



PUSAT PENDIDIKAN DAN PELATIHAN
BADAN PUSAT STATISTIK

MODUL PELATIHAN FUNGSIONAL PRANATA KOMPUTER TINGKAT AHLI

>>>>

SISTEM JARINGAN KOMPUTER

PUSDIKLAT BPS
2022

Hak Cipta © pada:

Pusat Pendidikan dan Pelatihan Badan Pusat Statistik
Edisi Tahun 2022

**Pusat Pendidikan dan Pelatihan Badan Pusat Statistik
Jl. Raya Jagakarsa NO. 70 Jakarta Selatan 12620**

SISTEM JARINGAN KOMPUTER

Modul Pelatihan Fungsional Pranata Komputer Tingkat Ahli

TIM PENGARAH SUBSTANSI:

1. Dr. Eni Lestariningsih, S.Si, MA
2. Dr. Pudji Ismartini M.App.Stat
3. Atas Parlindungan Lubis S.Si, M.Si

PENULIS MODUL:

1. Rosita Dewi Hadiyanti SST., M.T.I.
2. Sri herwanto Dwi Hatmo SSi., MA.
3. Nia Dwi Rahayuningtyas SST, M.T.I.
4. Utama Andri Arjita, ST., MT

EDITOR:

1. Rosita Dewi Hadiyanti SST., M.T.I.,
2. Nia Dwi Rahayuningtyas SST, M.T.I.

COVER: Else Huslijah S.Tr.Stat

JAKARTA – PUSDIKLAT BPS – 2022

ISBN: nomor ISBN

KATA PENGANTAR



Puji syukur kehadirat Allah SWT yang telah memberikan petunjuk sehingga Modul 6 Sistem Jaringan Komputer ini dapat disusun. Modul ini dimaksudkan untuk meningkatkan pengetahuan, keterampilan, dan sikap perilaku seorang administrator jaringan agar kompeten dalam melakukan jaringan komputer yang meliputi menganalisis kebutuhan, merancang, menerapkan, dan mengevaluasi sistem jaringan komputer.

Modul ini merupakan salah satu dari tiga belas modul yang diberikan kepada peserta Pelatihan Fungsional Pranata Komputer (Prakom). Ke-tigabelas modul adalah:

1. Modul 1: Information Technology Enterprise
2. Modul 2: Manajemen Layanan Teknologi Informasi
3. Modul 3: Pengelolaan Data
4. Modul 4: Manajemen Risiko Teknologi Informasi
5. Modul 5: Audit Teknologi Informasi
6. Modul 6: *Sistem Jaringan Komputer*
7. Modul 7: Manajemen Infrastruktur Teknologi Informasi
8. Modul 8: Sistem Informasi
9. Modul 9: Pengolahan Data
10. Modul 10: Area Teknologi Informasi Spesial
11. Modul 11: Dokumentasi dan Laporan
12. Modul 12: Pengembangan Profesi Pranata Komputer
13. Modul 13: Administrasi dan Penilaian Pranata Komputer

Ucapan terima kasih dan apresiasi kami sampaikan kepada seluruh pihak yang telah membantu dan memberikan masukan dalam penyusunan modul ini. Tanggapan dan saran yang konstruktif kami harapkan guna perbaikan dan pengembangan di masa mendatang. Semoga modul ini dapat bermanfaat bagi pengembangan kompetensi bidang prakom para peserta pelatihan.

Jakarta, Februari 2022
Kepala Pusdiklat BPS

Eni Lestariningsih, S.Si, M.A.
NIP. 197003101994012001

DAFTAR ISI

KATA PENGANTAR	i
DAFTAR ISI	ii
DAFTAR TABEL	v
DAFTAR GAMBAR.....	vi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Kompetensi Dasar	3
1.3 Indikator Keberhasilan	3
1.4 Panduan Penggunaan Modul.....	3
1.5 Materi Pokok dan Sub Materi Pokok.....	4
BAB II ANALISIS KEBUTUHAN SISTEM JARINGAN KOMPUTER.....	6
4.1. Sistem Jaringan Komputer.....	6
a. Konsep sistem jaringan komputer.....	6
a.1. Komunikasi Data.....	7
a.2. Definisi Jaringan Komputer.....	12
a.3. Manfaat Jaringan Komputer.....	13
a.4. Klasifikasi Jaringan Komputer	14
a.5. Perangkat Jaringan Komputer	20
a.6. Protokol	34
a.7. Layering	35
a.8. <i>Routing</i>	42
a.9. IP <i>Addressing</i>	44
b. Analisis kebutuhan pengguna	52
c. Analisis sistem berjalan.....	60
4.2. Rangkuman	70
4.3. Soal Latihan.....	71
4.4. Contoh Kasus.....	72
BAB III PERANCANGAN SISTEM JARINGAN KOMPUTER.....	77

4.1.	Uraian Materi	77
a.	Topologi Jaringan	79
a.1.	Jenis Topologi Jaringan	80
a.2.	Pertimbangan Pemilihan Topologi Jaringan.....	87
b.	Rancangan Logis Sistem Jaringan Komputer	90
c.	Rancangan Fisik Sistem Jaringan Komputer.....	92
d.	Tahapan Perancangan Sistem Jaringan Komputer	94
e.	<i>Tools</i> Perancangan Topologi Jaringan	100
4.2.	Rangkuman	104
4.3.	Soal Latihan.....	106
4.4.	Contoh Kasus.....	108
	BAB IV PENERAPAN SISTEM JARINGAN KOMPUTER	111
4.1.	Uraian Materi	111
a.	Penerapan Rancangan Fisik Jaringan Komputer	111
a.1.	Pemilihan perangkat keras jaringan dan platform	111
a.2.	Instalasi perangkat jaringan	114
b.	Penerapan Rancangan Logis Jaringan Komputer	114
c.	Pengujian Sistem Jaringan Komputer.....	117
d.	Contoh Penerapan dan Pengujian Sistem Jaringan Menggunakan Cisco Packet Tracker	118
4.2.	Contoh Kasus.....	133
	BAB V EVALUASI SISTEM JARINGAN KOMPUTER	139
4.1.	Uraian Materi	139
a.	Monitoring dan Evaluasi Sistem Jaringan Komputer.....	151
b.	Analisis Permasalahan Sistem Jaringan Komputer	160
c.	Optimalisasi Sistem Jaringan Komputer.....	165
4.2.	Rangkuman	168
4.3.	Soal Latihan.....	169
4.4.	Contoh Kasus.....	169
	BAB VI KESIMPULAN	170
	DAFTAR PUSTAKA.....	171
	DAFTAR LAMPIRAN	173

PENULIS	174
SINOPSIS	175

DAFTAR TABEL

Tabel 1. Proses Sistem Komunikasi Data.....	9
Tabel 2. Desimal dan Biner IP Address 167.205.206.100	46
Tabel 3. Perhitungan 2 pangkat N	47
Tabel 4. IP Address 192.168.1.254.....	53
Tabel 5. Prefix Number : /24.....	53
Tabel 6. IP Address PT. Y	64
Tabel 7. Tabel RMON 1 MIB.....	145

DAFTAR GAMBAR

Gambar 1. Jaringan komputer personal (PAN)	15
Gambar 2. Jaringan komputer Local (LAN)	17
Gambar 3. Jaringan komputer Metropolitan (MAN).....	18
Gambar 4. Jaringan komputer skala luas (WAN)	19
Gambar 5. Jaringan global (GAN)	20
Gambar 6. Perangkat Lunak Jaringan Komputer	21
Gambar 7. Perangkat Keras Jaringan Komputer	22
Gambar 8. Network Interface Cards (NIC) atau Kartu Jaringan	23
Gambar 9. Hub/ Switch/ Konsentrator	24
Gambar 10. Access Point.....	26
Gambar 11. Koneksi antara NIC dengan Hub/Switch	29
Gambar 12. Koneksi antara Hub dengan Hub, Switch dengan Switch, dan NIC dengan NIC.....	29
Gambar 13. Fiber Optic.....	31
Gambar 14. Komunikasi Radio.....	31
Gambar 15. Perangkat Wireless LAN	32
Gambar 16. Komunikasi satelit dengan VSAT	33
Gambar 17. Router Cisco dan RouterBoard	34
Gambar 18. Model OSI.....	41
Gambar 19. Model TCP/IP.....	42
Gambar 20. Perbedaan pada OSI dan TCP model	42
Gambar 21. Sebuah router menghubungkan dua tipe jaringan yang berbeda	44
Gambar 22. IP Private	45
Gambar 23. <i>IP Public</i>	46
Gambar 24. Contoh penggunaan NAT pada <i>IP private</i>	46
Gambar 25. Sebuah Jaringan di bagi menjadi 3	50
Gambar 26. Analogi Jalan pada jaringan	56
Gambar 27. Analogi memerah jalan.....	57
Gambar 28. Network, Hots dan Broadcast address	58
Gambar 29. Network, Hots dan Broadcast address yang sudah di segmen	58
Gambar 30. Back-to back DMZ konfigurasi	59
Gambar 31. Perimeter 3 kaki konfigurasi DMZ	59
Gambar 32. Topologi Jaringan PT. X	62
Gambar 33. Blok Diagram PT.Y	63
Gambar 34. Skema jaringan PT. Y	65
Gambar 35. Switch.....	68
Gambar 36. Solusi Teknologi <i>Business-Driven</i>	78
Gambar 37. Business-Driven vs Inisiatif TI,	79

Gambar 38. Topologi point-to-point.....	80
Gambar 39. Topologi Daisy-chain.....	81
Gambar 40. Topologi Bus	81
Gambar 41. Topologi Star.....	83
Gambar 42. Topologi Ring.....	84
Gambar 43. Topologi Mesh.....	85
Gambar 44. Topologi <i>Hybrid</i>	86
Gambar 45. Topologi Tree.....	87
Gambar 46. Rancangan Logis Level 0.....	91
Gambar 47. Rancangan Logis Level 1.....	92
Gambar 48. Rancangan Fisik Level 0.....	93
Gambar 49. Rancangan Fisik Level 1.....	93
Gambar 50. Rancangan Fisik Level 2	94
Gambar 51. Rancangan Fisik Level 3	94
Gambar 52. Layout interface Packet Tracer beserta menunya.....	101
Gambar 53. Status koneksi jaringan	102
Gambar 54. Jenis kabel penghubung	102
Gambar 55. Jenis device jaringan.....	102
Gambar 56. Jenis device jaringan layer 2	103
Gambar 57. Jenis device jaringan layer 3	103
Gambar 58. Jenis device jaringan wireless	104
Gambar 59. Platoform Switch.....	112
Gambar 60. Model Konfigurasi Switch	113
Gambar 61. Kepadatan Port pada Switch.....	113
Gambar 62. Desain jaringan LAN komputer klien	120
Gambar 63. Pengisian IP address pada pc.....	121
Gambar 64. Status hasil tes koneksi antar pc	122
Gambar 65. Desain jaringan LAN server farm.....	122
Gambar 66. Status hasil tes koneksi antar server.....	123
Gambar 67. Desain layout dua Jaringan LAN	123
Gambar 68. IP address interface router FE0/0, sisi komputer klien.....	124
Gambar 69. IP address interface router FE0/1, sisi server farm	125
Gambar 70. Status hasil tes koneksi dari pc5 ke server DNS.....	125
Gambar 71. Konfigurasi jaringan di pc dan server	126
Gambar 72. Status hasil tes koneksi pc dan server	126
Gambar 73. Konfigurasi Web server.....	127
Gambar 74. Kustomisasi file index.html pada web server.....	127
Gambar 75. Hasil tampilan web server pada browser	128
Gambar 76. Konfigurasi dan setting pada email server	128
Gambar 77. Konfigurasi dan setting email pada komputer klien	129
Gambar 78. Status hasil “ <i>send</i> ” dan “ <i>reply</i> ” email klien	129
Gambar 79. Konfigurasi DNS server	130

Gambar 80. Pengisian IP DNS server pada pc dan server	131
Gambar 81. Status hasil tes koneksi dari laptop1 menuju ke 3 server.....	131
Gambar 82. Status akses web-srv.com	132
Gambar 83. Konfigurasi pop3 dan smtp pada pc klien dan konfigurasi dns server	132
Gambar 84. Status hasil “send” dan “reply” email antara pc1 dan laptop1..	132

BAB I PENDAHULUAN

1.1 Latar Belakang

Modul Sistem Jaringan Komputer ini diharapkan dapat memperjelas dan mempermudah penyajian pesan agar tidak terlalu bersifat verbal, mengatasi keterbatasan waktu, ruang, dan daya indera, baik peserta/calon instruktur dan master instruktur, dapat digunakan secara tepat dan bervariasi, seperti: meningkatkan motivasi dan gairah belajar bagi peserta pelatihan; dan mengembangkan kemampuan peserta pelatihan dalam berinteraksi langsung dengan lingkungan dan sumber belajar lainnya, Memungkinkan peserta pelatihan belajar mandiri sesuai kemampuan dan minatnya, memungkinkan peserta pelatihan dapat mengukur atau mengevaluasi sendiri hasil belajarnya.

Tujuan Strategis diajarkannya Sistem Jaringan Komputer pada para peserta Pelatihan adalah untuk mempersiapkan dan mengkader Pranata Komputer yang lebih profesional dalam melaksanakan pekerjaan ataupun tanggap dalam menyikapi setiap proses perubahan dan perkembangan teknologi dan informasi, serta mempunyai sikap peka terhadap persoalan ketidakberdayaan yang dialami organisasi dan mempunyai ketrampilan/kemampuan untuk menyelesaikannya.

Mata Pelatihan Sistem Jaringan Komputer dimaksudkan untuk meningkatkan pengetahuan, keterampilan, dan sikap perilaku seorang administrator jaringan agar kompeten dalam melakukan jaringan komputer yang meliputi menganalisis kebutuhan, merancang, menerapkan, dan mengevaluasi sistem jaringan komputer Indikator Hasil belajar adalah setelah mengikuti mata pelatihan ini, peserta diharapkan mampu menganalisis kebutuhan, merancang, menerapkan, dan mengevaluasi sistem jaringan komputer

Agar pelaksanaan pelatihan dapat berjalan dengan baik, maka peserta pelatihan harus membaca dan mengikuti setiap petunjuk yang tertuang dalam buku modul serta mengerjakan tugas-tugas terstruktur yang akan diberikan oleh pengajar, dalam tahap-tahap pertemuan diklat.

1. Metode yang akan dipergunakan adalah metode case study.
2. Sebelum pertemuan pertama, peserta diklat harus sudah membaca buku modul ini terlebih dahulu untuk mengetahui apa yang harus dilakukan dalam mengikuti pelatihan.
3. Buku modul ini tersusun ke dalam enam BAB. Bab I sampai dengan Bab VI berisi materi diklat yang berisi pengetahuan tentang jaringan komputer serta hal-hal yang harus diperhatikan oleh peserta pelatihan dalam menyikapi permasalahan dalam jaringan komputer.
4. Materi Bab I sampai dengan Bab VI akan diberikan melalui syncrounous dan Asyncrounous. Karena terbatasnya waktu pertemuan, maka peserta diklat diwajibkan membaca terlebih dahulu secara mandiri materi Bab I sampai dengan VI. Dalam tatap muka di kelas, tutor (pengajar) hanya akan menegaskan garis besarnya saja, kemudian diikuti dengan tanya jawab serta tugas terstruktur untuk mengetahui tingkat pemahaman peserta. Peserta pelatihan harus mengerjakan tiap tugas yang diberikan oleh tutor pada akhir pertemuan.
5. Pada pertemuan keempat dan seterusnya, peserta pelatihan akan dilatih melakukan praktek merancang jaringan komputer dan studi kasus terhadap contoh kasus yang akan diberikan oleh tutor pengajar. Hal-hal yang harus diperhatikan dan dikerjakan dalam melakukan praktek merancang jaringan komputer dan studi kasus, sebagaimana telah dijelaskan atau disampaikan pada pertemuan sebelumnya, dipergunakan sebagai pedoman dalam melakukan pelatihan.
6. Materi diklat banyak menekankan pada aspek praktek/pelatihan. Oleh karena itu nilai sangat tergantung dari keaktifan peserta pelatihan dalam

mengerjakan tiap tugas dan latihan terstruktur yang diberikan oleh pengajar.

7. Sistem Evaluasi dilakukan sebagai berikut:

- ❖ Komponen evaluasi terdiri dari: keaktifan dalam mengajukan pertanyaan serta menjawab pertanyaan tutor, keaktifan selama diskusi dan presentasi, pengerjaan tugas-tugas terstruktur dan laporan tertulis hasil eksaminasi.
- ❖ Ujian praktik merancang jaringan komputer akan diselenggarakan sejauh, waktu dan peralatan memungkinkan, sedang ujian akhir secara tertulis tidak diselenggarakan.
- ❖ Nilai akhir sangat tergantung dari kuantitas dan kualitas jawaban, diskusi, presentasi,

1.2 Kompetensi Dasar

Pada akhir pelatihan peserta diharapkan mampu mengevaluasi sistem jaringan komputer dengan baik dan benar

1.3 Indikator Keberhasilan

Setelah mengikuti mata pelatihan ini, peserta diharapkan mampu menganalisis kebutuhan, merancang, menerapkan, dan mengevaluasi sistem jaringan komputer.

1.4 Panduan Penggunaan Modul

Langkah-langkah penggunaan modul system jaringan kompter ini dapat dijabarkan sebagai berikut :

1. Bacalah dan pahami dengan seksama uraian-uraian materi yang ada pada masing-masing kegiatan belajar. Bila ada materi yang kurang

jelas, peserta dapat bertanya pada instruktur yang mengampu kegiatan belajar.

2. Kerjakan setiap tugas formatif (soal latihan) untuk mengetahui seberapa besar pemahaman yang telah dimiliki terhadap materi-materi yang dibahas dalam setiap kegiatan belajar.
3. Untuk kegiatan belajar yang terdiri dari teori dan praktik, perhatikanlah hal-hal berikut ini:
 - a) Perhatikan petunjuk-petunjuk yang berlaku.
 - b) Pahami setiap langkah kerja dengan baik.
 - c) Jika belum menguasai level materi yang diharapkan, ulangi lagi pada kegiatan belajar sebelumnya atau bertanyalah kepada fasilitator atau fasilitator yang mengampu kegiatan pembelajaran yang bersangkutan

1.5 Materi Pokok dan Sub Materi Pokok

Materi pokok yang dibahas di dalam modul serta penjabaran ke dalam sub materi pokoknya adalah :

1. Analisis Kebutuhan system jaringan computer
 - 1.1. Konsep sistem jaringan komputer
 - 1.2. Analisis kebutuhan pengguna
 - 1.3. Analisis sistem berjalan
2. Perancangan sistem jaringan komputer
 - 2.1 Macam-macam topologi
 - 2.2 Topologi rancangan logis sistem jaringan computer
 - 2.3 Topologi rancangan fisik sistem jaringan komputer
3. Perancangan sistem jaringan komputer;
 - 3.1 Penerapan rancangan fisik
 - 3.2 Penerapan rancangan logik
 - 3.3 Pengujian sistem jaringan computer
 - 3.4 Tata kelola sistem jaringan computer

4. Evaluasi Sistem Jaringan Komputer

- 4.1. Evaluasi hasil pengujian
- 4.2. Analisis permasalahan sistem jaringan computer
- 4.3. Optimalisasi sistem jaringan computer

BAB II

ANALISIS KEBUTUHAN SISTEM JARINGAN KOMPUTER

4.1. Sistem Jaringan Komputer

a. Konsep sistem jaringan komputer

Sebagai sebuah sistem, sebuah komputer mampu beroperasi sendiri tanpa bantuan perangkat atau komputer lain (stand alone). Namun lama kelamaan timbul kebutuhan untuk berhubungan dengan perangkat lain dan membentuk jaringan komputer dengan berbagai alasan. Alasan pertama yang menarik adalah efisiensi. Misalnya hanya dengan satu printer yang dihubungkan pada jaringan semua komputer bisa mencetak ke printer tersebut, dan jika ada lebih dari satu printer maka pengguna bisa memilih dia akan mencetak di printer mana. Sehingga tidak dijumpai lagi pemasangan printer pada setiap komputer atau memindah-mindahkan kabel printer bila ingin mencetak. Efisien dalam penggunaan perangkat keras. Efisiensi tidak hanya untuk hal yang berhubungan dengan perangkat keras, namun juga efisiensi yang berhubungan dengan perangkat lunak dan informasi. Alasan lainnya adalah keamanan, kemudahan, dan semakin banyaknya layanan (service) yang diperoleh bila dibangun sebuah jaringan.

Perkembangan teknologi komunikasi yang pesat seiring dengan perkembangan teknologi komputer semakin menambah populer penggunaan jaringan komputer. Jaringan komputer tidak hanya digunakan oleh kalangan serius seperti universitas, perusahaan, dan pemerintahan, namun juga oleh kalangan rumahan dan bahkan perorangan. Penggunaan jaringan oleh kalangan perorangan mulai dari hanya sekedar menggunakan teknologi Bluetooth untuk PAN (Personal Area Network) sampai dengan mengakses WLAN dengan menggunakan laptop di tempat umum

Sebuah jaringan dapat dibuat mulai dari sebuah LAN yang sederhana, WAN yang lebih besar dan rumit, serta PAN yang hanya untuk kebutuhan personal. Tiap skala penggunaan membutuhkan teknologi yang berbeda karena adanya

batasan masing-masing teknologi. Kompatibilitas dalam membangun jaringan sangat penting untuk mempermudah koneksi dan merubah skala jaringan. Bila ada perangkat keras maupun lunak yang tidak kompatibel, jaringan bisa terganggu atau bahkan menjadi tidak berfungsi. Untuk itu perlu diperhatikan standar teknologi yang digunakan. Sebuah LAN masih mungkin digunakan satu teknologi yang sama karena umumnya pengelolaannya masih dalam satu organisasi. Namun begitu dibentuk gabungan antara LAN dengan LAN lainnya berbagai teknologi lain mulai terlibat seperti penggunaan fiber optik dan bahkan satelit.

Internet adalah sebuah gambaran jaringan komputer yang lebih besar dan luas. Berbagai gabungan teknologi bercampur dan saling berinteraksi membentuk suatu jaringan yang sifatnya global. Dengan bermacam layanan yang disediakan, efisiensi dengan penggunaan internet bukan lagi hanya sebuah angan-angan.

a.1. Komunikasi Data

Perkembangan teknologi komputer dan komunikasi data serta diiringi penggabungan dua teknologi tersebut telah memberikan banyak perubahan terhadap penggunaan dan cara pandang komputer dan komunikasi data. Beberapa fakta yang ada menunjukkan perubahan di atas antara lain adalah tidak adanya perbedaan yang mendasar antara pengolahan data (komputer) dengan komunikasi data (perangkat transmisi).

Tujuan utama sebuah sistem komunikasi data dibangun adalah untuk memungkinkan terjadinya pertukaran data antara dua bagian yang kemudian dinamakan sebagai source (sumber) dan destination (tujuan). Proses pertukaran data yang terjadi antara keduanya secara sesederhana dapat dibayangkan seperti halnya pengiriman sebuah paket pos antara seseorang dengan orang lainnya, walaupun proses yang sebenarnya terjadi ternyata lebih rumit karena ada perbedaan karakteristik "benda" yang dikirimkan.

Karakteristik data yang merupakan "benda" elektronik membutuhkan lebih banyak proses dan prosedur dalam proses pengirimannya. Proses dan

prosedur yang dilakukan dipergunakan untuk memastikan bahwa pengiriman data dilakukan secara benar dan efisien

a. Elemen Komunikasi Data

Secara sederhana, pada sebuah sistem komunikasi data terdapat lima elemen penting yaitu:

- 1) *Source*. Perangkat ini menghasilkan data yang siap untuk dikirimkan. Misalnya, telepon atau komputer.
- 2) *Transmitter*. Pada umumnya data yang diberikan oleh source untuk dikirimkan belumlah dalam bentuk (format) data yang siap dikirimkan pada sistem transmisi yang digunakan. Diperlukan suatu cara perubahan format data sehingga siap dan memenuhi persyaratan pengiriman data. Perubahan format data dilakukan oleh transmitter. Modem adalah contoh dari sebuah transmitter. Perangkat ini merubah data yang berformat digital dari komputer menjadi sinyal analog, sehingga siap untuk dikirimkan oleh sistem transmisi, dalam kasus ini adalah jaringan telepon.
- 3) *Transmission System*. Elemen ini dapat berupa sebuah rangkaian sederhana atau bahkan berbentuk lebih rumit, yang bertanggung jawab untuk menghubungkan kedua perangkat dan melakukan pertukaran data.
- 4) *Receiver*. Berfungsi sebaliknya dari transmitter, receiver merubah format data yang diterima dari sistem transmisi menjadi format yang dimengerti oleh Destination. Modem juga dapat berfungsi sebagai receiver. Modem merubah sinyal analog menjadi data berformat digital yang kemudian dikirimkan ke Destination.
- 5) *Destination*. Elemen akhir yang merupakan tujuan pengiriman data.

Kelima elemen di atas dapat disingkat menjadi tiga subsistem, yaitu *Source system* (*Source* dan *Transmitter*), *Transmission System*, serta *Destination System* (*Receiver* dan *Destination*).

b. Proses Sistem Komunikasi Data

Praktiknya, dalam sebuah sistem komunikasi data dijalankan beberapa proses yang harus dilakukan untuk memastikan berjalananya pertukaran data antara Source dan Destination. Proses-proses yang harus dijalankan dapat dilihat pada tabel 1

Tabel 1. Proses Sistem Komunikasi Data

<i>Transmission system utilization</i>	<i>Addressing</i>
<i>Interfacing</i>	<i>Routing</i>
<i>Signal generation</i>	<i>Recovery</i>
<i>Synchronization</i>	<i>Message Formating</i>
<i>Exchange Management</i>	<i>Security</i>
<i>Error detection and correction</i>	<i>Network Management</i>
<i>Flow control</i>	

Transmission system utilization ditujukan untuk efisiensi penggunaan perangkat transmisi dalam sistem komunikasi data. Proses ini diperlukan karena biasanya dalam sebuah sistem komunikasi data perangkat komunikasi yang ada digunakan secara bersama-sama. *Multiplexing* misalnya, digunakan untuk mengalokasikan kapasitas transmisi untuk sejumlah pengguna jalur transmisi. Teknik lainnya yang dikenal sebagai *Congestion Control* digunakan untuk memastikan tidak terjadinya kelebihan kapasitas pada sistem transmisi.

Terhubung (*interfacing*) pada sebuah sistem transmisi harus dilakukan agar perangkat bisa berkomunikasi dengan perangkat lainnya. Setelah perangkat terhubung, diperlukan *signal generation* (pembangkitan sinyal). Setidaknya diperlukan dua persyaratan pada proses *signal generation*. Persyaratan pertama adalah kesesuaian sinyal dengan sistem transmisi yang digunakan sehingga sinyal dapat dialirkan, dan berikutnya adalah dapat diinterpretasikannya sinyal menjadi data oleh *receiver*.

Walaupun sinyal dapat dibangkitkan, dialirkan, dan diinterpretasikan sesuai dengan proses di atas, diperlukan suatu proses lanjutan untuk

menentukan kapan sebuah sinyal mulai dikirimkan dan berakhir, serta durasi antara satu sinyal dengan sinyal lainnya. Untuk menentukan hal ini diperlukan suatu proses sinkronisasi (*synchronization*) antara *transmitter* dan *receiver*. Dalam komunikasi data juga diperlukan *Exchange management* yang akan mengatur proses pertukaran data antara dua perangkat. *Exchange Management* akan mengatur apakah pertukaran data akan dilakukan secara simultan atau bertahap, format data yang digunakan, besarnya data yang dikirimkan dalam satu waktu pengiriman, serta apa yang harus dilakukan bila terjadi suatu kesalahan dalam transmisi.

Terjadinya kesalahan pada sistem komunikasi data adalah hal yang mungkin terjadi sebagus apapun sistem yang digunakan. Data yang tidak dimengerti oleh receiver atau tidak sampai ke receiver adalah contoh kesalahan yang bisa terjadi. *Error detection and correction* diperlukan untuk menentukan kapan sebuah kesalahan tidak lagi bisa ditoleransi. Selain itu diperlukan juga *Flow control* yang akan memastikan bahwa *terminal source* tidak mengirimkan data lebih cepat melebihi kapasitas proses terminal *destination*.

Saat perangkat *source* dan *destination* melakukan pertukaran data melalui sebuah sistem transmisi yang digunakan oleh banyak perangkat lainnya secara bersama-sama, *source system* harus memberitahukan identitas terminal tujuan dan sistem komunikasi data harus dapat memastikan bahwa hanya terminal tujuan yang dapat menerima data. Saat itulah proses *Addressing* diperlukan. Selain itu diperlukan pula *Routing* yang akan memilih jalur yang spesifik untuk transmisi data dari beberapa pilihan jalur transmisi yang mungkin.

Berbeda dengan *Error correction*, *Recovery* dibutuhkan saat pertukaran data dihentikan karena ada permasalahan dalam sistem transmisi dan ditujukan untuk memungkinkan dilakukannya pengiriman ulang sejak dari titik penghentian transmisi ke *destination system*.

Message formating melakukan *formatting* pada data yang dikirimkan sesuai dengan format data yang disepakati antara *source* dan *destination*.

Satu hal penting yang juga dibutuhkan saat melakukan komunikasi data adalah *security*. Hal ini dilakukan untuk memastikan source bahwa hanya destination yang diinginkanlah yang bisa menerima data, tidak berubahnya data selama dalam sistem transmisi, serta diyakinkannya *destination* bahwa data memang benar dikirimkan oleh *source* tertentu.

Proses yang dijalankan oleh sebuah sistem komunikasi data bukanlah proses yang sederhana. Untuk itu diperlukan sebuah kontrol *Network Management* yang digunakan untuk melakukan konfigurasi dan memonitor status sistem. Selain itu *Network Management* juga bertanggung jawab saat terjadi kelebihan kapasitas jaringan (*overload*) dan kerusakan yang timbul di jaringan.

