikasi radio ada beberapa cara yaitu :

1. Memancarkan langsung, sesuai dengan permukaan bumi
2. Dipantulkan melalui lapisan atmosfer

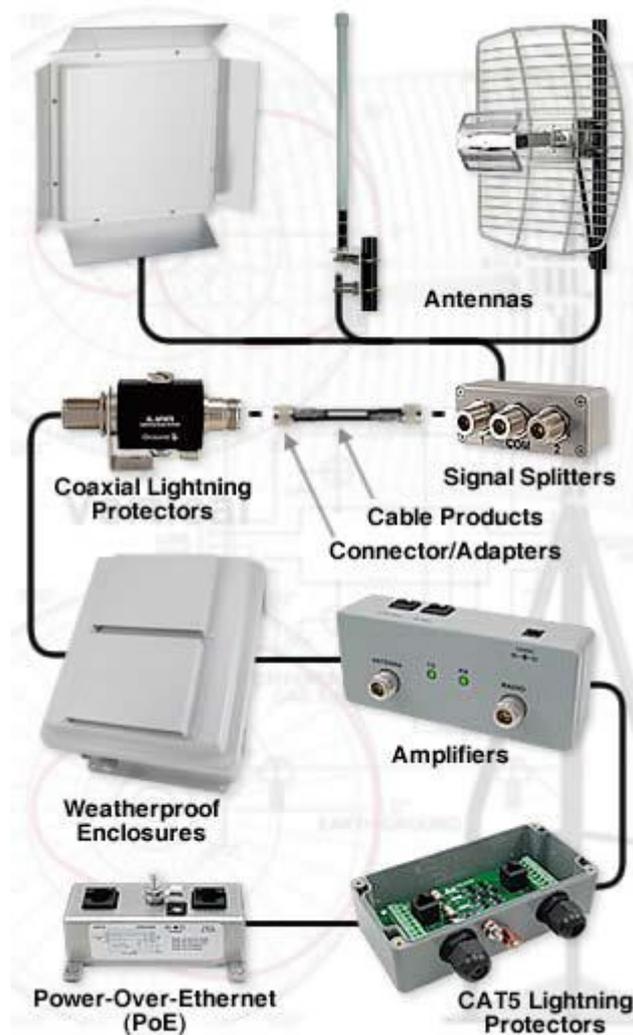


Gambar 27. Komunikasi radio

Komunikasi radio ini menggunakan frekuensi khusus supaya tidak mengakibatkan interference dengan penggunaan frekuensi lainnya, frekuensi yang boleh digunakan disebut ISM band. ISM singkatan dari Industrial, Scientific and Medical. Frekuensi yang bisa digunakan antara lain :

- 900 MHz
- GHz
- GHz

Contoh penggunaan perangkat Wireless-LAN seperti pada gambar dibawah ini :



Gambar 28. Perangkat Wireless LAN

5. Komunikasi Satelit

Komunikasi ini digunakan untuk komunikasi jarak jauh atau antar benua. Dimana untuk menghubungkannya diperlukan teknologi satelit. Menurut jaraknya satelit bisa dikategorikan menjadi :

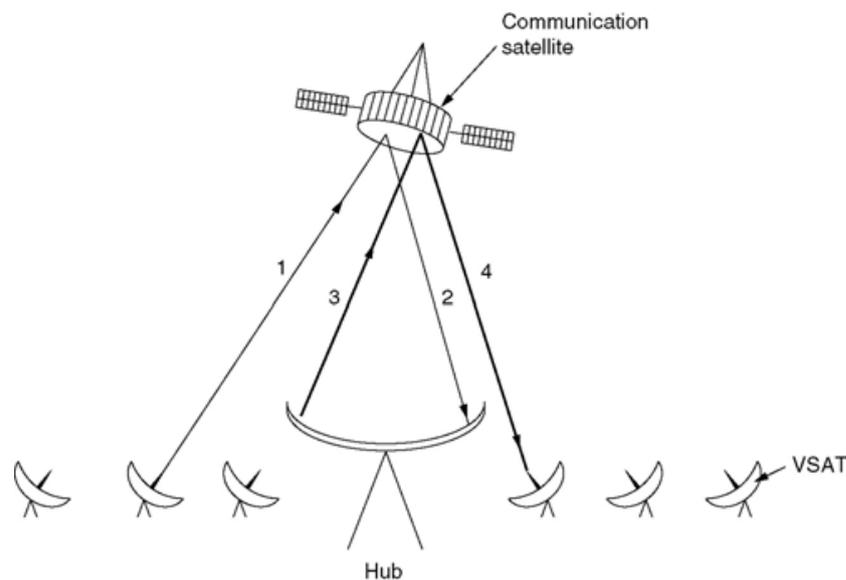
- Geostationary
- Medium-Earth Orbit
- Low-Earth Orbit

Komunikasi satelit menggunakan frekuensi / band

Table 7. Frekuensi Kerja Satelit

Band	Downlink	Uplink	Bandwidth	Permasalahan
L	1.5 GHz	1.6GHz	15 MHz	Bandwidth rendah, saluran penuh
S	1.9 GHz	2.2 GHz	70 MHz	Bnadwidth rendah, saluran penuh
C	4.0 GHz	6 GHz	500 MHz	Interferensi Terrestrial
Ku	11 GHz	14 GHz	500 MHz	Hujan
Ka	20 GHz	30 GHz	3500 MHz	Hujan, harga perangkat

Untuk menghubungi site yang lain, bisa dilakukan dengan Very Small Aperture Terminal (VSAT). VSAT adalah stasiun bumi 2 arah dengan antena parabola dengan diameter sekitar 3 – 10 meter.



Gambar 29. Komunikasi Satelit dengan VSAT

f. Routers

Sebuah Router mengartikan informasi dari satu jaringan ke jaringan yang lain, dia hampir sama dengan Bridge namun agak pintar sedikit, router akan mencari jalur yang terbaik untuk mengirimkan sebuah pesan yang berdasarkan atas alamat tujuan dan alamat asal.

Jika sebuah perusahaan mempunyai LAN dan menginginkan terkoneksi ke Internet, mereka harus membeli router. Ini berarti sebuah router dapat menterjemahkan informasi diantara LAN anda dan Internet. ini juga berarti mencari alternatif jalur yang terbaik untuk mengirimkan data melewati internet.

Ini berarti Router itu :

- o Mengatur jalur sinyal secara efisien

- Mengatur Pesan diantara dua buah protocol
- Mengatur Pesan diantara topologi jaringan linear Bus dan Bintang(star)
- Mengatur Pesan diantara melewati Kabel Fiber optic, kabel koaksialan atau kabel twisted pair



. Router Cisco dan RouterBoard

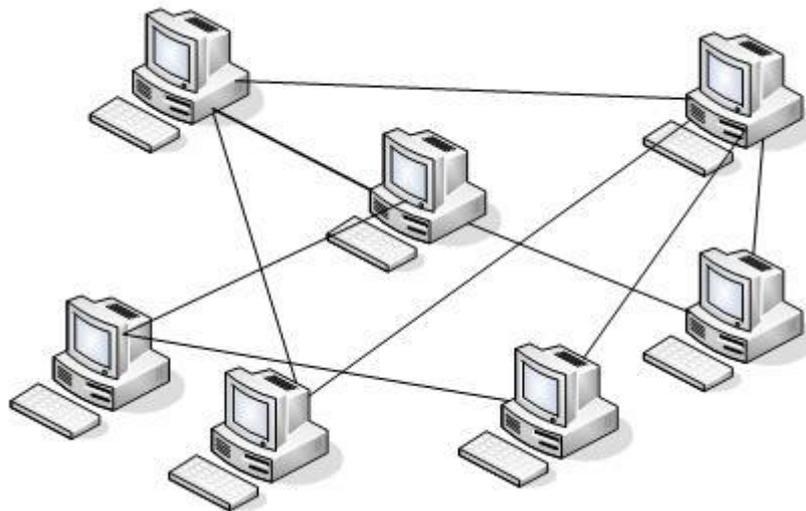
C. TOPOLOGI/ BENTUK JARINGAN

Topologi suatu jaringan didasarkan pada cara penghubung sejumlah node atau sentral dalam membentuk suatu sistem jaringan. Topologi jaringan yang umum dipakai adalah : Mess, Bintang (Star), Bus, Tree, dan Cincin (Ring).

1. Topologi Jaringan Mesh

Topologi Mesh adalah topologi yang tidak memiliki aturan dalam koneksi. Topologi ini biasanya timbul akibat tidak adanya perencanaan awal ketika membangun suatu jaringan, sehingga kegagalan komunikasi menjadi sulit dideteksi, dan ada kemungkinan boros dalam pemakaian media transmisi.

Topologi jaringan ini menerapkan hubungan antar sentral secara penuh. Jumlah saluran harus disediakan untuk membentuk jaringan Mesh adalah jumlah sentral dikurangi 1 ($n-1$, n = jumlah sentral). Tingkat kerumitan jaringan sebanding dengan meningkatnya jumlah sentral yang terpasang. Dengan demikian disamping kurang ekonomis juga relatif mahal dalam pengoperasiannya.



Gambar 30. Topologi Mesh

2. Topologi Jaringan Bintang (Star)

Dalam topologi jaringan bintang, salah satu sentral dibuat sebagai sentral pusat. Bila dibandingkan dengan sistem mesh, sistem ini mempunyai tingkat kerumitan jaringan yang lebih sederhana sehingga sistem menjadi lebih ekonomis, tetapi beban yang dipikul sentral pusat cukup berat. Dengan demikian kemungkinan tingkat kerusakan atau gangguan dari sentral ini lebih besar. Terminal kontrol pusat bisa berupa sebuah komputer yang difungsikan sebagai pengendali tetapi bisa juga berupa “HUB” atau “MAU” (Multi Access Unit).

Terdapat dua alternatif untuk operasi simpul pusat. Simpul pusat beroperasi secara “broadcast” yang menyalurkan data ke seluruh arah. Pada operasi ini walaupun secara fisik kelihatan sebagai bintang namun secara logik sebenarnya beroperasi seperti bus. Alternatif ini menggunakan HUB.

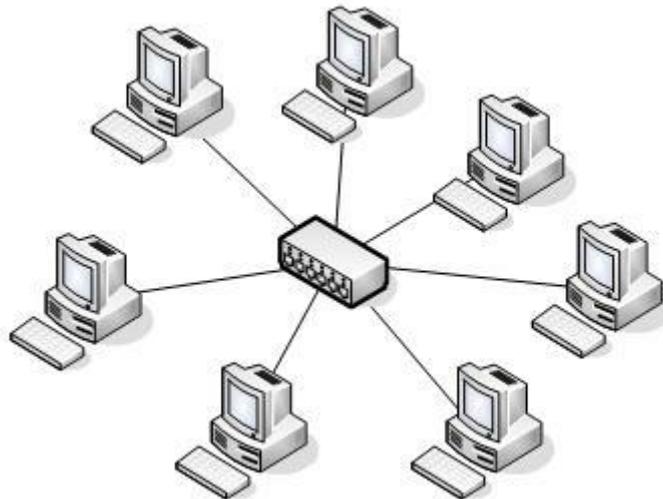
Simpul pusat beroperasi sebagai “switch”, data kiriman diterima oleh simpul kemudian dikirim hanya ke terminal tujuan (bersifat point-to-point), alternatif ini menggunakan MAU sebagai pengendali. Bila menggunakan HUB maka secara fisik sebenarnya jaringan berbentuk topologi Bintang namun secara logis bertopologi Bus. Bila menggunakan MAU maka baik fisik maupun logis bertopologi Bintang.

Kelebihan topologi bintang :

- Karena setiap komponen dihubungkan langsung ke simpul pusat maka pengelolaan menjadi mudah, kegagalan komunikasi mudah ditelusuri.
- Kegagalan pada satu komponen/terminal tidak mempengaruhi komunikasi terminal lain.

Kelemahan topologi bintang:

- Kegagalan pusat kontrol (simpul pusat) memutuskan semua komunikasi.
- Bila yang digunakan sebagai pusat kontrol adalah HUB maka kecepatan akan berkurang sesuai dengan penambahan komputer, semakin banyak semakin lambat.



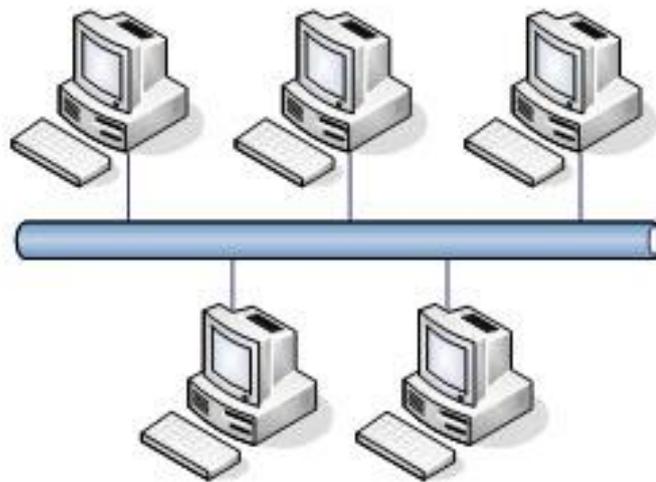
Gambar 31. Topologi Star

3. Topologi Jaringan Bus

Topologi bus ini sering juga disebut sebagai topologi backbone, dimana ada sebuah kabel coaxial yang dibentang kemudian beberapa komputer dihubungkan pada kabel tersebut.

Pada topologi ini semua sentral dihubungkan secara langsung pada medium transmisi dengan konfigurasi yang disebut Bus. Transmisi sinyal dari suatu sentral tidak dialirkan secara bersamaan dalam dua arah. Hal ini berbeda sekali dengan yang terjadi pada topologi jaringan mesh atau bintang, yang pada kedua sistem tersebut dapat dilakukan komunikasi atau interkoneksi antar sentral secara bersamaan. topologi jaringan bus tidak umum digunakan untuk interkoneksi antar sentral, tetapi biasanya digunakan pada sistem jaringan komputer

Secara sederhana pada topologi bus, satu kabel media transmisi dibentang dari ujung ke ujung, kemudian kedua ujung ditutup dengan “terminator” atau terminating-resistance (biasanya berupa tahanan listrik sekitar 60 ohm). Pada titik tertentu diadakan sambungan (tap) untuk setiap terminal. Wujud dari tap ini bisa berupa “kabel transeiver” bila digunakan “thick coax” sebagai media transmisi atau berupa “BNC T-connector” bila digunakan “thin coax” sebagai media transmisi atau berupa konektor “RJ-45” dan “hub” bila digunakan kabel UTP. Transmisi data dalam kabel bersifat “full duplex”, dan sifatnya “broadcast”, semua terminal bisa menerima transmisi data.



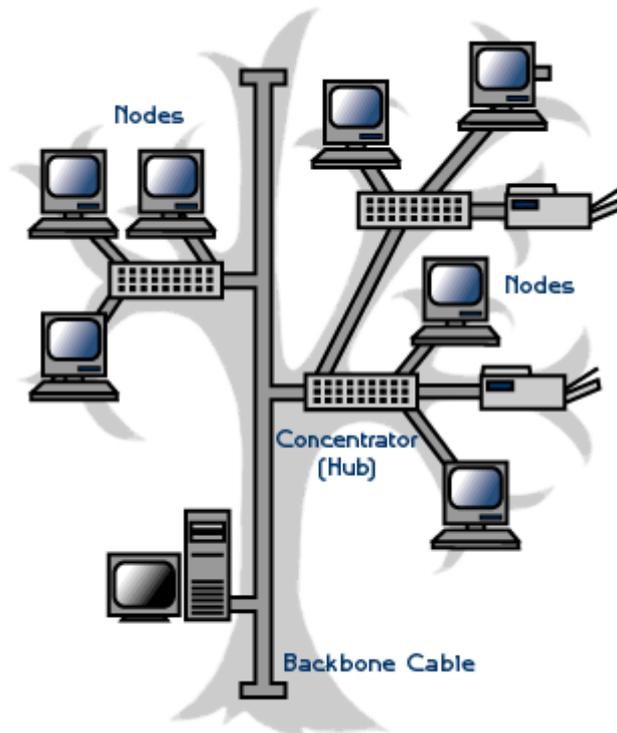
Gambar 32. Topologi Bus

4. Topologi Jaringan Pohon (Tree)

Topologi pohon adalah pengembangan atau generalisasi topologi bus. Media transmisi merupakan satu kabel yang bercabang namun loop tidak tertutup.

Topologi jaringan ini disebut juga sebagai topologi jaringan bertingkat. Topologi ini biasanya digunakan untuk interkoneksi antar sentral dengan hirarki yang berbeda. Untuk hirarki yang lebih rendah digambarkan pada lokasi yang rendah dan semakin keatas mempunyai hirarki semakin tinggi. Topologi jaringan jenis ini cocok digunakan pada sistem jaringan komputer.

Topologi pohon dimulai dari suatu titik yang disebut “headend”. Dari headend beberapa kabel ditarik menjadi cabang, dan pada setiap cabang terhubung beberapa terminal dalam bentuk bus, atau dicabang lagi hingga menjadi rumit. Ada dua kesulitan pada topologi ini, karena bercabang maka diperlukan cara untuk menunjukkan kemana data dikirim, atau kepada siapa transmisi data ditujukan. Kedua perlu suatu mekanisme untuk mengatur transmisi dari terminal terminal dalam jaringan.



Gambar 33. Topologi Cincin

5. Topologi Jaringan Cincin (Ring)

Untuk membentuk jaringan cincin, setiap sentral harus dihubungkan seri satu dengan yang lain dan hubungan ini akan membentuk loop tertutup. Cincin ini hampir sama fungsinya dengan concentrator pada topologi star yang menjadi pusat berkumpulnya ujung kabel dari setiap komputer yang terhubung.

Dalam sistem ini setiap sentral harus dirancang agar dapat berinteraksi dengan sentral yang berdekatan maupun berjauhan. Dengan demikian kemampuan melakukan switching ke berbagai arah sentral.

Secara lebih sederhana lagi topologi cincin merupakan untaian media transmisi dari satu terminal ke terminal lainnya hingga membentuk suatu lingkaran, dimana jalur transmisi hanya “satu arah”.

Tiga fungsi yang diperlukan dalam topologi cincin : penyelipan data, penerimaan data, dan pemindahan data.

- Penyelipan data adalah proses dimana data dimasukkan kedalam saluran transmisi oleh terminal pengirim setelah diberi alamat dan bit-bit tambahan lainnya.