Uraian proses di atas menggambarkan rumitnya fungsi yang dijalankan oleh sistem komunikasi data yang semula hanya digambarkan sebagai kesatuan proses di atas dilakukan untuk memastikan bahwa komunikasi data yang dilakukan mampu memberikan hasil yang baik dan efisien.

c. Data dan Transmisi

Umumnya kita sering beranggapan bahwa istilah “data” serta “informasi” mengandung pengertian yang sama dan dapat digunakan secara bergantian. Tetapi secara teknis kedua istilah tersebut memiliki perbedaan arti. Data adalah suatu entiti yang memiliki arti. Data-data disimpan dalam komputer sebagai sekumpulan muatan elektronik yang disusun sedemikian rupa sehingga merupakan suatu informasi. Dengan kata lain, data merupakan pembentuk informasi (pattern atau pola elektronik), dan bukannya informasi-informasi itu sendiri. Untuk kepentingan pembahasan selanjutnya di dalam buku ini, informasi akan diartikan sebagai data-data yang telah tersaji kedalam bentuk yang dapat dimengerti oleh manusia. Sebagai contoh, informasi

mungkin berupa data-data dalam suatu file yang telah ditampilkan ke layar komputer melalui aplikasi pengolah kata, atau yang sudah dicetak di kertas, seperti surat-surat bisnis dan sebagainya.

Transmisi dalam terminologi komunikasi dirujuk pada pengertian tentang cara atau tindakan mengirimkan sinyal melalui sebuah media. Media yang dicakup tidak hanya media yang bisa dilihat secara fisik namun juga yang tidak (unguided transmission media).

Ada dua jenis transmisi, yaitu paralel dan serial. Transmisi paralel mengirimkan sinyal secara serentak melalui beberapa jalur (path). Metode ini tidak efisien untuk pengiriman jarak jauh. Metode serial mengirimkan sinyal bit per bit melalui satu jalur dan mensyaratkan bahwa antara pengirim dan penerima harus sinkron. Metode ini masih dibagi menjadi dua jenis lagi, yaitu asynchronous dan synchronous. Keduanya mempunyai kelebihan dan kekurangan masing-masing. Asynchronous berorientasi pada karakter (character oriented) dan pengiriman datanya tidak teratur. Sedangkan synchronous pengirimannya per blok dan mempunyai kecepatan yang tinggi. Asynchronous secara teknis lebih mudah dan karenanya lebih murah. Namun karena mudah terpengaruh oleh noise, asynchronous harus dibatasi kecepatannya lebih rendah. Selain itu asynchronous lebih efisien bila mengirimkan data yang sedikit.

a.2. Definisi Jaringan Komputer

Jaringan komputer adalah sekumpulan perangkat-perangkat yang dapat menyimpan dan mengolah data-data elektronis, dimana satu perangkat dihubungkan dengan perangkat-perangkat lain sedemikian rupa sehingga para pemakai jaringan dapat menyimpan, mengambil serta berbagi informasi dengan pemakai-pemakai lain. Perangkat-perangkat pembentuk jaringan pada umumnya berupa komputer-komputer mikro misalnya PC, komputer-komputer mini, mainframe, terminal, printer, bermacam-macam media

penyimpanan data, dan sebagainya. Dimasa mendatang, sejalan dengan perkembangan teknologi informasi, maka berbagai ragam perangkat elektronik lain dapat menjadi bagian dari jaringan komputer. Termasuk diantaranya TV, videophone, dan sistem-sistem pengontrol lingkungan. Lebih dari itu, perangkat-perangkat elektronik rumah tangga pada akhirnya akan mampu memberikan akses dua arah ke dalam jaringan informasi global, atau yang sering disebut Information Superhighway.

Jenis-jenis informasi yang dapat disimpan dalam jaringan komputer juga menjadi cukup banyak ragamnya. Mulai dari informasi-informasi yang berupa teks seperti surat-surat, dokumen-dokumen; informasi-informasi audio seperti voice messages; hingga informasi-informasi grafis, seperti faksimili, foto-foto bahkan tayangan-tayangan video. Di dalam suatu jaringan, informasi-informasi tersebut akan demikian mudahnya untuk disampaikan ke pihak-pihak lain

a.3. Manfaat Jaringan Komputer

Tujuan dibangunnya suatu jaringan komputer adalah untuk membawa informasi secara tepat dan tanpa adanya kesalahan dari sisi pengirim (*transmitter*) menuju ke sisi penerima (*receiver*) melalui media komunikasi. Manfaat dari dibangunnya jaringan komputer adalah untuk *sharing resources*, media komunikasi, integrasi data, pengembangan dan pemeliharaan, serta keamanan data. Berikut diuraikan tentang masing-masing manfaat tersebut.

1. *Sharing resources*

Sharing resources bertujuan agar seluruh program, peralatan atau *peripheral* lainnya dapat dimanfaatkan oleh setiap orang yang ada pada jaringan komputer tanpa terpengaruh oleh lokasi maupun pengaruh dari pemakai

2. Media Komunikasi

Jaringan komputer memungkinkan terjadinya komunikasi antar pengguna, baik untuk *teleconference* maupun untuk mengirim pesan atau informasi yang penting lainnya.

3. Integrasi Data

Jaringan komputer dapat mencegah ketergantungan pada komputer pusat, karena setiap proses data tidak harus dilakukan pada satu komputer saja, melainkan dapat didistribusikan ke tempat lainnya. Oleh sebab inilah maka dapat terbentuk data yang terintegrasi yang memudahkan pemakai untuk memperoleh dan mengolah informasi setiap saat.

4. Pengembangan dan Pemeliharaan

Pengembangan peralatan dapat dilakukan dengan mudah dan menghemat biaya, karena setiap pembelian komponen seperti printer, maka tidak perlu membeli printer sejumlah komputer yang ada tetapi cukup satu buah karena printer itu dapat digunakan secara bersama – sama. Jaringan komputer juga memudahkan pemakai dalam merawat harddisk dan peralatan lainnya, misalnya untuk memberikan perlindungan terhadap serangan virus maka pemakai cukup memusatkan perhatian pada harddisk yang ada pada komputer pusat.

5. Keamanan Data

Sistem Jaringan Komputer dapat memberikan perlindungan terhadap data. Karena pemberian dan pengaturan hak akses kepada para pemakai, serta teknik perlindungan terhadap harddisk sehingga data mendapatkan perlindungan yang efektif.

a.4. Klasifikasi Jaringan Komputer

1. Jaringan komputer personal (PAN)

Personal area network (PAN) adalah jaringan komunikasi satu perangkat lain dengan perangkat lainnya dalam jarak yang sangat dekat. Misalnya antara komputer yang dihubungkan dengan *Personal Digital Assistance* (PDA), telepon seluler, laptop, dan lain sebagainya. PAN ini dapat digunakan untuk komunikasi antara suatu perangkat dengan perangkat yang lainnya ataupun penghubung antara device dengan jaringan yang lebih luas lagi seperti internet misalnya. Untuk membuat jaringan PAN ini, biasanya dengan menghubungkan melalui bus yang ada pada komputer seperti USB ataupun firewire. Selain itu PAN ini juga dapat dibuat dengan media wireless atau biasa disebut WPAN (Wireless PAN) dengan menggunakan media perantara IrDA (gelombang infra merah), bluetooth, UWB, Z-Wave, dan ZigBee. Jangkauannya untuk jaringan PAN adalah 6-9 meter



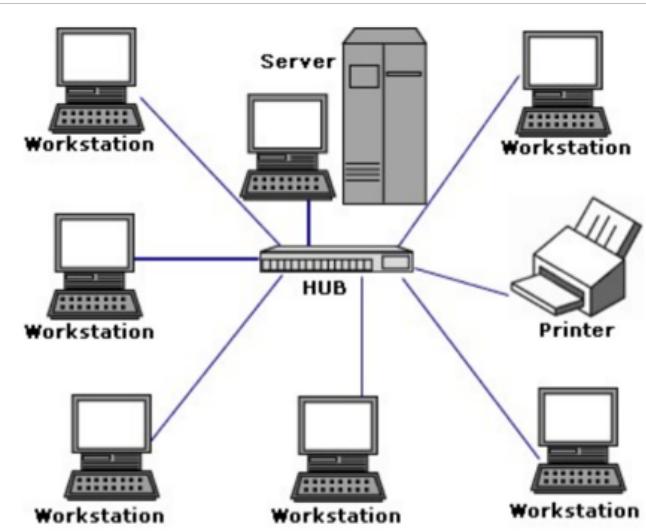
Gambar 1. Jaringan komputer personal (PAN)

2. Jaringan komputer Local (LAN)

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

seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan workstation dalam kantor suatu perusahaan atau pabrik-pabrik untuk pemakaian bersama sumber daya (misalnya printer) dan saling bertukar informasi. LAN adalah jaringan komputer yang jaringannya hanya mencakup wilayah kecil. misalnya jaringan komputer kampus, gedung, kantor, rumah, sekolah, atau yang lebih kecil. Saat ini, kebanyakan LAN berbasis pada teknologi IEEE 802.3 Ethernet menggunakan perangkat switch, yang mempunyai kecepatan transfer data 10, 100, atau 1000 Mbit/s. Selain teknologi Ethernet, saat ini teknologi 802.11b (atau biasa disebut Wi-fi) juga sering digunakan untuk membentuk LAN.

Tempat-tempat yang menyediakan koneksi LAN dengan teknologi Wi-fi biasa disebut hotspot. Pada sebuah LAN, setiap node atau komputer mempunyai daya komputasi sendiri, berbeda dengan konsep dump terminal. Setiap komputer juga dapat mengakses sumber daya yang ada di LAN sesuai dengan hak akses yang telah diatur. Sumber daya tersebut dapat berupa data atau perangkat seperti printer. Pada LAN, seorang pengguna juga dapat berkomunikasi dengan pengguna yang lain dengan menggunakan aplikasi yang sesuai. Biasanya salah satu komputer diantara jaringan komputer itu akan digunakan menjadi server yang mengatur semua sistem di dalam jaringan tersebut. Jangkauan LAN berkisar dari 10-300 meter.



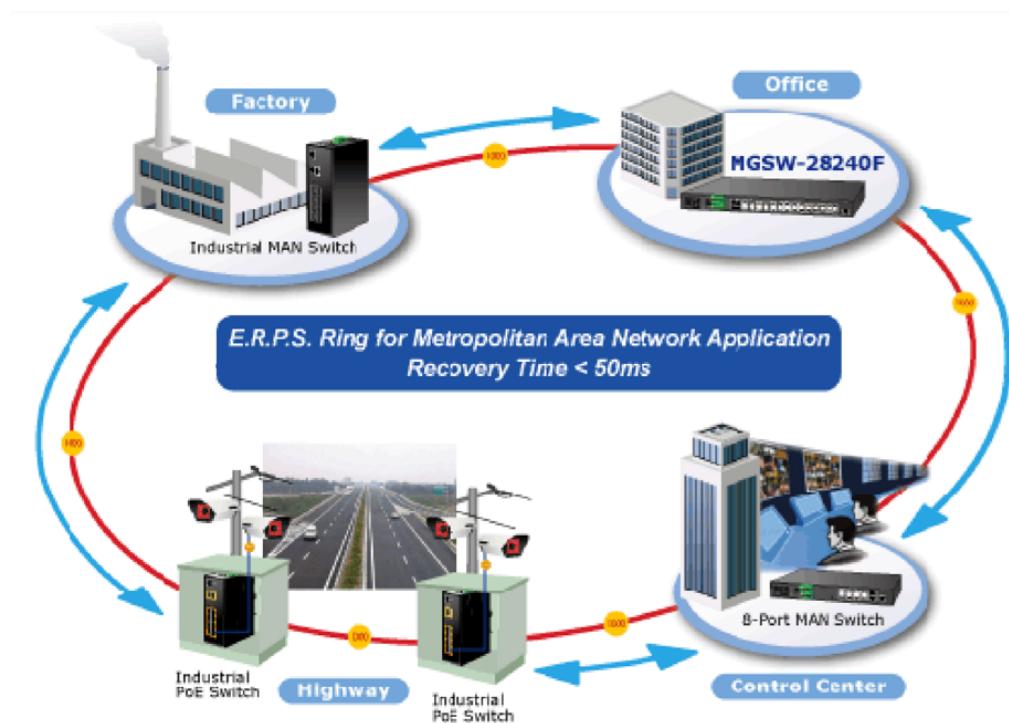
Gambar 2. Jaringan komputer Local (LAN)

3. Jaringan komputer Metropolitan (MAN)

Metropolitan Area Network (MAN), pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel. MAN meliputi area yang lebih besar dari LAN, misalnya antar gedung dalam suatu daerah (wilayah seperti propinsi atau negara bagian). Dalam hal ini jaringan menghubungkan beberapa buah jaringan kecil ke dalam lingkungan area yang lebih besar, sebagai contoh yaitu: jaringan beberapa kantor cabang sebuah bank di dalam sebuah kota besar yang dihubungkan antara satu dengan lainnya.

Metropolitan area network atau disingkat dengan MAN merupakan suatu jaringan dalam suatu kota dengan transfer data berkecepatan tinggi, yang menghubungkan berbagai lokasi seperti kampus, perkantoran, pemerintahan, dan sebagainya. Jaringan MAN adalah gabungan dari beberapa LAN. Jangkauan dari MAN ini antar 10 hingga 50 km, MAN ini

merupakan jaringan yang tepat untuk membangun jaringan antar kantor-kantor dalam satu kota antara pabrik/instansi dan kantor pusat yang berada dalam jangkauannya.



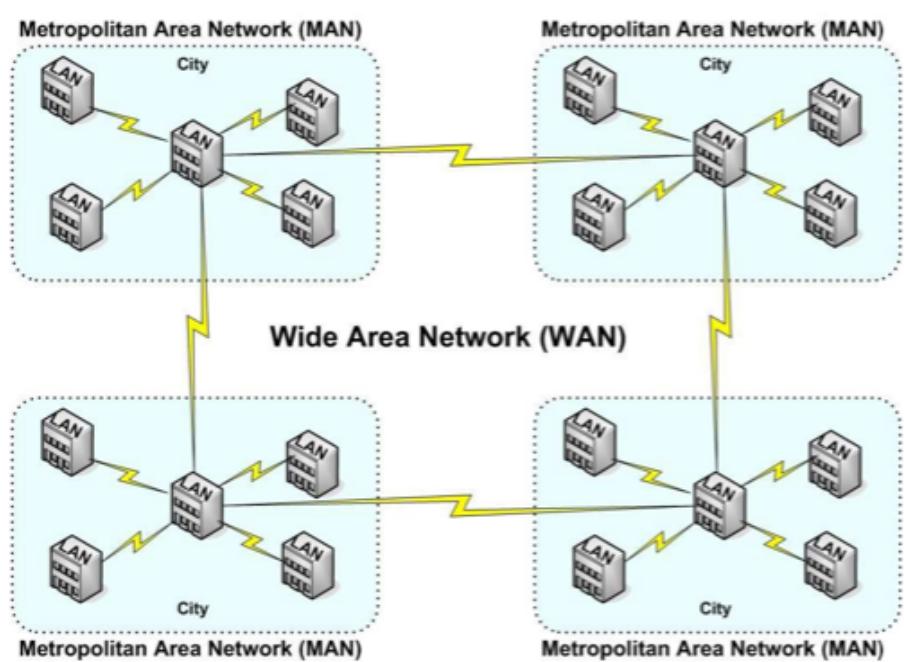
Gambar 3. Jaringan komputer Metropolitan (MAN)

4. Jaringan komputer skala luas (WAN)

Wide Area Network (WAN), jangkauannya mencakup daerah geografis yang luas, seringkali mencakup sebuah negara bahkan benua. WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan program-program (aplikasi) pemakai. *Wide Area Network (WAN)* adalah jaringan yang biasanya sudah menggunakan media wireless, sarana satelit ataupun kabel serat optik. Area jangkauannya sendiri lebih luas dibanding dengan jenis jaringan yang telah disebutkan di atas, bukan hanya meliputi satu kota atau antar kota dalam suatu wilayah, tetapi mulai menjangkau area/wilayah otoritas negara lain. Sebagai contoh jaringan komputer

kantor City Bank yang ada di Indonesia ataupun yang ada di negara lain yang saling berhubungan, jaringan ATM Master Card, Visa Card, atau Cirrus yang tersebar di seluruh dunia, dan lain sebagainya.

Biasanya WAN ini lebih rumit dan sangat kompleks bila dibandingkan LAN maupun MAN. WAN menggunakan banyak sarana untuk menghubungkan antara LAN dan WAN ke dalam komunikasi global seperti internet. Meski demikian antara LAN, MAN, dan WAN tidak banyak berbeda dalam beberapa hal, hanya lingkup areanya saja yang berbeda. WAN memiliki banyak kelebihan yang tentu saja diharapkan oleh pemakainya. Kelebihan adalah salah satu faktor utama seseorang atau sekelompok orang memilih menggunakan WAN sebagai solusi jaringannya

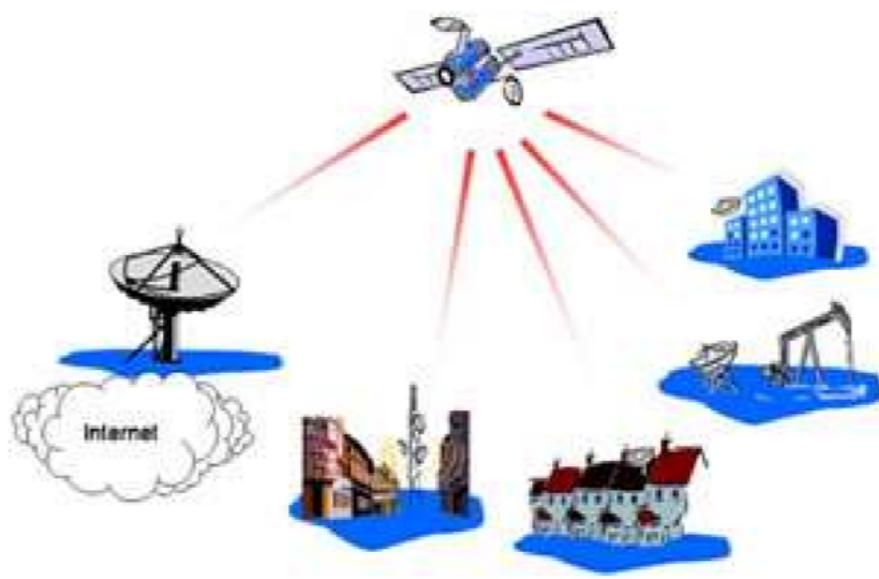


Gambar 4. Jaringan komputer skala luas (WAN)

5. Jaringan global (GAN)

Istilah untuk network yang akan menghubungkan berbagai wireless network, misalnya WLAN (WiFi dengan hotspotnya), cakupan area sebuah

satelit, dsb. Jangkauannya seperti MAN, yaitu melingkupi sebuah kota. Contohnya : IEEE 802.20, yaitu Mobile Broadband Wireless Access (MBWA).



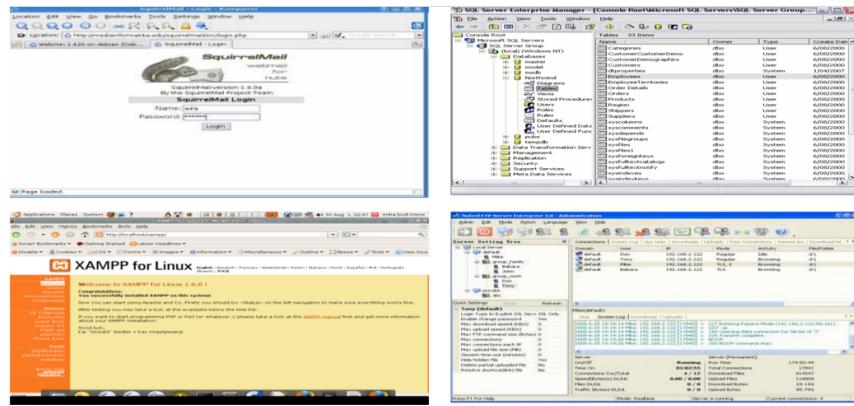
Gambar 5. Jaringan global (GAN)

a.5. Perangkat Jaringan Komputer

a) Perangkat Lunak Jaringan Komputer

a. 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. Tugas file server sangat kompleks, dia juga harus menyimpan informasi dan membaginya secara cepat.



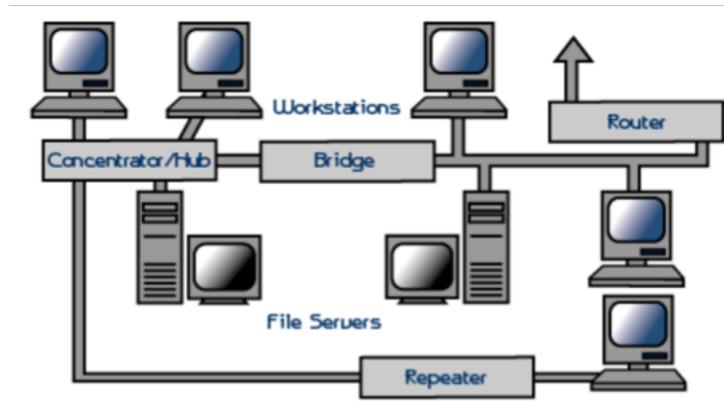
Gambar 6. Perangkat Lunak Jaringan Komputer

b. 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 Jaringan Komputer

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 proses transformasi data di dalam jaringan.



Gambar 7. Perangkat Keras Jaringan Komputer

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 internal, 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 koneksi dengan koaksial, twisted pair, ataupun dengan kabel fiber optik



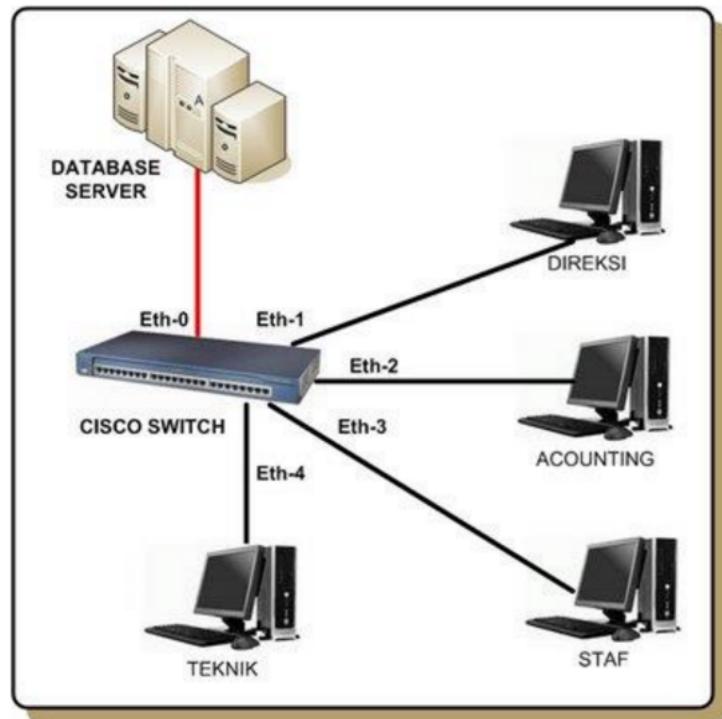
Gambar 8. Network Interface Cards (NIC) atau Kartu Jaringan

b. Hub/ Switch/ Konsentrator

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:

- 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 manjemen port tersebut.
- Biasanya disebut hub



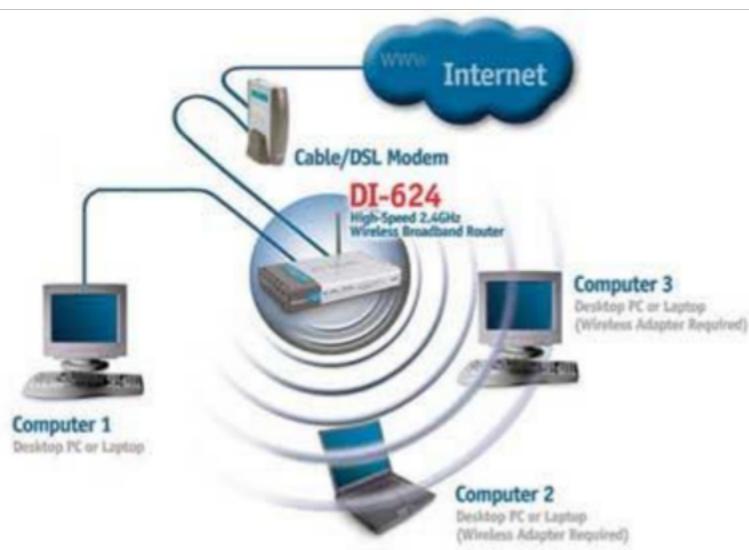
Gambar 9. Hub/ Switch/ Konsentrator

c. 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* 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 output 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 10. Access Point

d. Media Transmisi

1) Twisted Pair

Kabel Twisted Pair merupakan kabel yang terdiri dari kabel yang saling melilit dan warna yang berbeda. Kabel Twisted Pair ini terdiri dari 2 jenis yaitu Shielded Twisted Pair (STP) dan Unshielded Twisted Pair (UTP). Pada kedua jenis Kabel Twisted Pair ini tidak ada perbedaan yang spesifik bedanya kedua kabel ini adalah Shield dan Unshielded. Berikut Penjelasan dari Kabel UTP dan STP :

a) Kabel Unshielded Twister Paid (UTP)

Kabel UTP terdiri dari 8 buah kabel halus yang saling melilit menjadi 4 pasang. Ke empat pasang kabel tersebut adalah :

- Pasangan kabel warna hijau dengan Putih lease Hijau
- Pasangan kabel warna Orange dengan Putih lease Orange
- Pasangan kabel warna Biru dengan Putih lease Biru
- Pasangan kabel warna coklat dengan Putih lease Coklat

Kategori Kabel UTP :

- Cat 1 : Digunakan untuk perangkat komunikasi, seperti kabel telephon.
- Cat 2 : Kecepatan transfer data mencapai 4 Megabits per second.

- Cat 3 : Biasanya digunakan untuk topologi token ring dengan kecepatan transfer data mencapai 10 Mbps.
- Cat 4 : Kecepatan transfer data mencapai 16 Mbps
- Cat 5 : Kecepatan transfer data mencapai 100 Mbps
- Cat 5e : Kecepatan transfer data mencapai 100 Mbps – 1 Gigabits.
- Cat 6 : Kecepatan transfer data hingga 2,5 Gigabit Ethernet dalam jarak 100 Meter atau 10 Gigabits dalam jarak 25 Meter.

Standarisasi Kabel UTP Pemasangan urutan Kabel UTP umumnya mengikuti aturan standart international yaitu EIA/TIA 568A dan EIA/TIA 568B. Untuk urutan EIA/TIA 568A urutan kabel nya adalah sebagai berikut :

- Urutan ke 1 : Putih Hijau
- Urutan ke 2 : Hijau
- Urutan ke 3 : Putih Orange
- Urutan ke 4 : Biru
- Urutan ke 5 : Putih Biru
- Urutan ke 6 : Orange
- Urutan ke 7 : Putih Coklat
- Urutan ke 8 : Coklat

Sedangkan urutan EIA/TIA 568B urutan kabelnya adalah sebagai berikut:

- Urutan ke 1 : Putih Orange
- Urutan ke 2 : Orange
- Urutan ke 3 : Putih Hijau

- Urutan ke 4 : Biru
- Urutan ke 5 : Putih Biru
- Urutan ke 6 : Hijau
- Urutan ke 7 : Putih Coklat
- Urutan ke 8 : Coklat

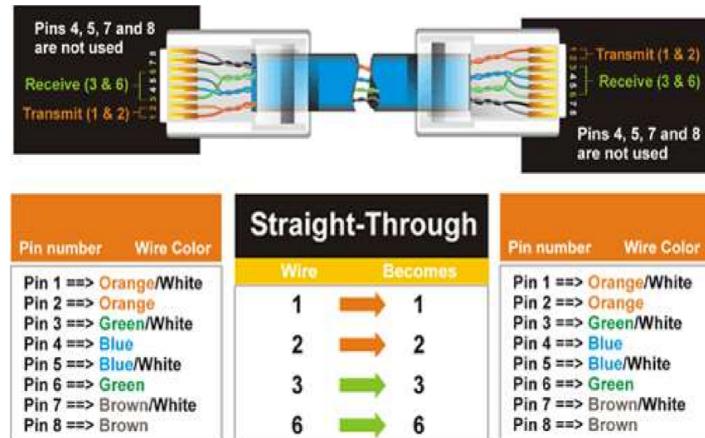
Tipe Pemasangan Kabel UTP Ada 2 jenis tipe pemasangan kabel UTP pada konektor RJ-45 yaitu type straight dan tipe cross.

- Tipe Straight Tipe Straight artinya ujung kabel yang satu dengan ujung kabel yang lainnya memiliki urutan kabel yang sama sesuai dengan standart EIA/TIA 568B. Tipe ini digunakan untuk menghubungkan antara PC ke Switch, Router ke Switch, Router ke Hub dan PC ke Hub.
- Tipe Cross Pada tipe ini ujung kabel yang satu menggunakan urutan standart EIA/TIA 568A dan ujung yang satu nya lagi menggunakan urutan kabel TIS/EIA 568B dan digunakan untuk menghubungkan PC ke PC, Switch/Hub ke Switch/Hub, dan PC ke Router.

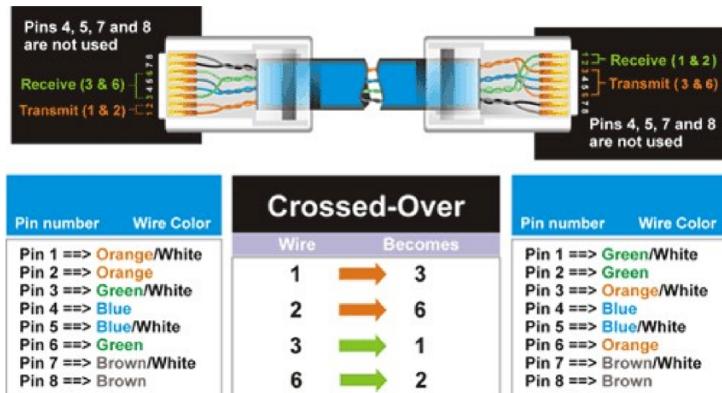
b) Kabel Shielded Twisted Pair (STP)

Kabel Shielded Twisted Pair (STP) sama dengan kabel UTP, tetapi kawatnya lebih besar dan diselubungi dengan lapisan pelindung isolasi untuk mencegah gangguan interferensi. Jenis kabel STP yang paling umum digunakan pada Jaringan LAN Dari 2 Jenis Kabel Twisted Pair tersebut tidak ada perbedaan lain yang spesifik kecuali Shielded dan Unshielded. Semua Warna Kabel, Kategori Kabel

UTP, Standarisasi Kabel, dan Tipe Pemasangan Kabel itu semua sama.



Gambar 11. Koneksi antara NIC dengan Hub/Switch



Gambar 12. Koneksi antara Hub dengan Hub, Switch dengan Switch, dan NIC dengan NIC

2) Fiber Optic

Fiber optic memiliki harga lebih mahal, tetapi cukup tahan terhadap interferensi elektromagnetik dan mampu beroperasi dengan kecepatan tinggi dan kapasitas data yang besar. Tiga jenis konektor yang umum digunakan

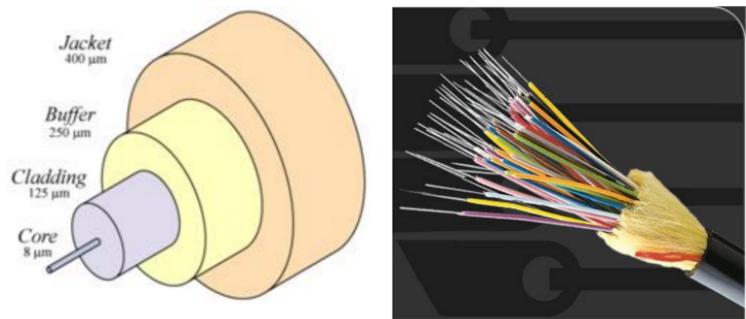
untuk media fiber optik adalah SC, ST, dan MTRJ. Jenis kabel yang satu ini tidak menggunakan tembaga (cooper), melainkan serat optik. Dimana sinyal yang dialirkan berupa berkas cahaya. Mampu mengirimkan bandwidth lebih banyak. Banyak digunakan untuk komunikasi antar *Backbone*, LAN dengan kecepatan tinggi. Jika melihat dekat pada serat optik tunggal, kita 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:

- Single-mode fibers
- 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 $2,5 \times 10^{-3}$ inci 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.

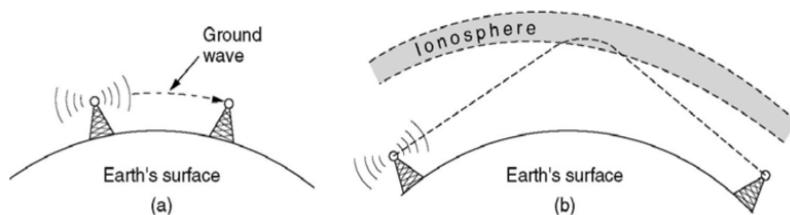


Gambar 13. Fiber Optic

3) Transmisi Radio

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

- Memancarkan langsung, sesuai dengan permukaan bumi
- Dipantulkan melalui lapisan atmosfir



Gambar 14. 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*.



Gambar 15. Perangkat Wireless LAN

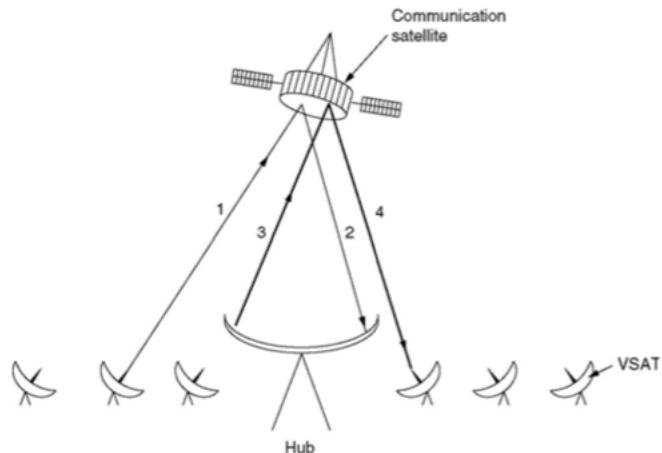
4) Komunikasi Satelit

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. 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 16. Komunikasi satelit dengan VSAT

e. 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 :

1. Mengatur jalur sinyal secara effisien
2. Mengatur Pesan diantara dua buah protocol
3. Mengatur Pesan diantara topologi jaringan linear Bus dan Bintang(star)
4. Mengatur Pesan diantara melewati Kabel Fiber optic, kabel koaksial atau kabel twisted pair



Gambar 17. Router Cisco dan RouterBoard

a.6. Protokol

Protokol merupakan aturan standar yang digunakan dalam komunikasi data yang mengatur tentang *data representation, signalling, authentication, dan error detection*. Dalam penerapannya, digunakan layer untuk membagi tugas sebuah protokol menjadi beberapa sub tugas. Tiap layer mempunyai tugas tersendiri dan mampu berhubungan dengan layer setingkat di atas dan di bawahnya. OSI (*Open System Interconnection*) Model merupakan standar referensi protokol yang banyak digunakan. Model ini membagi protokol menjadi tujuh layer. Karenanya sering pula disebut sebagai OSI seven layer model.

Urutan layer mulai dari yang pertama dalam OSI model adalah physical, data link, network, transport, session, presentation, dan application layer. Masing-masing mempunyai definisi dan tujuan tersendiri. Tiap layer memberikan layanan (service) pada layer yang lebih tinggi dan meminta layanan pada layer yang lebih rendah. Meskipun OSI model menyediakan sebuah protokol ideal untuk dipakai dalam sebuah jaringan, penerapannya sangat rumit, dan seringkali tidak praktis. Meskipun demikian model abstraksi yang

digunakan dalam OSI diterapkan di banyak protokol jaringan lainnya, di antaranya suite TCP/IP dan IPX/SPX.

Dua protokol yang paling banyak digunakan adalah TCP/IP dan IPX/SPX. TCP/IP adalah protokol yang digunakan di Internet, dan sekarang banyak pula digunakan di Local Area Network menggantikan IPX/SPX. Sedangkan protokol IPX/SPX adalah protokol yang pada mulanya digunakan oleh Novell Netware, namun kemudian diadopsi oleh banyak sistem operasi lainnya. IPX/SPX memberikan kemudahan dalam konfigurasi, namun karena kurang praktis apabila dipakai dalam sebuah WAN, maka protokol ini makin lama makin ditinggalkan. Protokol TCP/IP sebenarnya adalah sebuah *protocol suite* (kumpulan dari beberapa protokol jaringan) yang kurang lebih mempunyai hubungan yang mirip dengan OSI model.

Konsep awal TCP/IP berasal dari kebutuhan untuk menggabungkan komputer berbagai jenis dalam satu jaringan. Riset untuk ini dilakukan oleh *Defense Advanced Research Projects Agency* (DARPA), Departemen Pertahanan, Amerika Serikat. TCP/IP pertama kali diimplementasikan oleh DARPA dalam jaringan yang disebut sebagai ARPAnet, yang merupakan awal dari jaringan yang kini dikenal sebagai Internet. Aplikasi-aplikasi TCP/IP biasanya dikembangkan dengan menggunakan beberapa protokol dalam suite TCP/IP.

Keseluruhan *layer* protokol yang ada dalam suite tersebut, biasanya dinamakan sebagai sebuah *protocol stack*. Aplikasi pengguna berkomunikasi dengan layer paling atas yang kemudian akan mengemas data yang disampaikan dan dilalukan ke *layer* di bawahnya. Demikian seterusnya hingga sampai ke *physical layer* di mana data ditransfer dalam jaringan.

a.7. Layering

Dua model yang dapat digunakan untuk menjelaskan mekanisme komunikasi data pada Jaringan Komputer, yaitu model TCP/IP dan model OSI. OSI merupakan sebuah badan multinasional yang didirikan tahun 1947 yang bernama International Standards Organization (ISO) sebagai badan yang melahirkan standar-standar standar internasional. ISO ini mengeluarkan juga standar jaringan komunikasi yang mencakup segala aspek yaitu model OSI (Open System Interconnection).

Tujuan OSI ini adalah untuk membuat standar aturan komunikasi sehingga dapat terjalin interkomunikasi dari sistem yang berbeda tanpa memerlukan perubahan yang signifikan pada hardware dan software. Model OSI adalah suatu dekripsi abstrak mengenai desain lapisan-lapisan komunikasi dan protokol jaringan komputer yang dikembangkan sebagai bagian dari inisiatif Open Systems Interconnection (OSI). Model ini disebut juga dengan model “Tujuh lapisan OSI” (OSI seven layer model).

a. 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 mikrosekon 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.

b. Data-link layer atau Lapisan koneksi data

Tugas utama data link layer adalah sebagai fasilitas transmisi raw data dan mentransformasi data tersebut ke saluran yang bebas dari kesalahan transmisi. Sebelum diteruskan kenetwork 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.

c. 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.

d. 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.

e. Session layer

Session layer mengijinkan 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 kemesin 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.

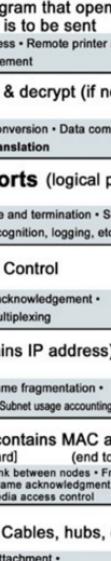
f. Presentation layer

Presentation layer melakukan fungsi-fungsi tertentu yang diminta untuk menjamin penemuan sebuah penyelesaian umum bagi masalah tertentu. Presentation Layer tidak mengijinkan 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 komplemen satu dan komplemen 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 datastruktur abstrak ini dan mengkonversi dari representation

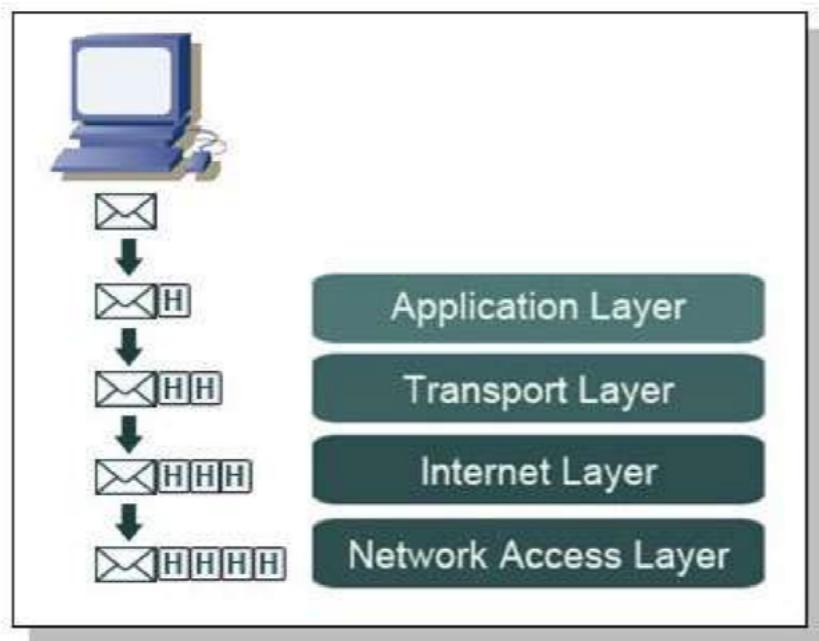
yang digunakan pada sebuah komputer menjadi representation standard jaringan, dan sebaliknya.

g. 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.

OSI (Open Source Interconnection) 7 Layer Model					
Layer	Application/Example		Central Device/Protocols	DOD4 Model	
Application (7) Serves as the window for users and application processes to access the network services.	End User layer Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		User Applications SMTP	GATEWAY 	Process Host to Host Internet Network
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	Syntax layer encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	Synch & send to ports (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		Logical Ports RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	TCP Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	F P A C K E T F I L T E R I N G	TCP/SPX/UDP		
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	Packets ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		Routers IP/IPX/ICMP		
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	Frames ("envelopes", contains MAC address) [NIC card —> Switch —> NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		Switch Bridge WAP PPP/SLIP	Land Based Layers	
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	Physical structure Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		Hub		

Gambar 18. Model OSI



Gambar 19. Model TCP/IP

OSI Model	TCP/IP Model
Application Layer	Application layer
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer
Network Layer	Internet Layer
Data link layer	Link Layer
Physical layer	

Gambar 20. Perbedaan pada OSI dan TCP model

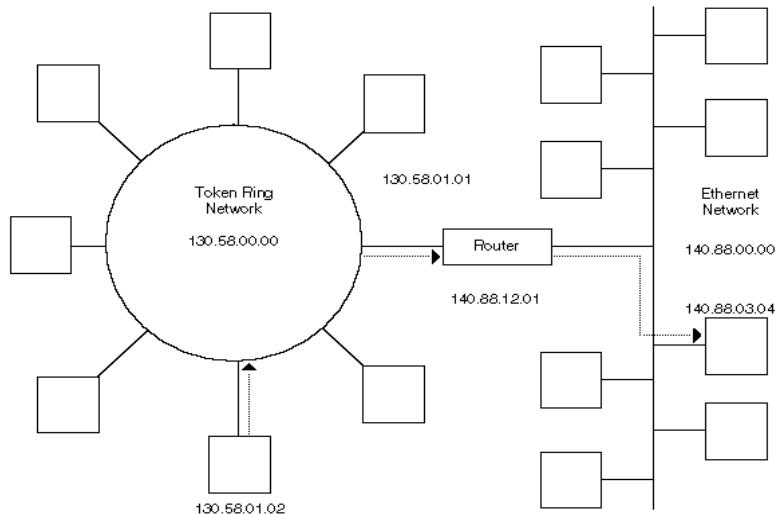
a.8. Routing

Terminologi routing digunakan untuk menggambarkan transmisi sebuah datagram dari komputer asal ke komputer tujuan, dalam sebuah network yang sama, atau beberapa network berbeda. Suatu route adalah jalur transmisi yang dipilih untuk mengirimkan sebuah IP datagram dari komputer asal ke tujuan, berdasarkan IP address komputer tujuan.

Dalam sebuah jaringan, sebuah komputer mengirimkan sebuah IP datagram bisa melakukan aksi sebagai berikut:

- a. Melakukan query ke semua perangkat dalam satu network untuk mengetahui physical address dari sebuah IP address.
- b. Melakukan enkapsulasi IP datagram dalam *physical frame* yang berisi physical address yang telah didapatkan
- c. Mengirimkan IP datagram yang telah dienkapsulasi langsung ke tujuan yang ditunjukkan oleh *physical address* tersebut dalam sebuah jaringan.

Apabila sebuah datagram dikirimkan ke sebuah node yang terdapat di jaringan yang berbeda, porsi network dari *IP address* asal, dan tujuan akan berbeda. Pengirim akan langsung mengatahui perbedaan ini dan mengirimkan paket ke sebuah router yang menghubungkan jaringan di mana pengirim berada ke jaringan lainnya. Dua buah jaringan atau lebih bisa dihubungkan dengan satu router asalkan router tersebut terhubung ke semua jaringan tersebut, dan bisa melalukan data dalam bentuk yang kompatibel dengan tipe jaringan-jaringan tersebut.



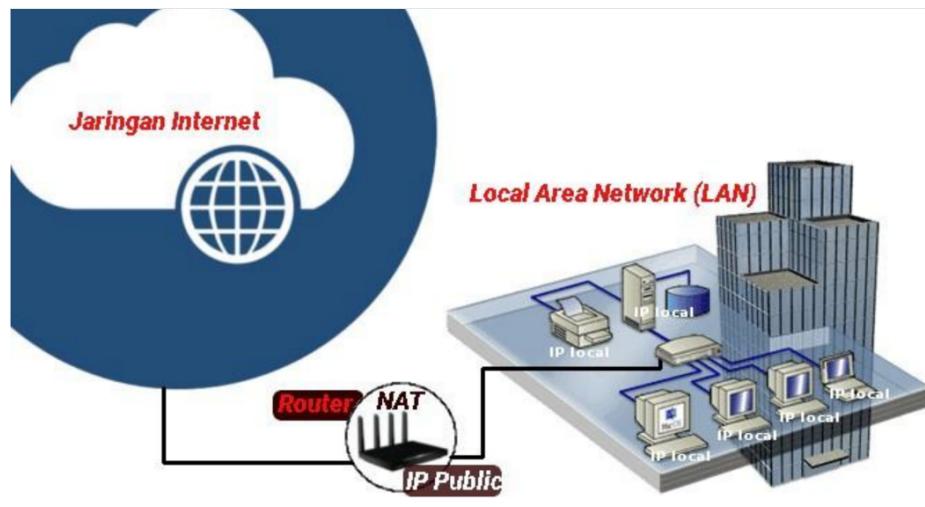
Gambar 21. Sebuah router menghubungkan dua tipe jaringan yang berbeda

Pengirim mempunyai satu tabel yang berisi satu atau lebih perangkat dalam jaringan yang sama yang berfungsi sebagai router ke jaringan yang lain. Pada saat proses pengiriman, komputer asal mengirimkan permintaan ARP ke router untuk mengetahui physical address dari router tersebut. Pengirim kemudian mengirimkan paket ke physical address dari router tersebut. Pada saat router menerima *IP datagram* tersebut, router akan menggunakan IP address tujuan yang terdapat dalam datagram untuk mengirimkan ke tujuan dengan proses yang sama seperti si pengirim mengirimkan ke router. Apabila ternyata tujuan berada di jaringan yang lain, maka router akan mengirimkan datagram ke router selanjutnya, demikian seterusnya hingga tujuan tercapai.

a.9. IP Addressing

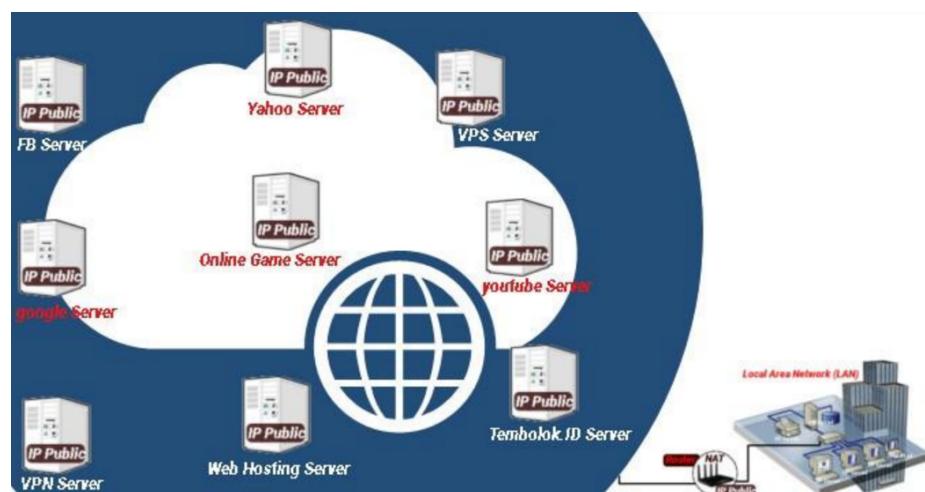
IP Address adalah protokol yang memberikan alamat atau identitas untuk peralatan di dalam jaringan . IP Address ada yang disebut sebagai IP Private dan IP Publik.

- IP Private adalah IP yang hanya bisa diakses dari jaringan lokal saja dan tidak bisa diakses melalui jaringan internet secara langsung tanpa bantuan router (NAT). IP private digunakan untuk jaringan lokal (LAN) agar sesama komputer dapat saling berkomunikasi.

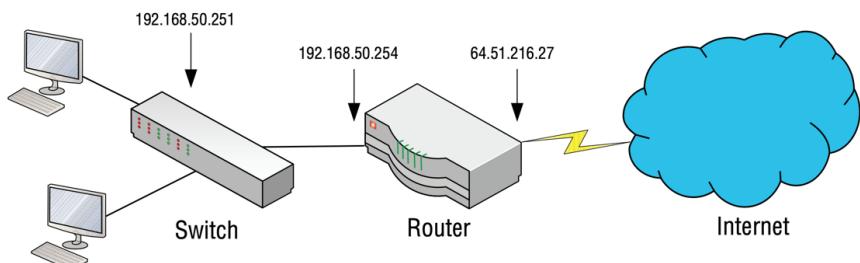


Gambar 22. IP Private

- IP Publik, adalah IP yang digunakan dalam jaringan global Internet. Karena kelas IP ini digunakan di dalam jaringan internet, maka IP ini bisa diakses melalui jaringan internet secara langsung. Perangkat yang menggunakan IP publik biasanya adalah server atau router



Gambar 23. IP Public



Gambar 24. Contoh penggunaan NAT pada IP private

IP address terdiri dari bilangan biner 32 bit yang dipisahkan oleh tanda titik setiap 8 bitnya. Tiap bit ini disebut sebagai octet. Bentuk IP address dapat dituliskan sebagai berikut:

xxxxxxxx.xxxxxxxx.xxxxxxxx

Jadi, IP address memiliki range dari

00000000.00000000.00000000.00000000

sampai

11111111.11111111.11111111.11111111.

Notasi IP address dengan bilangan biner seperti ini susah digunakan untuk digunakan, sehingga sering ditulis dalam 4 bilangan decimal yang masing-masing dipisahkan oleh 4 buah titik yang lebih dikenal dengan ‘notasi decimal bertitik’. Setiap bilangan decimal merupakan nilai dari satu oktet IP address. Contoh hubungan IP address dalam format biner dan decimal:

Tabel 2. Desimal dan Biner IP Address 167.205.206.100

Desimal	167	205	206	100
Biner	10100111	11001101	11001110	01100100

a. 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*. Subnet mask diperlukan oleh TCP/IP untuk menentukan, apakah jaringan yang dimaksud adalah jaringan lokal atau non lokal. Untuk jaringan non lokal 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.

Tabel 3. Perhitungan 2 pangkat N

Class	Subnet Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

b. Kelas IP Address

Jumlah IP address yang tersedia secara teoritis adalah $255 \times 255 \times 255 \times 255$ atau sekitar 4 miliar lebih yang harus dibagikan ke seluruh pengguna jaringan internet di seluruh dunia. Pembagian kelas-kelas ini ditujukan untuk mempermudah alokasi IP address, baik untuk host jaringan tertentu atau untuk keperluan tertentu. IP address dipisahkan menjadi 2 bagian yaitu bagian network (net ID) dan bagian host (host ID).

Net ID berperan dalam identifikasi suatu network dari network yang lain, sedangkan host ID berperan untuk identifikasi host dalam suatu network. Jadi seluruh host yang tersambung dalam jaringan yang sama memiliki net ID yang sama. Sebagian dari bit-bit bagian awal pada bagian awal address merupakan network bit/network

number, sedangkan sisanya untuk host. Garis pemisah antara bagian network dan host tidak tetap, bergantung kepada kelas network.

IP address dibagi ke dalam lima kelas yaitu kelas A, B, C, D, E. perbedaan tiap kelas adalah pada ukuran dan jumlahnya. Contohnya IP kelas A dipakai oleh sedikit jaringan namun jumlah host yang dapat ditampung oleh tiap jaringan sangat besar. Kelas D dan E tidak digunakan secara umum kelas D digunakan bagi jaringan multicast dan kelas E untuk keperluan eksperimental. Perangkat lunak Internet protocol menentukan pembagian jenis kelas ini dengan menguji beberapa bit pertama dari IP address

- **IP Address Kelas A**, merupakan IP address dengan jumlah yang sangat besar, sehingga biasanya digunakan untuk jaringan yang sangat besar dengan jumlah host yang sangat banyak. Sebagai contoh pada penggunaan IP address : 113.46.5.6 , 113 berfungsi sebagai network ID sedangkan 46.5.6 berfungsi sebagai host ID nya.
- **IP Address Kelas B**, merupakan IP address dengan jumlah host yang sedang, jumlah maksimal host berkisar 65.534 host, sehingga IP ini cocok untuk jaringan dengan jumlah host yang tidak terlalu besar dan tidak terlalu kecil. Sebagai contoh penggunaan IP address Kelas B adalah : 132.92.121.1 , 132.92 berfungsi sebagai network ID sedangkan 121.1 berfungsi sebagai host ID.
- **IP Address Kelas C**, merupakan IP address dengan jumlah host yang sangat kecil sehingga IP address ini digunakan untuk jaringan kecil seperti disekolah-sekolah, dikantor-kantor maupun instansi rumahan, jumlah maksimal host pada IP address ini hanya 254 host. Sebagai contoh penggunaan IP

Address Kelas C adalah : 192.168.1.2, 192.168.1 merupakan network ID dan 2 merupakan host ID-nya

- **IP Address Kelas**, disediakan hanya untuk alamat-alamat IP multicast, namun berbeda dengan tiga kelas di atas. Empat bit pertama di dalam IP kelas D selalu diset ke bilangan biner 1110. 28 bit sisanya digunakan sebagai alamat yang dapat digunakan untuk mengenali host.
- Alamat IP kelas E disediakan sebagai alamat yang bersifat eksperimental atau percobaan dan dicadangkan. Empat bit pertama selalu diset kepada bilangan biner 1111. 28 bit sisanya digunakan sebagai alamat yang dapat digunakan untuk mengenali host.

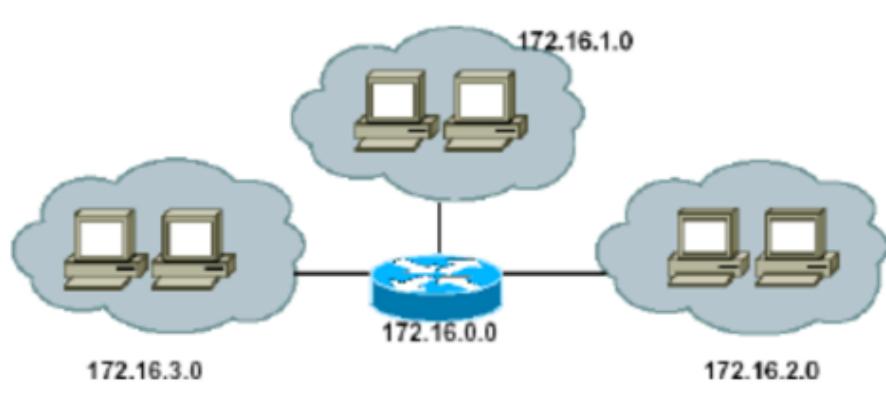
c. Subnetting

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 tablenya 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 diAND 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.



Gambar 25. Sebuah Jaringan di bagi menjadi 3

Tujuan Subnetting :

- 1) Membagi satu jaringan menjadi beberapa beberapa sub-jaringan atau jaringan yang lebih kecil.
- 2) Menempatkan suatu host apakah berada dalam satu jaringan atau tidak.
- 3) Mengatasi masalah pada perbedaan perangkat keras (*hardware*) dengan topologi jaringan yang digunakan.

- 4) Membuat penggunaan dari *IP Address* menjadi lebih efisien atau efektif.

Fungsi Subnetting :

- 1) Mengurangi *traffic* atau lalu lintas jaringan, sehingga data yang lewat atau sedang ditransfer tidak akan bertabrakan (*collision*).
- 2) Kinerja jaringan yang lebih optimalkan.
- 3) Membuat pengelolaan jaringan lebih sederhana.
- 4) Membantu pengembangan jaringan ke arah yang cenderung menjauh dari area jaringan itu sendiri.

Ada 2 cara untuk menghitung subnetting, yaitu dengan menggunakan CIDR dan VLSM.

- a. CIDR (*Classless Inter-Domain Routing*).

Classless Inter-Domain Routing (CIDR) adalah sebuah cara alternatif untuk mengklasifikasikan alamat-alamat IP berbeda dengan sistem klasifikasi ke dalam kelas A, kelas B, kelas C, kelas D, dan kelas E. Disebut juga sebagai supernetting. CIDR merupakan mekanisme routing dengan membagi alamat IP jaringan ke dalam kelaskelas A, B, dan C. CIDR digunakan untuk mempermudah penulisan notasi subnet mask agar lebih ringkas dibandingkan penulisan notasi subnet mask yang sesungguhnya. Untuk penggunaan notasi alamat CIDR pada classfull address pada kelas A adalah /8 sampai dengan /15, kelas B adalah /16 sampai dengan /23, dan kelas C adalah /24 sampai dengan /28. Subnet mask CIDR /31 dan /32 tidak pernah ada dalam jaringan yang nyata

- b. VLSM (*Variable Length Subnet Mask*)

Perhitungan IP Address menggunakan metode VLSM adalah metode yang berbeda dengan memberikan suatu *Network*

Address lebih dari satu subnetmask, berbeda jika menggunakan CIDR dimana suatu Network ID hanya memiliki satu subnetmask saja. VLSM memiliki manfaat untuk mengurangi jumlah alamat yang terbuang. Pada metode VLSM subnetting yang digunakan berdasarkan jumlah host, sehingga akan semakin banyak jaringan yang akan dipisahkan. Tahapan perhitungan menggunakan VLSM IP Address yang ada dihitung menggunakan CIDR selanjutnya baru dipecah kembali menggunakan VLSM. Maka setelah dilakukan perhitungan maka dapat dilihat subnet yang telah dipecah maka akan menjadi beberapa subnet lagi dengan mengganti subnetnya.

Manfaat VLSM:

- Efisien menggunakan alamat IP karena alamat IP yang dialokasikan sesuai dengan kebutuhan ruang host setiap subnet.
- VLSM mendukung hirarkis menangani desain sehingga dapat secara efektif mendukung rute agregasi, juga disebut route summarization.
- Berhasil mengurangi jumlah rute di routing table oleh berbagai jaringan subnets dalam satu ringkasan alamat. Misalnya subnets 192.168.10.0/24, 192.168.11.0/24 dan 192.168.12.0/24 semua akan dapat diringkas menjadi 192.168.8.0/21.

b. Analisis kebutuhan pengguna

Kebutuhan pengguna harus dilakukan dengan berbagai pertimbangan. Dalam menganalisis kebutuhan pengguna, ada beberapa hal yang harus di perhatikan, diantaranya adalah jumlah pengguna dalam satu LAN, media transmisinya, besaran bandwithnya.

1. Menghitung jumlah pengguna (*device*)

Menghitung jumlah pengguna untuk memaksimalkan client dalam blok IP Address perlu kiranya kita ketahui terlebih dahulu tentang prefix number. Prefix number adalah angka yang digunakan untuk mewakili subnet mask sebuah Blok IP Address. Biasanya prefix number ditulis setelah IP Address dan setelah tanda '/'.

contoh:

192.168.1.100/24 prefix numbernya adalah 24

10.10.10.23/18 prefix numbernya adalah 18

172.16.30.25/27 prefix numbernya adalah 27

Konversi Prefix Number Menjadi Subnet Mask

IP Address v4 memiliki 4 oktet dan tiap oktet memiliki 8 bit biner.

Sehingga total bit pada sebuah IP Address v4 adalah 32 bit biner.