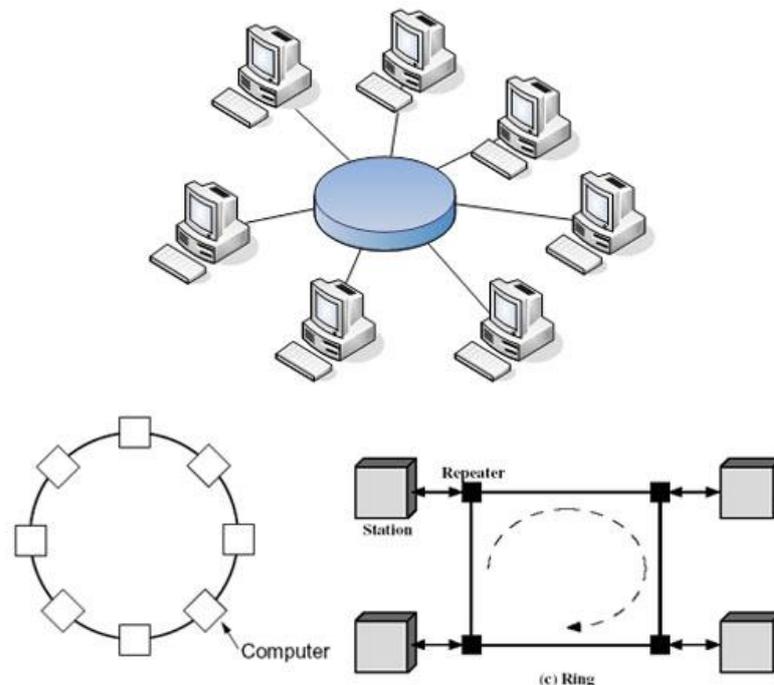
- Penerimaan data adalah proses ketika terminal yang dituju telah mengambil data dari saluran, yaitu dengan cara membandingkan alamat yang ada pada paket data dengan alamat terminal itu sendiri. Apabila alamat tersebut sama maka data kiriman disalin.
- Pemindahan data adalah proses dimana kiriman data diambil kembali oleh terminal pengirim karena tidak ada terminal yang menerimanya (mungkin akibat salah alamat). Jika data tidak diambil kembali maka data ini akan berputar-putar dalam saluran. Pada jaringan bus hal ini tidak akan terjadi karena kiriman akan diserap oleh “terminator”.

Pada hakekatnya setiap terminal dalam jaringan cincin adalah “repeater”, dan mampu melakukan ketiga fungsi dari topologi cincin. Sistem yang mengatur bagaimana komunikasi data berlangsung pada jaringan cincin sering disebut token-ring.

Kemungkinan permasalahan yang bisa timbul dalam jaringan cincin adalah:

- Kegagalan satu terminal / repeater akan memutuskan komunikasi ke semua terminal.
- Pemasangan terminal baru menyebabkan gangguan terhadap jaringan, terminal baru harus mengenal dan dihubungkan dengan kedua terminal tetangganya.

Keuntungan dari topologi jaringan ini antara lain : tingkat kerumitan jaringan rendah (sederhana), juga bila ada gangguan atau kerusakan pada suatu sentral maka aliran trafik dapat dilewatkan pada arah lain dalam sistem.

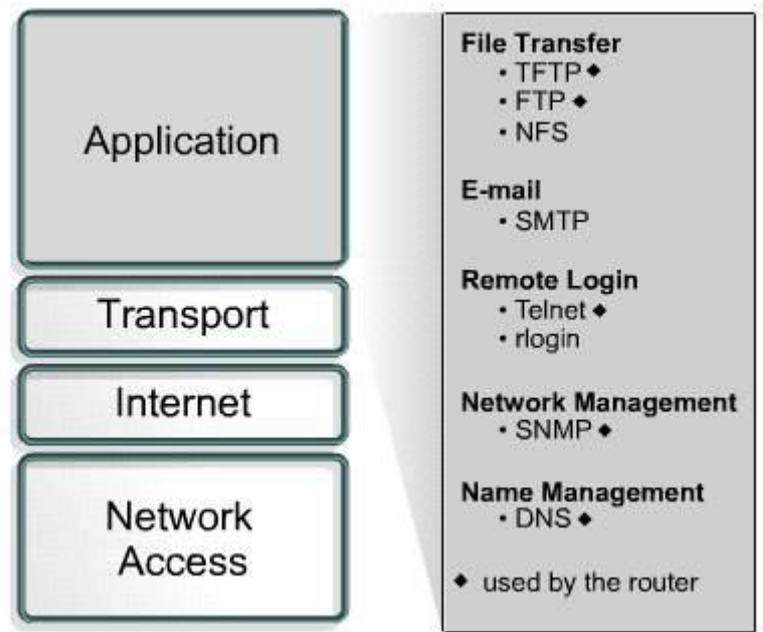


Gambar 34. Topologi Ring



BAB 4 TCP/IP

A. MODEL TCP/ IP PROTOKOL



Gambar 35. TCP/ IP Layer

TCP/IP adalah protokol internet yang paling banyak digunakan saat ini. TCP/IP (Transmission Control Protocol/Internet Protocol) memiliki beberapa keunggulan, diantaranya :

1. Open Protocol Standard, yaitu tersedia secara bebas dan dikembangkan independen terhadap komputer hardware ataupun sistem operasi apapun. Karena didukung secara meluas, TCP/IP sangat ideal untuk menyatukan bermacam hardware dan software, walaupun tidak berkomunikasi lewat internet.
2. Independen dari physical network hardware. Ini menyebabkan TCP/IP dapat mengintegrasikan bermacam network, baik melalui ethernet, token ring, dial-up, X.25/AX.25 dan media transmisi fisik lainnya.

3. Skema pengalamatan yang umum menyebabkan device yang menggunakan TCP/IP dapat menghubungi alamat device-device lain di seluruh network, bahkan Internet sekalipun.
4. High level protocol standar, yang dapat melayani user secara luas

Application layer menangani protocol level tertinggi, representation, encoding, and dialog control. TCP/IP protocol menggabungkan dari semua aplikasi yang berhubungan ke dalam satu layer. TCP/IP merupakan protocol yang support terhadap file transfer, e-mail, and remote login, dan beberapa protocol lain yang diantaranya:

- a. **File Transfer Protocol (FTP)**, Program yang memungkinkan kita memindahkan data di antara dua komputer yang berjauhan letaknya. Protokol yang dipakai pada Internet untuk mengirim file. FTP menggunakan connection oriented, reliable, dan mendukung transfer binary dan transfer ASCII.
- b. **Trivial File Transfer Protocol (TFTP)**, TFTP termasuk connectionless service dan menggunakan protocol the User Datagram Protocol (UDP). TFTP digunakan oleh router untuk transfer file configuration dan Cisco IOS images, dan untuk mentransfer file antara system yang mendukung TFTP.
- c. **Network File System (NFS)**, adalah protocol utama yang spesialisasi dalam file sharing (berbagi file). NFS dapat termasuk distributed file system protocol yang dikembangkan oleh Sun Microsystems yang mengijikan untuk mengakses file ke tempat penyimpanan seperti hardisk melalui jaringan
- d. **Simple Mail Transfer Protocol (SMTP)**, adalah protokol standar untuk pengiriman electronic mail (email) di internet. SMTP adalah protokol yang cukup sederhana, berbasis teks dimana protokol ini menyebutkan satu atau lebih penerima email untuk kemudian diverifikasi. Jika penerima email valid, maka email akan segera dikirim. SMTP menggunakan port 25 dan dapat dihubungi melalui program telnet. Karena protokol SMTP berawal dari protokol yang benar-benar berbasis teks ASCII, maka SMTP tidak bekerja terlalu baik dalam mengirimkan file-file binary. Standar untuk mengencode file-file biner agar dapat dikirimkan lewat SMTP dikembangkan dan menelurkan standar-standar seperti MIME (Multipurposes Internet Mail Extensions). Saat ini, hampir semua SMTP server mendukung 8BITMIME, yang dapat mengirimkan file-file biner semudah mengirimkan file teks. SMTP hanya protokol

- yang melakukan “push”, artinya dia hanya bisa mengambil email dari client tetapi tidak bisa melakukan “pull”, yaitu melayani pengambilan email di server oleh client. Pengambilan pesan atau email tersebut dilakukan dengan menggunakan protocol tersendiri yaitu protokop POP3 (Post Office Protokol) atau IMAP (Internet Message Access Protocol).
- e. Multipurpose Internet Mail Extensions (MIME) MIME adalah format standar internet untuk email. MIME mendefinisikan pengiriman pesan selain 8 bit karakter ASCII dengan file yang berisi image, suara, movie, dan program komputer. MIME adalah salah satu komponen dasar pendukung protokol HTTP.
 - f. Telnet, Telnet digunakan untuk mengakses computer lain lewat emulasi terminal seperti command prompt. Telnet client dikenaldengan local host. Telnet server dikenal dengan remote host.
 - g. Simple Network Management Protocol (SNMP), SNMP is a protocol that provides a way to monitor and control network devices. SNMP is also used to Manage configurations, statistics, performance, and security.
 - h. Domain Name System (DNS) – adalah distribute database system yang digunakan untuk pencarian nama komputer (name resolution) di jaringan yang menggunakan TCP/IP (Transmission Control Protocol/Internet Protocol). DNS biasa digunakan pada aplikasi yang terhubung ke Internet seperti web browser atau e-mail, dimana DNS membantu memetakan host name sebuah komputer ke IP address. Selain digunakan di Internet, DNS juga dapat di implementasikan ke private network atau intranet dimana DNS memiliki keunggulan seperti:
 - Mudah, DNS sangat mudah karena user tidak lagi direpotkan untuk mengingat IP addresssebuah komputer cukup host name (nama Komputer).
 - Konsisten, IP address sebuah komputer bisa berubah tapi host name tidak berubah.
 - Simple, user hanya menggunakan satu nama domain untuk mencari baik di Internet maupun di Intranet.

B. Internet Layer

Protokol yang berhubungan dengan internet layer ini adalah sebagai berikut :

☞ **IP (Internet Protocol)**, merupakan inti dari protocol TCP /IP, IP melakukan beberapa operasi :

- Defines a packet and an addressing scheme
- Transfers data between the Internet layer and network access layer
- Routes packets to remote hosts

IP memiliki sifat yang dikenal unreliable, connectionless, datagram delivery service ,best effort delivery . Unreliable / Ketidakandalan berarti bahwa Protokol IP tidak menjamin datagram yang dikirim pasti sampai ke tempat tujuan. Protocol IP hanya berjanji ia akan melakukan usaha sebaik-baiknya (best effort delivery) ,agar packet yang dikirim tersebut sampai ketujuan. 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 bisa jadi berbeda satu dengan yang lainnya, karena jalur yang ditempuh berbeda, kedatangan paket pun bisa jadi tidak berurutan.

☞ **Internet Control Message Protocol (ICMP)** adalah protokol yang bertugas mengirimkan pesan-pesan kesalahan dan kondisi lain yang memerlukan perhatian khusus. Pesan atau paket ICMP dikirim jika terjadi masalah pada layer IP dan layer atasnya (TCP/UDP). ICMP Error Message dibagi menjadi beberapa jenis diantaranya :

- Destination Unreachable, Pesan ini dihasilkan oleh router jika pengiriman paket mengalami kegagalan akibat masalah putusnya jalur, baik secara fisik maupun secara logic. Destination Unreachable ini dibagi menjadi beberapa tipe. Beberapa tipe yang penting adalah:
 - Network Unreachable, jika jaringan tujuan tak dapat dihubungi
 - Host Unreachable, jika host tujuan tak bisa dihubungi
 - Protocol at Destination is Unreachable, jika ditujuan tak tersedia protocol tersebut
 - Port is Unreachable, jika tidak ada port yang dimaksud pada tujuan
 - Destination Network is Unknown, jika network tujuan tak diketahui
 - Destination Host is Unknown, jika host tujuan tidak diketahui

- Time exceeded, Paket ICMP jenis ini dikirimkan jika isi field TTL dalam paket IP sudah habis dan paket belum juga sampai ke tujuannya. Sebagaimana telah diterangkan pada bagian IP diatas, tiap kali sebuah paket IP melewati satu router, nilai TTL dalam paket tersebut dikurangi satu. TTL ini diterapkan untuk mencegah timbulnya paket IP yang terus menerus berputar dinetwork karena suatu kesalahan tertentu, sehingga menghabiskan sumberdaya jaringan yang ada.
- Parameter Problem, paket ini dikirimkan jika terdapat kesalahan paameter pada header paket IP
- Source Quench, Paket ICMP ini dikirimkan jika router atau tujuan mengalami kongesti. Sebagai resspons pada paket ini, pihak pengirim paket harus memperlambat pengiriman paketnya.
- Redirect, paket ini dikirimkan jika router merasa host mengirimkan paket IP melalui router yang salah. Paket ini seharusnya dikirimkan melalui router lain.

Sedangkan ICMP Query Messages terdiri atas:

- Echo dan Echo Reply. Bertujuan untuk memeriksa apakah system tujuan dalam keadaan aktif. Program ping merupakan program pengiriman paket ini. Responder harus mengembalikan data yang sama dengan data yang dikirimkan.
- Timestamp dan Timestamp Reply. Menghasilkan informasi waktu yang diperlukan system tujuan untuk memproses suatu paket.
- Address mask, Untuk mengetahui berapa netmask yang harus digunakan oleh suatu host dalam suatu network.

☞ **Address Resolution Protocol (ARP)**, mencari alamat hardware dari host yang sudah diketahui alamat IPnya . ARP menerjemahkan alamat IP menjadi alamat Ethernet (MAC)

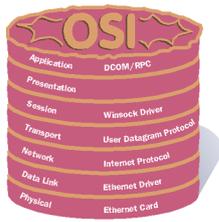
☞ **Reverse Address Resolution Protocol (RARP)**, ketika IP digunakan oleh mesin diskless (mesin tanpa menggunakan disk) tidak ada cara untuk mengetahui alamat IP nya ,Namun alamat MAC bisa diketahui. RARP mengetahui identitas alamat IP untuk alamat MAC tersebut. Mesin yang ditunjuk dinamakan RARP Server ,menjawab permintaan tersebut dan berakhirlah krisis identitas ini. RARP menggunakan informasi

alamat mesin MAC yang diketahui untuk mempelajari alamat IP dan melengkapi identitas mesin, RARP menerjemahkan alamat ethernet (MAC) menjadi alamat IP.

- ☞ **SLIP, (serial line internet protocol)** ,sebuah enkapsulasi serial standard industri untuk koneksi titik ke titik yang mendukung hanya sebuah routed protocol tunggal, yaitu TCP/IP. SLIP adalah pendahulu PPP.
- ☞ **PPP (Point to point protocol)**, Protokol yang paling umum digunakan untuk akses internet dial up, melebihi protocol SLIP yang mendahuluinya, Fitur nya termasuk pemberitahuan alamat, otentifikasi dengan CHAP atau PAP ,dukungan dengan banyak protocol, dan monitoring link .PPP mempunyai dua layer :Link control protocol (LCP) yang membuat ,mengkonfigurasi, dan menguji sebuah link, dan kemudian Network Control Protocol yang bervariasi, yang melakukan transport lalu lintas untuk sebuah kelompok protocol tertentu, seperti IPX.
- ☞ **PAP (Password Authentification Protocol)** :Dalam network Point to point protocol (PPP) adalah sebuah metode untuk memvalidasi permintaan koneksi. Alat yang meminta (ditempat remote) harus mengirimkan sebuah permintaan otentifikasi ,mengandung sebuah password dan ID. Kepada router local ketika mencoba koneksi. Tidak seperti CHAP (Challenge Handshake Autentification Protocol) yang lebih aman. PAP mengirimkan password tanpa enkripsi dan tidak mencoba untuk melakukan verifikasi apakah user mempunyai izin atau otorisasi untuk mengakses sumber daya yang diminta .ia hanya mengidentifikasi ujung yang remote.
- ☞ **CHAP (Challenge Handshake Autehintification Protocol)** :didukung pada sambungan sambungan yang menggunakan enkapsulasi PPP, merupakan sebuah fitur keamanan yang mengidentifikasi host yang meremote ,membantu mencegah user –user yang tidak mempunyai otorisasi, Setelah CHAP dilakukan, router atau access server menentukan apakah seorang user diperbolehkan akses atau tidak, merupakan potokol yang lebih baru dan lebih aman dibandingkan PAP.
- ☞ **FDDI, Fiber Distributed Data Interface**, Sebuah standard LAN, didefinisikan oleh ANSI X3T9.5 yang dapat bekerja pada kecepatan hingga 200 Mbps dan menggunakan media access token passing pada kabel serat optic .Untuk redundancy ,FDDI dapat menggunakan sebuah arsitektur dual ring.
- ☞ **Frame Relay**. Sebuah pengganti protocol X.25 sebuah teknologi relay paket yang tidak berhubungan dengan frame relay, yang menjamin pengiriman data) yang lebih

efisien. Frame relay adalah enkapsulasi layer Data Link Switch dengan usaha terbaik (best effort) dari akses yang dibagi (shared access) dan merupakan sebuah standard industri, yang melayani beberapa rangkaian virtual dan protocol diantara mekanisme yang berhubungan .

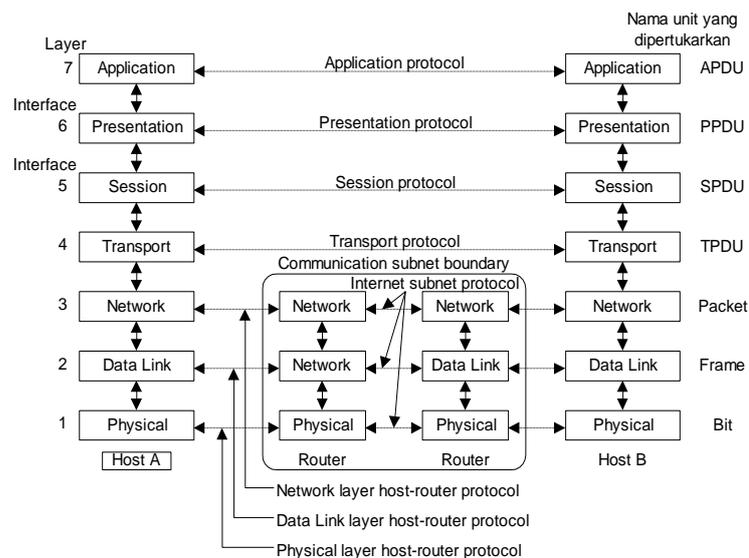
- ☞ **ATM Asynchronous Transfer Mode**, Standard Internasional. diidentifikasi oleh sel-sel (cells) 53 byte yang panjangnya sudah ditetapkan untuk mentransmisi sel-sel dalam banyak system layanan seperti voice, video dan data. Delay dari transit dikurangi karena sel-sel dengan panjang yang sudah ditetapkan tersebut memungkinkan pemrosesan untuk terjadi di hardware, ATM dirancang untuk memaksimalkan keuntungan dari media transmisi kecepatan tinggi seperti SONET, E3 dan T3 .