Untuk lebih jelasnya lihat tabel berikut:

Tabel 4. IP Address 192.168.1.254

IP Address	192	168	1	254
	Oktet 1	Oktet 2	Oktet 3	Oktet 4
BINARY	11000000	10101000	00000001	11111110
BANYAK BIT PER OKTET	8 Buah	8 Buah	8 Buah	8 Buah

Seperti halnya IP Address, Subnet mask pun memiliki 4 buah oktet dan 8 bit biner per oktetnya. Sehingga jumlah bit biner Subnet Mask juga adalah 32.

Hubungan antara prefix number dan subnet mask adalah prefix number mewakili jumlah angka biner 1 pada 32 bit biner subnet mask. Sebagai contoh jika prefix yang diberikan adalah /24 maka binary subnetnya adalah:

Tabel 5. Prefix Number : /24

11111111 11111111 11111111	00000000
Total angka biner 1 ada 24 buah	Bit 25 sampai 32 ditulis dengan angka 0

Jika prefixnya /25

maka binary

subnetnya: 11111111.11111111.11111111.10000000

dan seterusnya.

Setelah itu kita ubah binary per oktet tersebut menjadi bilangan desimal. Misalkan disebuah perusahaan terdapat 200 komputer (host). Tanpa menggunakan subnetting maka semua komputer (host) tersebut dapat kita hubungkan kedalam sebuah jaringan tunggal dengan perincian sebagai berikut: Misal kita gunakan *IP Address Private* kelas C dengan subnet mask defaultnya yaitu 255.255.255.0 sehingga perinciannya sebagai berikut:

Network Perusahaan

Alamat Jaringan : 192.168.1.0

Host Pertama : 192.168.1.1

Host Terakhir : 192.168.1.254

Broadcast Address : 192.168.1.255

Misalkan diperusahaan tersebut terdapat 2 divisi yang berbeda sehingga kita akan memecah network tersebut menjadi 2 buah subnetwork, maka dengan teknik subnetting kita akan menggunakan subnet mask 255.255.255.128 (nilai subnet mask ini berbeda-beda tergantung berapa subnetwork yang akan kita buat) sehingga akan menghasilkan 2 buah blok subnet, dengan perincian sebagai berikut:

Network Divisi A

Alamat Jaringan / Subnet A : 192.168.1.0

Host Pertama : 192.168.1.1

Host Terakhir : 192.168.1.126

Broadcast Address : 192.168.1.127

Network Divisi B

Alamat Jaringan / Subnet B : 192.168.1.128

Host Pertama : 192.168.1.129

Host Terakhir : 192.168.1.254

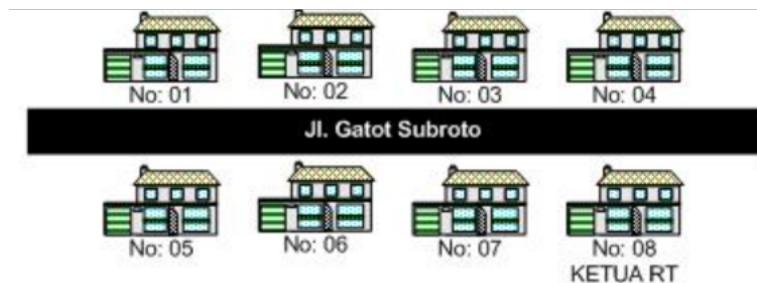
Broadcast Address : 192.168.1.255

Dengan demikian dengan teknik subnetting akan terdapat 2 buah subnetwork yang masing-masing network maksimal terdiri dari 125 host (komputer). Masing-masing komputer dari subnetwork yang berbeda tidak akan bisa saling berkomunikasi sehingga meningkatkan security dan mengurangi terjadinya kongesti. Apabila dikehendaki agar beberapa komputer dari network yang berbeda tersebut dapat saling berkomunikasi maka kita harus menggunakan Router.

2. Kebutuhan keamanan (pemisahan segmen)

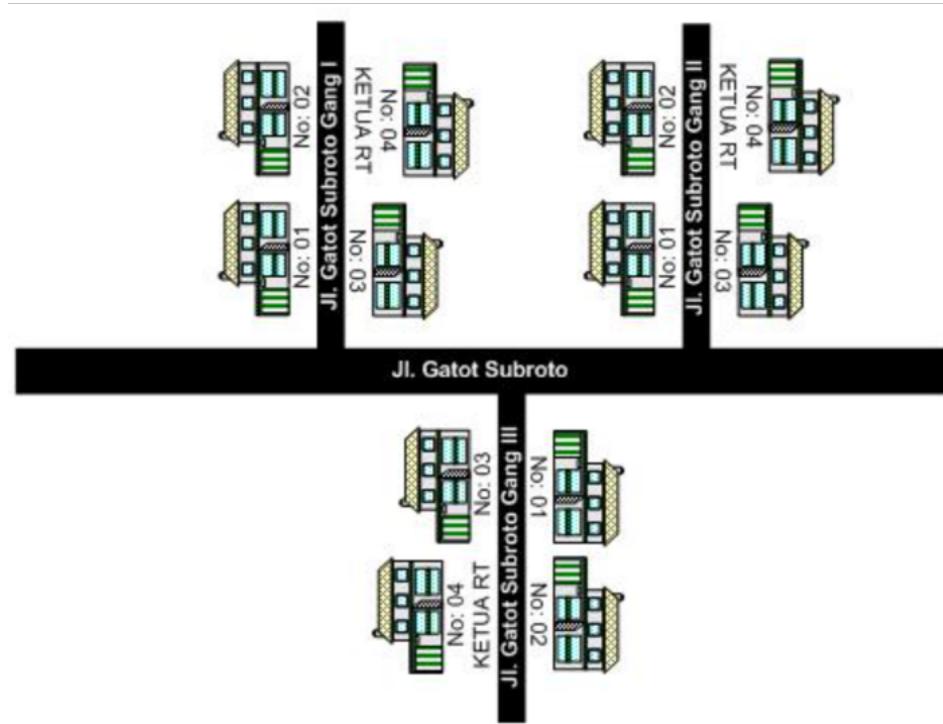
Keamanan dalam jaringan komputer sangat penting dilakukan, proses pemisahan segmen jaringan menjadi solusi yang dapat di diterapkan pada jaringan computer. Analoginya adalah sebuah jalan. Ada sebuah jalan bernama Gatot Subroto terdiri dari beberapa rumah bernomor 01-08, dengan rumah nomor 08 adalah

rumah Ketua RT yang memiliki tugas mengumumkan informasi apapun kepada seluruh rumah di wilayah Jl. Gatot Subroto.



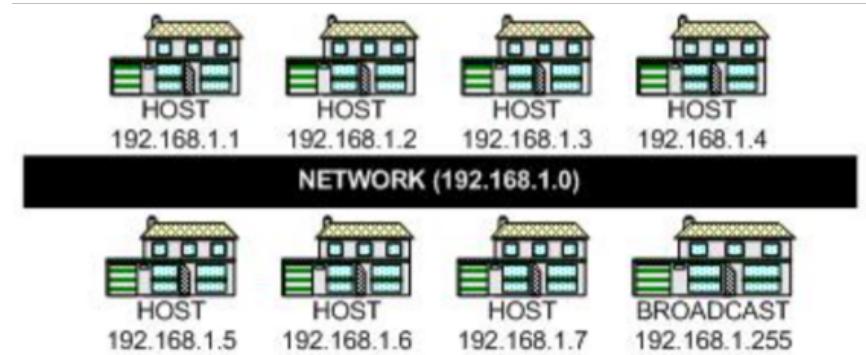
Gambar 26. Analogi Jalan pada jaringan

Ketika rumah di wilayah itu makin banyak, tentu kemungkinan menimbulkan keruwetan dan kemacetan. Karena itulah kemudian diadakan pengaturan lagi, dibuat gang-gang, rumah yang masuk ke gang diberi nomor rumah baru, masing-masing gang ada Ketua RTnya sendiri-sendiri. Sehingga ini akan memecahkan kemacetan, efisiensi dan optimalisasi transportasi, serta setiap gang memiliki privilege sendirisendiri dalam mengelola wilayahnya. Jadilah gambar wilayah baru seperti di bawah:



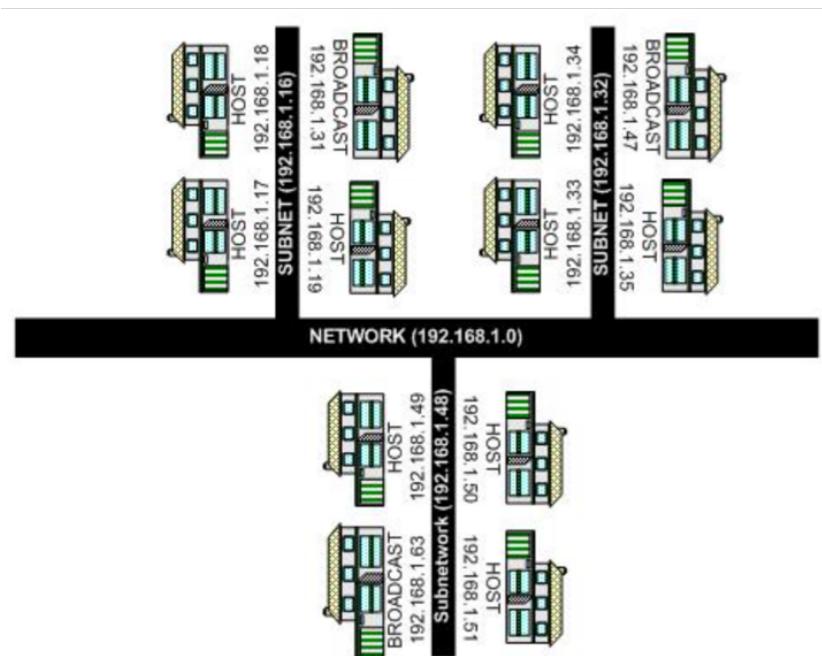
Gambar 27. Analogi memesah jalan

Konsep seperti inilah sebenarnya konsep subnetting itu. Disatu sisi ingin mempermudah pengelolaan, misalnya suatu kantor ingin membagi kerja menjadi 3 divisi dengan masing-masing divisi memiliki 15 komputer (host). Disisi lain juga untuk optimalisasi dan efisiensi kerja jaringan, karena jalur lalu lintas tidak terpusat di satu network besar, tapi terbagi ke beberapa ruas-ruas gang. Yang pertama analogi Jl Gatot Subroto dengan rumah disekitarnya dapat diterapkan untuk jaringan adalah seperti NETWORK ADDRESS (nama jalan) dan HOST ADDRESS (nomer rumah). Sedangkan Ketua RT diperankan oleh BROADCAST ADDRESS (192.168.1.255), yang bertugas mengirimkan message ke semua host yang ada di network tersebut.



Gambar 28. Network, Hots dan Broadcast address

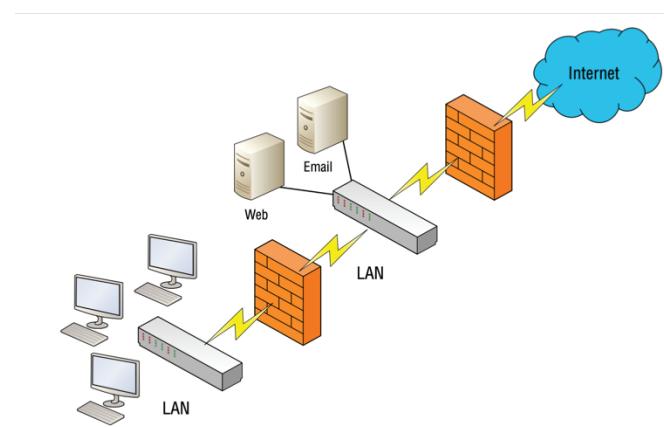
Masih mengikuti analogi jalan diatas, kita terapkan ke subnetting jaringan adalah seperti gambar di bawah. Gang adalah SUBNET, masing-masing subnet memiliki HOST ADDRESS dan BROADCAST ADDRESS.



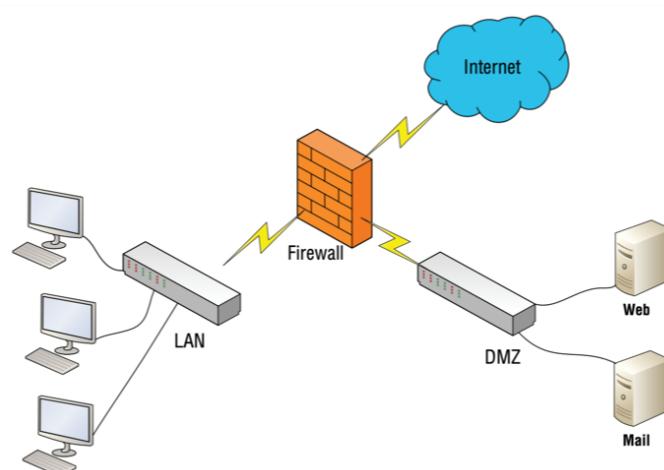
Gambar 29. Network, Hots dan Broadcast address yang sudah di segmen

3. Kebutuhan Jaringan Komputer.

Analisa kebutuhan jaringan adalah penguraian dari suatu jaringan yang akan digunakan, dengan maksud untuk mengidentifikasi, sehingga dapat diusulkan perbaikan maupun pengembangan pada jaringan tersebut. Hal-hal yang harus dijabarkan dalam kebutuhan jaringan adalah, jumlah client yang ada dan pengembangannya, topologi jaringan, arsitektur jaringan, skema jaringan, keamanan pada jaringan, Spesifikasi Hardware dan Software Jaringan. Keamanan pada jaringan juga bisa menerapkan konfigurasi DMZ



Gambar 30. Back-to back DMZ konfigurasi



Gambar 31. Perimeter 3 kaki konfigurasi DMZ

c. Analisis sistem berjalan

Analisa system jaringan yang berjalan adalah penguraian dari suatu jaringan yang sudah digunakan, dengan maksud untuk mengidentifikasi dan mengevaluasi permasalahan, hambatan yang terjadi dan kebutuhan yang diharapkan, sehingga dapat diusulkan perbaikan maupun pengembangan pada jaringan tersebut. Pada bagian ini, akan mengalisa dan memonitoring jaringan yang sudah digunakan.

Misalnya pada PT. X merupakan perusahaan yang aktif menggunakan jaringan internet setiap harinya agar mempermudah aktifitas perusahaan, yang didalamnya terdapat beberapa komputer yang saling terhubung satu dengan yang lainnya, serta memiliki suatu komputer yang dijadikan sebagai server. Server tersebut akan terhubung pada jaringan internet publik yang disediakan oleh ISP (*Internet Service Provider*), sehingga komputer lainnya yang terhubung dengan komputer server atau disebut *client* dapat terhubung secara bersamaan ke jaringan internet publik/ISP.

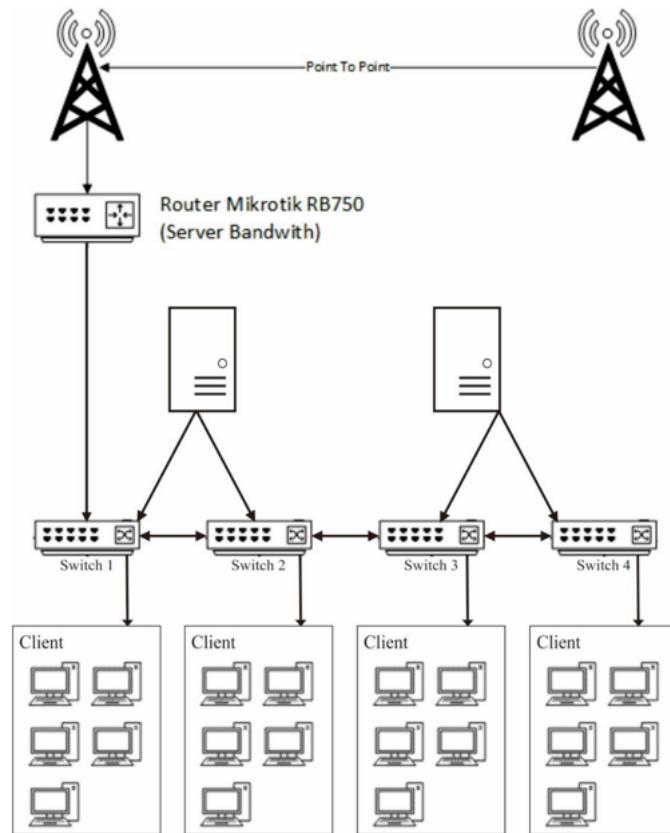
PT. X memiliki 4 lantai disetiap lantai memiliki 5 komputer yang digunakan sebagai client dan memiliki 1 komputer digunakan sebagai server. Untuk menghubungkan seluruh komputer dan perangkat lainnya, pemilik menggunakan media kabel UTP yang dihubungkan ke tower sebagai penangkap sinyal dari ISP (*Internet Service Provider*) Nusanet dengan menggunakan metode *Point To Point*. Kemudian sinyal dari tower akan dihubungkan ke router Mikrotik RB750 yang digunakan untuk memanajemen *bandwith* pada komputer *client*, dan dari router Mikrotik tersebut akan dihubungkan ke HUB/Switch yang digunakan sebagai media penghubung ke komputer *client*. *Server diskless* akan digunakan sebagai media penyimpanan bagi komputer client berupa file-file dan sistem operasi yang digunakan oleh

komputer *client*, sehingga pada komputer *client* tidak memerlukan media penyimpanan didalamnya.

Saat ini jaringan internet di PT. X masih dapat digunakan secara bebas oleh seluruh karyawan dan tanpa batasan akses. Hal ini mengakibatkan kualitas jaringan internet menjadi lambat, karena sering kali digunakan oleh karyawan tidak untuk aktifitas kerja, melainkan membuka sosial media, toko online, download film atau lagu dan kegiatan tidak produktif lainnya

a. Topologi Jaringan

Topologi jaringan komputer yang digunakan pada PT. X adalah topologi BUS, karena dengan menggunakan topologi BUS perusahaan ini dapat mengurangi biaya instalasi jaringan dan dapat juga meminimalisir permasalah yang akan terjadi pada jaringan perusahaan tersebut.



Gambar 32. Topologi Jaringan PT. X

b. Analisis permasalahan

Adapun permasalahan yang dapat penulis ambil adalah sebagai berikut :

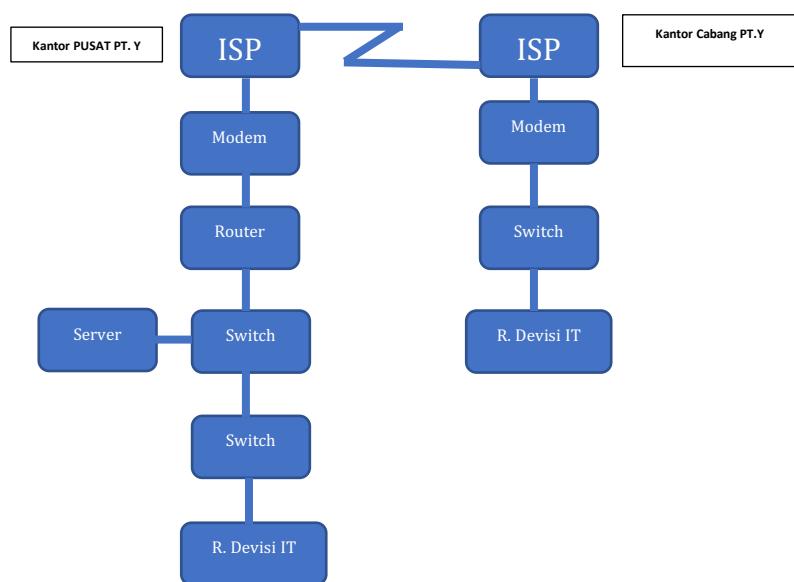
- 1) PT. X saat ini masih menggunakan jaringan LAN, yang perangkat keras jaringannya cukup banyak sehingga sulit untuk memonitoring secara manual sehingga dibutuhkan monitoring secara otomatis.
 - 2) Dengan adanya monitoring jaringan sehingga mengurangi budget yang cukup besar dalam penanganan jaringan.

c. Usulan Monitoring Perancangan Jaringan

memonitoring jaringan pada PT. X dibutuhkan aplikasi yang bernama *The Dude*, aplikasi ini dikenal merupakan sebuah aplikasi yang lengkap. Selain bisa monitoring jaringan dalam bentuk MAP, notifikasi perubahan status perangkat, juga tersedia *tool* seperti

SSH, Telnet, Webfig yang dapat melakukan secara langsung remote akses ke perangkat. Nantinya jaringan PT. X akan terpantau dengan menggunakan aplikasi *The Dude*, sehingga semua *device* jaringan akan terselesaikan sebelum rusak parah.

Contoh analisis system berjalan lainnya misalnya, PT.Y mempunya blok diagram jaringan. Blok diagram jaringan adalah gambaran jaringan komputer yang ada pada PT. Y.



Gambar 33. Blok Diagram PT.Y

a. Topologi

PT.Y terdapat satu buah server yang berfungsi untuk melayani, membatasi, dan mengontrol akses terhadap client-client dan sumber daya pada suatu jaringan computer. Pada jaringan terdapat Router, Pada setiap router dihubungkan kabel Fiber Optic melalui jaringan kabel didalam tanah. Internet Service Provider yang digunakan adalah ISP Telkom Speedy. Dalam setiap jaringan terdapat satu modem dan satu switch. Dari gambar jaringan, Topologi yang digunakan adalah Topologi Star.

b. Arsitektur Jaringan

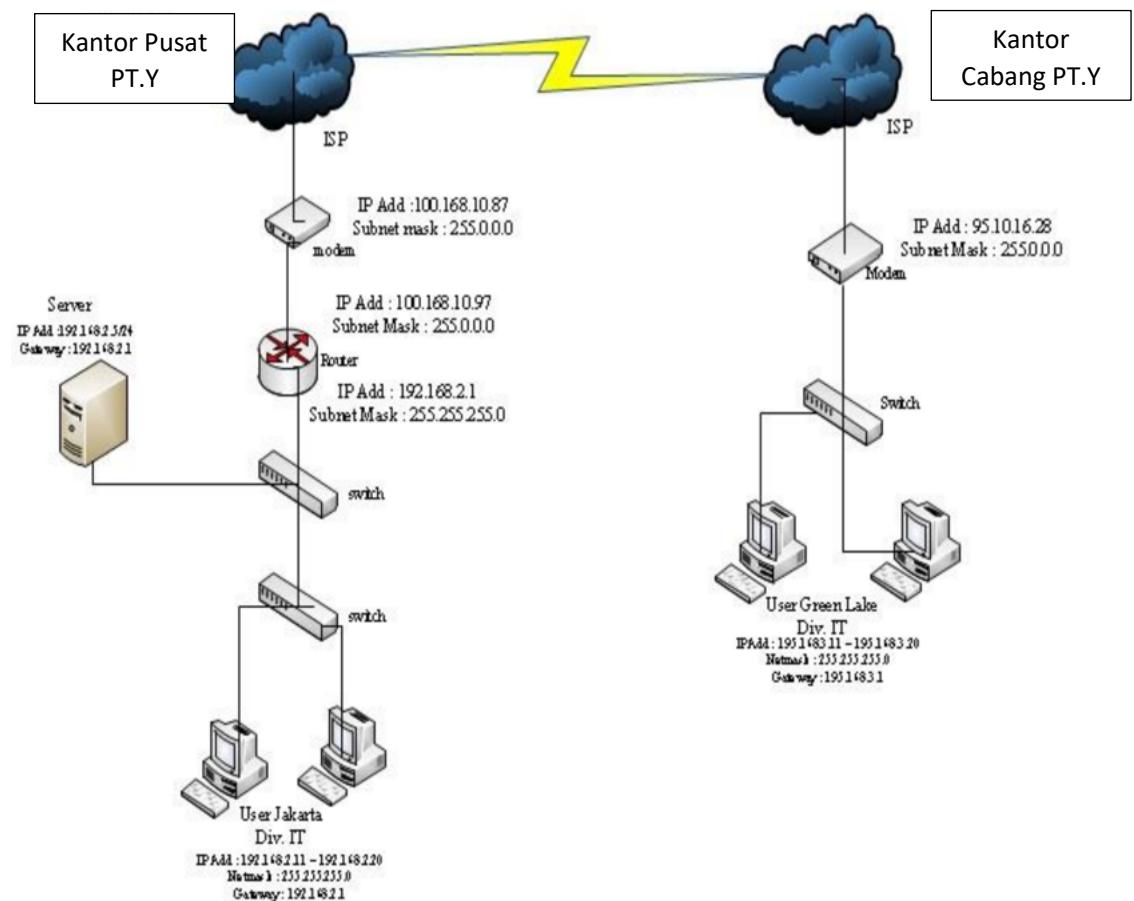
Arsitektur jaringan VPN yang di buat menggunakan metode PPTP yaitu protokol jaringan yang memungkinkan pengamanan transfer data dari remote client (client yang berada jauh dari server) ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP. Teknologi jaringan PPTP merupakan pengembangan dari remote access Point-to-Point protocol. PPTP merupakan protokol jaringan yang merubah paket PPP menjadi IP datagram agar dapat ditransmisikan melalui intenet. Berikut IP Address yang digunakan

Tabel 6. IP Address PT. Y

PERANGKAT	PORT	ALAMAT IP	KETERANGAN	RANGE IP
Modem Pusat	Eth 1	36.69.Y.Z	IP Publik	
Modem Cabang	Eth 1	26.18.Y.Z	IP Publik	
Mikrotik Pusat	Eth 1	36.69.Y.Z	IP Publik	
	Eth 2	192.168.2.1	IP Statik	
Switch 1 Pusat	Eth 1	192.168.2.2	IP Statik	192.168.2.2 – 192.168.2.8
	Eth 2	192.168.2.1	IP Statik	
Switch 2 Pusat	Eth 1	192.168.2.2	IP Statik	192.168.2.2 – 192.168.20
Swicth Cabang	Eth 1	192.168.3.1	IP Statik	192.168.3.1 – 192.168.3.20

c. Skema Jaringan

Skema Jaringan yang dimaksud adalah penjabaran detail dari blok diagram jaringan yang ada.



Gambar 34. Skema jaringan PT. Y

d. Keamanan Jaringan

Untuk Masalah Keamanan jaringan, PT.Y mengamankan jaringan yang terhubung ke Publik menggunakan fasilitas firewall DMZ dan untuk mengamankan dari virus, antivirus yang dipakai pada server dan client menggunakan antivirus clamAV dan smadav

e. Spesifikasi Hardware dan Software Jaringan

- Spesifikasi Hardware dan Software

Sebuah jaringan komputer memiliki perangkat keras karena komponen ini sangat penting untuk menunjang kinerja kerja dari jaringan tersebut, terutama pada server. Adapun perangkat keras yang digunakan pada PT.Y adalah:

- ❖ *Personal computer (PC)*

Personal computer adalah komputer yang diciptakan khusus untuk digunakan oleh perorangan untuk memenuhi kebutuhan seseorang pada sebuah sistem yang mampu untuk membantu mempermudah pekerjaannya. Berikut spesifikasi komputer client pada PT.Y :

Spesifikasi PC

Peripheral	Spesifikasi
Monitor	Lenovo 19"
Processor	Intel Core I7 3,5 Ghz
RAM	16 GB
VGA	Interl HD Graphics (integrated)
Harddisk	Seagete SSD 1 Tb
Optical Drive	Lenovo DVD
Keyboard dan Mouse	Lenovo
Operating System	Windows 10 64 bit

❖ *Server*

adalah komputer yang berfungsi untuk melayani, membatasi, dan mengontrol akses terhadap client-client dan sumber daya pada suatu jaringan komputer. Server didukung spesifikasi/kemampuan hardware yang besar (berbeda dengan komputer biasa), server juga menggunakan sistem operasi khusus, yang disebut sebagai sistem operasi jaringan.

Spesifikasi Server

Peripheral	Spesifikasi
Monitor	Lenovo 19"

Processor	One 2nd or 3rd Generation AMD EPYC™ Processor with up to 64 cores
RAM	64 GB
VGA	Interl HD Graphics (integrated)
Harddisk	Seagete SSD 16 Tb
Optical Drive	Lenovo DVD
Keyboard and Mouse	Lenovo
Operating System	Windows 10 64 bit

❖ *Router*

adalah perangkat network yang digunakan untuk menghubungkan beberapa network, baik network yang sama maupun berbeda dari segi teknologinya seperti menghubungkan network yang menggunakan topologi Bus, Star and Ring. Pada PT. Yi menggunakan router Mikrotik RB750G.

Spesifikasi Router

Peripheral	Spesifikasi
Merk	Mikrotik RouterOS RB750G
Processor	AR7161 680/800 MHz
RAM	64 GB
Port	5
Memory	32 Mb DDR SDRAM
Operating System	Mikrotik RouterOS v3, Level 4 License

❖ *Switch*

adalah perangkat jaringan komputer yang bekerja di OSI Layer 2, Data *Link Layer*. Switch kerjanya sebagai penyambung atau concentrator dalam Jaringan komputer. Switch mengenal *MAC Addressing* sehingga dia bisa memilah paket data mana yang akan di teruskan/dilanjutkan ke mana. Salah satu switch yang digunakan pada PT. Y adalah switch Allied Telesis, switch D-Link, dan Switch 3com.



Gambar 35. Switch

f. Permasalahan

Analisa permasalahan yang ada pada PT.Y adalah :

- 1) Pengiriman data dari kantor cabang ke kantor pusat atau sebaliknya, masih menggunakan pengiriman email yang masih rentan keamanannya.
- 2) Pengiriman data dari kantor cabang ke kantor pusat atau sebaliknya, masih belum terenkripsi yang mengakibatkan data bisa dilihat atau diambil oleh orang yang tidak berkepentigan dan kerahasiaan perusahaan bisa terancam.
- 3) Belum tersediannya koneksi jaringan ke kantor pusat bagi mobile user untuk mengakses maupun mengirimkan data ketika berada diluar kantor atau di luar kota.