BAB 5 Model Referensi OSI

A. APA ITU OSI LAYER ?

Model referensi OSI (Open System Interconnection) menggambarkan bagaimana informasi dari suatu software aplikasi di sebuah komputer berpindah melewati sebuah media jaringan ke suatu software aplikasi di komputer lain. Model referensi OSI secara konseptual terbagi ke dalam 7 lapisan dimana masing-masing lapisan memiliki fungsi jaringan yang spesifik, seperti yang dijelaskan oleh gambar 2.1 (tanpa media fisik). Model ini diciptakan berdasarkan sebuah proposal yang dibuat oleh the International Standards Organization (ISO) sebagai langkah awal menuju standarisasi protokol internasional yang digunakan pada berbagai layer . Model ini disebut ISO OSI (Open System Interconnection) Reference Model karena model ini ditujukan bagi pengkoneksian open system. Open System dapat diartikan sebagai suatu sistem yang terbuka untuk berkomunikasi dengan sistem-sistem lainnya. Untuk ringkas-nya, kita akan menyebut model tersebut sebagai model OSI saja.



Gambar 36. Model Referensi OSI

Model OSI memiliki tujuh layer. Prinsip-prinsip yang digunakan bagi ketujuh layer tersebut adalah :

1. Sebuah layer harus dibuat bila diperlukan tingkat abstraksi yang berbeda.
2. Setiap layer harus memiliki fungsi-fungsi tertentu.
3. Fungsi setiap layer harus dipilih dengan teliti sesuai dengan ketentuan standar protocol internasional.
4. Batas-batas layer diusahakan agar meminimalkan aliran informasi yang melewati interface.
5. Jumlah layer harus cukup banyak, sehingga fungsi-fungsi yang berbeda tidak perlu disatukan dalam satu layer diluar keperluannya. Akan tetapi jumlah layer juga harus diusahakan sesedikit mungkin sehingga arsitektur jaringan tidak menjadi sulit dipakai.

Di bawah ini kita membahas setiap layer pada model OSI secara berurutan, dimulai dari layer terbawah. Perlu dicatat bahwa model OSI itu sendiri bukanlah merupakan arsitektur jaringan, karena model ini tidak menjelaskan secara pasti layanan dan protokolnya untuk digunakan pada setiap layernya. Model OSI hanya menjelaskan tentang apa yang harus dikerjakan oleh sebuah layer. Akan tetapi ISO juga telah membuat standard untuk semua layer, walaupun standard-standard ini bukan merupakan model referensi itu sendiri. Setiap layer telah dinyatakan sebagai standard internasional yang terpisah.

B. KARAKTERISTIK LAPISAN OSI

Ke tujuh lapisan dari model referensi OSI dapat dibagi ke dalam dua kategori, yaitu lapisan atas dan lapisan bawah.

Lapisan atas dari model OSI berurusan dengan persoalan aplikasi dan pada umumnya diimplementasi hanya pada software. Lapisan tertinggi (lapisan aplikasi) adalah lapisan penutup sebelum ke pengguna (user), keduanya, pengguna dan lapisan aplikasi saling berinteraksi proses dengan software aplikasi yang berisi sebuah komponen komunikasi. Istilah lapisan atas kadang-kadang digunakan untuk menunjuk ke beberapa lapisan atas dari lapisan lapisan yang lain di model OSI.

Lapisan bawah dari model OSI mengendalikan persoalan transport data. Lapisan fisik dan lapisan data link diimplementasikan ke dalam hardware dan software. Lapisan-lapisan bawah yang lain pada umumnya hanya diimplementasikan dalam software. Lapisan terbawah,

yaitu lapisan fisik adalah lapisan penutup bagi media jaringan fisik (misalnya jaringan kabel), dan sebagai penanggung jawab bagi penempatan informasi pada media jaringan. Tabel berikut ini menampilkan pemisahan kedua lapisan tersebut pada lapisan-lapisan model OSI.

Table 8. Pemisahan Lapisan atas dan Lapisan bawah pada model OSI

Application	Application	Lapisan Atas
Presentatio n		
Session		
Transport	Data Transport	Lapisan Bawah
Network		
Data Link		
Physical		

C. PROTOKOL

Model OSI menyediakan secara konseptual kerangka kerja untuk komunikasi antar komputer, tetapi model ini bukan merupakan metoda komunikasi. Sebenarnya komunikasi dapat terjadi karena menggunakan protokol komunikasi. Di dalam konteks jaringan data, sebuah protokol adalah suatu aturan formal dan kesepakatan yang menentukan bagaimana komputer bertukar informasi melewati sebuah media jaringan. Sebuah protokol mengimplementasikan salah satu atau lebih dari lapisan-lapisan OSI. Sebuah variasi yang lebar dari adanya protokol komunikasi, tetapi semua memelihara pada salah satu aliran group: protokol LAN, protokol WAN, protokol jaringan, dan protokol routing. Protokol LAN beroperasi pada lapisan fisik dan data link dari model OSI dan mendefinisikan komunikasi di atas macam-macam media LAN. Protokol WAN beroperasi pada ketiga lapisan terbawah dari model OSI dan mendefinisikan komunikasi di atas macam-macam WAN. Protokol routing adalah protokol lapisan jaringan yang bertanggung jawab untuk menentukan jalan dan pengaturan lalu lintas. Akhirnya protokol jaringan adalah berbagai protokol dari lapisan teratas yang ada dalam sederetan protokol.

D. LAPISAN-LAPISAN MODEL OSI

1. Physical Layer

Physical Layer berfungsi dalam pengiriman raw bit ke channel komunikasi. Masalah desain yang harus diperhatikan disini adalah memastikan bahwa bila satu sisi mengirim data 1 bit, data tersebut harus diterima oleh sisi lainnya sebagai 1 bit pula, dan bukan 0 bit. Pertanyaan yang timbul dalam hal ini adalah : berapa volt yang perlu digunakan untuk menyatakan nilai 1? dan berapa volt pula yang diperlukan untuk angka 0?. Diperlukan berapa mikrosekond suatu bit akan habis? Apakah transmisi dapat diproses secara simultan pada kedua arahnya? Berapa jumlah pin yang dimiliki jaringan dan apa kegunaan masing-masing pin? Secara umum masalah-masalah desain yang ditemukan di sini berhubungan secara mekanik, elektrik dan interface prosedural, dan media fisik yang berada di bawah physical layer.

2. Data Link Layer

Tugas utama data link layer adalah sebagai fasilitas transmisi raw data dan mentransformasi data tersebut ke saluran yang bebas dari kesalahan transmisi. Sebelum diteruskan ke network layer, data link layer melaksanakan tugas ini dengan memungkinkan pengirim memecah-mecah data input menjadi sejumlah data frame (biasanya berjumlah ratusan atau ribuan byte). Kemudian data link layer mentransmisikan frame tersebut secara berurutan, dan memproses acknowledgement frame yang dikirim kembali oleh penerima. Karena physical layer menerima dan mengirim aliran bit tanpa mengindahkan arti atau arsitektur frame, maka tergantung pada data link layer-lah untuk membuat dan mengenali batas-batas frame itu. Hal ini bisa dilakukan dengan cara membubuhkan bit khusus ke awal dan akhir frame. Bila secara insidental pola-pola bit ini bisa ditemui pada data, maka diperlukan perhatian khusus untuk menyakinkan bahwa pola tersebut tidak secara salah dianggap sebagai batas-batas frame.

Terjadinya noise pada saluran dapat merusak frame. Dalam hal ini, perangkat lunak data link layer pada mesin sumber dapat mengirim kembali frame yang rusak tersebut. Akan tetapi transmisi frame sama secara berulang-ulang bisa menimbulkan duplikasi frame. Frame duplikat perlu dikirim apabila acknowledgement frame dari penerima yang dikembalikan ke pengirim telah hilang. Tergantung pada layer inilah untuk mengatasi masalah-masalah yang disebabkan rusaknya, hilangnya dan duplikasi frame. Data link layer menyediakan beberapa kelas layanan bagi network layer. Kelas layanan ini dapat dibedakan dalam hal kualitas dan harganya.

Masalah-masalah lainnya yang timbul pada data link layer (dan juga sebagian besar layer-layer di atasnya) adalah mengusahakan kelancaran proses pengiriman data dari pengirim yang cepat ke penerima yang lambat. Mekanisme pengaturan lalu-lintas data harus memungkinkan pengirim mengetahui jumlah ruang buffer yang dimiliki penerima pada suatu saat tertentu. Seringkali pengaturan aliran dan penanganan error ini dilakukan secara terintegrasi.

Saluran yang dapat mengirim data pada kedua arahnya juga bisa menimbulkan masalah. Sehingga dengan demikian perlu dijadikan bahan pertimbangan bagi software data link layer. Masalah yang dapat timbul di sini adalah bahwa frame-frame acknowledgement yang mengalir dari A ke B bersaing saling mendahului dengan aliran dari B ke A. Penyelesaian yang terbaik (piggy backing) telah bisa digunakan; nanti kita akan membahasnya secara mendalam.

Jaringan broadcast memiliki masalah tambahan pada data link layer. Masalah tersebut adalah dalam hal mengontrol akses ke saluran yang dipakai bersama. Untuk mengatasinya dapat digunakan sublayer khusus data link layer, yang disebut medium access sublayer.

Masalah mengenai data link control akan diuraikan lebih detail lagi pada bab tiga.

3. Network Layer

Network layer berfungsi untuk pengendalian operasi subnet. Masalah desain yang penting adalah bagaimana caranya menentukan route pengiriman paket dari sumber ke tujuannya. Route dapat didasarkan pada table statik yang “dihubungkan ke” network. Route juga dapat ditentukan pada saat awal percakapan misalnya session terminal. Terakhir, route dapat juga sangat dinamik, dapat berbeda bagi setiap paketnya. Oleh karena itu, route pengiriman sebuah paket tergantung beban jaringan saat itu.

Bila pada saat yang sama dalam sebuah subnet terdapat terlalu banyak paket, maka ada kemungkinan paket-paket tersebut tiba pada saat yang bersamaan. Hal ini dapat menyebabkan terjadinya bottleneck. Pengendalian kemacetan seperti itu juga merupakan tugas network layer.

Karena operator subnet mengharap bayaran yang baik atas tugas pekerjaannya. seringkali terdapat beberapa fungsi accounting yang dibuat pada network layer. Untuk membuat informasi tagihan, setidaknya software mesti menghitung jumlah paket atau karakter

atau bit yang dikirimkan oleh setiap pelanggannya. Accounting menjadi lebih rumit, bilamana sebuah paket melintasi batas negara yang memiliki tarif yang berbeda.

Perpindahan paket dari satu jaringan ke jaringan lainnya juga dapat menimbulkan masalah yang tidak sedikit. Cara pengalamatan yang digunakan oleh sebuah jaringan dapat berbeda dengan cara yang dipakai oleh jaringan lainnya. Suatu jaringan mungkin tidak dapat menerima paket sama sekali karena ukuran paket yang terlalu besar. Protokolnyapun bisa berbeda pula, demikian juga dengan yang lainnya. Network layer telah mendapat tugas untuk mengatasi semua masalah seperti ini, sehingga memungkinkan jaringan-jaringan yang berbeda untuk saling terinterkoneksi.

4. Transport Layer

Fungsi dasar transport layer adalah menerima data dari session layer, memecah data menjadi bagian-bagian yang lebih kecil bila perlu, meneruskan data ke network layer, dan menjamin bahwa semua potongan data tersebut bisa tiba di sisi lainnya dengan benar. Selain itu, semua hal tersebut harus dilaksanakan secara efisien, dan bertujuan dapat melindungi layer-layer bagian atas dari perubahan teknologi hardware yang tidak dapat dihindari.

Dalam keadaan normal, transport layer membuat koneksi jaringan yang berbeda bagi setiap koneksi transport yang diperlukan oleh session layer. Bila koneksi transport memerlukan throughput yang tinggi, maka transport layer dapat membuat koneksi jaringan yang banyak. Transport layer membagi-bagi pengiriman data ke sejumlah jaringan untuk meningkatkan throughput. Di lain pihak, bila pembuatan atau pemeliharaan koneksi jaringan cukup mahal, transport layer dapat menggabungkan beberapa koneksi transport ke koneksi jaringan yang sama. Hal tersebut dilakukan untuk membuat penggabungan ini tidak terlihat oleh session layer.

Transport layer juga menentukan jenis layanan untuk session layer, dan pada gilirannya jenis layanan bagi para pengguna jaringan. Jenis transport layer yang paling populer adalah saluran error-free point to point yang meneruskan pesan atau byte sesuai dengan urutan pengirimannya. Akan tetapi, terdapat pula jenis layanan transport lainnya. Layanan tersebut adalah transport pesan terisolasi yang tidak menjamin urutan pengiriman, dan membroadcast pesan-pesan ke sejumlah tujuan. Jenis layanan ditentukan pada saat koneksi dimulai.

Transport layer merupakan layer end to end sebenarnya, dari sumber ke tujuan. Dengan kata lain, sebuah program pada mesin sumber membawa percakapan dengan program

yang sama dengan pada mesin yang dituju. Pada layer-layer bawah, protokol terdapat di antara kedua mesin dan mesin-mesin lain yang berada didekatnya. Protokol tidak terdapat pada mesin sumber terluar atau mesin tujuan terluar, yang mungkin dipisahkan oleh sejumlah router. Perbedaan antara layer 1 sampai 3 yang terjalin, dan layer 4 sampai 7 yang end to end. Hal ini dapat dijelaskan seperti pada gambar 2-1.

Sebagai tambahan bagi penggabungan beberapa aliran pesan ke satu channel, transport layer harus hati-hati dalam menetapkan dan memutuskan koneksi pada jaringan. Proses ini memerlukan mekanisme penamaan, sehingga suatu proses pada sebuah mesin mempunyai cara untuk menerangkan dengan siapa mesin itu ingin bercakap-cakap. Juga harus ada mekanisme untuk mengatur arus informasi, sehingga arus informasi dari host yang cepat tidak membanjiri host yang lambat. Mekanisme seperti itu disebut pengendalian aliran dan memainkan peranan penting pada transport layer (juga pada layer-layer lainnya). Pengendalian aliran antara host dengan host berbeda dengan pengendalian aliran router dengan router. Kita akan mengetahui nanti bahwa prinsip-prinsip yang sama digunakan untuk kedua jenis pengendalian tersebut.

5. Session Layer

Session layer mengizinkan para pengguna untuk menetapkan session dengan pengguna lainnya. Sebuah session selain memungkinkan transport data biasa, seperti yang dilakukan oleh transport layer, juga menyediakan layanan yang istimewa untuk aplikasi-aplikasi tertentu. Sebuah session digunakan untuk memungkinkan seseorang pengguna log ke remote timesharing system atau untuk memindahkan file dari satu mesin ke mesin lainnya.

Sebuah layanan session layer adalah untuk melaksanakan pengendalian dialog. Session dapat memungkinkan lalu lintas bergerak dalam bentuk dua arah pada suatu saat, atau hanya satu arah saja. Jika pada satu saat lalu lintas hanya satu arah saja (analog dengan rel kereta api tunggal), session layer membantu untuk menentukan giliran yang berhak menggunakan saluran pada suatu saat.

Layanan session di atas disebut manajemen token. Untuk sebagian protokol, adalah penting untuk memastikan bahwa kedua pihak yang bersangkutan tidak melakukan operasi pada saat yang sama. Untuk mengatur aktivitas ini, session layer menyediakan token-token yang dapat digilirkan. Hanya pihak yang memegang token yang diijinkan melakukan operasi kritis.

Layanan session lainnya adalah sinkronisasi. Ambil contoh yang dapat terjadi ketika mencoba transfer file yang berdurasi 2 jam dari mesin yang satu ke mesin lainnya dengan kemungkinan mempunyai selang waktu 1 jam antara dua crash yang dapat terjadi. Setelah masing-masing transfer dibatalkan, seluruh transfer mungkin perlu diulangi lagi dari awal, dan mungkin saja mengalami kegagalan lain. Untuk mengurangi kemungkinan terjadinya masalah ini, session layer dapat menyisipkan tanda tertentu ke aliran data. Karena itu bila terjadi crash, hanya data yang berada sesudah tanda tersebut yang akan ditransfer ulang.

6. Presentation Layer

Presentation layer melakukan fungsi-fungsi tertentu yang diminta untuk menjamin penemuan sebuah penyelesaian umum bagi masalah tertentu. Presentation Layer tidak mengizinkan pengguna untuk menyelesaikan sendiri suatu masalah. Tidak seperti layer-layer di bawahnya yang hanya melakukan pemindahan bit dari satu tempat ke tempat lainnya, presentation layer memperhatikan syntax dan semantik informasi yang dikirimkan.

Satu contoh layanan presentation adalah encoding data. Kebanyakan pengguna tidak memindahkan string bit biner yang random. Para pengguna saling bertukar data seperti nama orang, tanggal, jumlah uang, dan tagihan. Item-item tersebut dinyatakan dalam bentuk string karakter, bilangan interger, bilangan floating point, struktur data yang dibentuk dari beberapa item yang lebih sederhana. Terdapat perbedaan antara satu komputer dengan komputer lainnya dalam memberi kode untuk menyatakan string karakter (misalnya, ASCII dan Unicode), integer (misalnya komplement satu dan komplement dua), dan sebagainya. Untuk memungkinkan dua buah komputer yang memiliki presentation yang berbeda untuk dapat berkomunikasi, struktur data yang akan dipertukarkan dapat dinyatakan dengan cara abstrak, sesuai dengan encoding standard yang akan digunakan “pada saluran”. Presentation layer mengatur data-struktur abstrak ini dan mengkonversi dari representation yang digunakan pada sebuah komputer menjadi representation standard jaringan, dan sebaliknya.

7. Application Layer

Application layer terdiri dari bermacam-macam protokol. Misalnya terdapat ratusan jenis terminal yang tidak kompatibel di seluruh dunia. Ambil keadaan dimana editor layar penuh yang diharapkan bekerja pada jaringan dengan bermacam-macam terminal, yang masing-masing memiliki layout layar yang berlainan, mempunyai cara urutan penekanan

tombol yang berbeda untuk penyisipan dan penghapusan teks, memindahkan sensor dan sebagainya.

Suatu cara untuk mengatasi masalah seperti di atas, adalah dengan menentukan terminal virtual jaringan abstrak, sehingga editor dan program-program lainnya dapat ditulis agar saling bersesuaian. Untuk menangani setiap jenis terminal, satu bagian software harus ditulis untuk memetakan fungsi terminal virtual jaringan ke terminal sebenarnya. Misalnya, saat editor menggerakkan cursor terminal virtual ke sudut layar kiri, software tersebut harus mengeluarkan urutan perintah yang sesuai untuk mencapai cursor tersebut. Seluruh software terminal virtual berada pada application layer.