- 4) Belum adanya teknologi internet yang dipisahkan secara khusus tanpa dapat diakses oleh orang yang tidak berkepentingan.
- g. Alternatif pemecahan masalah
- Hasil pengamatan tentang permasalahan jaringan komputer Wide Area Network (WAN) yang kerap terjadi di PT. Y, dapat memberikan sedikit pemecahan masalah untuk mengurangi masalah tersebut, yaitu dengan cara :
- 1) Pemanfaatan internet untuk pengiriman data atau pengambilan data dan keefektifitasnya dalam masalah keamanan data disini penulis mengusulkan untuk membangun sebuah jaringan *Virtual Private Network* (VPN), karena jaringan VPN membuat seolah olah jarak antara kantor pusat dan kantor cabang yang berada di jaringan WAN menjadi seperti berada di jaringan LAN.
 - 2) Untuk masalah keamanan disini penulis merancang pengunaan jaringan Virtual Private Network (VPN) karena VPN menggunakan keamanan berlapis dan data akan terenkripsi sehingga data yang dikirim aman. Teknik yang digunakan penulis dalam perancangan jaringan VPN ini adalah menggunakan teknik *PPTP Tunnel (Point to Point Tunneling Protocol)* yang di sesuaikan dengan kebutuhan lapangan.
 - 3) Untuk optimalisasi jaringan disini penulis menggunakan metode Remote Access VPN sehingga setiap user dapat tergabung dengan jaringan VPN tanpa terbatas jarak dan waktu asalkan mempunyai hak akses dan koneksi internet.
 - 4) Authentifikasi user VPN mengijinkan *client* dan *server* membangun identitas dalam jaringan dengan benar.

4.2. Rangkuman

1. Elemen pembentuk sistem komunikasi data adalah source, transmitter, sistem transmisi, receiver, dan destination. Kelimanya dapat disingkat menjadi tiga subsistem, yaitu Source system (Source dan Transmitter), Transmission System, serta Destination System (Receiver dan Destination).
2. Proses yang dilakukan pada sistem komunikasi data adalah Transmission system utilization, Interfacing, Signal generation, Synchronization, Exchange Management
3. Error detection and correction, Flow control, Addressing, Routing, Recovery, Message Formating, Security, dan Network Management
4. Protokol merupakan aturan standar yang digunakan dalam komunikasi data yang mengatur tentang data representation, signalling, authentication, dan error detection. Model standar protokol adalah OSI model. Sedangkan yang umum dan banyak dipakai adalah TCP/IP.
5. Tiap-tiap node dalam jaringan TCP/IP mempunyai IP Address yang unik. IP address bersifat independen dari perangkat keras, struktur network, topologi network, dan jenis protokol physical yang digunakan. IP address terdiri dari 4-byte numerik (total 32-bit) yang dituangkan dalam dotted decimal notation. Tiap byte seringkali dituangkan dalam bentuk desimal, heksadesimal, atau oktal, seperti 129.47.6.17, 0x81.0x2F.0x6.0x11, 0c201.0c57.0c6.0c21.
6. Tidak semua IP Address bisa digunakan untuk host. Di antaranya adalah Network Address, Broadcast address, Loopback address, dan Reserved address. Sedangkan untuk keperluan internet, beberapa IP address hanya boleh digunakan pada jaringan privat, yaitu: 10.0.0.0/8, 172.16.0.0/19 (172.168.0.0/24 s/d

172.16.31.0/24), dan 192.168.0.0/16 (192.168.1.0/24 s/d 192.168.254.0/24)

7. Jaringan komputer adalah sekumpulan perangkat-perangkat yang dapat menyimpan, mengolah data-data elektronis dan saling berhubungan, sehingga para pemakain jaringan dapat menyimpan, mengambil serta berbagi informasi dengan pemakai-pemakai lain.
8. Media transmisi merupakan salah satu komponen jaringan. Dikategorikan dalam guided dan unguided media. Guided media menggunakan kabel atau serat optik, sedangkan unguided media menggunakan gelombang infra merah atau microwave.
9. Gangguan keamanan komputer dapat terjadi dari dua sisi, internal dan eksternal. Terjadi dari internal karena selalu ada kelemahan pada sistem komputer sebagus apapun.
10. Pendekatan keamanan yang umum dilakukan adalah: identifikasi apa yang ingin diproteksi, dari apakah ia diproteksi, seperti apakah serangan yang akan terjadi, ukuran proteksi keseluruhan aset dalam ukuran biaya, Amati terus menerus dan perbaiki bila ditemukan kelemahan.
11. Security incident handling dibutuhkan ketika insiden keamanan terjadi. Prosedur untuk membangunnya dimulai dari persiapan dan perencanaan, pemberitahuan, identifikasi, penanganan, dan tindakan setelah insiden.

4.3. Soal Latihan

1. Terdapat 5 divisi, 1 divisi = 25 komputer, menggunakan subnetting dan network yang digunakan 192.168.52.0. berapakah subnetmask yang baru untuk network tersebut dan Sebutkan beberapa range dari network yang baru !
2. Network Address : 192.168.10.0
Subnet Mask : 255.255.255.224

(Biner: 11111111.11111111.11111111.11100000)

Pertanyaan:

- Jumlah subnet ?
- Jumlah host per subnet ?
- Alamat tiap subnet ?
- Alamat broadcast per subnet ?
- Gambarkan

4.4. Contoh Kasus

Kasus 1 :

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 apabila menggunakan kelas C !

Jawaban :

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 jumlah host adalah $2^8=256-2 = 254$ host, 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 adalah 5 bit. Maka menjadi $255.255.255.11100000 = 255.255.255.224$. Subnet mask yang terbaru adalah IP Address : 192.168.1.1 dan Subnet 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 $2^5 = 32$.

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 - 192.168.1.126	192.168.1.96	192.168.1.127
192.168.1.129 - 192.168.1.158	192.168.1.128	192.168.1.159
192.168.1.161 - 192.168.1.190	192.168.1.160	192.168.1.191
192.168.1.193 - 192.168.1.222	192.168.1.192	192.168.1.123
192.168.1.225 - 192.168.1.254	192.168.1.224	192.168.1.255

Dalam tabel 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 2 :

Di sebuah sekolah terpasang sebuah IP 202.40.10.0/24 dan IP tersebut akan dibagi ke dalam 5 bagian yaitu :

Pimpinan dengan 3 host

Guru dengan 55 host

Siswa dengan 108 host

Teknisi 26 host dan

Administrasi 11 host

Tentukanlah *network address, Range IP, dan Broadcast Address* pada setiap bagian yang telah ditentukan !

Jawaban :

Urutkan terlebih dahulu jaringan dari yang paling banyak hostnya:

1. Siswa = 108 host
2. Guru = 55 host
3. Teknisi = 26 host
4. Administrasi = 11 host
5. Pimpinan = 3 host

Urutan Jaringan

Net Mask Desimal	Net Mask Biner	Format CIDR	Jumlah HOST
255.255.255.0	11111111.11111111.11111111.00000000	/24	254
255.255.255.128	11111111.11111111.11111111.10000000	/25	126
255.255.255.192	11111111.11111111.11111111.11000000	/26	62
255.255.255.224	11111111.11111111.11111111.11100000	/27	30

255.255.255.240	11111111.11111111.11111111.11110000	/28	14
255.255.255.248	11111111.11111111.11111111.11111000	/29	6
255.255.255.252	11111111.11111111.11111111.11111100	/30	2

1. Siswa : 108 host

$108 \leq 2^n - 2$ (untuk menentukan 2^n hasil harus lebih besar dari host)

$$108 \leq 2^7 - 2$$

$$108 \leq 128 - 2$$

$$108 \leq 126$$

Network Address : 202.40.10.0/25

Range IP Address : 202.40.10.1 – 202.40.10.126

Broadcast Address : 202.40.10.127

2. Guru : 55 host

$55 \leq 2^n - 2$ (untuk menentukan 2^n hasil harus lebih besar dari host)

$$55 \leq 2^6 - 2$$

$$55 \leq 64 - 2$$

$$55 \leq 62$$

Network Address : 202.40.10.128/26

Range IP Address : 202.40.10.129 – 202.40.10.190

Broadcast Address : 202.40.10.191

3. Teknisi : 26 host

$26 \leq 2^n - 2$ (untuk menentukan 2^n hasil harus lebih besar dari host)

$$26 \leq 2^5 - 2$$

$$26 \leq 32 - 2$$

$$26 \leq 30$$

Network Address : 202.40.10.192/27

Range IP Address : 202.40.10.193 – 202.40.10.222

Broadcast Address : 202.40.10.223

4. Administrasi : 11 host

$11 \leq 2^n - 2$ (untuk menentukan 2^n hasil harus lebih besar dari host)

$$11 \leq 2^4 - 2$$

$$11 \leq 16 - 2$$

$$11 \leq 14$$

Network Address : 202.40.10.224/28

Range IP Address : 202.40.10.225 – 202.40.10.238

Broadcast Address : 202.40.10.239

5. Pimpinan : 3 host

$3 \leq 2^n - 2$ (untuk menentukan 2^n hasil harus lebih besar dari host)

$$3 \leq 2^3 - 2$$

$$3 \leq 8 - 2$$

$$3 \leq 6$$

Network Address : 202.40.10.240/27

Range IP Address : 202.40.10.241 – 202.40.10.246

Broadcast Address : 202.40.10.247

BAB III PERANCANGAN SISTEM JARINGAN KOMPUTER

4.1. Uraian Materi

Perancangan sistem jaringan komputer adalah kegiatan membuat rancangan yang menggambarkan hubungan fisik atau logis antar perangkat/komponen dalam sebuah jaringan komputer. Perancangan jaringan dapat didefinisikan sebagai filosofi yang mendorong bagaimana berbagai komponen, protokol, dan teknologi harus diintegrasikan dan disebarluaskan berdasarkan pendekatan dan prinsip tertentu untuk membangun lingkungan infrastruktur jaringan yang kohesif yang dapat memfasilitasi pencapaian tujuan bisnis taktis atau strategis. Memilih jenis jaringan yang tepat untuk organisasi sangat penting dalam merancang jaringan komputer yang hemat biaya dan meminimalkan konsumsi sumber daya.

Rancangan sistem jaringan komputer yang baik adalah sejalan dengan kebutuhan bisnis atau kebutuhan pengguna. Oleh karena itu, sebelum melakukan perancangan sistem jaringan komputer diperlukan analisis kebutuhan pengguna dan analisis sistem berjalan. Pertanyaan mendasar untuk mengetahui kebutuhan lingkungan sistem jaringan komputer sebelum melakukan perancangan antara lain:

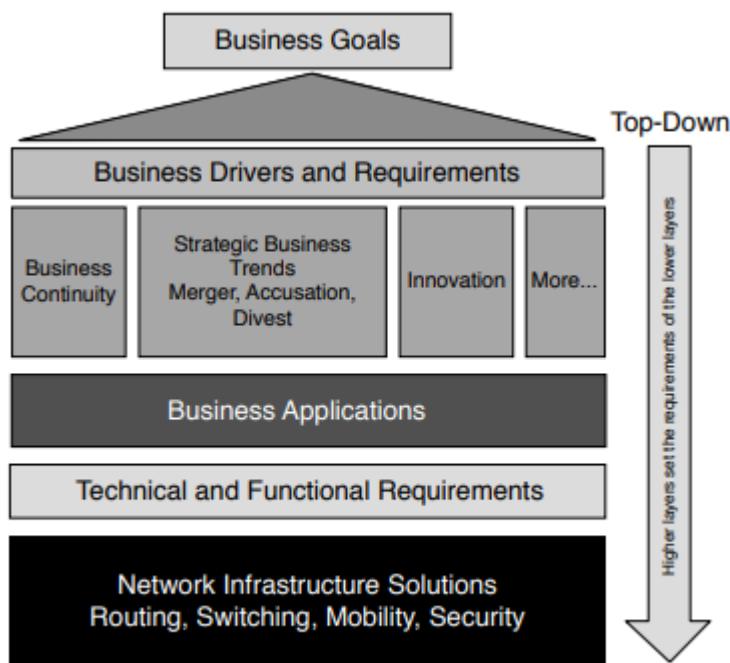
- Apa masalah atau tantangan yang mengakibatkan kesenjangan TI dengan bisnis?
- Bagaimana kita ingin bekerja dengan teknologi yang dimiliki organisasi? Apakah diperlukan akses jarak jauh untuk melakukan pekerjaan?
- Apa strategi manajemen TI organisasi?
- Bagaimana lingkungan jaringan mendukung strategi bisnis organisasi?
- Risiko keamanan siber apa yang dihadapi organisasi?
- Apakah diperlukan lingkungan jaringan di-host di cloud?

- Bagaimana anggaran pembiayaan yang disediakan untuk membangun sistem jaringan?

Terdapat dua pendekatan atau metode dalam analisis dan perancangan sistem jaringan, yaitu:

- 1) Pendekatan *top-down*

Pendekatan desain *top-down* menyederhanakan proses desain dengan membagi tugas perancangan agar lebih fokus pada ruang lingkup desain dan dilakukan dengan cara yang lebih terkontrol. Pada akhirnya dapat membantu desainer jaringan untuk melihat solusi desain jaringan dari pendekatan berbasis bisnis (*business-driven*).

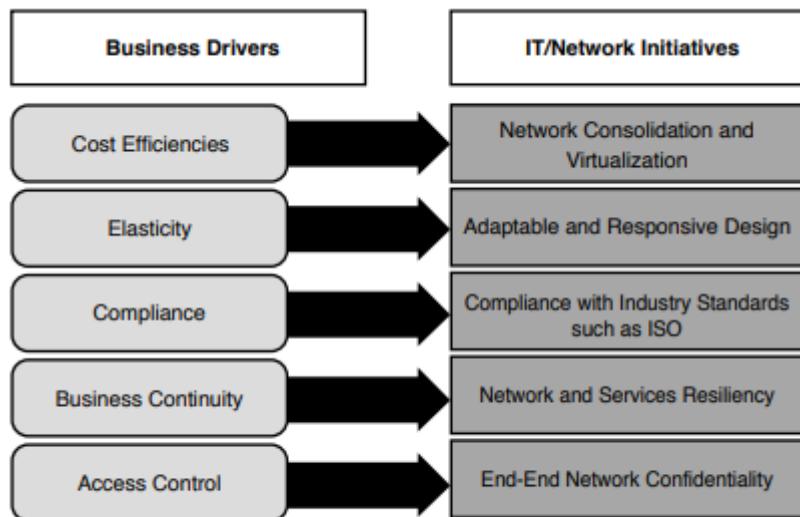


Gambar 36. Solusi Teknologi *Business-Driven*

- 2) Pendekatan *bottom-up*

Sebaliknya, pendekatan *bottom-up* berfokus pada pemilihan teknologi jaringan dan model desain terlebih dahulu. Hal ini dapat menimbulkan potensi kegagalan desain yang tinggi, karena jaringan tidak akan memenuhi persyaratan bisnis atau aplikasi. Untuk mencapai desain strategis yang sukses, harus ada penekanan tambahan pada

pendekatan berbasis bisnis. Ini menyiratkan fokus utama pada tujuan bisnis dan tujuan teknis, di samping layanan dan aplikasi yang ada dan yang akan datang. Faktanya, di jaringan saat ini, kebutuhan bisnis mendorong inisiatif TI dan jaringan seperti yang ditunjukkan pada gambar berikut.



Gambar 37. Business-Driven vs Inisiatif TI,

a. Topologi Jaringan

Topologi jaringan dapat disebut sebagai susunan struktur jaringan. Topologi jaringan dapat digambarkan secara fisik atau logis. Perangkat jaringan digambarkan sebagai node dan koneksi antara perangkat sebagai garis untuk membangun model grafis. Dengan kata lain, topologi jaringan berarti cara jaringan diatur, bagaimana node diatur dan terhubung satu sama lain. Masing-masing jaringan dapat diatur dalam beberapa cara yang berbeda, masing-masing pengaturan atau topologi memiliki pro dan kontra. Pilihan topologi dipengaruhi oleh sejumlah faktor, yang paling penting adalah ukuran dan skala jaringan serta biaya. Namun, faktor jangka panjang termasuk manajemen konfigurasi, pemantauan, dan kinerja umum juga perlu dipertimbangkan.

Pilihan topologi jaringan yang tepat dapat membantu untuk:

- Mengurangi biaya operasional dan pemeliharaan jaringan.
- Meningkatkan kinerja jaringan.
- Memastikan kesehatan jaringan yang optimal dengan alokasi sumber daya yang efektif
- Membantu menemukan dan mengatasi kesalahan dengan lebih cepat.

Topologi jaringan dapat dibedakan dalam dua kategori, yaitu Topologi Logis dan Topologi Fisik. Topologi logis digunakan dalam perancangan logis system jaringan, begitu juga dengan topologi fisik digunakan untuk perancangan fisik jaringan. Kedua kategori topologi ini sangat penting sebelum dilakukan implementasi system jaringan computer. Pembahasan perancangan logis dan fisik secara lebih lengkap dibahas pada poin b dan c.

a.1. Jenis Topologi Jaringan

Beberapa jenis topologi jaringan beserta kelebihan dan keuntungannya antara lain:

1) Topologi *point-to-point*

Seperti namanya, point-to-point adalah topologi jaringan dengan tautan khusus antara dua endpoint, oleh karenanya topologi ini merupakan topologi yang paling sederhana. Keuntungan dari jaringan seperti itu adalah bahwa semua bandwidth jaringan yang tersedia didedikasikan untuk dua perangkat yang terhubung.



Gambar 38. Topologi point-to-point

2) Topologi *daisy-chain*

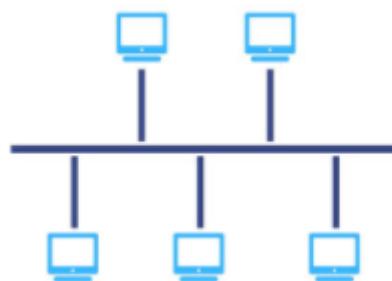
Daisy chain adalah topologi jaringan sederhana lainnya yang dibuat dengan menghubungkan setiap simpul ujung ke ujung secara seri. Ketika data ditransmisikan dalam jaringan daisy-chain, setiap node memantulkannya secara berurutan hingga mencapai tujuan. Jaringan daisy-chain dapat terdiri dari dua bentuk dasar yaitu linier dan cincin, yang akan dibahas selanjutnya.



Gambar 39. Topologi Daisy-chain

3) Topologi bus

Sebuah topologi bus terdiri dari satu kabel (bus), berjalan dari satu ujung jaringan ke ujung lainnya. Dalam pengaturan jaringan ini, setiap node terhubung ke kabel atau bus pusat melalui konektor antarmuka. Sebuah sinyal, yang berisi alamat dan data, ditransmisikan dari node sumber berjalan di kedua arah ke semua node sampai mencapai node tujuan, penerima data. Jika alamat sinyal yang dikirim tidak sesuai dengan alamat node penerima, bagian data dari sinyal diabaikan.



Gambar 40. Topologi Bus

Keuntungan topologi bus

- Karena menggunakan lebih sedikit kabel, mudah dibuat dan lebih murah dibandingkan dengan topologi jaringan lainnya. Menambahkan node baru ke jaringan lebih mudah dan dapat dicapai hanya dengan menggabungkan kabel tambahan dengan konektor.

Kekurangan topologi bus

- Karena seluruh jaringan bergantung pada satu kabel untuk transmisi data, jika kabel itu gagal, seluruh jaringan akan mati. Satu titik kegagalan seperti itu tidak ideal karena dapat menyebabkan banyak waktu henti dan akan memakan waktu dan mahal untuk dipulihkan. Topologi bus dapat sesuai digunakan untuk jaringan kecil di mana tidak ada terlalu banyak perangkat namun jaringan yang lebih besar dengan jumlah lalu lintas yang besar akan mengalami kecepatan transmisi yang lambat. Juga, pemecahan masalah dan menemukan masalah akan sangat memakan waktu untuk jaringan yang lebih besar.

4) Topologi star

Topologi star adalah topologi di mana setiap node periferal terhubung ke hub atau sakelar pusat. Ini mungkin topologi jaringan yang paling umum digunakan untuk LAN karena dianggap sebagai topologi termudah untuk dirancang dan diimplementasikan. Hub pusat berfungsi sebagai server untuk node periferal atau klien. Semua lalu lintas jaringan melewati hub pusat dan ini adalah satu-satunya persyaratan agar topologi diklasifikasikan sebagai topologi star. Jaringan tidak harus menyerupai bintang dalam pengaturan fisik.



Gambar 41. Topologi Star

Keuntungan topologi star

- Desain dan implementasinya sederhana.
- Ini menggunakan kabel yang relatif lebih sedikit, karena itu kurang padat karya.
- Seluruh jaringan dapat dengan mudah dikelola dari satu lokasi.
- Karena node terhubung secara independen ke hub, masalah dengan satu node tidak akan mempengaruhi seluruh jaringan.
- Node baru dapat ditambahkan atau dihapus tanpa membuat seluruh jaringan offline.
- Pemecahan masalah dan pemeliharaan jaringan lebih mudah.

Kekurangan topologi star

- Karena semua lalu lintas harus melewati hub pusat, ini adalah satu-satunya titik kegagalan, yang tidak ideal.
- Performa jaringan dan bandwidth keseluruhan dibatasi oleh spesifikasi teknis hub pusat.

5) Topologi ring

Topologi ring mirip dengan topologi daisy chain tetapi dengan loop tertutup sehingga node diatur dalam cincin atau lingkaran. Setiap node memiliki tepat dua peer dan data bergerak dalam satu arah melewati setiap node perantara pada ring sampai mencapai node tujuan. Data dapat dibuat lewat dua arah dengan menambahkan koneksi kedua antara node jaringan, menciptakan topologi ring ganda.

Dalam topologi ring, "token" listrik beredar di sekitar jaringan. Setiap node yang ingin mengirimkan data harus menunggu sampai memiliki token.



Gambar 42. Topologi Ring

Keuntungan topologi ring

- Karena hanya satu node yang dapat mengirimkan data pada satu waktu, yang mengurangi tabrakan paket, topologi ring lebih efisien dalam transmisi data.
- Topologi ring hemat biaya dan pemasangannya relatif murah
- Identifikasi dan pemecahan masalah lebih mudah.

Kekurangan topologi ring

- Jika salah satu node gagal, seluruh jaringan akan down.
- Jaringan ring yang besar akan mengalami transmisi yang lambat karena bandwidth jaringan digunakan bersama oleh semua perangkat.
- Sangat mudah untuk membebani sumber daya dan kapasitas jaringan.
- Saat menambah atau menghapus node mengharuskan seluruh jaringan menjadi offline.

6) Topologi *mesh*

Topologi *mesh* adalah topologi di mana setiap node terhubung secara langsung dan dinamis ke banyak node lainnya. Terdapat topologi mesh parsial, di mana beberapa node memiliki dua atau lebih koneksi, dan

topologi mesh penuh, di mana semua node sepenuhnya terhubung ke setiap node lainnya. Topologi mesh memiliki struktur non-hierarki dan node bekerja sama dalam routing data yang efisien. Karena kurangnya ketergantungan pada satu node atau rute, setiap node dapat berpartisipasi dalam menyampaikan informasi.



Gambar 43. Topologi Mesh

Struktur mesh memungkinkan dua metode transmisi data, yaitu:

- Routing - di mana node menggunakan logika untuk menentukan jalur terpendek dari sumber ke tujuan, dan
- Flooding, dimana informasi dikirimkan ke setiap node dalam jaringan.

Keuntungan topologi mesh

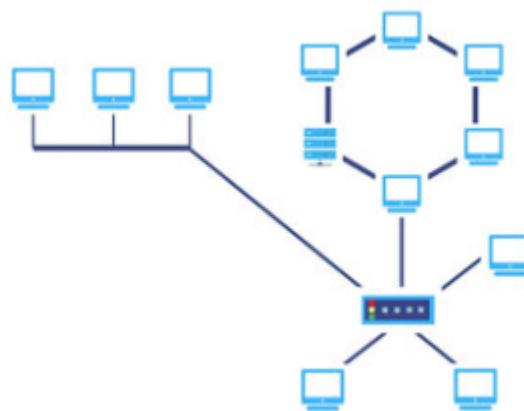
- Jaringan mesh adalah topologi yang paling stabil dan dapat diandalkan.
- Jaringan mesh tahan terhadap kegagalan karena tingkat interkoneksi yang besar.
- Tidak ada satu titik kegagalan. Bahkan jika satu atau dua node gagal, jaringan tidak akan mati.

Kekurangan topologi mesh

- Jaringan mesh membutuhkan banyak resource karena membutuhkan banyak kabel.
- Kabel, tenaga kerja, dan waktu konfigurasi membuatnya mahal.

7) Topologi *hybrid*

Sebuah topologi *hybrid* adalah topologi di mana dua atau lebih topologi yang berbeda digabungkan untuk membangun jaringan sedemikian rupa sehingga tidak menunjukkan salah satu topologi standar. Topologi hybrid biasanya ditemukan pada organisasi yang lebih besar di mana masing-masing departemen dapat memiliki topologi jaringan yang dipersonalisasi berdasarkan kebutuhan dan persyaratan jaringan masing-masing. Contoh paling umum dari topologi hybrid adalah topologi tree.



Gambar 44. Topologi *Hybrid*

Keuntungan topologi *hybrid*

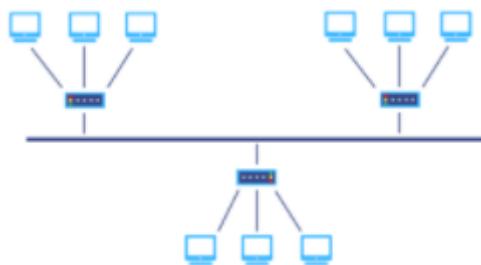
- Keuntungan yang paling menonjol dari topologi hybrid adalah fleksibilitas dan derajat kebebasan yang diberikannya. Dengan struktur jaringan hybrid, hanya ada sedikit batasan tentang bagaimana jaringan diatur.

Kekurangan topologi *hybrid*

- Setiap topologi standar yang tergabung dalam topologi hybrid akan membawa kekurangannya masing-masing sehingga topologi hybrid tidak akan terbebas dari masalah. Selain itu, seiring dengan pertumbuhan jaringan hybrid, kompleksitas dalam mengelola jaringan juga akan bertambah.

8) Topologi *tree*

Topologi *tree* adalah jaringan hybrid yang dihasilkan dari kombinasi topologi *bus* dan topologi *star*. Bus menyerupai batang pohon sedangkan simpul perifer menyerupai daun, oleh karena itu dinamakan topologi *tree*. Topologi *tree* dapat dilihat sebagai susunan hierarki jaringan *star* karena memiliki hierarki induk-anak untuk bagaimana node terhubung.



Gambar 45. Topologi Tree

Keuntungan topologi *tree*

- Perluasan jaringan dan penambahan node baru dapat dilakukan dengan mudah.
- Karena setiap cabang jaringan dapat dinilai secara individual, pemecahan masalah menjadi lebih mudah.

Kekurangan topologi *tree*

- Seluruh jaringan tergantung pada bus pusat, yang menyajikan satu titik kegagalan (*single point of failure*).
- Topologi tree bisa mahal karena jumlah kabel yang dibutuhkan.
- Karena struktur hierarkis, mungkin sulit untuk dikonfigurasi.

a.2. Pertimbangan Pemilihan Topologi Jaringan

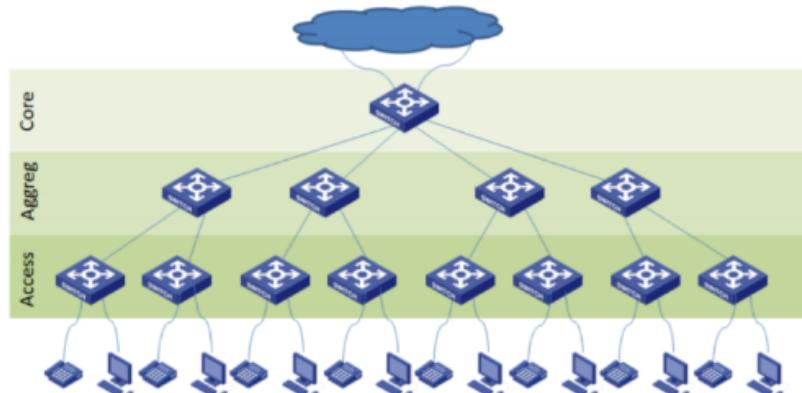
Ada beberapa pertimbangan yang perlu dipikirkan ketika akan membentuk topologi jaringan, yaitu berkaitan dengan:

Skalabilitas: Jaringan yang akan dibuat harus mampu dikembangkan dengan mudah, hal ini bisa terjadi misalnya adanya penambahan segment network baru maupun penambahan jumlah router. Pengembangan ini juga tidak boleh mengakibatkan perubahan besar terhadap keseluruhan topologi yang sudah ada (existing), sehingga tidak perlu merombak keseluruhan jaringan.

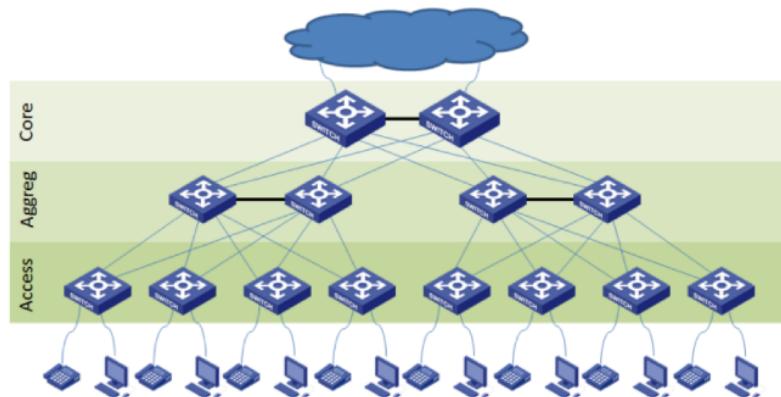
Redundant: Topologi yang baik harus menyediakan link cadangan (redundant), antara device router satu dengan device router lainnya (antar jaringan yang berbeda). Terjadinya kegagalan pada suatu link akan mudah dibackup oleh link yang lain, sehingga akan meningkatkan kehandalan dari suatu jaringan.