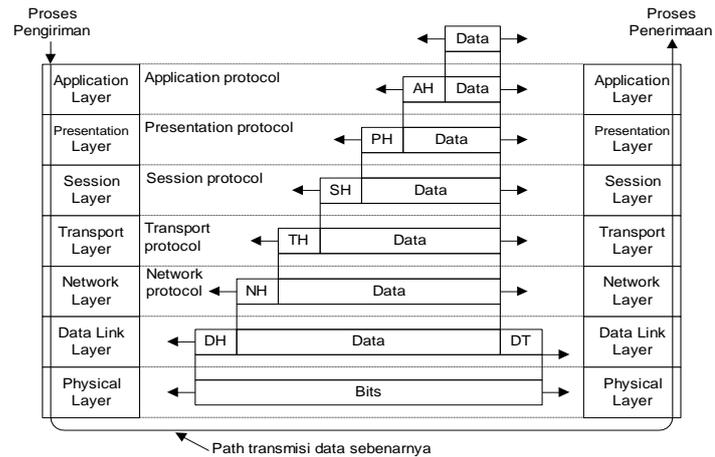
Fungsi application layer lainnya adalah pemindahan file. Sistem file yang satu dengan yang lainnya memiliki konvensi penamaan yang berbeda, cara menyatakan baris-baris teks yang berbeda, dan sebagainya. Perpindahan file dari sebuah sistem ke sistem lainnya yang berbeda memerlukan penanganan untuk mengatasi adanya ketidak-kompatibelan ini. Tugas tersebut juga merupakan pekerjaan application layer, seperti pada surat elektronik, remote job entry, directory lookup, dan berbagai fasilitas bertujuan umum dan fasilitas bertujuan khusus lainnya.

E. TRANSMISI DATA PADA MODEL OSI

Gambar 37 menjelaskan sebuah contoh tentang bagaimana data dapat ditransmisikan dengan menggunakan model OSI. Proses pengiriman memiliki data yang akan dikirimkan ke proses penerima. Proses pengirim menyerahkan data ke application layer, yang kemudian menambahkan application header, AH (yang mungkin juga kosong), ke ujung depannya dan menyerahkan hasilnya ke presentation layer.

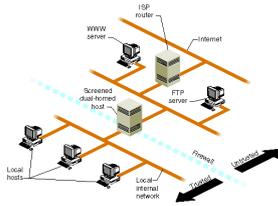
Presentation layer dapat membentuk data ini dalam berbagai cara dan mungkin saja menambahkan sebuah header di ujung depannya, yang diberikan oleh session layer. Penting untuk diingat bahwa presentation layer tidak menyadari tentang bagian data yang mana yang diberi tanda AH oleh application layer yang merupakan data pengguna yang sebenarnya.

Proses pemberian header ini berulang terus sampai data tersebut mencapai physical layer, dimana data akan ditransmisikan ke mesin lainnya. Pada mesin tersebut, semua header tadi dicopoti satu per satu sampai mencapai proses penerimaan.



Gambar 37. Contoh tentang bagaimana model OSI digunakan

Yang menjadi kunci di sini adalah bahwa walaupun transmisi data aktual berbentuk vertikal seperti pada gambar 1-17, setiap layer diprogram seolah-olah sebagai transmisi yang bersangkutan berlangsung secara horizontal. Misalnya, saat transport layer pengiriman mendapatkan pesan dari session layer, maka transport layer akan membubuhkan header transport layer dan mengirimkannya ke transport layer penerima.



BAB 6 IP ADDRESS DAN SUBNETTING

A. IP ADDRESS

Agar unik setiap computer yang terkoneksi ke Internet diberi alamat yang berbeda. Alamat ini supaya seragam seluruh dunia maka pemberian alamat IP address diseluruh dunia diberikan oleh badan internasional Internet Assigned Number Authority (IANA), dimana IANA hanya memberikan IP address Network ID nya saja sedangkan host ID diatur oleh pemilik IP address tersebut.

IP Address direpresentasikan dalam 32 bit data, dan biasanya dituliskan dalam 4 buah angka yang masing-masing merepresentasikan 8 bit bilangan, dan dipisahkan oleh tanda titik. Contoh IP address untuk cisco.com adalah 198.133.210.16.

Alamat yang unik terdiri dari 32 bit yang dibagi dalam 4 oktet (8 bit)

00000000 . 00000000 . 00000000 . 00000000

o 1 o 2 o 3 o 4

Ip address dibagi menjadi 2 bagian yaitu Network ID dan Host ID, Network ID yang akan menentukan alamat dalam jaringan (network address) sedangkan Host ID menentukan alamat dari peralatan jaringan yang sifatnya unik untuk membedakan antara satu mesin dengan mesin lainnya Ibaratkan Network ID Nomor jalan dan alamat jalan sedangkan Host ID adalah nomor rumahnya.

B. KELAS

Berdasarkan jumlah host yang dapat dimiliki sebuah jaringan, jaringan terbagi atas 5 kelas IP, yaitu kelas A, B, C, D dan E. Namun karena yang paling sering dan umum digunakan adalah kelas A, B, dan C, maka kali ini hanya akan dibahas ketiga kelas IP tersebut.

Kelas juga berfungsi untuk menentukan bagian oktet mana merupakan bagian NetworkID dan HostID.

IP address class	IP address range (First Octet Decimal Value)
Class A	1-126 (00000001-01111110) *
Class B	128-191 (10000000-10111111)
Class C	192-223 (11000000-11011111)
Class D	224-239 (11100000-11101111)
Class E	240-255 (11110000-11111111)

Gambar 38. Kelas IP Address

Kelas yang umum digunakan adalah kelas A sampai dengan kelas C. Pada setiap kelas angka pertama dengan angka terakhir tidak dianjurkan untuk digunakan karena sebagai valid host ids, misalnya kelas A 0 dan 127, kelas B 128 dan 192, kelas C 191 dan 224. ini biasanya digunakan untuk loopback addresses.

Catatan :

- Alamat Network ID dan Hos ID tidak boleh semuanya 0 atau 1 karena jika semuanya angka biner 1 : 255.255.255.255 maka alamat tersebut disebut flobroadcast
- alamat network, digunakan dalam routing untuk menunjukkan pengiriman paket remote network, contohnya 10.0.0.0, 172.16.0.0 dan 192.168.10.0

1. Network kelas A

Jaringan kelas A memiliki ciri bit pertama adalah 0, sedangkan 7 bit berikutnya mengidentifikasi jaringan, dan 24 bit berikutnya adalah host. Jadi pada kelas ini hanya akan terdapat 27 jaringan, atau 128 buah jaringan, namun setiap jaringan dapat memiliki jutaan host (224 buah host). Jadi network kelas A akan memiliki angka pertama dari IP Address antara 0-127.

2. Network kelas B

Apabila dua bit pertama dari IP Address adalah 1 0, maka jaringan tersebut termasuk dalam jaringan kelas B. Dua bit pertama akan mengidentifikasikan kelas dari jaringan, 14 bit berikutnya akan mengidentifikasikan jaringannya, sedangkan 16 berikutnya mengidentifikasi host. Ada ribuan jaringan kelas B, dan tiap jaringan memiliki ribuan host. Angka pertama dari IP Address untuk jaringan kelas B berkisar antara 128-191.

3. Network kelas C

Jaringan kelas C bercirikan tiga bit pertama dari IP Address adalah 1 1 0. Tiga bit pertama ini mencirikan jenis jaringannya, 21 bit berikutnya mengidentifikasi jaringannya sendiri, dan 8 bit sisanya mengidentifikasi host. Ada jutaan network kelas C, namun tiap jaringan hanya memiliki maksimal 254 host. Angka pertama dari IP Address untuk jaringan kelas C berkisar antara 192-223.

Selain ke tiga kelas di atas, ada 2 kelas lagi yang ditujukan untuk pemakaian khusus, yakni kelas D dan kelas E. Jika 4 bit pertama adalah 1110, IP Address merupakan kelas D yang digunakan untuk multicast address, yakni sejumlah komputer yang memakai bersama suatu aplikasi (bedakan dengan pengertian network address yang mengacu kepada sejumlah komputer yang memakai bersama suatu network).

Salah satu penggunaan multicast address yang sedang berkembang saat ini di Internet adalah untuk aplikasi real-time video conference yang melibatkan lebih dari dua host (multipoint), menggunakan Multicast Backbone (MBone). Kelas terakhir adalah kelas E (4 bit pertama adalah 1111 atau sisa dari seluruh kelas). Pemakaiannya dicadangkan untuk kegiatan eksperimental. Jenis kelas address yang diberikan oleh koordinator IP Address bergantung kepada kebutuhan instansi yang meminta, yakni jumlah host yang akan diintegrasikan dalam network dan rencana pengembangan untuk beberapa tahun mendatang. Untuk perusahaan, kantor pemerintah atau universitas besar yang memiliki puluhan ribu komputer dan sangat berpotensi untuk tumbuh menjadi jutaan komputer, koordinator IP Address akan mempertimbangkan untuk memberikan kelas A. Contoh IP Address kelas A yang dipakai di Internet adalah untuk amatir paket radio seluruh dunia, mendapat IP nomor 44.xxx.xxx.xxx. Untuk kelas B, contohnya adalah nomor 172.16.xxx.xxx .

Untuk mempermudah dalam menentukan kelas mana IP yang kita lihat, perhatikan gambar dibawah ini. Pada saat kita menganalisa suatu alamat IP maka perhatikan ocbit pertamanya

Class A	Network			Host
Octet	1	2	3	4

Class B	Network		Host	
Octet	1	2	3	4

Class C	Network			Host
Octet	1	2	3	4

Class D	Host			
Octet	1	2	3	4

Gambar 39. Pembagian Oktet tiap kelas

Pada kelas A : 8 oktet pertama adalah alamat networknya, sedangkan sisanya 24 bits merupakan alamat untuk host yang bisa digunakan. Jadi admin dapat membuat banyak sekali alamat untuk hostnya, dengan memperhatikan →

$$2^{24} - 2 = 16.777.214 \text{ host}$$

N ; jumlah bit terakhir dari

(2) adalah alamat loopback

Pada kelas B : menggunakan 16 bit pertama untuk mengidentifikasi network sebagai bagian dari address. Dua oktet sisanya (16 bits) digunakan untuk alamat host → $2^{16} - 2 = 65.534 \text{ Host}$

Pada Kelas C : menggunakan 24 bit pertama untuk network dan 8 bits sisanya untuk alamat host → $2^8 - 2 = 254 \text{ Host}$

2 ¹⁵	2 ¹⁴	2 ¹³	2 ¹²	2 ¹¹	2 ¹⁰	2 ⁹	2 ⁸	2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Gambar 40. Perhitungan 2 pangkat N

C. SUBNET MASK

Setiap jaringan TCP/IP memerlukan nilai subnet yang dikenal sebagai subnet mask atau address mask.

Nilai subnet mask memisahkan network id dengan host id. Dapat dilihat pada table dibawah ini :

Table 9. Perhitungan 2 pangkat N

CLASS	Subnet Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnet mask diperlukan oleh TCP/IP untuk menentukan, apakah jaringan yang dimaksud adalah jaringan local atau non local. Untuk jaringan non local berarti harus mentransmisi paket data melalui sebuah router. Dengan demikian diperlukan address mask untuk menyaring (filter) IP address dan paket data yang keluar masuk jaringan tersebut.

D. NETWORK ADDRESS

Address ini digunakan untuk mengenali suatu network pada jaringan Internet. Misalkan untuk host dengan IP Address kelas B 167.205.4.60. Tanpa memakai subnet, network address dari host ini adalah 167.205.0.0. Address ini didapat dengan membuat seluruh bit host pada 2 segmen terakhir menjadi 0. Tujuannya adalah untuk menyederhanakan informasi routing pada Internet.

Router cukup melihat network address (167.205) untuk menentukan kemana paket tersebut harus dikirimkan. Contoh untuk kelas C, network address untuk IP address 202.152.1.250 adalah 202.152.1.0. Analogi yang baik untuk menjelaskan fungsi network address ini adalah dalam pengolahan surat pada kantor pos.

Petugas penyortir surat pada kantor pos cukup melihat kota tujuan pada alamat surat (tidak perlu membaca seluruh alamat) untuk menentukan jalur mana yang harus ditempuh surat tersebut. Pekerjaan “routing” surat-surat menjadi lebih cepat. Demikian juga halnya dengan router di Internet pada saat melakukan routing atas paket-paket data.

E. BROADCAST ADDRESS

Address ini digunakan untuk mengirim/menerima informasi yang harus diketahui oleh seluruh host yang ada pada suatu network. Seperti diketahui, setiap paket IP memiliki header

alamat tujuan berupa IP Address dari host yang akan dituju oleh paket tersebut. Dengan adanya alamat ini, maka hanya host tujuan saja yang Memproses paket tersebut, sedangkan host lain akan mengabaikannya.

Bagaimana jika suatu host ingin mengirim paket kepada seluruh host yang ada pada networknya ? Tidak efisien jika ia harus membuat replikasi paket sebanyak jumlah host tujuan. Pemakaian bandwidth akan meningkat dan beban kerja host pengirim bertambah, padahal isi paket-paket tersebut sama. Oleh karena itu, dibuat konsep broadcast address.

Host cukup mengirim ke alamat broadcast, maka seluruh host yang ada pada network akan menerima paket tersebut. Konsekuensinya, seluruh host pada network yang sama harus memiliki address broadcast yang sama dan address tersebut tidak boleh digunakan sebagai IP Address untuk host tertentu.

Jadi, sebenarnya setiap host memiliki 2 address untuk menerima paket : pertama adalah IP Addressnya yang bersifat unik dan kedua adalah broadcast address pada network tempat host tersebut berada. Address broadcast diperoleh dengan membuat seluruh bit host pada IP Address menjadi 1. Jadi, untuk host dengan IP address 167.205.9.35 atau 167.205.240.2, broadcast addressnya adalah 167.205.255.255 (2segmen terakhir dari IP Address tersebut dibuat berharga 11111111.11111111, sehingga secara desimal terbaca 255.255). Jenis informasi yang dibroadcast biasanya adalah informasi routing.

F. LOOPBACK ADDRESS

Yaitu IP address dengan harga 127.0.0.1. Beberapa aplikasi menggunakan alamat ini untuk keperluan loopbacking process. Secara teori loopback address akan menunjuk dirinya sendiri didalam jaringan yang menggunakan protokol CTP/IP, sehingga paket yang dikirim kealamat ini akan kembali ke dirinya sendiri.

Jika host milik kita ingin bergabung dengan jaringan internet, tentu kita harus memiliki IP address untuk host kita. IP address bersifat unik, yang artinya dalam satu jaringan internet tidak boleh ada dua host yang memiliki IP address yang sama. Dengan demikian kita tidak boleh sembarangan memakai IP address sesuka kita. Biasanya kita mendapatkan IP address dengan jalan membeli dari pihak yang berwenang, misalnya dari sebuah ISP.

Arsitektur TCP/IP memungkinkan kita menggunakan beberapa range IP address untuk kepentingan LAN atau intranet secara cuma-cuma dengan suatu kondisi dan persyaratan

tertentu. IP address ini disebut dengan Privat IP address yang daftarnya dapat dilihat pada tabel dibawah:

Table 10. Network Class

Address Range	Network Class
10.0.0.0 -10.255.255.255	Class A
172.16.0.0-172.31.255.255.255	Class B
192.168.0.0-192.168.255.255	Class C

G. SUBNETTING

Subnetting berfungsi untuk menyembunyikan detail dari internal network suatu organisasi ke router eksternal. Selain itu, subnetting juga mempermudah manajemen jaringan dan menambah efisiensi dari jaringan tersebut. Dengan subnetting kita dapat membatasi jumlah maksimal host yang dapat dialokasikan pada suatu subnet. Dengan subnetting kita dapat memeriksa kesalahan jaringan dengan cepat karena kesalahan tersebut sudah terlokalisasi.

Bayangkan jika organisasi yang memiliki 1000 komputer tidak melakukan subnetting, jika terjadi satu kesalahan, maka semua network akan down. Demikian pula administrator yang harus memperbaiki kesalahan tersebut harus mencari kesalahan satu per satu dalam 1000 komputer tersebut.

Network tanpa subnetting juga akan memperberat tugas router karena routing table-nya yang sangat banyak dan harus membroadcast host sekian banyak tersebut. IP Address v4 memiliki struktur alamat yang tersusun atas bilangan 32 bit. Subnet mask adalah suatu bilangan biner 32 bit yang akan di-AND-kan dengan IP Address untuk mendapatkan subnet host.

Misalnya alamat IP Address 10.126.11.16 dan 10.126.11.17 dengan netmask 255.255.255.0. Untuk mendapatkan lokasi subnet host ini, IP Address 10.126.11.16 akan di-AND dengan netmask-nya. Jika IP Address 10.126.11.17 di-AND dengan netmasknya menghasilkan hasil yang sama dengan hasil AND dari 10.126.11.16 dengan netmasknya, maka 2 IP Address tersebut berada dalam satu subnet . IP Address dengan alamat 10.126.11.x dengan netmask 255.255.255.0 (24 bit) akan memiliki Net Address 10.126.11.0 dan Broadcast Address 10.126.11.255. Alamat IP diantara 10.126.11.0 dan 10.126.11.255 adalah alamat IP yang dapat dialokasikan dalam subnet tersebut.

Contoh :

Sebuah Perusahaan PT.XYZ mempunyai 5 departement, dimana setiap department mempunyai 30 komputer, dengan menggunakan subnetting , berapa subnet yang dapat tercipta, dan berapa subnet mask yang digunakan !

Jawab :

department = 30 komputer, alamat kelas yang mendekati adalah kelas C ,dan kita akan menggunakan IP Private yaitu 192.168.0.0 -192.168.255.255 . Yang dipilih misalkan adalah 192.168.1.1 IP Address : 192.168.1.1 Subnet Mask : 255.255.255.0 (Default Subnet Mask)

Dengan default subnet mask 255.255.255.0 berarti jumlah computer yang dapat terhubung adalah 254, di dapat dari jumlah 0 pada 255.255.255.0 adalah 8 bit , Maka $2^8 = 256 - 2 = 254$, 2 berasal dari network ID dan Broadcast ID 255.255.255.0000000 = jumlah 0 = 28 artinya jumlah host ada 254 Jika hanya 30 komputer, yang mendekati adalah $2^5 = 32$, atau artinya jumlah bit 0 yang diperlukan adaah 5 bit

Maka menjadi 255.255.255.11100000 = 255.255.255.224

Subnet mask yang terbaru adalah IP Address : 192.168.1.1 dan Subent Mask : 255.255.255.224. Setelah didapatkan subnet mask, maka selanjutnya adalah IP Address . IP Address :192.168 .1 .1 Subnet Mask : 255.255.255.224. Telah terjadi penambahan 3 bit pada octet ke empat. Jika dirubah ke decimal, maka IP Address :192.168 .1 .00000000 Subnet Mask : 255.255.255.11100000. perlu diketahui bahwa dalam hal ini menggunakan 2 5 artinya jumlah bit 0 terdapat 5 buah, maka range yang didapat adalah $2^5 = 32$.