Manfaat redundansi antara lain:

- Mengurangi kemungkinan kegagalan jaringan
- Mengoptimalkan waktu dan biaya
- Meningkatkan uptime jaringan
- Meningkatkan keamanan jaringan



Gambar X. Contoh rancangan jaringan non-redundant



Gambar X. Contoh rancangan jaringan redundan

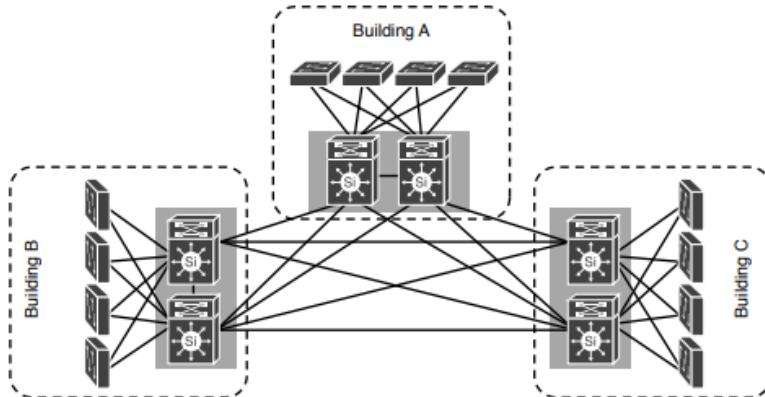
Performa Jaringan: Untuk meningkatkan kecepatan dari setiap link yang tersedia pada sebuah jaringan, topologi yang dibangun harus bisa mendukung teknik link aggregation (penggabungan link) ataupun mendukung teknik load balancing. Dengan adanya peningkatan kecepatan dari link antar device, maka sebuah jaringan akan memiliki bandwidth yang besar sehingga dapat digunakan untuk mengirim data dalam jumlah yang besar juga.

Keamanan: Topologi yang dibangun maupun device/perangkat yang digunakan harus mendukung penerapan teknik-teknik keamanan jaringan (security). Semua hal ini dilakukan bertujuan untuk menjaga keamanan dan kerahasiaan daya yang dikirim.

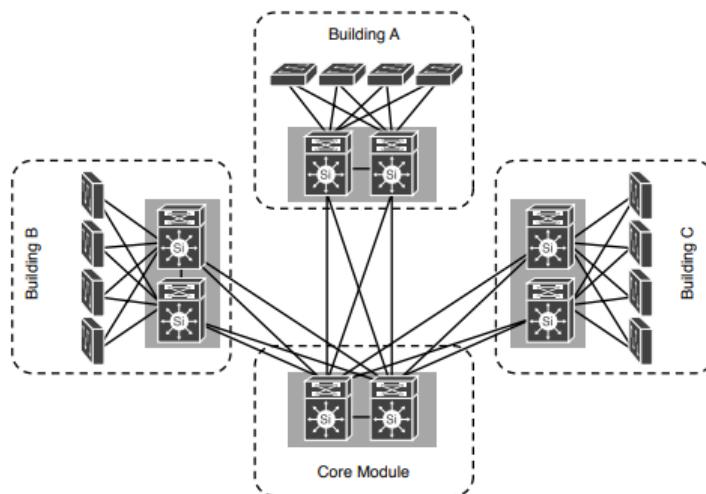
Manajemen dan maintenance: Tindakan dalam melakukan pengendalian dan manajemen terhadap lalu lintas jaringan bisa dikelola dan diatur dengan mudah. Begitu juga dengan manajemen setiap device/perangkat, seharusnya konfigurasinya dapat dilakukan dengan mudah oleh administrator jaringan pada keseluruhan device/perangkat. Demikian juga dengan maintenance/perawatannya.

Fleksibilitas. Rancangan yang fleksibel akan mudah beradaptasi jika terdapat perubahan. Selain itu juga dapat mendukung jika diperlukan integrasi dengan sistem jaringan lain. Misalnya pada kasus merger atau

akuisisi. Perubahan proses bisnis dan perkembangan teknologi akan menjadi tantangan bagi desainer dalam merancang sistem jaringan.



Gambar X. Contoh rancangan jaringan yang tidak fleksibel



Gambar X. Contoh rancangan jaringan yang fleksibel

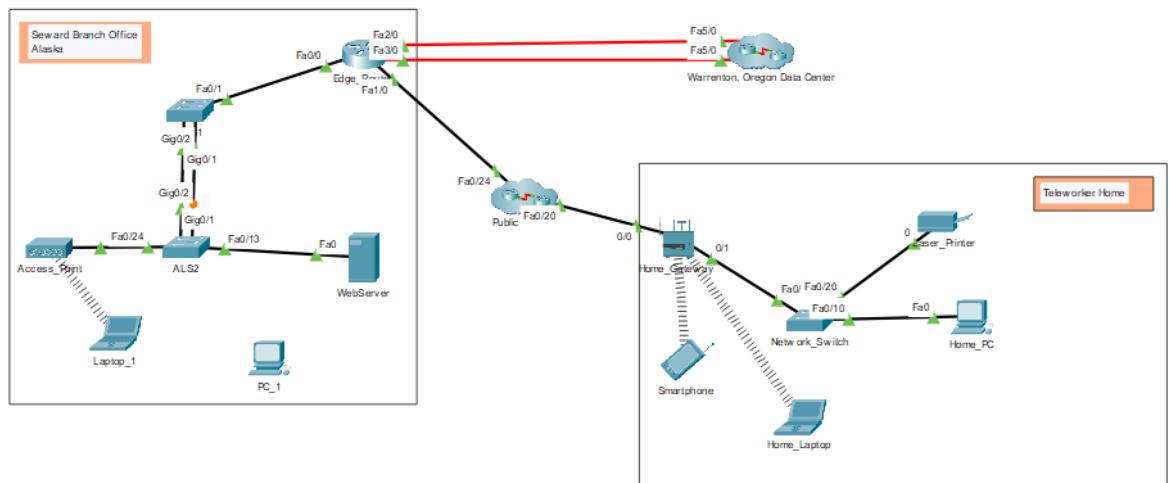
b. Rancangan Logis Sistem Jaringan Komputer

Topologi logis mengacu pada gagasan tentang bagaimana data mengalir dalam jaringan. Ini menjelaskan bagaimana jaringan diatur, bagaimana node termasuk sumber daya virtual dan cloud terhubung satu sama lain, dan bagaimana data ditransmisikan melalui jaringan. Topologi logis juga menerangkan bagaimana jaringan diatur melalui konfigurasi alamat IP (IP

addressing) dan konfigurasi subnet (subnetting). Memiliki pemahaman yang baik tentang topologi logis sangat penting untuk manajemen dan pemantauan jaringan yang efektif, efisien dan sehat.

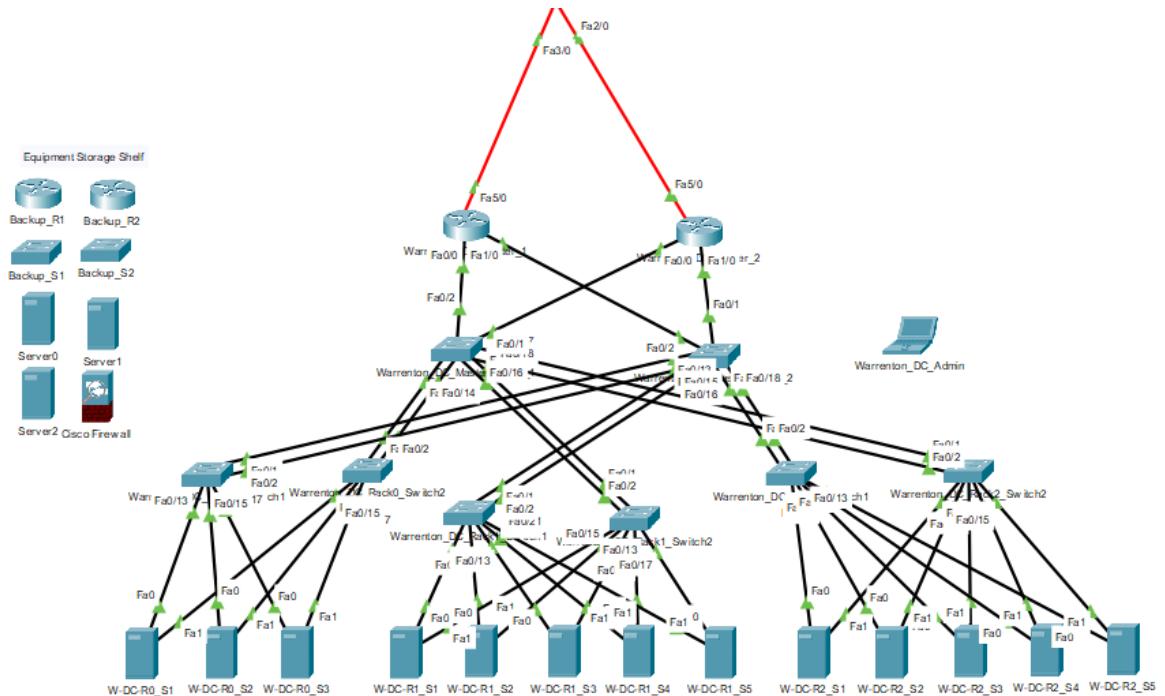
Contoh: Rancangan logis jaringan yang menghubungkan Data Center dan kantor karyawan di Warenton dengan kantor cabang di Seward. Rancangan logis secara menyeluruh merupakan level 0, selanjutnya dapat di-breakdown ke dalam beberapa level sesuai kebutuhan.

1) Rancangan logis level 0



Gambar 46. Rancangan Logis Level 0

2) Rancangan logis level 1 (Data Center)



Gambar 47. Rancangan Logis Level 1

c. Rancangan Fisik Sistem Jaringan Komputer

Topologi fisik adalah tata letak actual perangkat keras (hardware) jaringan secara fisik. Ini mengacu pada penempatan berbagai perangkat jaringan seperti router, switch, akses point nirkabel, komputer, dll. Termasuk metode yang digunakan untuk menghubungkan perangkat tersebut, yaitu kabel jaringan. Mengetahui topologi fisik jaringan adalah penting karena akan membantu mengatur perluasan, dengan pemeliharaan, dan untuk tugas-tugas penyediaan.

Contoh: Rancangan Fisik jaringan yang menghubungkan Data Center dan kantor karyawan di Warenton dengan kantor cabang di Seward. Seperti halnya pada rancangan logis, rancangan fisik secara menyeluruh merupakan level 0, selanjutnya dapat di-breakdown sesuai kebutuhan.

1) Rancangan fisik level 0



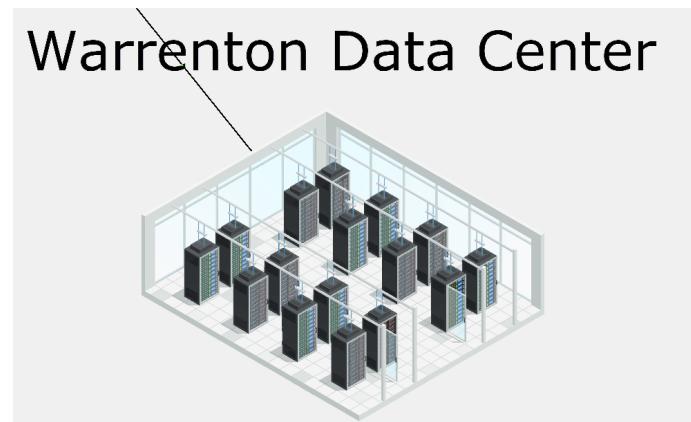
Gambar 48. Rancangan Fisik Level 0

2) Rancangan fisik level 1 (Kantor cabang di Warrenton)



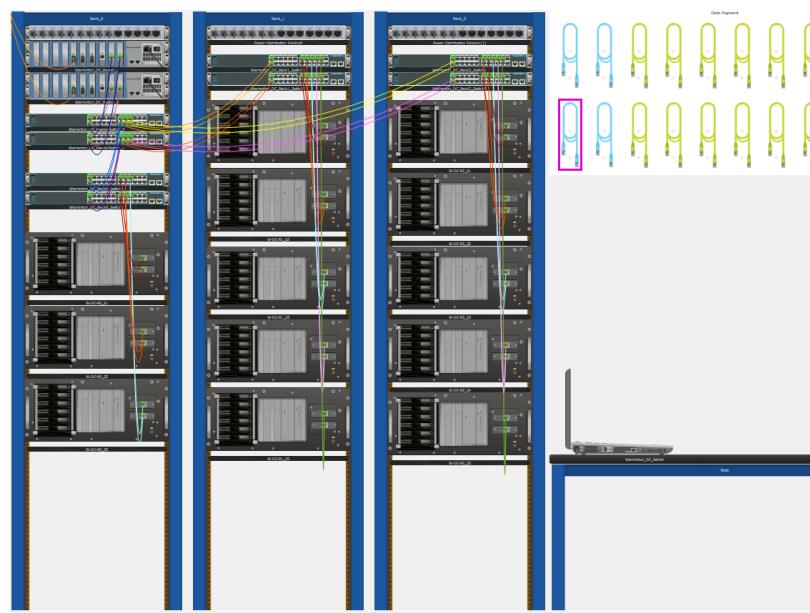
Gambar 49. Rancangan Fisik Level 1

3) Rancangan fisik level 2 (Data Center)



Gambar 50. Rancangan Fisik Level 2

4) Rancangan fisik level 3 (Server)



Gambar 51. Rancangan Fisik Level 3

d. Tahapan Perancangan Sistem Jaringan Komputer

Berikut ini adalah tahapan dalam melakukan perancangan sistem jaringan komputer:

1) Mengumpulkan persyaratan

Yaitu mendefinisikan kondisi sistem jaringan saat ini dan sistem jaringan yang ingin dicapai. Pengumpulan persyaratan terdiri dari 3 tahapan yaitu:

a. Identifikasi jaringan eksisting

Pada tahapan ini dilakukan evaluasi jaringan yang dipakai saat ini untuk mengidentifikasi infrastruktur jaringan, komponen, dan layanan yang berjalan di atasnya. Data yang dikumpulkan mengenai:

- Tipe perangkat jaringan, termasuk server dan lokasinya
- Teknologi WAN dan kecepatan sirkuit
- Layout pengkabelan pada lantai dan gedung
- Potokol routing, manajemen jaringan, dan control keamanan.

b. Menentukan tujuan perancangan jaringan baru

Definisikan dengan jelas apa yang menjadi tujuan utama, bisa berupa kombinasi tujuan bisnis dan teknis. Contohnya:

- Meningkatkan performa jaringan (*throughput, latency, uptime, dll*)
- Meningkatkan keamanan jaringan
- Menyederhanakan pengelolaan jaringan

c. Mendefinisikan batasan/konstrain yang mungkin

Perancangan sistem jaringan perlu memperhatikan konstrain atau kondisi dimana parameter-parameter yang sudah ada menjadi batasan yang tidak bisa diubah. Beberapa konstrain yang paling umum antara lain:

- Biaya
- Waktu. Waktu menjadi konstrain perancangan jaringan jika ada jangka waktu yang ditetapkan untuk penyelesaian proyek.

- Lokasi. Lokasi bisa menjadi konstrain secara tidak langsung. Misalnya jika terkait dengan wilayah geografis yang berbeda, terpencil, atau jarak yang jauh yang tidak terjangkau infrastruktur fiber optic, sehingga satu-satunya solusi adalah menggunakan koneksi wireless.
- Infrastruktur peralatan jaringan. Misalnya, peralatan jaringan lama yang tidak mendukung fitur dan protocol baru, sehingga perlu peralatan baru.
- Keahlian dan pengetahuan SDM. Keahlian dan pengetahuan pegawai bisa menjadi konstrain dalam perancangan sistem jaringan, akan tetapi kemampuan SDM dapat diupgrade dengan melakukan pelatihan.

Selain konstrain yang disebutkan di atas ada beberapa faktor teknis yang perlu dipertimbangkan dalam merancangan sistem jaringan komputer antara lain: cakupan area, lalu lintas jaringan (*traffic*), performa, keamanan jaringan, redundansi, manajemen dan pemeliharaan sistem jaringan.

2) Menentukan skala/ukuran jaringan

Untuk memberikan kinerja jaringan yang optimal, dalam perancangan perlu memperhatikan ukuran jaringan, yang berarti perlu diketahui jumlah perangkat dan intensitas penggunaannya, serta perlu ditekankan area dan fungsi yang harus ditangani. Misalnya: pada area jaringan campus organisasi dan site jarak jauh, maka ruang lingkup perancangan mencakup implementasi IP telepony di seluruh perusahaan. Sehingga perlu perancangan ulang terkait VLAN, *Quality of Service* (QoS) pada lintas LAN, WAN, *data center*, dan akses jarak jauh.

3) Mempelajari denah lantai dan gedung

Pelajari denah lantai pada kantor dan lakukan plot lokasi yang tepat dari semua *endpoint* seperti desktop, server, printer, dll. Ini diperlukan untuk menentukan lokasi switch. Perlu juga diketahui lokasi meja, ruang rapat, area kerja, dan perangkat apa pun yang terhubung dengan Wi-Fi sehingga lokasi titik akses dapat ditentukan. Anda juga perlu menginventarisasi outlet listrik, soket jaringan, dan panel tambalan yang dipasang di dinding.

Informasi yang menyeluruh tentang tata letak kantor akan membantu dalam merancang tata letak jaringan yang optimal di mana perangkat endpoint tidak terlalu jauh dengan titik akses. Lokasi endpoint juga akan membantu dengan cepat menetapkan sakelar dan/atau port ke subnet yang tepat.

4) Memilih ISP

Pilihan Penyedia Layanan Internet (ISP) dapat berdampak besar pada kinerja jaringan. Pengalaman dan keahlian penyedia layanan TI akan membantu dalam memilih ISP yang paling sesuai berdasarkan lokasi dan kebutuhan.

5) Membuat rancangan sistem jaringan komputer

Tahapan ini adalah inti dari proses perancangan jaringan. Spesifikasi perancangan akan menjadi dasar untuk tahap implementasi dan kebutuhan untuk mendukung ketersediaan, keamanan, dan tujuan kinerja seperti yang ditentukan dalam persyaratan. Oleh karena itu, pada tahap ini, akan dibuat topologi logis dan fisik, diagram jaringan, menentukan informasi desain khusus seperti protokol routing, pengalaman IP, subnet, dan konfigurasi keamanan.

a. Topologi jaringan

Topologi jaringan merupakan susunan struktural jaringan, di mana endpoint jaringan digambarkan sebagai node dan koneksi di antara mereka sebagai tautan. Ini adalah fase penting dalam proses perancangan jaringan karena pilihan topologi memiliki

dampak besar pada skalabilitas, manajemen konfigurasi, pemantauan, dan kinerja umum jaringan. Pemilihan jenis topologi jaringan harus didasarkan pada spesifikasi yang telah dihimpun dengan memperhatikan keuntungan dan kerugian masing-masing pilihan. Tidak ada satu topologi jaringan terbaik untuk semua kasus penggunaan.

b. Tipe jaringan

Penentuan luas fisik jaringan merupakan faktor penting dalam perancangan. Pertimbangan yang mungkin adalah organisasi menempati bagian pada kantor Bersama, seluruh lantai gedung, beberapa lantai, atau memiliki kantor di beberapa lokasi. Setiap kasus akan memerlukan tipe jaringan yang berbeda. Rancangan yang mungkin dapat berupa LAN sederhana hingga WAN dengan area yang luas dan kompleks.

c. Perangkat jaringan fisik

Jaringan fisik meliputi pemasangan kabel, faceplate, panel tambahan, dan lain-lain. Jenis kabel akan tergantung pada jenis jaringan yang dipilih. Pengkabelan jaringan dasar yang solid merupakan prasyarat untuk jaringan yang efisien. Pertimbangkan perangkat seperti printer, kamera IP, dan lain-lain. Selain itu penggunaan Power over Ethernet (PoE) juga perlu dipertimbangkan sehingga memungkinkan pengiriman daya DC ke perangkat melalui kabel ethernet.

d. Peralatan jaringan

Peralatan jaringan seperti router, switch, dan hub akan membentuk inti dari infrastruktur jaringan yang menghubungkan perangkat Bersama seperti komputer, printer, dan server dalam jaringan. Router akan mengarahkan lalu lintas, memilih rute yang paling efisien untuk paket data saat melintasi jaringan. Selain itu juga menghubungkan jaringan lokal ke

jaringan lain seperti Internet. Pengetahuan dan pemahaman mengenai komponen jaringan dapat membantu memilih jenis peralatan yang tepat untuk kebutuhan jaringan.

e. *Addressing dan subnetting*

Addressing dan subnetting ini merupakan bagian logis jaringan. Pada tahapan ini, ditetapkan alamat IP (IP Address). Setiap perangkat yang terhubung ke jaringan memiliki alamat IP sendiri. Penetapan alamat IP dapat bersifat statis atau dinamis tergantung pada praktik dan fitur jaringan. DHCP (*Dynamic Host Configuration Protocol*) merupakan protocol yang paling umum digunakan untuk menetapkan alamat IP secara otomatis ke perangkat yang terhubung dengan jaringan.

Subnetting diperlukan untuk manajemen jaringan yang efektif, alokasi resource, dan juga alasan keamanan. Endpoint jaringan dapat ditetapkan ke subnet berdasarkan lokasi, departemen, fungsi, atau kriteria lainnya sesuai kebutuhan.

Addressing dan subnetting sudah dibahas lebih lengkap pada Bab II.

6) Membuat dokumentasi perancangan jaringan

Saat mendesain jaringan, hal terpenting yang harus diingat adalah Anda tidak dapat mendesain seluruh jaringan di kepala Anda. Anda mungkin berpikir bahwa Anda hanya perlu menghubungkan peralatan jaringan Anda dan semuanya akan berfungsi dengan baik. Tapi itu tidak pernah terjadi di lingkungan bisnis, yang sangat kompleks. Setiap perangkat yang Anda tambahkan atau hapus dari jaringan Anda memengaruhi kinerjanya. Oleh karena itu, sangat disarankan untuk mendokumentasikan setiap langkah proses desain jaringan Anda. Rencana yang jelas dan diagram fisik akan memastikan bahwa Anda

tidak melewatkkan aspek penting dari jaringan dan yang lebih penting, akan membantu dalam implementasi jaringan.

Dokumen perancangan jaringan minimal harus mencakup hal-hal berikut:

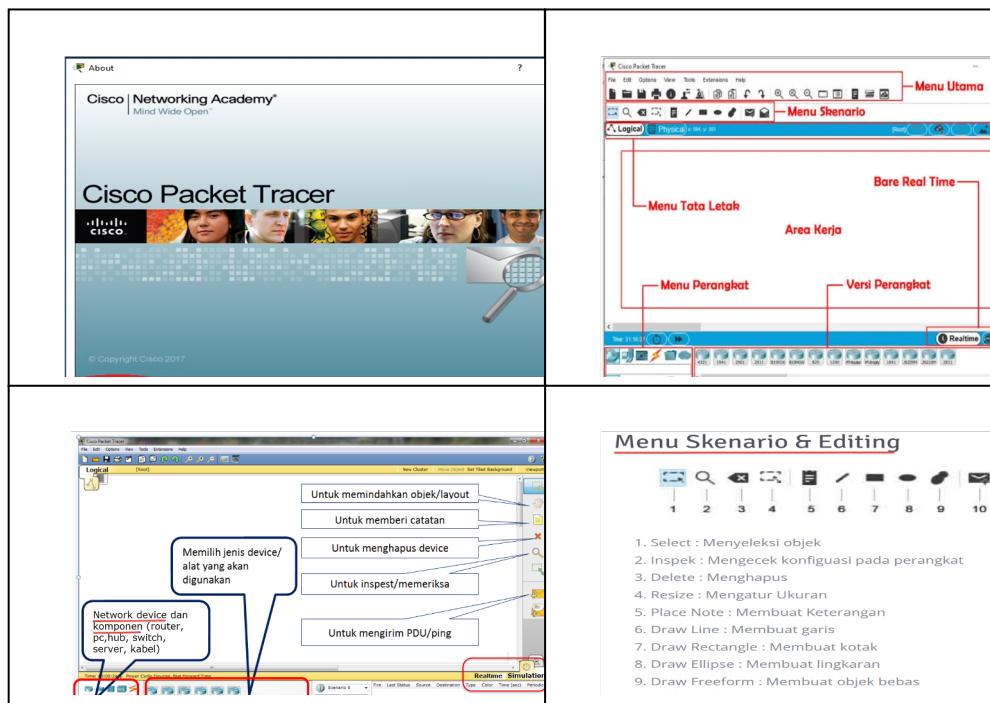
- Tujuan proyek.
- Persyaratan dan batasan perancangan.
- Rincian infrastruktur jaringan yang ada termasuk diagram topologi, metrik kinerja jaringan, protokol routing, daftar aplikasi yang berjalan, daftar peralatan, dan konfigurasi.
- Detail rancangan jaringan termasuk topologi logis dan fisik, diagram jaringan, pengalamatan IP, protokol routing, dan konfigurasi.
- Rencana implementasi yang merinci langkah-langkah untuk penginstalan, pengaturan, dan konfigurasi baru.

e. Tools Perancangan Topologi Jaringan

Ada banyak sekali tools untuk melakukan perancangan jaringan yang tersebar di internet baik gratis maupun berbayar. Tools yang sudah tidak asing salah satunya adalah Microsoft Visio. Pada modul ini, akan digunakan Cisco Packet Tracker untuk melakukan perancangan pada contoh kasus yang akan dibahas pada poin 3.4. Cisco Packet Tracker adalah aplikasi gratis dan dapat diinstal pada OS Windows, Mac OS, dan Ubuntu. Cisco Packet Tracker berfungsi sebagai simulator untuk melakukan perancangan sekaligus bereksperimen seperti merancang dan konfigurasi jaringan yang sebenarnya. Tutorial lengkap dapat diakses pada link <https://www.netacad.com/courses/packet-tracer>. Ikuti petunjuk instalasi dan panduan *step by step* pembuatan rancangan jaringan.

Berikut ini secara sekilas akan di jelaskan mengenai area dan komponen-komponen pada aplikasi Packet Tracer sebagai berikut:

Tampilan awal Cisco Packet Tracer dan penjelasan singkat item-item dari menu:



Gambar 52. Layout interface Packet Tracer beserta menunya

Beberapa penjelasan dari menu: berkaitan dengan proses.

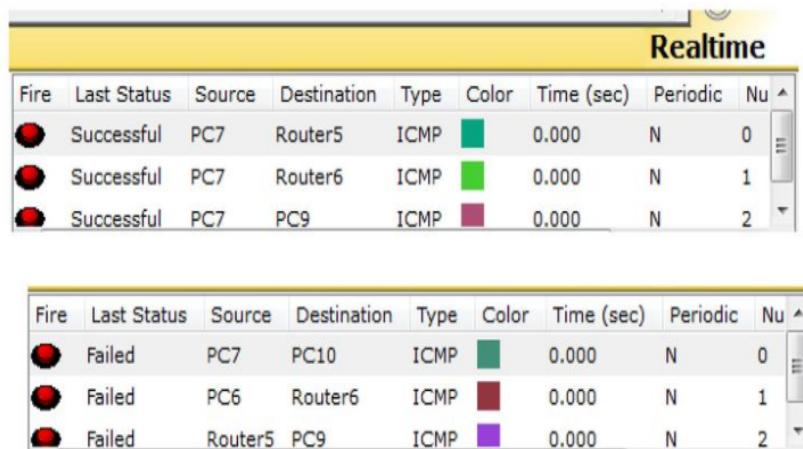
Mode realtime: Mode realtime digunakan untuk melakukan simulasi seperti kejadian aslinya. Contoh untuk mengetahui jaringan terhubung atau tidak dapat menggunakan perintah ping ke alamat tujuan.

Mode simulation: Mode Simulation menginformasikan bagaimana proses pengiriman data dan penerimaan paket data yang disimulasikan dengan PDU (packet data unit) atau pesan/informasi.

Warna indikator kabel/connection

- Warna merah menunjukkan bahwa kabel tidak terhubung atau kesalahan pemilihan kabel;
- Warna orange menunjukkan kabel mulai berhasil terhubung antar device;
- Warna hijau menunjukkan kabel berhasil terhubung dengan normal.

Indikator koneksi jaringan sukses atau gagal dalam simulasi jaringan

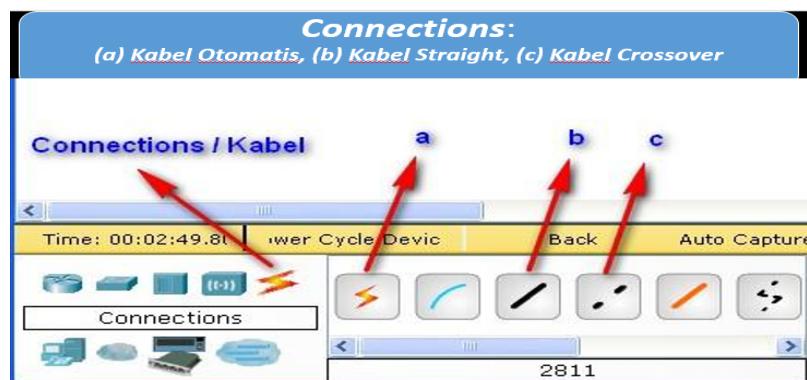


Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Nu
●	Successful	PC7	Router5	ICMP	Green	0.000	N	0
●	Successful	PC7	Router6	ICMP	Green	0.000	N	1
●	Successful	PC7	PC9	ICMP	Maroon	0.000	N	2

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Nu
●	Failed	PC7	PC10	ICMP	Green	0.000	N	0
●	Failed	PC6	Router6	ICMP	Maroon	0.000	N	1
●	Failed	Router5	PC9	ICMP	Purple	0.000	N	2

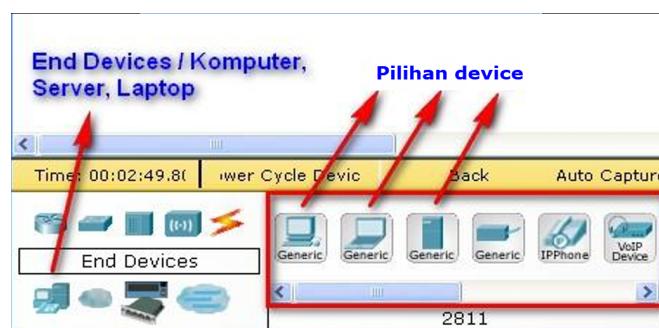
Gambar 53. Status koneksi jaringan

Komponen penghubung jaringan



Gambar 54. Jenis kabel penghubung

Komponen device jaringan



Gambar 55. Jenis device jaringan

Komponen device jaringan layer 2



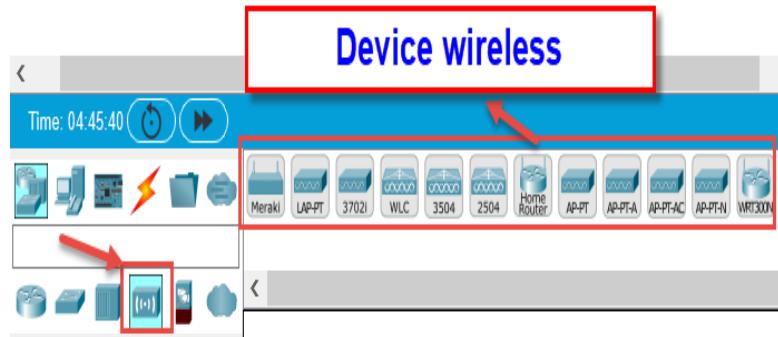
Gambar 56. Jenis device jaringan layer 2

Komponen device jaringan layer 3



Gambar 57. Jenis device jaringan layer 3

Komponen device jaringan wireless



Gambar 58. Jenis device jaringan wireless

4.2. Rangkuman

- 1) Untuk mencapai desain jaringan yang memberikan nilai bagi bisnis dan sejalan dengan tujuan dan arahnya, desainer jaringan harus mengikuti pendekatan terstruktur. Pendekatan ini harus dimulai dari tingkat atas, dengan fokus pada kebutuhan, penggerak, dan arah bisnis, untuk menghasilkan desain yang berbasis pada bisnis. Selain itu, dengan pendekatan top-down, perancang dan arsitek jaringan selalu dapat menghasilkan arsitektur jaringan berbasis bisnis yang pada tahap selanjutnya dapat memfasilitasi, pemilihan platform perangkat keras dan fitur teknologi serta protokol yang diinginkan untuk menerapkan desain yang dimaksud. Hal ini membuat desain jaringan lebih responsif terhadap kebutuhan bisnis atau teknologi baru. Selanjutnya, mempertimbangkan prinsip-prinsip desain yang berbeda yang dibahas dalam bab ini dan mempertimbangkan persyaratan yang berbeda (aplikasi bisnis, fungsional, dan misi-kritis) dapat membantu desainer jaringan untuk merencanakan dan membuat pilihan desain yang tepat yang pada akhirnya akan membuat jaringan dilihat sebagai "penggerak bisnis (*business-driven*).
- 2) Tahapan yang dilakukan sebelum perancangan sistem jaringan komputer adalah: fase perencanaan yaitu : i) Mendefinisikan tujuan: yakni untuk menentukan tujuan yang ingin dicapai, maupun bahan pertimbangan

- dalam membangun jaringan: ii) Studi kelayakan, misalnya melakukan survei mengenai berbagai aspek kaitannya dengan membangun jaringan, serta iii) Perencanaan dalam menganalisis sistem jaringan yang akan dibangun dengan segala aspeknya (komponen perangkat keras, lunak, layanan, dan sebagainya).
- 3) Dalam perancangan sistem jaringan, perlu memperhatikan design konfigurasinya baik dalam skema pengalamatan, topologi, maupun pelayanan (*services*) yang akan diberikan oleh jaringan, serta bagaimana cara mengelolanya dengan baik. Untuk memudahkan dalam merancang, membuat design jaringan dibutuhkan semacam simulasi, untuk melihat proses tahapan berlangsung sehingga bisa dianalisa hasil simulasi tersebut.
 - 4) Didalam klasifikasi jaringan komputer terbagi menjadi 5 yaitu 1. berdasarkan topologi, 2. berdasarkan geografis, 3. berdasarkan fungsi, 4. berdasarkan distribusi sumber informasi dan 5. berdasarkan media transmisi. Klasifikasi jaringan sehubungan dengan rancangan jaringan yang akan kita bangun pendekatannya berdasarkan topologi.
 - 5) Beberapa hal yang perlu diketahui dan ditelaah berkenaan dengan topologi jaringan:
 - a. Identifikasi Topologi Dan Standar Jaringan:
Topologi menguraikan cara bagaimana komputer terhubung dalam suatu jaringan.
 - b. Identifikasi Topologi Jaringan:
Topologi jaringan mendefinisikan koneksi fisik host dalam jaringan. Ada beberapa jenis topologi fisik jaringan yaitu bus, ring, star, mesh, dan tree.
 - 6) Pertimbangan Pembentukan Topologi Jaringan:
 - a. Skalabilitas;
 - b. Redundant;
 - c. Performa Jaringan;

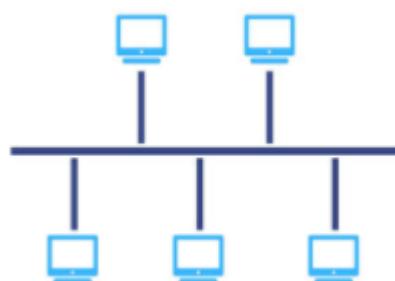
- d. Keamanan;
 - e. Manajemen dan maintenance.
- 7) Khusus mengenai topologi rancangan logis sistem jaringan Komputer: pertama-tama kebutuhan yang perlu dipersiapkan adalah alamat IP. Kebutuhan utama dalam topologi rancangan logis sistem jaringan komputer ini adalah dengan melakukan pengaturan alamat IP (IP address).
- 8) Perbedaan antara topologi logic dan topologi fisik adalah:
- a. Topologi logic mempunyai makna untuk mendefinisikan mekanisme aliran data atau informasi didalam jaringan
 - b. Topologi fisik mendefinisikan bagaimana layout secara aktual diuraikan dan dijabarkan melalui perangkat keras jaringan.
- 9) Dengan menggunakan Packet Tracer, kita dapat melakukan beberapa hal diantaranya:
- a. Mendesain topologi jaringan komputer beserta perangkat-perangkat lainnya;
 - b. Konfigurasi perangkat jaringan komputer;
 - c. Membuat skenario rancangan jaringan komputer

4.3. Soal Latihan

Pilihan Ganda

1. *Business-driven* merupakan salah satu pendekatan dalam perancangan system jaringan computer yang disebut juga sebagai metode
 - a. Top-down network design
 - b. Bottom-up network design
 - c. Physical network design
 - d. Logical network design
2. Dalam tahapan perancangan system jaringan computer, kegiatan yang pertama kali dilakukan adalah
 - a. Membuat rincian perangkat-perangkat infrastruktur jaringan

- b. Membuat topologi rancangan fisik
 - c. Membuat topologi rancangan logis
 - d. Mengumpulkan persyaratan bisnis
3. Rancangan layout jaringan dalam bentuk skema hubungan perangkat-perangkat fisik disebut
- a. LAN
 - b. Ethernet
 - c. Topologi Fisik
 - d. Topologi Logis
4. Berikut ini adalah jenis topologi yang paling sederhana
- a. *Point-to-point*
 - b. *Bus*
 - c. *Star*
 - d. *Ring*
5. Berikut ini adalah jenis topologi yang paling fleksibel
- a. *Bus*
 - b. *Star*
 - c. *Ring*
 - d. *Mesh*
6. Gambar berikut merupakan jenis topologi



- a. *Bus*
- b. *Star*
- c. *Ring*
- d. *Mesh*

7. Routing penentuan jalur transmisi terpendek memungkinkan dilakukan pada jenis topologi
 - a. Bus
 - b. Star
 - c. Ring
 - d. Mesh
8. Salah satu kekurangan jenis topologi tree, kecuali
 - a. Single point of failure
 - b. Mahal
 - c. Sulit dikonfigurasi
 - d. Sulit dilakukan troubleshoot jika ada masalah

Essay:

1. Buatlah rancangan desain jaringan LAN pada aplikasi Packet Tracer. Berikut ini kebutuhannya: Tersedia 4 pc dan 1 perangkat switch, dengan penjelasan uraian ip address sebagai berikut:
Pc0:10.10.1.1 dan subnet mask 255.255.255.0;
Pc1:10.10.1.2 dan subnet mask 255.255.255.0;
Pc2:10.10.1.3 dan subnet mask 255.255.255.0;
Pc3:10.10.1.4 dan subnet mask 255.255.255.0
Default gateway dan dns server kosong
 - a. Koneksikan ke 4 pc tersebut yaitu pc0, pc1, pc2 dan p3 pada switch, melalui media kabel: pc0 dan pc1 menggunakan kabel straight, sedang pc2 dan pc3 menggunakan kabel cross!
 - b. Uji tes koneksi dengan perintah ping ke 4 pc tersebut dan apa hasilnya ?
 - c. Berikan kesimpulan terhadap koneksi 4 pc tersebut ketika dihubungkan dengan 2 jenis kabel yang berbeda!

4.4. Contoh Kasus

Pada sebuah perkantoran SOHO, ingin dibangun jaringan LAN dengan spesifikasi kebutuhan sebagai berikut:

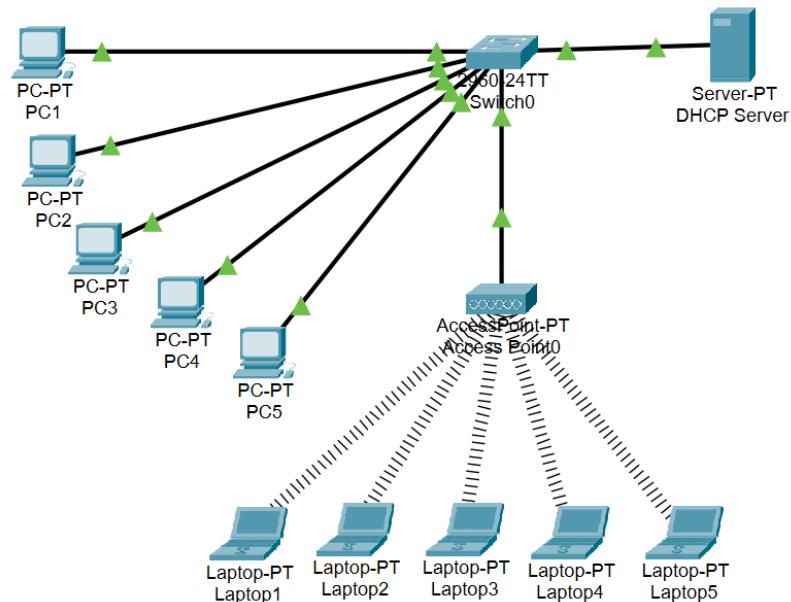
- 1 server, 1 AP, 1 switch, 5 pc dan 5 laptop;
- 1 server utk DHCP server dengan IP static 192.168.1.100, 5 pc dan 5 laptop akan menggunakan IP private dengan network 192.168.1.0 dengan ketentuan: 5 pc koneksinya menggunakan kabel sedangkan 5 laptop koneksinya menggunakan wireless.(nirkabel). Baik pc maupun laptop metode ip nya dilakukan secara random/ auto detect (DHCP);
- Jaringan LAN ini koneksinya menggunakan media nirkabel (wireless).

Penugasan:

Buatlah rancangan logis jaringan LAN tersebut!

Pemecahan:

Desain jaringan atau rancangan jaringan berdasarkan soal contoh kasus diatas digambarkan sebagai berikut ini:



BAB IV PENERAPAN SISTEM JARINGAN KOMPUTER

4.1. Uraian Materi

Tahapan implementasi atau penerapan rancangan jaringan yang efektif memerlukan pemahaman yang kuat tentang kondisi terkini dari model jaringan yang direkomendasikan dan kemampuan untuk berkembang seiring dengan pertumbuhan jaringan.

Beberapa poin penting dalam implementasi rancangan jaringan yang harus dipahami antara lain:

- 1) Kebutuhan untuk Skalabilitas Jaringan
- 2) Rancangan Jaringan secara Hirarkis
- 3) Rancangan Jaringan secara Enterprise
- 4) Domain Kegagalan (Failure Domain)
- 5) Penerapan Redundansi

Beberapa tahapan dalam implementasi rancangan jaringan computer antara lain:

- 1) Penerapan rancangan fisik
- 2) Penerapan rancangan logis
- 3) Uji coba system jaringan
- 4) Evaluasi hasil uji coba system jaringan
- 5) Go live

a. Penerapan Rancangan Fisik Jaringan Komputer

Beberapa tahapan dalam implementasi rancangan fisik jaringan computer antara lain:

a.1. Pemilihan perangkat keras jaringan dan platform

Saat merancang jaringan, penting untuk memilih perangkat keras yang tepat untuk memenuhi persyaratan jaringan saat ini, serta memungkinkan pertumbuhan jaringan. Dalam jaringan perusahaan, baik switch dan router

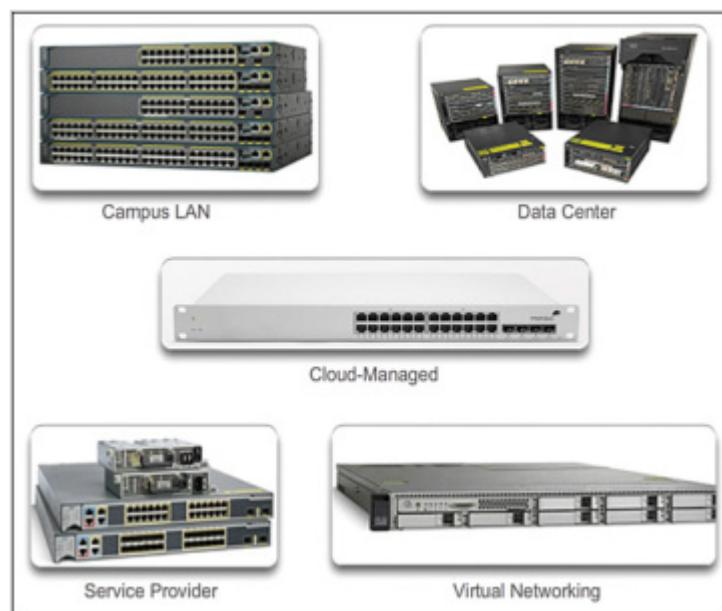
memainkan peran penting dalam komunikasi jaringan. Dalam pengadaan perangkat jaringan perlu menentukan spesifikasi. Spesifikasi perangkat harus jelas dan detail berdasarkan kebutuhan yang telah ditetapkan pada tahapan perancangan.

1) Pemilihan Switch

- Menentukan platform Switch

Ada 5 kategori switch, yaitu:

- Campus LAN Switches
- Cloud-Managed Switches
- Data Center Switches
- Service Provider Switches
- Virtual Networking



Gambar 59. Platoform Switch

- Pemilihan model konfigurasi

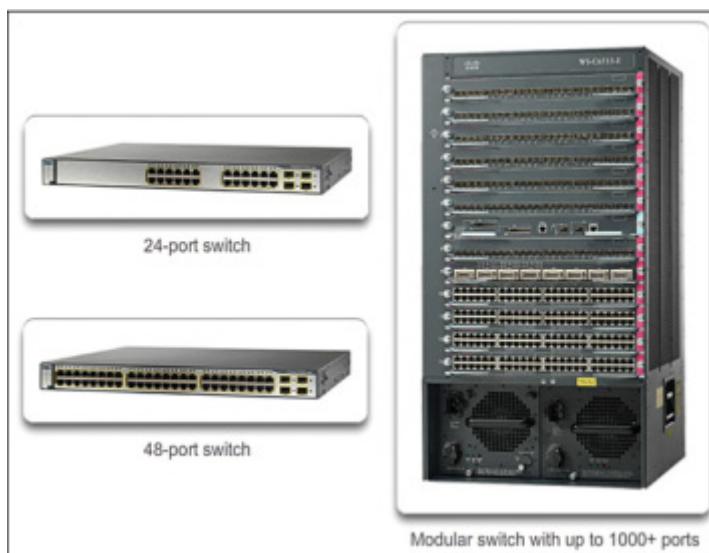
Model konfigurasi switch antara lain:

- Fixed configuration
- Modular configuration
- Stackable configuration



Gambar 60. Model Konfigurasi Switch

- Pemilihan kepadatan dan kecepatan port switch



Gambar 61. Kepadatan Port pada Switch

- Fitur Power over Ethernet (PoE) untuk fleksibilitas
- Switch Multilayer untuk redundansi

2) Pemilihan Router

Di Layer Distribusi jaringan perusahaan, *routing* (perutean) diperlukan. Tanpa proses perutean, paket tidak dapat meninggalkan jaringan lokal. Router memainkan peran penting dalam jaringan dengan menghubungkan beberapa situs dalam jaringan perusahaan, menyediakan jalur yang berlebihan, dan menghubungkan ISP di Internet. Router juga dapat bertindak sebagai penerjemah antara berbagai jenis media dan protokol. Misalnya, router dapat menerima paket dari jaringan Ethernet dan merangkumnya kembali untuk

diangkut melalui jaringan serial. Router menggunakan bagian jaringan dari alamat IP tujuan untuk merutekan paket ke tujuan yang tepat. Mereka memilih jalur alternatif jika tautan terputus atau lalu lintas macet. Semua host di jaringan lokal menentukan alamat IP dari interface router lokal dalam konfigurasi IP mereka.

a.2. Instalasi perangkat jaringan

Proses instalasi biasanya merupakan bagian dari tahapan pengadaan perangkat jaringan. Instalasi dapat dilakukan oleh pihak penyedia ataupun teknisi yang memahami pemasangan router. Proses instalasi perangkat jaringan meliputi pemasangan kabel (*cabling*) jaringan pada port router dan switch termasuk perangkat endpoint (server, PC, dan perangkat lainnya) berdasarkan rancangan fisik.

Pada perangkat endpoint perlu dipastikan telah terpasang ethernet card dan terinstal drivernya.

b. Penerapan Rancangan Logis Jaringan Komputer

Tahapan penerapan rancangan logis meliputi kegiatan pengaturan (*setting*) dan konfigurasi perangkat jaringan yang telah terpasang. Pengaturan dan konfigurasi dilakukan pada perangkat jaringan dan perangkat endpoint. Konfigurasi dapat dilakukan menggunakan perintah (*command*) pada CLI atau melalui GUI.

1) Konfigurasi Router dan Switch (*Core, Distribution, Access Point*)

Berikut ini adalah konfigurasi yang diperlukan beserta contoh *command* pada CLI.

- Menghidupkan mode konfigurasi
 - switch>enable*
- Setting jam dan tanggal

```
switch>enable  
switch#clock set 12:20:20 5 February 2022  
switch#show clock
```

- Pengaturan hostname

```
Switch(config)#hostname Sw-Master
```

- Pengaturan nama domain

```
Sw-Master(config)#vtp domain BPS
```

```
Sw-Master(config)#vtp mode server
```

```
Sw-Master(config)#vtp version 2
```

```
Sw-Master(config)#vtp password password12345
```

- Pembuatan VLAN

```
Sw-Master(config)#vlan 10
```

```
Sw-Master(config-vlan)#name VLAN10
```

```
Sw-Master(config)#vlan 20
```

```
Sw-Master(config-vlan)#name VLAN20
```

- Pengaturan interface

```
Sw-Master(config)#interface FastEthernet0/1
```

```
Sw-Master(config-if)#switchport mode trunk
```

```
Sw-Master(config-if)#switchport trunk native vlan 10
```

```
Sw-Master(config)#interface FastEthernet0/2
```

```
Sw-Master(config-if)#switchport mode trunk
```

```
Sw-Master(config-if)#switchport trunk native vlan 20
```

- Pengaturan interlace VLAN

```
Sw-Master(config)#interface vlan 10
```

```
Sw-Master(config-if)#ip address 192.158.10.10 255.255.255.0
```

```
Sw-Master(config)#interface vlan 20
```

```
Sw-Master(config-if)#ip address 192.158.20.10 255.255.255.0
```

- Reboot switch setelah selesai melakukan konfigurasi

```
Switch#reboot
```

2) Konfigurasi Perangkat Keamanan

Perangkat keamanan baik berupa IDS (*Intrusion Detection System*), IPS (*Intrusion Prevention System*), maupun Firewall memerlukan konfigurasi. Konfigurasi diatur menurut kebutuhan.

3) Konfigurasi Endpoint (Server dan PC Client)

Beberapa pengaturan umum yang diperlukan meliputi: pengaturan ethernet card, nama computer dan workgroup dan pengaturan IP Address (Statis atau DHCP), Subnet Mask ID, DNS.

Bebberapa hal penting yang perlu diperhatikan pada konfigurasi server agar dapat terkoneksi dengan jaringan antara lain:

- Memastikan beberapa perintah (command) seperti ifconfig, nslookup, dig, traceroute, netstat sudah terpasang dan dilakukan update.
- Melakukan pengecekan keberadaan lokasi direktori jaringan yaitu /etc/resolv.conf yang diperlukan untuk pengisian IP DNS resolvers.
- Mengubah DHCP pada server menjadi IP statis, dengan cara:
 - Perubahan isian pada file konfigurasi ifcfg-enp0s3 di lokasi direktori /etc/sysconfig/network-script;
 - Penambahan nama pada hostname di lokasi /etc/hostname;
 - Penambahan pemetaan IP address dan nama pada hosts di lokasi /etc/hosts
- Pastikan informasi status jaringan seperti alamat IP perangkat, konfigurasi jaringan yang sedang aktif, alamat netmask, broadcast ditemukan, dengan #ifconfig atau ifconfig -a atau ip a
- Pastikan setiap selesai melakukan perubahan konfigurasi jaringan dengan perintah #systemctl restart network
-

Perintah di atas dapat dijalankan pada server dengan OS berbasis Linux, untuk OS Windows biasanya menggunakan GUI.

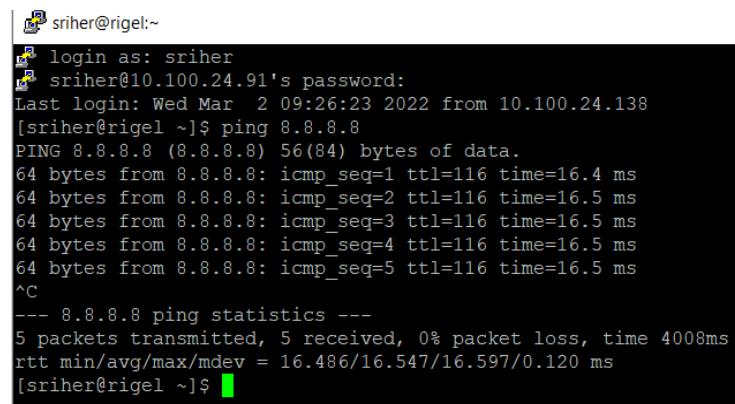
c. Pengujian Sistem Jaringan Komputer

Pengujian sistem jaringan komputer adalah kegiatan melakukan uji coba terhadap koneksi jaringan. Uji coba dilakukan untuk memastikan bahwa jaringan telah terpasang dan dikonfigurasi dengan benar.

Perintah (*command*) umum yang digunakan untuk melihat bahwa perangkat telah terhubung ke jaringan adalah *ping*.

```
#ping ip gateway
```

```
#ping ip dns
```



```
sriher@rigel:~$ login as: sriher
[sriher@rigel ~]$ sriher@10.100.24.91's password:
Last login: Wed Mar  2 09:26:23 2022 from 10.100.24.138
[sriher@rigel ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=16.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=16.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=16.5 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=16.5 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=116 time=16.5 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 16.486/16.547/16.597/0.120 ms
[sriher@rigel ~]$
```

Gambar 62. Tes koneksi dengan ping

Pengujian jaringan juga dapat dilakukan dengan melakukan remote system ke host tujuan. Disarankan menggunakan user selain root, yang sebelumnya sudah diberikan hak level setingkat root.

- Terlebih dahulu lakukan instalasi openssh-server openssh-client

```
$sudo openssh-server openssh-client
```

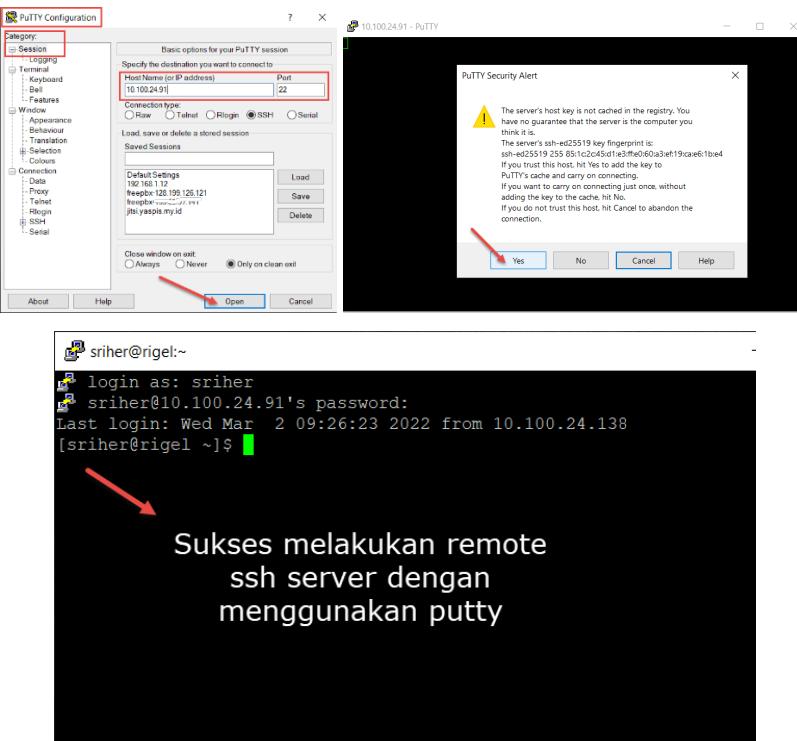
Operasional seputar remote sshd

- ✓ Mengaktifkan sshd service
\$sudo systemctl start sshd
- ✓ Menghentikan sshd service
\$sudo systemctl stop sshd
- ✓ Pengecekan status sshd

`$sudo systemctl status sshd`

- ✓ Membuat otomatis aktif sshd, ketika sistem operasi linux CentOS setelah proses booting/restart
- `$sudo systemctl enable sshd`

b. Pastikan remote ssh bisa dilakukan dengan aplikasi putty



Gambar 63. Serangkaian remote ssh dengan Putty

d. Contoh Penerapan dan Pengujian Sistem Jaringan Menggunakan Cisco Packet Tracker

Untuk memudahkan pemahaman dalam penerapan rancangan jaringan, berikut ini dicontohkan perancangan sistem jaringan, dengan skenario sebagai berikut:

Dalam satu lantai sebuah gedung, akan dibangun 2 jaringan LAN, 1 jaringan untuk kebutuhan komputer klien (LAN 1), dan 1 jaringan lagi

untuk kebutuhan server farm (LAN 2). Inventarisasi secara lengkap ketersediaan perangkat jaringan sebagai berikut:

- ✓ Jumlah switch 2, router 1
- ✓ Jumlah server 3, yaitu server untuk DNS, Email dan Web;
- ✓ Jumlah komputer 10, 7 pc terkoneksi dengan media kabel, dan 3 laptop terhubung wireles (nirkabel);
- ✓ IP address untuk server menggunakan IP private 10.0.0.x;
- ✓ sedang untuk komputer klien adalah 192.168.1.x dan laptop diisikan IP addressnya mulai dari 192.168.1.50 dst;
- ✓ Koneksi jaringan dan pemberian IP addressnya menggunakan IP address statik.

Target perancangan dan konfigurasi adalah sebagai berikut:

1. Jaringan LAN komputer klien saling terhubung;
2. Jaringan LAN antar server (server farm) saling terhubung;
3. Jaringan LAN komputer klien dan server farm saling terhubung;
4. Fungsionalitas layanan server untuk web bisa berfungsi;
5. Fungsionalitas layanan server untuk email bisa berfungsi;
6. Fungsionalitas layanan server untuk DNS bisa berfungsi.