Table 11. Range IP Address

IP Address Range	Network ID	Broadcast Address
192.168.1.1 - 192.168.1.30	192.168.1.0	192.168.1.31
192.168.1.33 - 192.168.1.62	192.168.1.32	192.168.1.63
192.168.1.65 - 192.168.1.94	192.168.1.64	192.168.1.95
192.168.1.97 -	192.168.1.96	192.168.1.127

192.168.1.126			
192.168.1.129	-	192.168.1.128	192.168.1.159
192.168.1.158			
192.168.1.161	-	192.168.1.160	192.168.1.191
192.168.1.190			
192.168.1.193	-	192.168.1.192	192.168.1.223
192.168.1.222			
192.168.1.225	-	192.168.1.224	192.168.1.255
192.168.1.254			

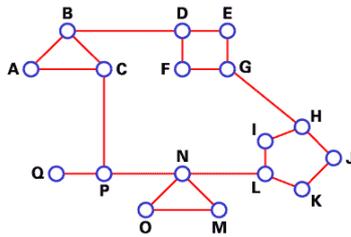
Dalam table diatas terdapat 8 subnet yang dapat digunakan, artinya untuk perusahaan PT.XTZ, dapat memilih dari 8 subnet yang tersedia, karena hanya 5 divisi maka 3 untuk dicadangkan, dan maksimum host dari subnet diatas adalah 30 host, lebih baik dari pada menggunakan 255.255.255.0 yang sampai 254 komputer .

Pertanyaanya:

Jika terdapat IP Address 192.168.1.200, subnet mask : 255.255.255.224, berapa network ID dan broadcast ID Dan apa maksud dari 192.168.1.200/27 !

Kasus lain:

- Terdapat 5 divisi, 1 divisi = 25 komputer, menggunakan subnetting dan network yang digunakan 192.168.52.0 berapakah subnetmask yang baru untuk network tersebut.
- Sebutkan beberapa range dari network yang baru



BAB 6 ROUTING

A. KONSEP ROUTING

Routing IP adalah subjek yang penting untuk dimengerti, karena ia menyangkut semua router dan konfigurasi-konfigurasi yang menggunakan IP.

Routing IP adalah proses memindahkan paket dari satu network ke network lain menggunakan router-router. Kita harus memahami perbedaan antara routing protocol dan routed protocol.

Sebuah routing protocol digunakan oleh router untuk secara dinamis menemukan semua network di sebuah internetwork, dan memastikan bahwa semua router memiliki routing table yang sama. Pada dasarnya sebuah routing protocol menentukan jalur (path) yang dilalui oleh sebuah paket melalui sebuah internetwork. Contoh dari routing protocol adalah RIP, IGRP, EIGRP, dan OSPF. Setelah semua router mengetahui tentang semua network, sebuah routed protocol dapat digunakan untuk mengirimkan data user (paket) melalui jaringan yang sudah ada. Routed protocol ditugaskan ke sebuah interface dan menentukan metode pengiriman paket. Contoh dari routed protokol adalah IP dan IPX.

B. DASAR-DASAR ROUTING

Setelah kita menciptakan sebuah internetwork dengan mengkoneksikan WAN dan LAN ke sebuah router, kita akan perlu untuk mengkonfigurasi alamat network logikal, seperti alamat IP, untuk semua host pada internetwork sehingga mereka dapat berkomunikasi melalui internetwork tersebut.

Istilah routing digunakan untuk proses pengambilan sebuah paket dari sebuah alat dan mengirimkannya melalui network ke alat lain di sebuah network yang berbeda. Router tidak peduli atau tidak memperhatikan tentang host, router hanya memperhatikan tentang network dan jalur terbaik ke setiap network. Alamat network logikal dari host tujuan digunakan untuk menyampaikan paket ke sebuah network melalui sebuah network yang routed (network yang terhubung ke satu atau beberapa network melalui satu atau beberapa route), kemudian alamat

hardware dari host digunakan untuk mengirimkan paket dari router ke host tujuan yang benar. Jika network kita tidak memiliki router, maka jelas kita tidak melakukan routing. Router melakukan routing lalu lintas data ke semua network di internetwork. Agar kita bisa melakukan routing paket, sebuah router harus mengetahui paling sedikit hal-hal berikut :

- Alamat tujuan
- Router-router tetangga (neighbor routers) dari mana sebuah router bisa mempelajari tentang network remote.
- Route yang mungkin ke semua network remote
- Route terbaik untuk setiap network remote.

C. MEMVERIFIKASI INFORMASI ROUTING

Router mempelajari tentang network-network remote dari router-router tetangga atau dari seorang administrator. Router kemudian akan membuat sebuah routing table yang menggambarkan bagaimana menemukan network-network remote. Jika sebuah network terhubung secara langsung maka router sudah tahu bagaimana menghubungi network itu. Jika sebuah network tidak terhubung secara langsung router harus mempelajari bagaimana cara mencapai network remote tersebut dengan dua cara menggunakan routing statis, yang berarti seseorang harus mengetikkan dengan tangan tentang semua lokasi network ke routing table atau melalui apa yang disebut routing dinamis.

Pada routing dinamis sebuah protokol pada satu router berkomunikasi dengan protokol yang sama yang bekerja di router tetangga. Router kemudian akan saling melakukan update tentang semua network yang mereka ketahui dan menempatkan informasi tersebut ke routing table. Jika suatu perubahan terjadi di network, maka protokol routing dinamis secara otomatis akan memberitahukan semua router tentang apa yang terjadi. Jika routing statis digunakan, maka seorang administrator bertanggung jawab untuk melakukan update semua perubahan tersebut, secara manual ke semua router. Biasanya, pada sebuah network yang besar digunakan sebuah kombinasi dari routing dinamis dan routing statis.

Table 12. Router dan Switch

Features	Router	Switch
Speed	Slower	Faster
OSI Layer	Layer 3	Layer 2
Addressing used	IP	MAC
Broadcasts	Blocks	Forwards
Security	Higher	Lower

D.ROUTING STATIS

Routing statis terjadi jika kita secara manual menambah route-route di routing table dari setiap router. Terdapat pro dan kontra terhadap routing statis, tetapi itu juga berlaku untuk semua proses routing Routing statis memiliki keuntungan-keuntungan berikut :

- Tidak ada overhead (waktu pemrosesan) pada CPU router, yang berarti kita mungkin dapat membeli router yang lebih murah daripada jika kita menggunakan routing dinamis.
- Tidak ada bandwidth yang digunakan di antara router, yang berarti kita mungkin dapat menghemat uang untuk link WAN
- Routing statis menambah keamanan, karena administrator dapat memilih untuk mengizinkan akses routing ke network tertentu saja.

Routing statis memiliki kerugian-kerugian berikut :

- Administrator harus benar-benar memahami internetworking dan bagaimana setiap router dihubungkan untuk dapat mengkonfigurasi router dengan benar.
- Jika sebuah network ditambahkan ke internetwork, administrator harus menambahkan sebuah route ke semua router secara manual.
- Routing statis tidak sesuai untuk network-network yang besar karena
- menjaganya akan menjadi sebuah pekerjaan full-time sendiri.

Berikut ini adalah syntax perintah yang kita gunakan untuk menambah sebuah route statis ke sebuah routing table :

```
Ip route [destination_network] [mask] [next-hop_address or exit interface]  
[administrative_distance] [permanent]
```

Daftar ini menggambarkan setiap perintah dalam string:

- Ip route Perintah ini digunakan untuk menciptakan routing statis.
- Destination_address Network yang kita tempatkan di routing table.
- Mask Subnet mask yang digunakan di network.
- Next-hop_address Alamat dari router di hop berikutnya (next-hop) yang akan menerima paket dan meneruskannya ke network remote.
- Alamat next-hop address adalah sebuah interface router yang berada disebuah network yang terhubung secara langsung. Kita harus mampu melakukan ping ke interface

router ini sebelum kita menambahkan route. Jika kita mengetikkan alamat di hop berikutnya yang salah, atau interface ke router sedang mati, route statis akan muncul di konfigurasi router, tetapi tidak di routing table.

- Exit interface Kita dapat menggunakan ini untuk menggantikan nexthop_address jika kita menginginkannya, tetapi ini hanya dapat diterapkan di sebuah link point-to-point, seperti sebuah WAN. Perintah ini tidak akan bekerja pada sebuah LAN seperti Ethernet.
- Administrative_distance Secara default, route statis memiliki sebuah administrative distance (jarak administrasi) 1 (atau bahkan 0 jika kita menggunakan sebuah exit interface dibandingkan sebuah alamat next-hop). Kita dapat mengubah nilai default dengan menambahkan apa yang disebut administrative weight (bobot administrasi) pada akhir dari perintah ini.
- Permanent jika interface dimatikan (shut down), atau router tidak dapat berkomunikasi ke router hop berikutnya, secara otomatis route akan dibuang dari routing table. Pilihan permanent akan membuat entri route ini tetap ada di routing table meski apa pun yang terjadi.

E. ROUTING DEFAULT

Kita menggunakan routing default untuk mengirimkan paket-paket ke sebuah network tujuan yang remote yang tidak ada di routing table, ke router hop berikutnya. Kita hanya dapat menggunakan routing default pada networknetwork stub yaitu network yang hanya memiliki satu jalur keluar (exit path) dari network itu.

Untuk mengkonfigurasi sebuah route default, kita menggunakan wildcard di alamat network dan lokasi mask dari sebuah route statis. Bahkan sebenarnya, kita dapat menganggap sebuah route default sebagai route statis yang menggunakan wildcard daripada informasi network dan mask.

Berikut ini adalah syntax perintah yang kita gunakan untuk menambah sebuah route default ke sebuah routing table :

```
Ip route 0.0.0.0 0.0.0.0 [next-hop_address]
```

F. ROUTING DINAMIS

Routing dinamis adalah ketika routing protokol digunakan untuk menemukan network dan melakukan update routing table pada router. Ini lebih mudah daripada menggunakan routing statis dan default, tapi ia akan membebani dalam hal proses-proses di CPU router dan pengguna bandwidth dari link jaringan. Sebuah routing protokol mendefinisikan kumpulan peraturan yang digunakan oleh router ketika router berkomunikasi tentang informasi routing dengan router-router yang bertetangga.

Terdapat dua jenis routing protokol yang digunakan di internetwork: internet gateway protocol (IGP) dan exterior gateway protocol (EGP). IGP digunakan untuk melakukan pertukaran informasi routing dengan router-router yang berada di autonomous system (AS) yang sama. Sebuah AS adalah sekumpulan network yang berada dibawah sebuah domain administrasi yang sama, yang pada dasarnya berarti semua router yang berbagi informasi routing table yang sama adalah berada di AS yang sama. Sedangkan EGP digunakan untuk berkomunikasi antar-AS.

Sebuah contoh EGP adalah Border Gateway Protocol (BGP) Administrative Distance (disingkat AD) digunakan untuk mengukur apa yang disebut trustworthiness (ke-dapat-dipercaya-an) dari informasi routing yang diterima oleh sebuah router dari router tetangga. Sebuah administrative distance adalah sebuah bilangan bulat dari 0 sampai 255, dimana 0 adalah yang paling dapat dipercaya dan 255 berarti tidak akan lalu lintas data yang akan melalui route ini.

Jika sebuah router menerima dua update mengenai network yang sama, maka hal pertama yang dicek oleh router adalah AD. Jika satu dari route yang di-advertised (diumumkan oleh router lain) memiliki AD yang lebih rendah dari yang lain, maka route dengan AD terendah tersebut akan ditempatkan di routing table.

Jika kedua route yang di-advertised memiliki AD yang sama, maka yang disebut metrics dari routing protokol (misalnya jumlah hop atau bandwidth dari sambungan) akan digunakan untuk menemukan jalur terbaik ke network remote. Router yang diadvertised dengan metrics terendah akan ditempatkan di routing table. Tetapi jika kedua route memiliki AD dan metric yang sama, maka routing protokol akan melakukan load-balance (pengimbangan beban) ke network remote (yang berarti router akan mengirimkan paket melalui kedua link yang memiliki AD dan metric yang sama tersebut).

Jika sebuah network terhubung secara langsung, router akan selalu menggunakan interface yang terhubung ke network itu. Jika seorang administrator mengkonfigurasi

sebuah route statis, router akan lebih mempercayai route statis tersebut dibandingkan route dinamis yang dipelajari dari router lain. Kita dapat mengubah administrative distance dari route statis tetapi secara default mereka memiliki AD 1.

Jika anda memiliki sebuah route statis, route yang diumumkan oleh RIP (RIP-advertised route), dan sebuah route yang diumumkan oleh IGRP (IGRPadvertised route), maka secara default router akan selalu menggunakan route statis kecuali jika kita mengubah AD dari route statis tersebut.

Terdapat tiga class routing protokol :

1. Distance Vector Protokol, distance-vector menemukan jalur terbaik ke sebuah network remote dengan menilai jarak. Setiap kali sebuah paket melalui sebuah router disebut sebagai sebuah hop. Route dengan hop yang paling sedikit ke network yang dituju akan menjadi route terbaik. Vektor menunjukkan arah (direction) ke network remote. Baik RIP dan IGRP adalah routing protokol jenis distance-vector. RIP dan IGRP mengirimkan semua routing table ke router-router tetangga yang terhubung secara langsung.
2. Link state Pada protokol link-state atau yang juga disebut protokol shortestpath-first setiap router akan menciptakan tiga buah tabel terpisah. Satu dari tabel ini mencatat perubahan dari network-network yang terhubung secara langsung. Satu tabel lain menentukan topologi dari keseluruhan internetwork, dan tabel yang terakhir digunakan sebagai routing table. Router yang link-state mengetahui lebih banyak tentang internetwork dibandingkan semua jenis routing protokol yang distance-vector. OSPF adalah sebuah routing protokol IP yang sepenuhnya link-state. Protokol link-state mengirimkan update-update yang berisi status dari link mereka sendiri ke semua router lain di network.
3. Hybrid Protokol hybrid menggunakan aspek-aspek dari routing protokol jenis distance-vector dan routing protokol jenis link-state. Sebagai contoh adalah EIGRP. Tidak ada cara tunggal untuk mengkonfigurasi routing protokol untuk digunakan di semua bisnis atau pekerjaan. Mengkonfigurasi routing protokol adalah hal yang harus kita lakukan secara kasus-per-kasus. Jika kita mengerti bagaimana cara kerja

routing protokol yang berbeda, kita dapat membuat keputusan yang baik, kuat, dan yang benar-benar memenuhi kebutuhan semua orang di semua jenis bidang usaha.

G. RIP (ROUTING INFORMATION PROTOCOL)

RIP merupakan salah satu protokol routing distance vector yang digunakan oleh ribuan jaringan di dunia. Fakta membuktikan bahwa RIP berdasarkan open standard dan mudah diimplementasikan. Akan tetapi RIP membutuhkan konsumsi daya yang tinggi dan membutuhkan fitur router routing protokol.

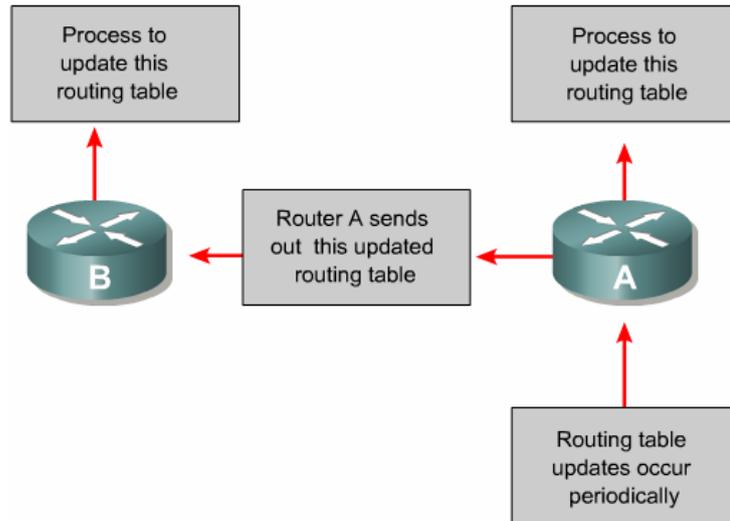
IGRP yang merupakan contoh routing protokol yang menggunakan algoritma distance vector yang lain. Tidak seperti RIP, IGRP merupakan routing protokol yang dibuat oleh Cisco. IGRP juga sangat mudah diimplementasikan, meskipun IGRP merupakan routing potokol yang lebih kompleks dari RIP dan banyak factor yang dapat digunakan untuk mencapai jalur terbaik.

Pada modul ini diharapkan Anda dapat:

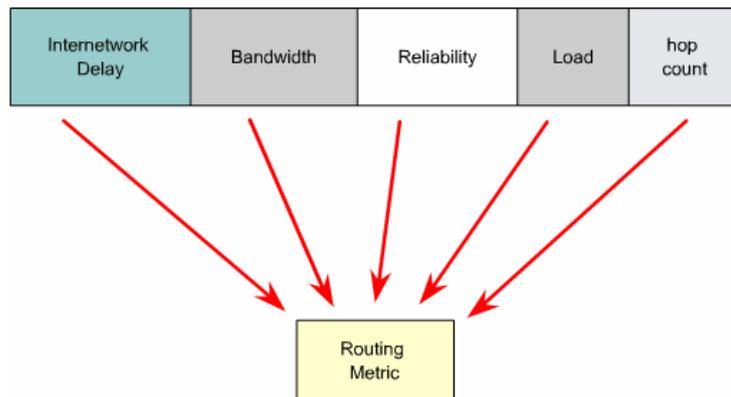
- ☞ Menggambarkan bagaimana routing loop terjadi dalam routing distance vector
- ☞ Menggambarkan beberapa metode yang digunakan oleh distance vector untuk meyakinkan bahwa informasi routing akurat atau tidak
- ☞ Mengkonfigurasi RIP
- ☞ Menggunakan perintah ip classless
- ☞ Troubleshooting RIP
- ☞ Mengkonfigurasi routing statis untuk RIP
- ☞ Memverifikasi RIP

1. Routing update distance vector

Routing update terjadi secara periodik atau ketika topologi jaringan mengalami perubahan. Adalah hal yang sangat penting untuk routing protokol untuk meng-update table routing. Algoritma distance vector dijalankan di setiap router untuk mengirimkan informasi isi table routingnya ke router-router tetangganya. Table routing tersebut juga berisi informasi mengenai total cost jalur. Total cost jalur ditentukan oleh metric dan alamat logic dari router pertama pada jalur tiap-tiap jaringan dalam table routing.



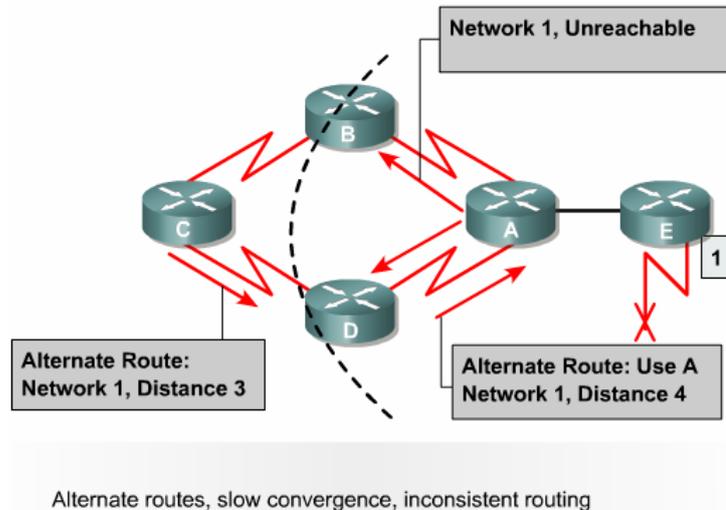
Gambar 41. Perubahan topologi distance vector



Gambar 42. perubahan topologi distance vector

2. Distance vector routing loop

Routing loop dapat terjadi pada saat ketidak konsistenan table routing. Contoh berikut ini menggambarkan kejadian tersebut:



Gambar 43. routing loop

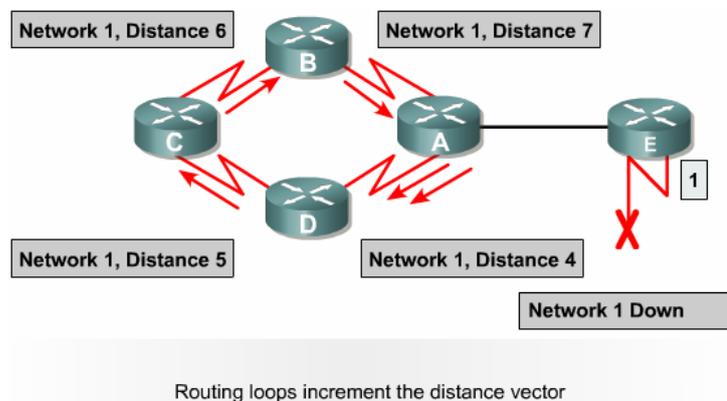
- Sebelum jaringan 1 putus, semua router memiliki table routing yang benar. Dalam hal ini jaringan dikatakan konvergen. Untuk router C, menuju ke jaringan 1 melalui router B dan jarak dari router C ke jaringan 1 adalah 3.
- Ketika jaringan 1 putus, router E mengirimkan update ke router A. router A menghentikan routing paket ke jaringan 1, tapi router B, C dan D tetap meneruskan routing karena mereka tidak diberi informasi bahwa jaringan 1 putus. Ketika router A mengirimkan update, router B dan D menghentikan routing ke jaringan 1. Router C masih belum menerima update. Untuk router C, jaringan 1 masih dapat dicapai melalui router B.
- Sekarang router C mengirimkan update secara periodic ke router D, yang menunjukkan jalur ke jaringan 1 lewat router B. Router D mengubah isi table routingnya dan mengirimkan informasi ke router A. Router A mengirimkan informasi ke router B dan E dan proses berlangsung terus. Paket-paket yang ditujukan ke jaringan 1 sekarang akan mengalami loop dari router C ke B ke A ke D dan kembali lagi ke C.

3. Pendefinisian maximum count

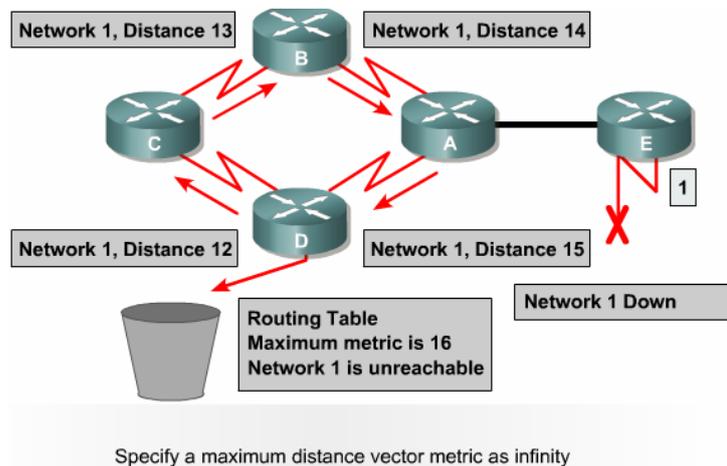
Update invalid jaringan 1 akan meneruskan loop sampai beberapa proses lain berhenti looping. Kondisi ini disebut dengan count to infinity, paket-paket looping terjadi dalam jaringan. Tanpa memberikan counter untuk menghentikan proses, hop count dari distance vector akan meningkatkan waktu paket melalui jaringan. Hal ini akan menyebabkan informasi yang tidak benar dalam table routing sehingga routing loop terjadi.

Algoritma distance vector memiliki kemampuan untuk self-correcting, tapi masalah routing loop dapat menyebabkan count to infinity. Untuk mencegah masalah ini, protokol distance vector mendefinisikan infinity ini sebagai maximum number. Nomor ini menunjukkan metric, dimana batas hop count maksimumnya.

Dengan metode seperti ini, routing protokol mengizinkan routing loop terus sampai metric mencapai batas maksimum. Nilai maksimum batas hop count pada distance vector defaultnya adalah 15 sehingga paket akan dibuang kalau hop count lebih dari 15 dan dianggap jaringan unreachable.



Gambar 44. masalah: counting to infinity



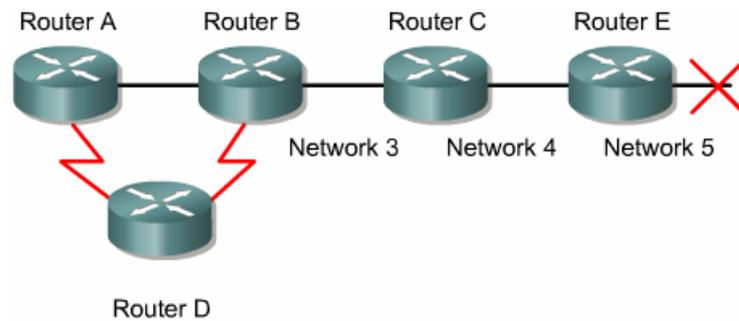
Gambar 45. solusi: mendefinisikan nilai maksimum

4. Eliminasi routing loop

a. Metode Split Horizon

Beberapa routing loop terjadi ketika terdapat informasi salah yang dikirim kembali ke router. Seperti yang digambarkan oleh contoh berikut:

route poison dari router E, ia mengirimkan update yang disebut dengan poison reverse, kembali ke router E. Hal ini akan menyebabkan semua router dalam segmen menerima informasi route poison.



When Network 5 goes down, Router E initiates route poisoning by entering a table entry metric of 16, which is unreachable.

Gambar 47. route poisoning

Ketika route poisoning digunakan dengan triggered update, ia akan menyebabkan waktu konvergen cepat karena router-router tetangga tidak harus menunggu waktu 30 detik sebelum mereka advertise route poison.

Route poisoning menyebabkan routing protokol advertise infinite-metric untuk jalur yang putus. Route poisoning tidak merusak konsep split horizon. Split horizon dengan poison reverse merupakan route poisoning yang ditempatkan pada link-link dimana split horizon secara tidak normal menerima informasi routing.

c. Metode Triggered update

Tabel routing baru dikirim ke router-router tetangga. Contoh, RIP update terjadi setiap 30 detik. Bagaimanapun, triggered update dikirim secara langsung atas respon terjadinya perubahan table routing. Router yang mengetahui telah terjadi perubahan topologi jaringan secara langsung mengirimkan pesan update ke router-router terdekatnya. Kemudian router-router ini membangkitkan triggered update untuk router-router tetangganya yang lain. Pada saat terjadi jalur putus, update secara langsung dikirim. Triggered update, digunakan sebagai hubungan dengan route poisoning untuk meyakinkan bahwa semua router tahu tentang router-router yang putus sebelum holddown timer habis waktunya.

H. OSPF (OPEN SHORTEST PATH FIRST)

OSPF ini merupakan protocol link-state. Teknologi link-state dikembangkan dalam ARPAnet untuk menghasilkan protokol yang terdistribusi yang jauh lebih baik daripada protokol distance-vector. Alih-alih saling bertukar jarak (distance) ke tujuan, setiap router dalam jaringan memiliki peta jaringan yang dapat diperbarui dengan cepat setelah setiap perubahan topologi. Peta ini digunakan untuk menghitung route yang lebih akurat daripada menggunakan protokol distance-vector. Perkembangan teknologi ini akhirnya menghasilkan protokol Open Shortest Path First (OSPF) yang dikembangkan oleh IETF untuk digunakan di Internet. Bahkan sekarang Internet Architecture Board (IAB) telah merekomendasikan OSPF sebagai pengganti RIP.

Prinsip link-state routing sangat sederhana. Sebagai pengganti menghitung route “terbaik” dengan cara terdistribusi, semua router mempunyai peta jaringan dan menghitung semua route yang terbaik dari peta ini. Peta jaringan tersebut disimpan dalam sebuah basis data dan setiap record dalam basis data tersebut menyatakan sebuah link dalam jaringan. Record-record tersebut dikirimkan oleh router yang terhubung langsung dengan masing-masing link. Karena setiap router perlu memiliki peta jaringan yang menggambarkan kondisi terakhir topologi jaringan yang lengkap, setiap perubahan dalam jaringan harus diikuti oleh perubahan dalam basis data link-state yang terletak di setiap router.

Perubahan status link yang dideteksi router akan mengubah basis data link-state router tersebut, kemudian router mengirimkan perubahan tersebut ke router-router lain. Protokol yang digunakan untuk mengirimkan perubahan ini harus cepat dan dapat diandalkan. Ini dapat dicapai oleh protokol flooding. Dalam protokol flooding, pesan yang dikirim adalah perubahan dari basis data serta nomor urut pesan tersebut. Dengan hanya mengirimkan perubahan basis data, waktu yang diperlukan untuk pengiriman dan pemrosesan pesan tersebut lebih sedikit dibandingkan mengirim seluruh isi basis data tersebut. Nomor urut pesan diperlukan untuk mengetahui apakah pesan yang diterima lebih baru daripada yang terdapat dalam basis data. Nomor urut ini berguna pada kasus link yang putus menjadi tersambung kembali.

Pada saat terdapat link putus dan jaringan menjadi terpisah, basis data kedua bagian jaringan tersebut menjadi berbeda. Ketika link yang putus tersebut hidup kembali, basis data di semua router harus disamakan. Basis data ini tidak akan kembali sama dengan

mengirimkan satu pesan link-state saja. Proses penyamaan basis data pada router yang bertetangga disebut sebagai menghidupkan adjacency.

Dua buah router bertetangga disebut sebagai adjacent bila basis data link-state keduanya telah sama. Dalam proses ini kedua router tersebut tidak saling bertukar basis data karena akan membutuhkan waktu yang lama. Proses menghidupkan adjacency terdiri dari dua fasa. Fasa pertama, kedua router saling bertukar deskripsi basis data yang merupakan ringkasan dari basis data yang dimiliki setiap router. Setiap router kemudian membandingkan deskripsi basis data yang diterima dengan basis data yang dimilikinya. Pada fasa kedua, setiap router meminta tetangganya untuk mengirimkan record-record basis data yang berbeda, yaitu bila router tidak memiliki record tersebut, atau nomor urut record yang dimiliki lebih kecil daripada yang dikirimkan oleh deskripsi basis data.

Setelah proses ini, router memperbarui beberapa record dan ini kemudian dikirimkan ke router-router lain melalui protokol flooding. Protokol link-state lebih baik daripada protokol distance-vector disebabkan oleh beberapa hal: waktu yang diperlukan untuk konvergen lebih cepat, dan lebih penting lagi protokol ini tidak menghasilkan routing loop. Protokol ini mendukung penggunaan beberapa metrik sekaligus. Throughput, delay, biaya, dan keandalan adalah metrik-metrik yang umum digunakan dalam jaringan. Di samping itu protokol ini juga dapat menghasilkan banyak jalur ke sebuah tujuan. Misalkan router A memiliki dua buah jalur dengan metrik yang sama ke host B. Protokol dapat memasukkan kedua jalur tersebut ke dalam forwarding table sehingga router mampu membagi beban di antara kedua jalur tersebut.

Rancangan OSPF menggunakan protokol link-state dengan beberapa penambahan fungsi. Fungsi-fungsi yang ditambahkan antara lain mendukung jaringan multiakses, seperti X.25 dan Ethernet, dan membagi jaringan yang besar mejadi beberapa area.

Telah dijelaskan di atas bahwa setiap router dalam protokol link-state perlu membentuk adjacency dengan router tetangganya. Pada jaringan multi-akses, tetangga setiap router dapat lebih dari satu. Dalam situasi seperti ini, setiap router dalam jaringan perlu membentuk adjacency dengan semua router yang lain, dan ini tidak efisien. OSPF mengefisienkan adjacency ini dengan memperkenalkan konsep designated router dan designated router cadangan. Semua router hanya perlu adjacent dengan designated router tersebut, sehingga hanya designated router yang adjacent dengan semua router yang lain.

Designated router cadangan akan mengambil alih fungsi designated router yang gagal berfungsi.

Langkah pertama dalam jaringan multi-akses adalah memilih designated router dan cadangannya. Pemilihan ini dimasukkan ke dalam protokol Hello, protocol dalam OSPF untuk mengetahui tetangga-tetangga router dalam setiap link. Setelah pemilihan, baru kemudian router-router membentuk adjacency dengan designated router dan cadangannya. Setiap terjadi perubahan jaringan, router mengirimkan pesan menggunakan protokol flooding ke designated router, dan designated router yang mengirimkan pesan tersebut ke router-router lain dalam link. Designated router cadangan juga mendengarkan pesan-pesan yang dikirim ke designated router. Jika designated router gagal, cadangannya kemudian menjadi designated router yang baru serta dipilih designated router cadangan yang baru. Karena designated router yang baru telah adjacent dengan router-router lain, tidak perlu dilakukan lagi proses penyamaan basis data yang membutuhkan waktu yang lama tersebut.

Dalam jaringan yang besar tentu dibutuhkan basis data yang besar pula untuk menyimpan topologi jaringan. Ini mengarah kepada kebutuhan memori router yang lebih besar serta waktu perhitungan route yang lebih lama. Untuk mengantisipasi hal ini, OSPF menggunakan konsep area dan backbone. Jaringan dibagi menjadi beberapa area yang terhubung ke backbone. Setiap area dianggap sebagai jaringan tersendiri dan router-router di dalamnya hanya perlu memiliki peta topologi jaringan dalam area tersebut. Router-router yang terletak di perbatasan antar area hanya mengirimkan ringkasan dari link-link yang terdapat dalam area dan tidak mengirimkan topologi area satu ke area lain. Dengan demikian, perhitungan route menjadi lebih sederhana.

I. KESEDERHANAAN VS. KEMAMPUAN

Kita sudah lihat sepintas bagaimana RIP dan OSPF bekerja. Setiap protokol routing memiliki kelebihan dan kekurangannya masing-masing. Protokol RIP sangat sederhana dan mudah diimplementasikan tetapi dapat menimbulkan routing loop.

Protokol OSPF merupakan protokol yang lebih rumit dan lebih baik daripada RIP tetapi membutuhkan memori dan waktu CPU yang besar. Di berbagai tempat juga terdapat yang menggunakan gabungan antara routing statik, RIP, RIP-v2, dan OSPF. Hasilnya di jaringan ini menunjukkan bahwa administrasi routing statik jauh lebih memakan waktu dibanding routing dinamik.

Pengamatan pada protokol routing dinamik juga menunjukkan bahwa RIP menggunakan bandwidth yang lebih besar daripada OSPF dan semakin besar jaringan, bandwidth yang digunakan RIP bertambah lebih besar pula. Jadi, jika Anda sedang mendesain jaringan TCP/IP yang besar tentu OSPF merupakan pilihan protokol routing yang tepat.



BAB 6 MIKROTIK

A. PENGERTIAN MIKROTIK ROUTER OS

MikroTik RouterOS™, merupakan sistem operasi Linux base yang diperuntukkan sebagai network router. Didesain untuk memberikan kemudahan bagi penggunanya. Administrasinya bisa dilakukan melalui Windows Application (WinBox). Selain itu instalasi dapat dilakukan pada Standard komputer PC (Personal Computer). PC yang akan dijadikan router mikrotik pun tidak memerlukan resource yang cukup besar untuk penggunaan standard, misalnya hanya sebagai gateway. Untuk keperluan beban yang besar (network yang kompleks, routing yang rumit) disarankan untuk mempertimbangkan pemilihan resource PC yang memadai.

B. SEJARAH MIKROTIK

MikroTik adalah sebuah perusahaan kecil berkantor pusat di Latvia, bersebelahan dengan Rusia. Pembentukannya diprakarsai oleh John Trully dan Arnis Riekstins. John Trully adalah seorang berkewarganegaraan Amerika yang bermigrasi ke Latvia. Di Latvia ia bejumpa dengan Arnis, Seorang darjana Fisika dan Mekanik sekitar tahun 1995. John dan Arnis mulai me-routing dunia pada tahun 1996 (misi MikroTik adalah merouting seluruh dunia). Mulai dengan sistem Linux dan MS-DOS yang dikombinasikan dengan teknologi Wireless-LAN (WLAN) Aeronet berkecepatan 2 Mbps di Moldova, negara tetangga Latvia, baru kemudian melayani lima pelanggannya di Latvia.

Prinsip dasar mereka bukan membuat Wireless ISP (W-ISP), tetapi membuat program router yang handal dan dapat dijalankan diseluruh dunia. Latvia hanya merupakan tempat eksperimen John dan Arnis, karena saat ini mereka sudah membantu negara-negara lain termasuk Srilanka yang melayani sekitar 400 pengguna.

Linux yang pertama kali digunakan adalah Kernel 2.2 yang dikembangkan secara bersama-sama dengan bantuan 5-15 orang staff Research and Development (R&D) MikroTik

yang sekarang menguasai dunia routing di negara-negara berkembang. Menurut Arnis, selain staf di lingkungan MikroTik, mereka juga merekrut tenaga-tenaga lepas dan pihak ketiga yang dengan intensif mengembangkan MikroTik secara marathon.

C. JENIS JENIS MIKROTIK

Jenis-jenis Mikrotik ada dua, yaitu

1. MikroTik RouterOS yang berbentuk software yang dapat di-download di www.mikrotik.com. Dapat diinstal pada kompuetr rumahan (PC).
2. BUILT-IN Hardware MikroTik dalam bentuk perangkat keras yang khusus dikemas dalam board router yang didalamnya sudah terinstal MikroTik RouterOS.

D. FITUR-FITUR MIKROTIK

Sedangkan Fitur-fitur Mikrotik adalah sebagai berikut :

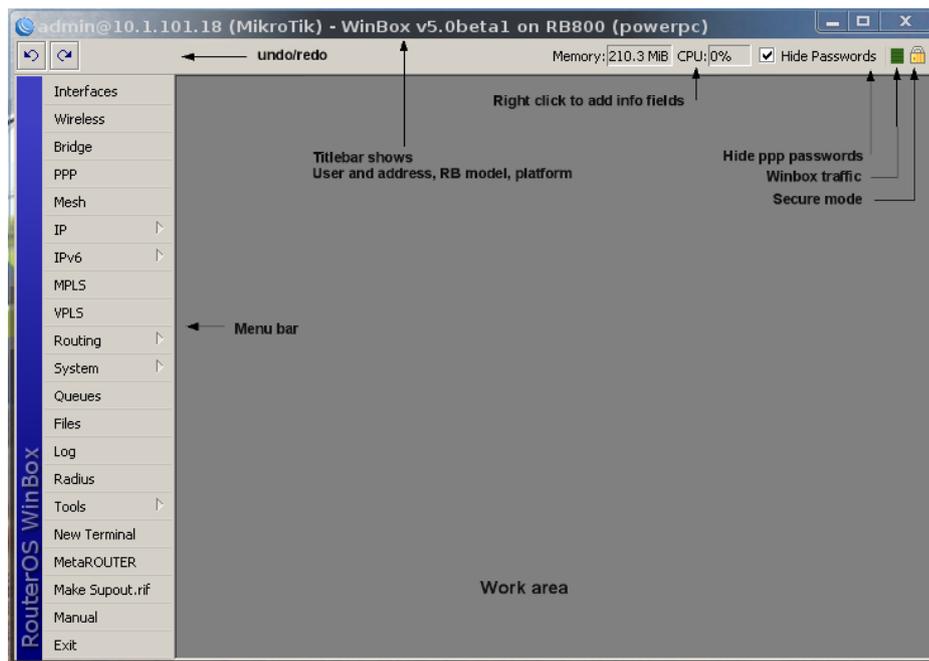
1. Address List : Pengelompokan IP Address berdasarkan nama
2. Asynchronous : Mendukung serial PPP dial-in / dial-out, dengan otentikasi CHAP, PAP, MSCHAPv1 dan MSCHAPv2, Radius, dial on demand, modem pool hingga 128 ports.
3. Bonding : Mendukung dalam pengkombinasian beberapa antarmuka ethernet ke dalam 1 pipa pada koneksi cepat.
4. Bridge : Mendukung fungsi bridge spinning tree, multiple bridge interface, bridging firewalling.
5. Data Rate Management : QoS berbasis HTB dengan penggunaan burst, PCQ, RED, SFQ, FIFO queue, CIR, MIR, limit antar peer to peer
6. DHCP : Mendukung DHCP tiap antarmuka; DHCP Relay; DHCP Client, multiple network DHCP; static and dynamic DHCP leases.
7. Firewall dan NAT : Mendukung pemfilteran koneksi peer to peer, source NAT dan destination NAT. Mampu memfilter berdasarkan MAC, IP address, range port, protokol IP, pemilihan opsi protokol seperti ICMP, TCP Flags dan MSS.
8. Hotspot : Hotspot gateway dengan otentikasi RADIUS. Mendukung limit data rate, SSL ,HTTPS.
9. IPSec : Protokol AH dan ESP untuk IPSec; MODP Diffie-Hellmann groups 1, 2, 5; MD5 dan algoritma SHA1 hashing; algoritma enkripsi menggunakan DES, 3DES,

- AES-128, AES-192, AES-256; Perfect Forwarding Secresy (PFS) MODP groups 1, 2,5
10. ISDN : mendukung ISDN dial-in/dial-out. Dengan otentikasi PAP, CHAP, MSCHAPv1 dan MSCHAPv2, Radius. Mendukung 128K bundle, Cisco HDLC, x751, x75ui, x75bui line protokol.
 11. M3P : MikroTik Protokol Paket Packer untuk wireless links dan ethernet.
 12. MNDP : MikroTik Discovery Neighbour Protokol, juga mendukung Cisco Discovery Protokol (CDP).
 13. Monitoring / Accounting : Laporan Traffic IP, log, statistik graph yang dapat diakses melalui HTTP.
 14. NTP : Network Time Protokol untuk server dan clients; sinkronisasi menggunakan system GPS.
 15. Poin to Point Tunneling Protocol : PPTP, PPPoE dan L2TP Access Concentrator; protokol otentikasi menggunakan PAP, CHAP, MSCHAPv1, MSCHAPv2; otentikasi dan laporan Radius; enkripsi MPPE; kompresi untuk PPOE; limit data rate.
 16. Proxy : Cache untuk FTP dan HTTP proxy server, HTTPS proxy; transparent proxy untuk DNS dan HTTP; mendukung protokol SOCKS; mendukung parent proxy; static DNS.
 17. Routing : Routing statik dan dinamik; RIP v1/v2, OSPF v2, BGP v4.
 18. SDSL : Mendukung Single Line DSL; mode pemutusan jalur koneksi dan jaringan.
 19. Simple Tunnel : Tunnel IP/IP dan EoIP (Ethernet over IP).
 20. SNMP : Simple Network Monitoring Protocol mode akses read-only.
 21. Synchronous : V.35, V.24, E1/T1, X21, DS3 (T3) media ttypes; sync-PPP, Cisco HDLC; Frame Relay line protokol; ANSI-617d (ANDI atau annex D) dan Q933a (CCITT atau annex A); Frame Relay jenis LMI.
 22. Tool : Ping, Traceroute; bandwidth test; ping flood; telnet; SSH; packet sniffer; Dinamik DNS update.
 23. UPnP : Mendukung antarmuka Universal Plug and Play.
 24. VLAN : Mendukung Virtual LAN IEEE 802.1q untuk jaringan ethernet dan wireless; multiple VLAN; VLAN bridging.
 25. VoIP : Mendukung aplikasi voice over IP.
 26. VRRP : Mendukung Virtual Router Redudant Protocol.

27. WinBox : Aplikasi mode GUI untuk meremote dan mengkonfigurasi MikroTik RouterOS.

E. INISIALISASI MIKROTIK

Untuk melakukan inisialisasi/ setting mikrotik dapat menggunakan aplikasi yang telah disediakan oleh mikrotik sebagai interface antara computer dan MikrotikOS yang tertanam baik pada Routerboard maupun PC. Aplikasi ini bernama winbox dapat berjalan pada sisitem operasi windows.



Gambar 48. Tampilan Winbox

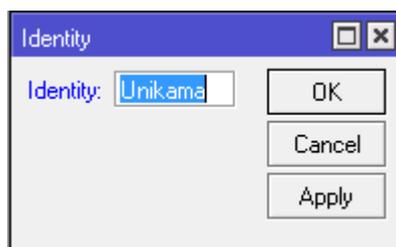
a. *Indetiity/* member nama mikrotik

```
[admin@unikama] > system identity print name: "Mikrotik"
```

```
[admin@unikama] > system identity edit value-name: name
```

masuk ke editor ketik misal saya ganti dengan nama “Unikama”:

Kalo menggunakan winbox, tampilannya seperti ini:



Gambar 49. Memberi nama pada Mikrotik

b. Mengganti nama interface:

```
[admin@unikama] > /interface print
```

Flags: X - disabled, D - dynamic, R - running

#	NAME	TYPE	RX-RATE	TX-RATE	MTU
0	R ether1	ether	0	0	1500
1	R ether2	ether	0	0	1500

```
[admin@unikama] > /interface edit 0
```

value-name: name

Nilai 0 adalah nilai ether1, jika ingin mengganti ether2 nilai 0 diganti dengan 1.

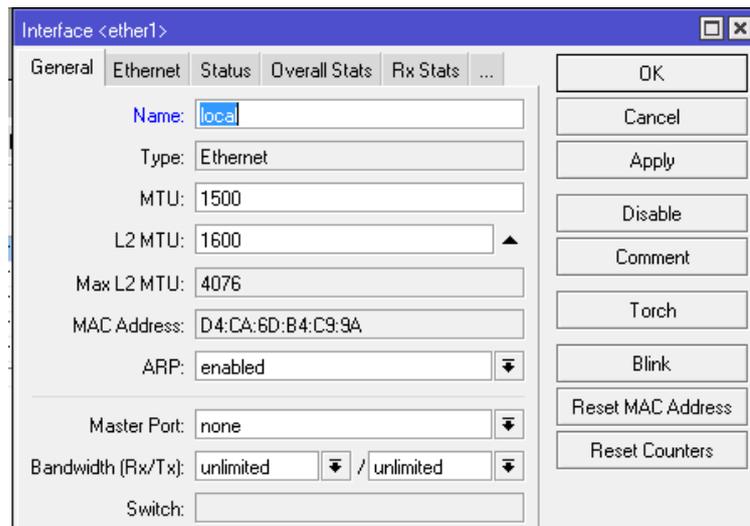
masuk ke editor ketik missal saya ganti dengan nama "local"

C-c quit C-o save&quit C-u undo C-k cut line C-y paste

Edit kemudian tekan Ctrl-o untuk menyimpan dan keluar dari editor

Lakukan hal yang sama untuk interface ether 2, sehingga jika dilihat lagi akan muncul seperti ini:

Via winbox:



Gambar 50. Mengganti nama interface

Pilih menu interface, klik nama interface yg ingin di edit, sehingga muncul jendela edit interface.

c. Seting IP Address :

```
[admin@unikama] > /ip address add
```

address: 192.168.1.1/24

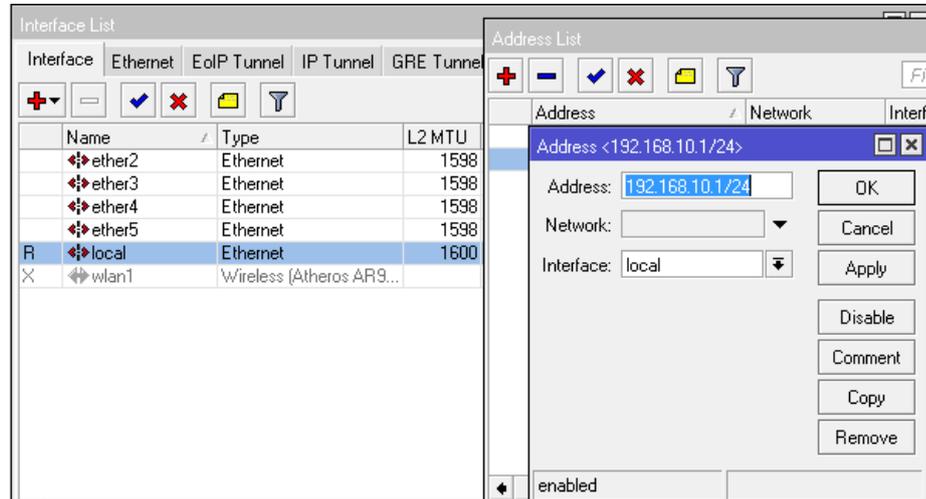
interface: local

```
[admin@unikama] > /ip address print
```

Flags: X - disabled, I - invalid, D - dynamic

```
# ADDRESS NETWORK BROADCAST INTERFACE
0 50.1.1.1/24 192.168.0.0 192.168.0.255 local
```

Via winbox:



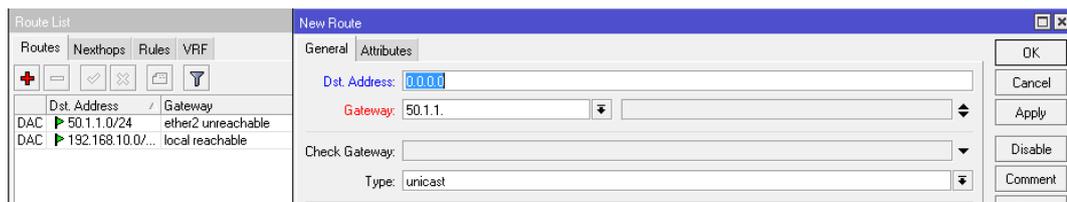
Gambar 51. Setting IP Address

F. MIKROTIK SEBAGAI GATEWAY

Langkah-langkah MikrotikOS sebagai Gateway

1. Memberikan default Gateway, diasumsikan gateway untuk koneksi internet adalah

```
50.1.1.1 [admin@unikama] > /ip route add gateway=50.1.1.1
```



Gambar 52 Setting default route

2. Melihat Tabel routing pada Mikrotik Routers

```
[admin@ unikama] > ip route print Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf
```

```
# DST-ADDRESS PREFSRC G GATEWAY DISTANCE INTERFACE
```

```
0 ADC 50.1.1.0/24 50.1.1.1 ether2
```

```
1 ADC 192.168.10.0/26 192.168.10.1 local
```

```
2 A S 0.0.0.0/0 r 50.1.1.1 ether2
```

3. Tes Ping ke Gateway untuk memastikan konfigurasi sudah benar

```
[admin@unikama] > ping 50.1.1.1
```

```
50.1.1.1 64 byte ping: ttl=64 time<1 ms
```

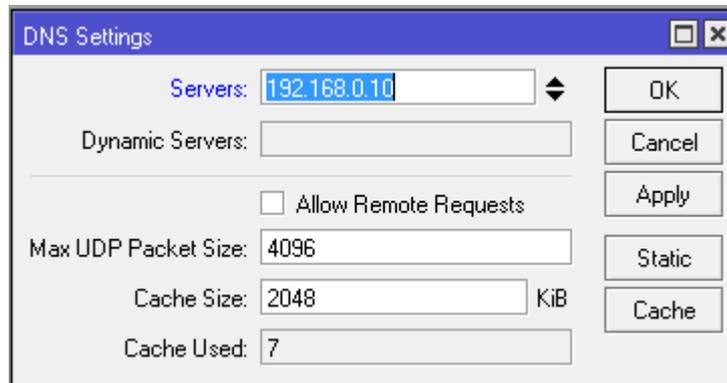
```
50.1.1.1 64 byte ping: ttl=64 time<1 ms
```

```
2 packets transmitted, 2 packets received, 0% packet loss round-trip min/avg/max =  
0/0.0/0 ms
```

4. Setup DNS pada Mikrotik Routers

```
[admin@Unikama] > ip dns set primary-dns=192.168.0.10 allow-remoterequests=no
```

```
[admin@Unikama] > ip dns set secondary-dns=192.168.0.11 allow-  
remoterequests=no
```



Gambar 53. Setting DNS

Untuk melihat Melihat konfigurasi DNS:

```
[admin@Unikama] > ip dns print
```

```
primary-dns: 192.168.0.10
```

```
secondary-dns: 192.168.0.11
```

```
allow-remote-requests: no
```

```
cache-size: 2048KiB
```

```
cache-max-ttl: 1w
```

```
cache-used: 16KiB
```

Tes untuk akses domain, misalnya dengan ping nama domain

```
[admin@Unikama] > ping yahoo.com
```

```
216.109.112.135 64 byte ping: ttl=48 time=250 ms
```

```
10 packets transmitted, 10 packets received, 0% packet loss
```

round-trip min/avg/max = 571/571.0/571 ms

5. Setup Masquerading, Jika Mikrotik akan kita pergunakan sebagai gateway server maka agar client computer pada network dapat terkoneksi ke internet perlu kita masquerading.

```
[admin@Unikama]> ip firewall nat add action=masquerade outinterface=  
ether1 chain:srcnat
```



Gambar 54. Setting SRC-NAT Masquerading

Melihat konfigurasi Masquerading

```
[admin@Unikama]ip firewall nat print  
Flags: X - disabled, I - invalid, D - dynamic  
0 chain=srcnat out-interface=ether1 action=masquerade
```

Setelah langkah ini bisa dilakukan pemeriksaan untuk koneksi dari jaringan local. Dan jika berhasil berarti kita sudah berhasil melakukan instalasi Mikrotik Router sebagai Gateway server.

G. MIKROTIK SEBAGAI DHCP SERVER

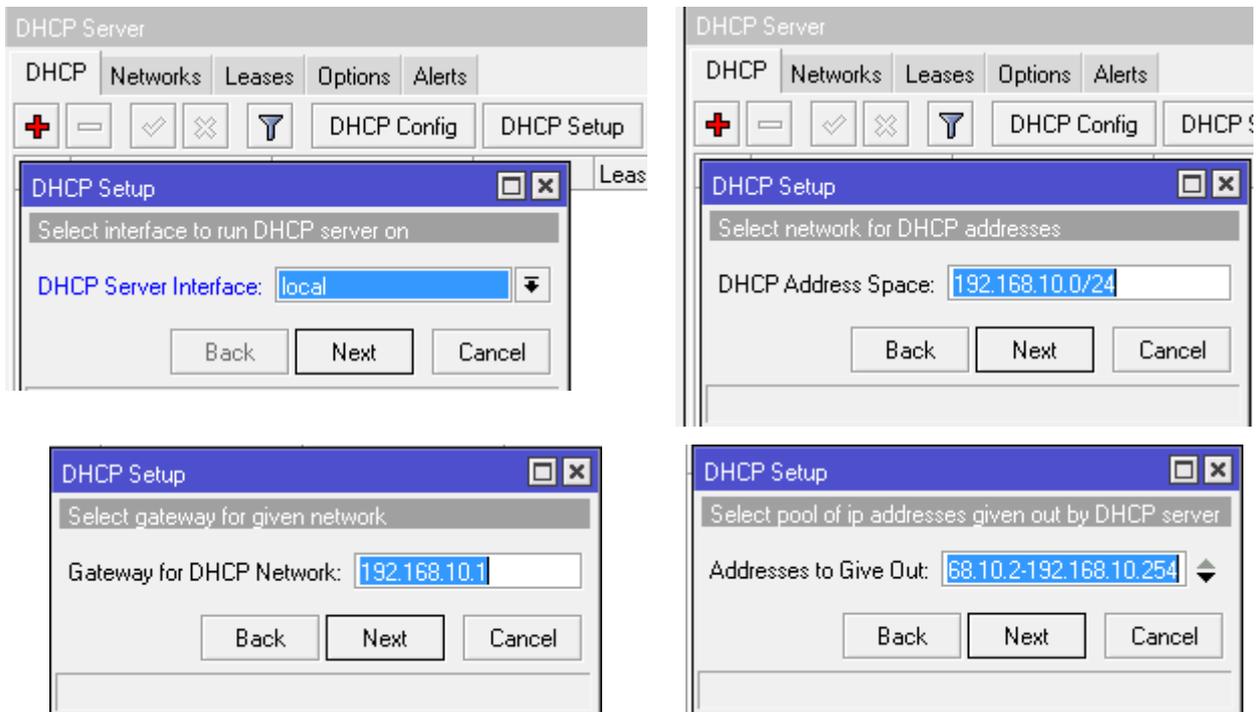
Dynamic Host Configuration Protocol adalah protokol yang berbasis arsitektur client/server yang dipakai untuk memudahkan pengalokasian alamat IP dalam satu jaringan. Sebuah jaringan lokal yang tidak menggunakan DHCP harus memberikan alamat IP kepada semua komputer secara manual. Jika DHCP server dipasang di jaringan lokal, maka semua komputer yang tersambung di jaringan akan mendapatkan alamat IP secara otomatis dari server DHCP. Selain alamat IP, banyak parameter jaringan yang dapat diberikan oleh DHCP, seperti default gateway dan DNS server.

Protokol DHCP terdiri dari dua bagian. Kedua bagian ini adalah:

1. **Server DHCP**, MikroTik yang berperan memberikan otomatis IP address, IP DNS, dan default gateway pada PC client-client kita. Jadi kita tidak perlu pusing pembagian IP pada masing-masing PC, coba anda bayangkan jika PC client anda ada 200 PC yang harus mempunyai IP untuk bisa terhubung dengan mikrotik anda.
2. **Client DHCP**, yang memungkinkan MikroTik untuk dapat berkomunikasi dengan DHCP Server. Agar dapat menerima informasi IP address, IP DNS, dan default gateway dari DHCP Server.

Winbox:

Masuk winbox ke menu IP > DHCP Server > tab DHCP Klik DHCP Setup (kita pakai feature wizard Setting MikroTik Sebagai DHCP Server di Winbox)

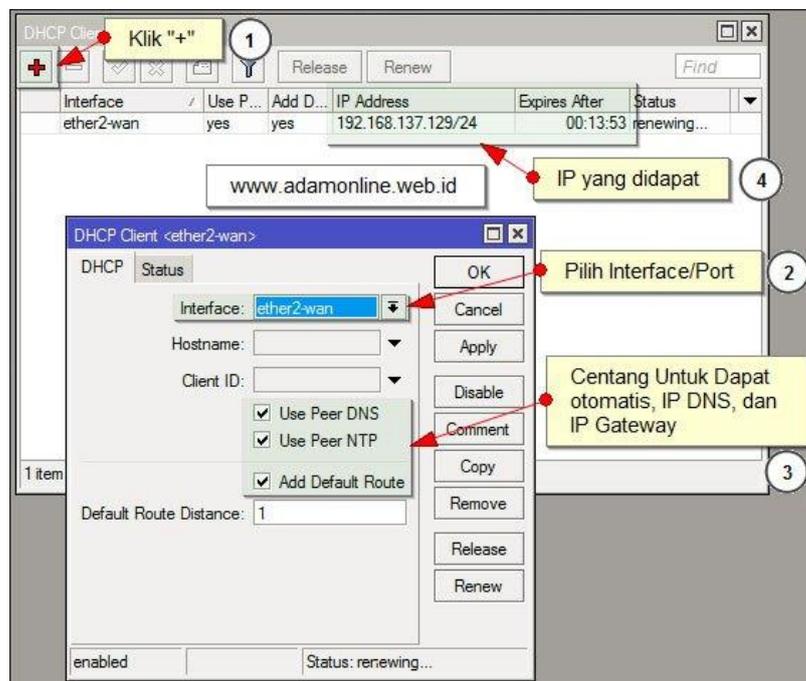


Gambar 55. DHCP Server Setup

Setelah menentukan interfaces mana untuk menjalankan DHCP Server, lalu menentukan IP Network yang akan digunakan, menentukan IP Gateway yang terakhir menentukan IP Address Pool, yang artinya range IP Address yang akan diberikan pada client nantinya.

H. MIKROTIK SEBAGAI DHCP CLIENT

Pada pembahasan ini akan menjadikan MikroTik sebagai DHCP Client, contoh kasus jika ISP/provider internet anda memberikan IP address dynamic (berubah-ubah) atau jika anda menggunakan ISP Telkom Speedy, mikrotik akan menerima IP otomatis dari modem speedy atau menggunakan ISP FastNet agar menerima IP Public dari modem FastNet agar mikrotik dapat terkoneksi dengan internet. Pada Winbox masuk menu IP > DHCP Client Klik icon “+” Pada tab DHCP kolom “Interface:” pilih interface/port atau contoh port yang terhubung dengan modem speedy/fastnet. Centang “Use Peer DNS“, “Use Peer NTP” dan “Add Default Route” dan klik Apply. Pada tab “Status”, terlihat mikrotik anda menerima IP Address, DNS dan default gateway dari server DHCP.



Gambar 56. DHCP Client Setup

I. MIKROTIK SEBAGAI BRIDGING

Bridge adalah suatu cara untuk menghubungkan dua segmen network terpisah bersama-sama dalam suatu protokol sendiri. Paket yang diforward berdasarkan alamat ethernet, bukan IP address (seperti halnya router). Karena forwarding paket dilaksanakan pada Layer 2, maka semua protokol dapat melalui sebuah bridge.

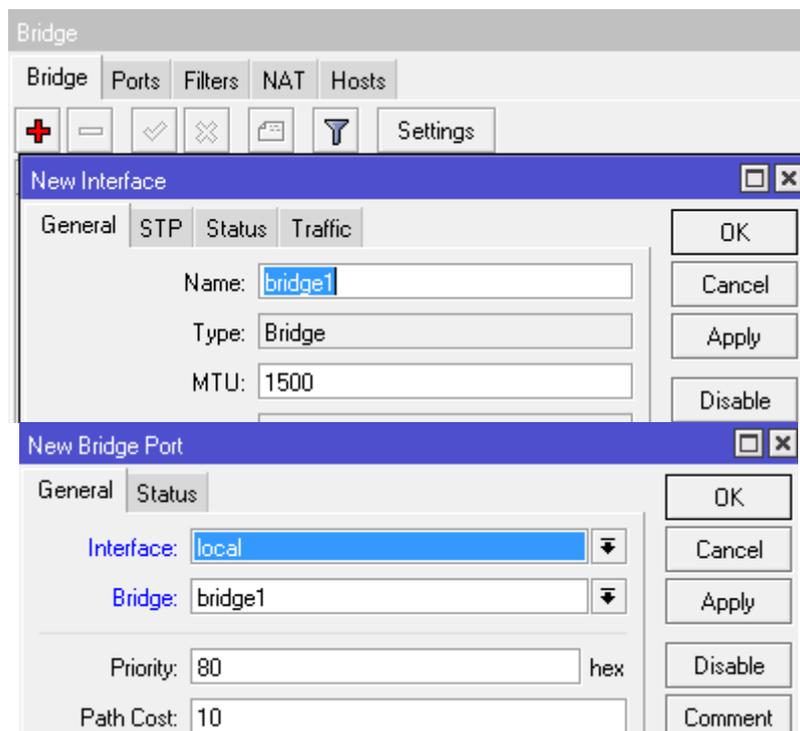
Jadi analoginya seperti ini, anda mempunyai sebuah jaringan local 192.168.0.0/24 gateway ke sebuah modem ADSL yg juga sebagai router dengan ip local 50.1.1.1 dan ip public 222.124.21.26.

Anda ingin membuat proxy server dan mikrotik sebagai BW management untuk seluruh client. Nah mau ditaruh dimanakan PC mikrotik tersebut? Diantara hub/switch dan gateway/modem? Bukankah nanti jadinya dia sebagai NAT dan kita harus menambahkan 1 blok io privat lagi yang berbeda dari gateway modem?

Solusinya mikrotik di set sebagai bridging, jadi seolah2 dia hanya menjembatani antar kabel UTP saja. Topologinya sbb:

Internet-----Modem/router-----Mikrotik-----Switch/Hub-----Client

Setting bridging menggunakan winbox



Gambar 57. Interface Bridging Setup

1. Menambahkan interface bridge

Klik menu Interface kemudian klik tanda + warna merah untuk menambahkan interface, pilih Bridge

memberi nama interface bridge, missal kita beri nama bridge1

2. Menambahkan interface ether local dan public pada interface

Klik menu IP>Bridge>Ports , kemudian klik tanda + untuk menambahkan rule baru:

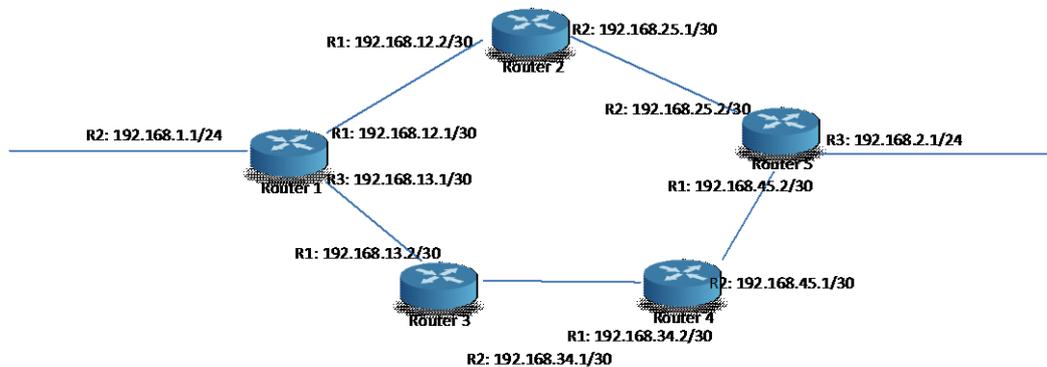
Buat 2 rules, untuk interface local dan public.

3. Memberi IP address untuk interface bridge

Klik menu IP kemudian klik tanda + untuk menambahkan IP suatu interface, missal 192.168.0.100, pilih interface bridge1 (atau nama interface bridge yang kita buat tadi.

Dengan memberikan IP Address pada interface bridge, maka mikrotik dapat di remote baik dari jaringan yg terhubung ke interface local ataupun public.

J. RIP (ROUTING INFORMATION PROTOCOL) PADA MIKROTIK



Gambar 58. Topologi Jaringan RIP

Tahapan Setting RIP pada Mikrotik :

1. Sekarang kita lanjutkan untuk konfigurasi **ROUTING RIP** pada router1 dengan menambahkan interface R1 dengan perintah

Routing rip interface add interface=R1

#	ADDRESS	NETWORK	BROADCAST	INTERFACE
0	192.168.12.1/30	192.168.12.0	192.168.12.3	R1
1	192.168.1.1/24	192.168.1.0	192.168.1.255	R2
2	192.168.13.1/30	192.168.13.0	192.168.13.3	R3

[admin@MikroTik] >

2. Kemudian menambahkan network address R1 dengan perintah

Routing rip address add address=192.168.12.0

```
[admin@MikroTik] > routing rip interface add interface=R1
[admin@MikroTik] > routing rip network add address=192.168.12.0
```

3. Lakukan langkah 10 dan 11 untuk konfigurasi pada router yang lain dengan menambahkan interface dan network address berikut:

a. Router1

Interface = R1, R2, dan R3

Network

- 192.168.12.0 (R1)
- 192.168.1.0 (R2)

- 192.168.13.0 (R3)

b. Router2

Interface = R1 dan R2

Network

- 192.168.12.0 (R1)

- 192.168.25.0 (R2)

c. Router3

Interface = R1 dan R2

Network

- 192.168.13.0 (R1)

- 192.168.34.0 (R2)

d. Router4

Interface = R1 dan R2

Network

- 192.168.34.0 (R1)

- 192.168.45.0 (R2)

e. Router5

Interface = R1, R2, dan R3

Network

- 192.168.45.0 (R1)

- 192.168.25.0 (R2)

192.168.2.0 (R3)

K. OSPF (OPEN SHORTEST PATH FIRST) PADA MIKROTIK

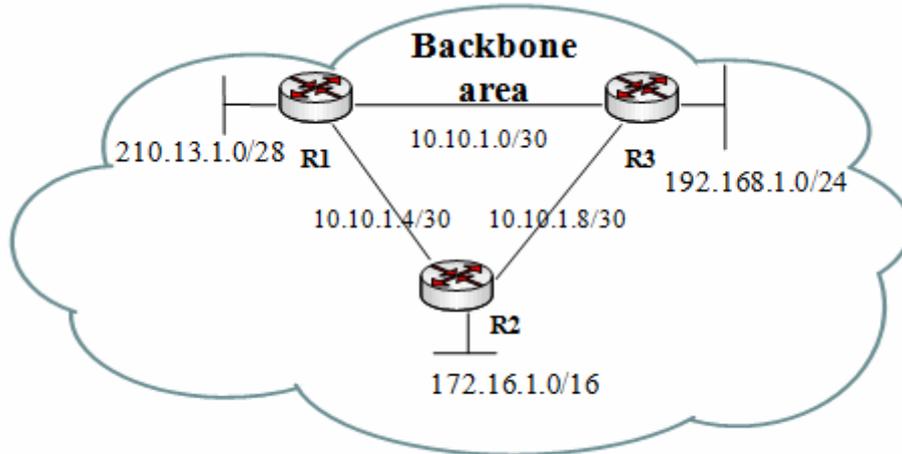


Figure 6.6. Example of single area OSPF network

Gambar 59. Topologi Jaringan OSPF

Tahapan setup OSPF pada Mikrotik, pertama - tama kita set ip address di masing - masing router R1, R2, R3, caranya seperti dibawah ini :

```
[admin@MikroTikR1]/ip address add address=10.10.1.1/30 interface=ether1
[admin@MikroTikR1]/ip address add address=10.10.1.5/30 interface=ether2
[admin@MikroTikR1]/ip address add address=210.13.1.0/28 interface=ether3
[admin@MikroTikR2]/ip address add address=10.10.1.6/30 interface=ether1
[admin@MikroTikR2]/ip address add address=10.10.1.9/30 interface=ether2
[admin@MikroTikR2]/ip address add address=172.16.1.0/16 interface=ether3
[admin@MikroTikR3]/ip address add address=10.10.1.2/30 interface=ether1
[admin@MikroTikR3]/ip address add address=10.10.1.10/30 interface=ether2
[admin@MikroTikR3]/ip address add address=192.168.1.0/24 interface=ether3
```

Menurut konsep ada 3 element yang harus di configure yaitu:

- OSPF instance
- OSPF area dan
- OSPF network

1. Konfigurasi OSPF Instance

```
R1:[admin@MikroTikR1] /routing ospf instance> add name=default
```

```
R2: [admin@MikroTikR2] /routing ospf instance> add name=default
```

```
R3:[admin@MikroTikR3] /routing ospf instance> add name=default
```

2. Show OSPF instance information:

```
[admin@MikroTikR1] /routing ospf instance> print
Flags: X – disabled
0 name="default" router-id=0.0.0.0 distribute-default=never
redistribute-connected=as-type-1 redistribute-static=as-type-1
redistribute-rip=no redistribute-bgp=no redistribute-other-ospf=no
metric-default=1 metric-connected=20 metric-static=20 metric-rip=20
metric-bgp=auto metric-other-ospf=auto in-filter=ospf-in
out-filter=ospf-out
```

3. Buat bridge dengan nama misalnya, “loopback”:

```
[admin@MikroTikR1] /interface bridge> add name=loopback
[admin@MikroTikR1] > ip address add address=10.255.255.1/32 interface=loopback
[admin@MikroTikR1] /routing ospf instance> set 0 router-id=10.255.255.1
```

Ulangi langkah untuk bridge dan loopback diatas untuk R2 dan R3, sesuaikan ip nya dengan router-id R1

4. Konfigurasi OSPF Network

Pada R1 :

```
[admin@MikroTikR1] /routing ospf network> add network=210.13.1.0/28
area=backbone
[admin@MikroTikR1] /routing ospf network> add network=10.10.1.0/30
area=backbone
[admin@MikroTikR1] /routing ospf network> add network=10.10.1.4/30
area=backbone
```

Pada R2:

```
[admin@MikroTikR2] /routing ospf network> add network=172.16.1.0/16
area=backbone
[admin@MikroTikR2] /routing ospf network> add network=10.10.1.0/24
area=backbone
```

Pada R3:

```
[admin@MikroTikR3] /routing ospf network> add network=192.168.1.0/24
area=backbone
[admin@MikroTikR3] /routing ospf network> add network=10.10.1.0/24
area=backbone
```

5. Verifikasi

Terakhir lakukan verifikasi di tiap - tiap router, misalnya di R1 dan jangan lupa ping juga dari tiap - tiap router ke router lainnya

```
[admin@MikroTikR1] /routing ospf interface> print
```

```
[admin@MikroTikR1] /routing ospf neighbor> print
```

```
[admin@MikroTikR1] > ip route print
```

Sedikit penjelasan soal router-id dan loopback, jika loopback dan router id tidak dibuat sebetulnya ga jadi masalah, cumin lebih baik dibuat karena ketika router-id ga dibuat otomatis salah satu ip di masing2 router diatas akan dijadikan router-id oleh mikrotik, dan fatalnya ketika router-id td down/kabel diskonek maka OSPF juga akan bermasalah.

DAFTAR PUSTAKA

Stallings, William, 1994, *Data and Computer Communications*, Prentice Hall

Onno W. Purbo, 1999, *TCP/ IP Standar, Desain dan Implementasi*, Jakarta, ISBN no. 979-20-0759-8.

Wendel Odom, 2004, *Computer Networking First-Step*, Cisco Systems, Inc.

Nial Mansfield, 2002, *Practical TCP/ IP Designing, Using and Troubleshooting TCP/ IPNetwork on Linux® and Windows®*, Pearson Education, Inc.

Darmawan Hery, 2013, *Mikrotik Certified Network Association (MTCNA)*, Belajarmikrotik.com

Darmawan Hery, 2013, *Mikrotik Certified Router Engineer (MTCRE)*, Belajarmikrotik.com

Darmawan Hery, 2014, *Mikrotik Certified Traffict Engineer (MTCTCE)*, Belajarmikrotik.com