Tahapan penyelesaian:

Setiap pc dengan media kabel jaringan dihubungkan ke perangkat switch dan masing masing diisikan IP addressnya, baik pada jaringan LAN 1 (Komputer klien) dan LAN 2 (Server farm). Untuk memudahkan dalam memetakan alokasi IP address, datususun dalam bentuk tabel sebagai berikut:

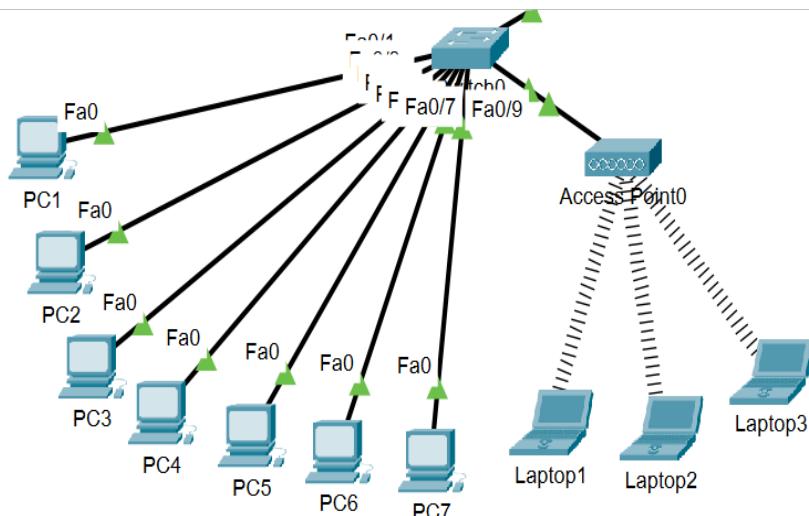
JARINGAN LAN 1 (KOMPUTER KLIEN)				
NO	DEVICE	IP ADDRESS	GATEWAY	SUBNET MASK
1	PC1	192.168.1.1	192.168.1.254	255.255.255.0
2	PC2	192.168.1.2	192.168.1.254	255.255.255.0

3	PC3	192.168.1.3	192.168.1.254	255.255.255.0
4	PC4	192.168.1.4	192.168.1.254	255.255.255.0
5	PC5	192.168.1.5	192.168.1.254	255.255.255.0
6	PC6	192.168.1.6	192.168.1.254	255.255.255.0
7	PC7	192.168.1.7	192.168.1.254	255.255.255.0
8	LAPTOP1	192.168.1.50	192.168.1.254	255.255.255.0
9	LAPTOP2	192.168.1.51	192.168.1.254	255.255.255.0
10	LAPTOP3	192.168.1.53	192.168.1.254	255.255.255.0
JARINGAN LAN 2 (SERVER FARM)				
NO	DEVICE	IP ADDRESS	GATEWAY	SUBNET MASK
1	Server DNS	10.0.0.1	10.0.0.254	255.255.255.0
2	Server Web	10.0.0.2	10.0.0.254	255.255.255.0
3	Server Email	10.0.0.3	10.0.0.254	255.255.255.0

Jaringan LAN komputer klien saling terhubung:

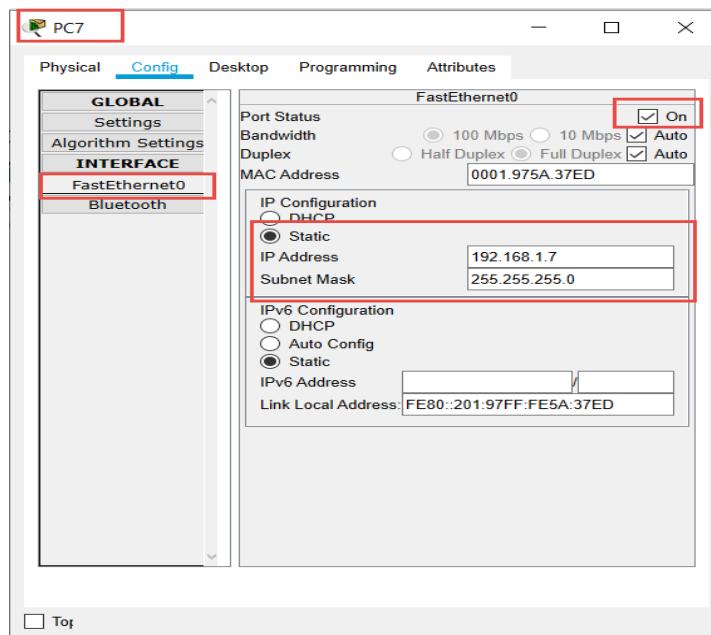
Rancangan gambar design berdasarkan isian tabel diatas seperti berikut:

Perancangan LAN Komputer Klien



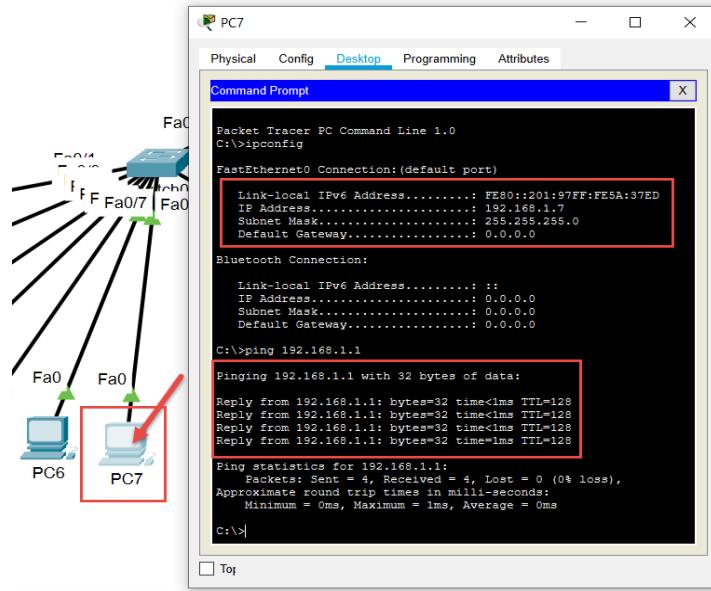
Gambar 64. Desain jaringan LAN komputer klien

Setelah melakukan perancangan topologi jaringan, kemudian dilakukan penerapan dengan melakukan konfigurasi. Konfigurasi pada masing-masing pc dan laptop untuk diisikan IP addressnya, misalnya pada pc7 seperti pada gambar berikut ini:



Gambar 65. Pengisian IP address pada pc

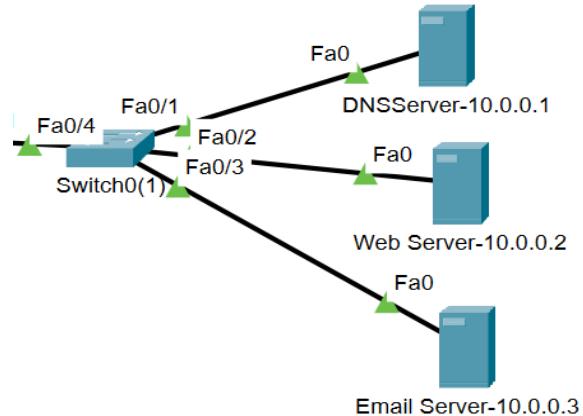
Kemudian dilakukan pengecekan koneksi antar pc, dengan menggunakan perintah ping, misalnya test koneksi dari pc 7 ke pc1, dan sebaliknya, terlihat seperti pada gambar berikut ini:



Gambar 66. Status hasil tes koneksi antar pc

2. Jaringan Lan antar server (server farm) saling terhubung:

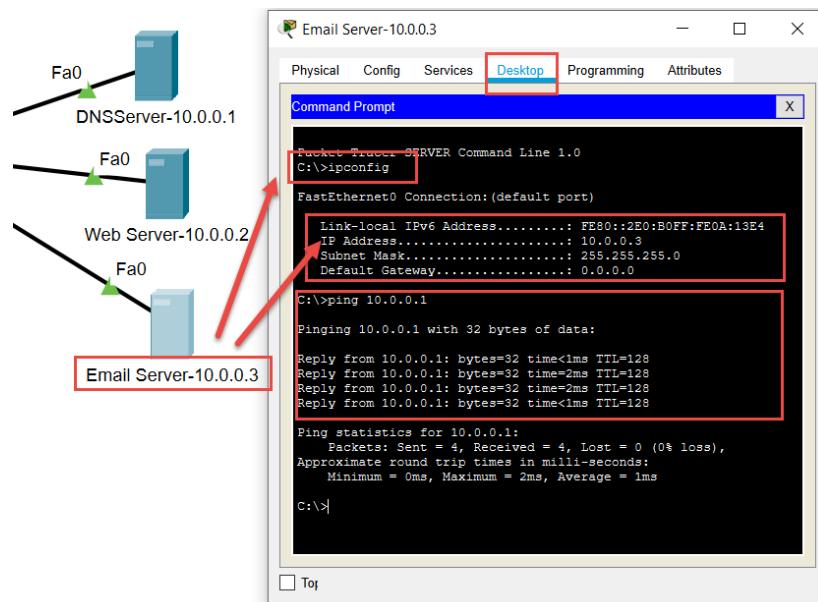
Perancangan LAN Server Farm



Gambar 67. Desain jaringan LAN server farm

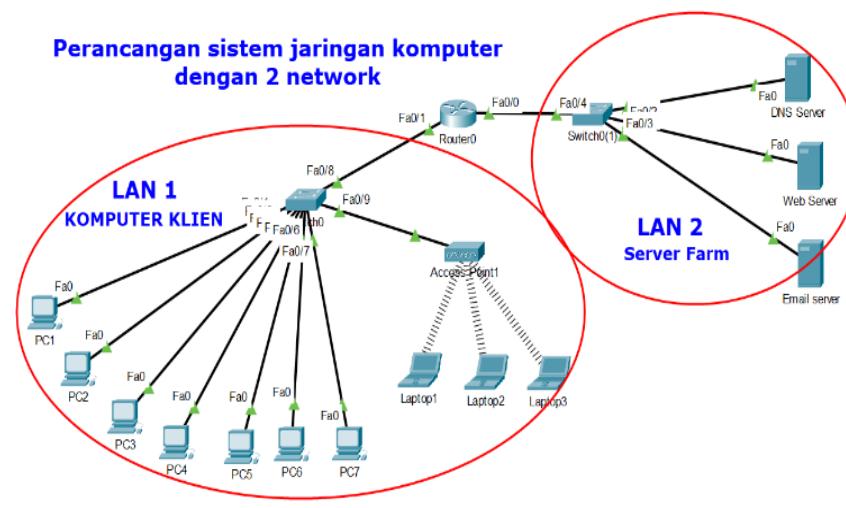
Tes koneksi antar server juga dilakukan. Server dengan IP address 10.0.0.3 yaitu server email ditujukan ke server 10.0.0.1 yaitu server DNS, dengan perintah ping, demikian juga untuk server web, dan

server email dilakukan hal yang sama. Contoh berikut adalah hasil tes koneksi nya seperti terlihat pada gambar dibawah ini:



Gambar 68. Status hasil tes koneksi antar server

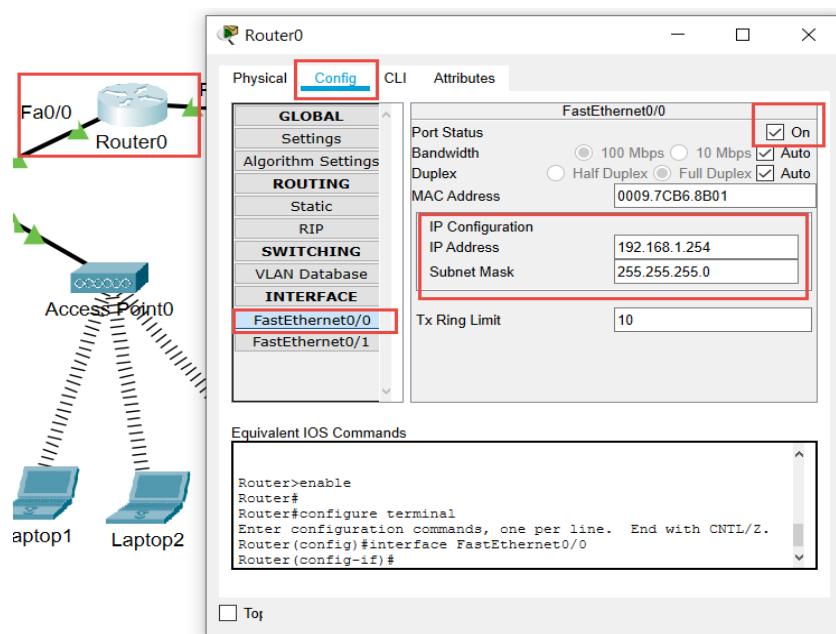
Untuk menghubungkan antara jaringan LAN 1 dan Jaringan LAN 2 dibutuhkan perangkat router, sehingga akan terbentuk rancangannya seperti gambar berikut ini:



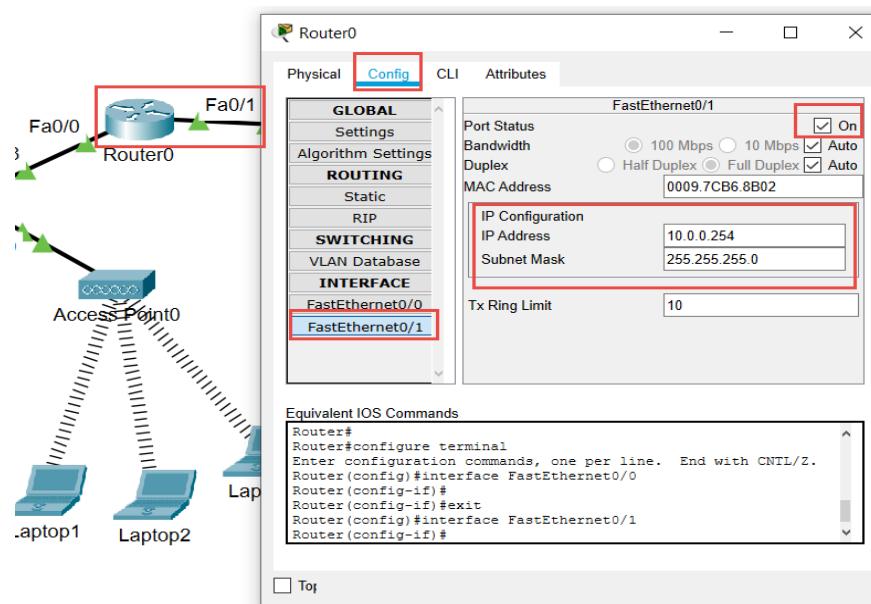
Gambar 69. Desain layout dua Jaringan LAN

3. Jaringan LAN komputer klien dan server farm saling terhubung:

Dalam jaringan yang sama, hal yang perlu diketahui adalah tidak menjadi masalah isian pada gateway dikosongkan. Namun jika ingin terhubung dari jaringan 1 ke jaringan lainnya terlebih dahulu pada masing-masing komputer klien dan setiap server harus diisikan alamat gatewaynya. Sehingga kedua jaringan yang berbeda bisa saling berkomunikasi. Isian alamat gateway ini mengacu pada konfigurasi pada routernya. Berikut ini konfigurasi pada router yang harus diisikan baik dari sisi jaringan LAN 1 (komputer klien) dan dari sisi LAN 2 (server farm).

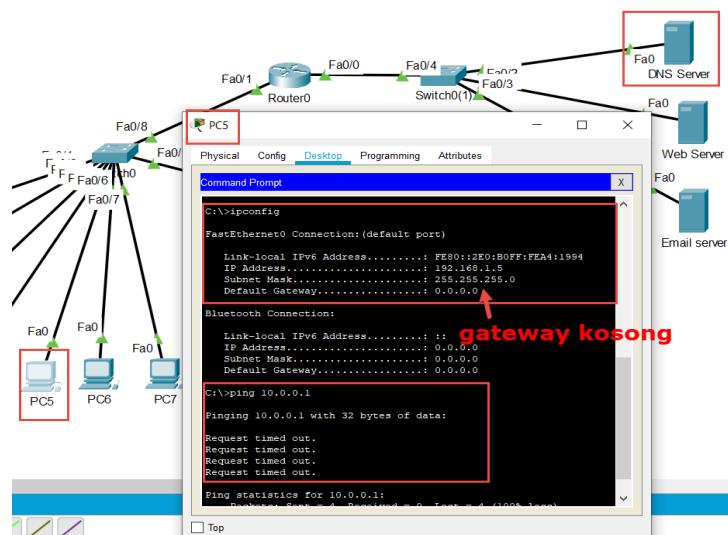


Gambar 70. IP address interface router FE0/0, sisi komputer klien



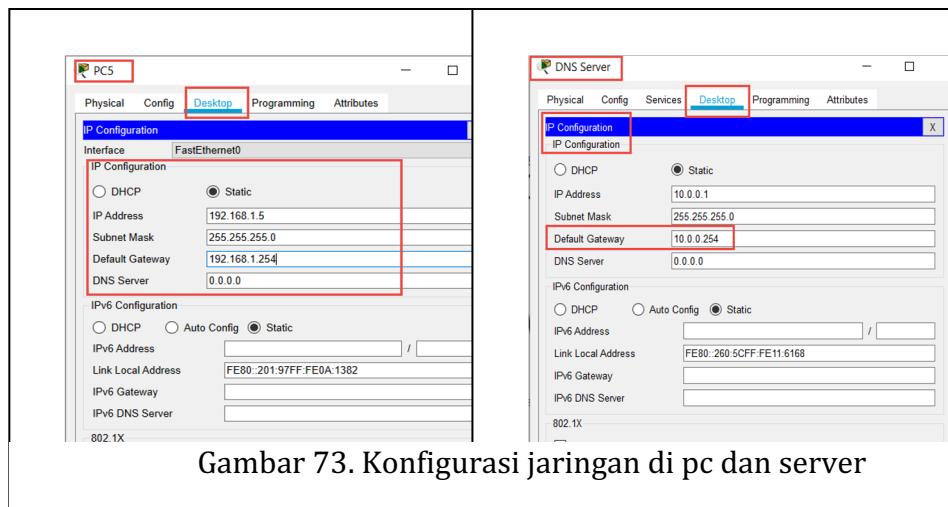
Gambar 71. IP address interface router FE0/1, sisi server farm

Setelah kedua sisi router yaitu interface FE0/0 dan interface FE0/1 terisi IP addressnya, maka masing-masing pc, laptop dan server harus juga ditambahkan isian pada gatewaynya. Jika tidak mengisikan gatewaynya, maka ketika dilakukan pengecekan koneksi antar jaringan, maka hasilnya akan RTO, terlihat seperti pada gambar berikut ini:



Gambar 72. Status hasil tes koneksi dari pc5 ke server DNS

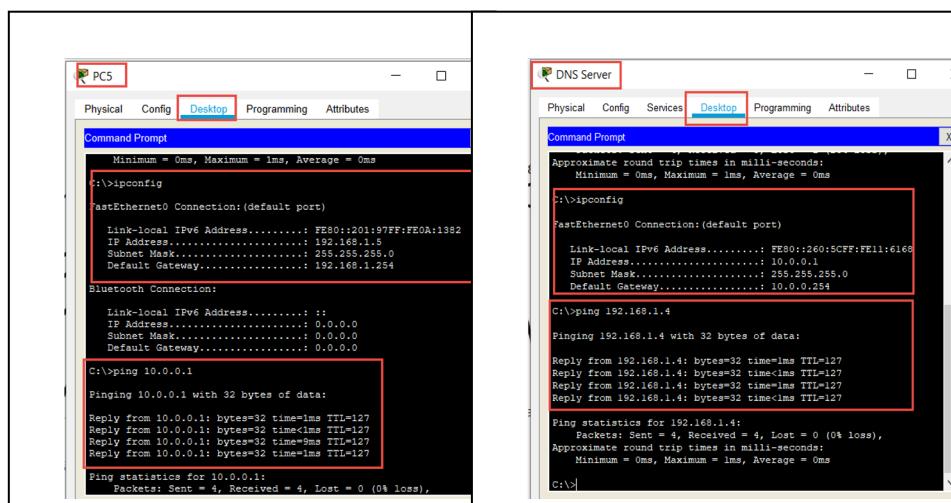
Permasalahan diatas, pemecahannya cukup sederhana, hanya dengan mengisikan IP address gateway pada masing-masing pc yaitu 192.168.1.254, pada LAN komputer klien, dan mengisikan gateway pada masing-masing server dengan IP address 10.0.0.254. Berikut ini dicontohkan capture isian gateway pada pc5, dan server DNS, sekaligus dilakukan tes koneksi dari pc 5 ke server DNS, maupun sebaliknya.



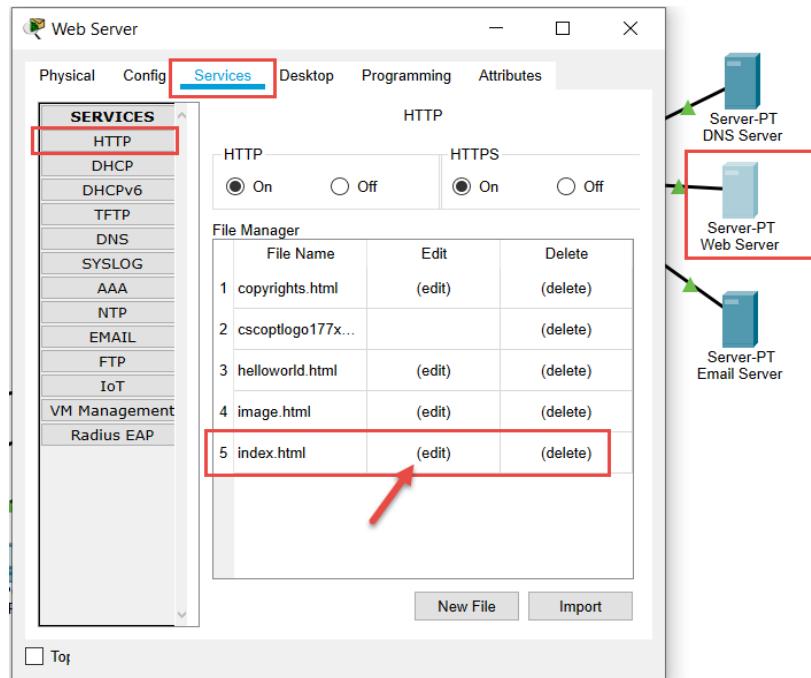
Gambar 73. Konfigurasi jaringan di pc dan server

4. Fungsionalitas layanan server untuk web bisa berfungsi:

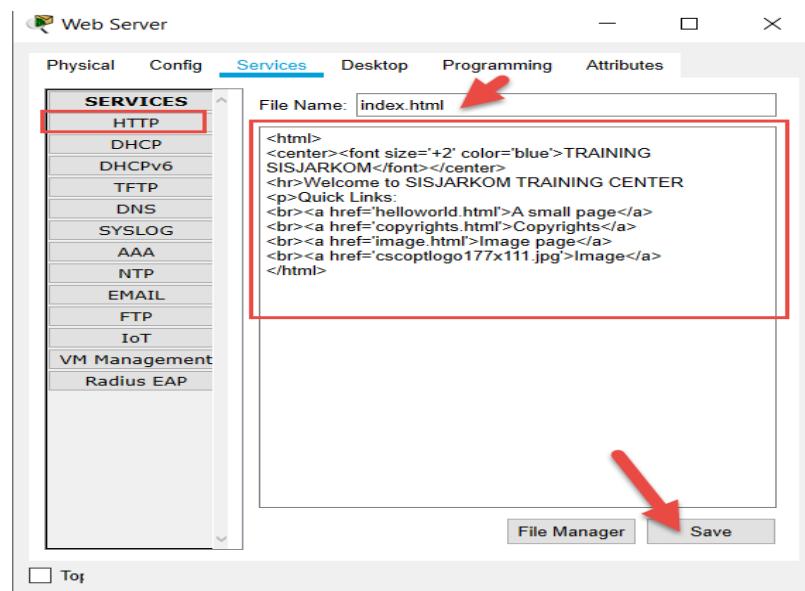
Konfigurasi dan setting web server pada Packet Tracer, terlihat seperti pada capture gambar berikut ini



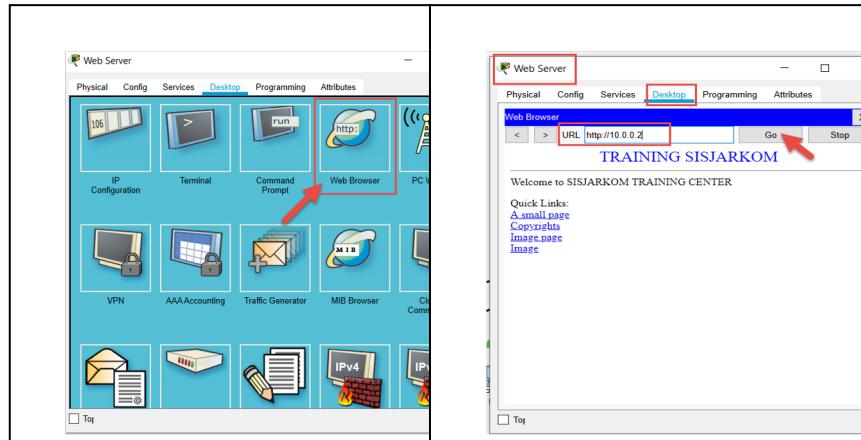
Gambar 74. Status hasil tes koneksi pc dan server



Gambar 75. Konfigurasi Web server



Gambar 76. Kustomisasi file index.html pada web server



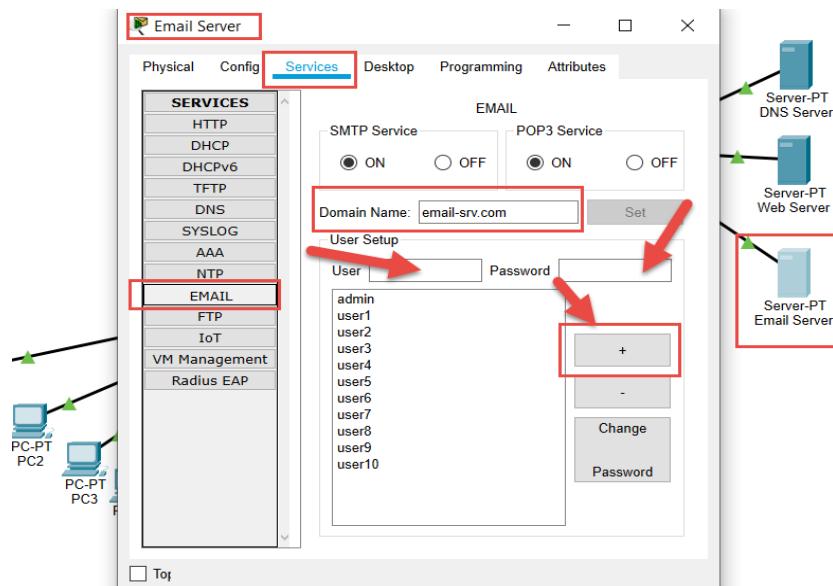
Gambar 77. Hasil tampilan web server pada browser

Setelah itu dilakukan pengecekan di browser pada Packet Tracer: terlihat pada gambar berikut ini:

Dari tampilan diatas, pada browser ketika di akses dengan alamat <http://10.0.0.2> memberikan informasi sesuai dengan isian pada file index.html. Hal ini berarti konfigurasi pada web server sudah berhasil dilakukan dengan benar.

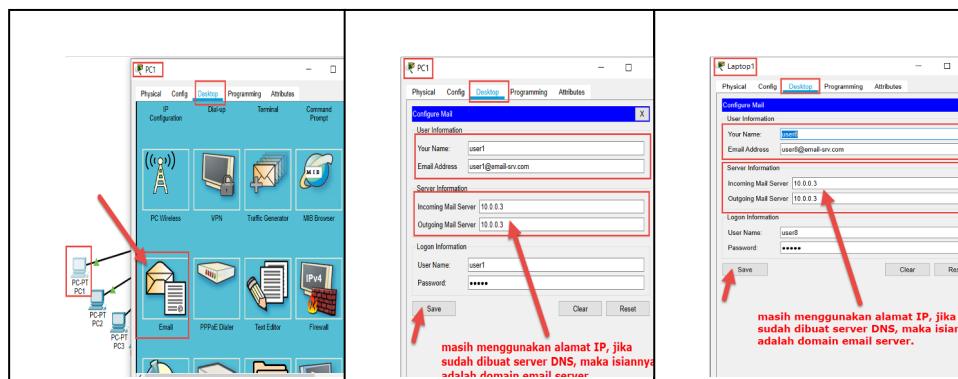
5. Fungsionalitas layanan server untuk email bisa berfungsi:

Konfigurasi dan setting email server pada Packet Tracer, terlihat seperti pada capture gambar berikut ini:



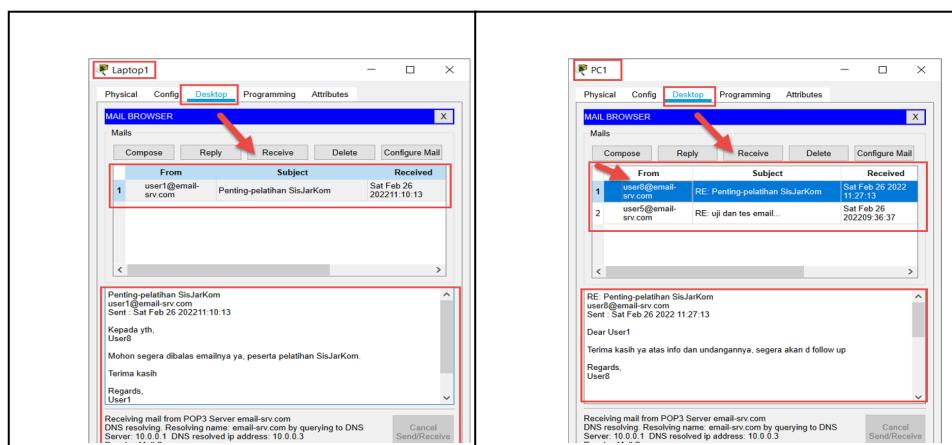
Gambar 78. Konfigurasi dan setting pada email server

Setelah selesai konfigurasi pada server email, maka agar semua pc dan laptop dalam jaringan tersebut bisa menggunakan emailnya, terlebih dahulu perlu dilakukan setting pada masing-masing pc. Berikut ini di contohkan isian konfigurasi pada pc 1 (user1) dan laptop1 (user8).



Gambar 79. Konfigurasi dan setting email pada komputer klien

server dan pc klien, dicoba dilakukan tes dan uji coba apakah email server berfungsi dengan benar, sehingga masing-masing pc yang sudah di konfigurasi untuk email bisa saling melakukan komunikasi (mengirim dan menerima email). Berikut ini capture gambar mengenai pengiriman dan penerimaan email antara pc1 dan laptop1.

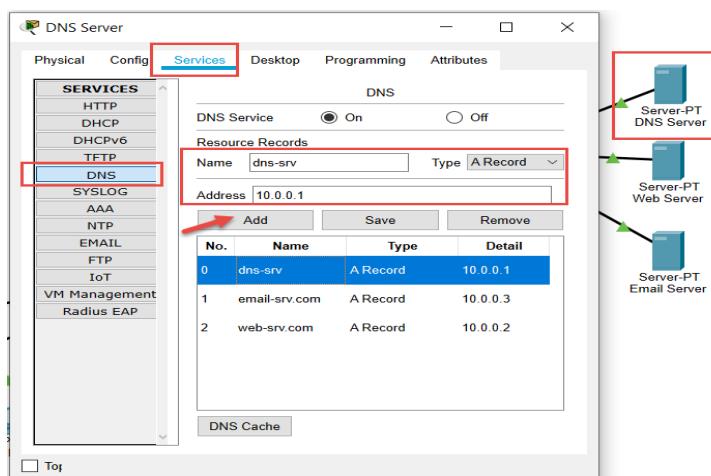


Gambar 80. Status hasil "send" dan "reply" email klien

Berdasarkan capture gambar diatas, dapat disimpulkan bahwa fungsionalitas email server sudah berfungsi dengan benar.

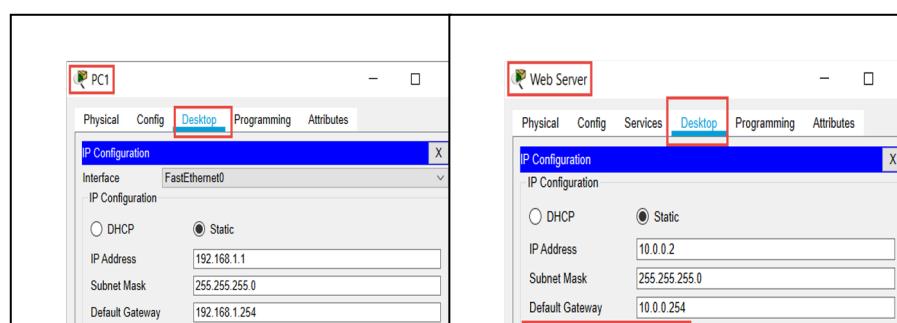
6. Fungsionalitas layanan server untuk DNS bisa berfungsi:

Seperti diketahui bersama, DNS atau *Domain Name System* adalah suatu sistem database terdistribusi untuk mencari suatu nama situs atau domain yang terhubung dengan jaringan menggunakan protokol TCP/IP. Sedang server DNS adalah sistem komputer yang menjalankan layanan kerja DNS yaitu menterjemahkan alamat domain menjadi IP address, dan dipahami oleh komputer. Cara melakukan konfigurasi pengisian dns, server web dan server email pada server DNS, seperti terlihat pada capture berikut ini:



Gambar 81. Konfigurasi DNS server

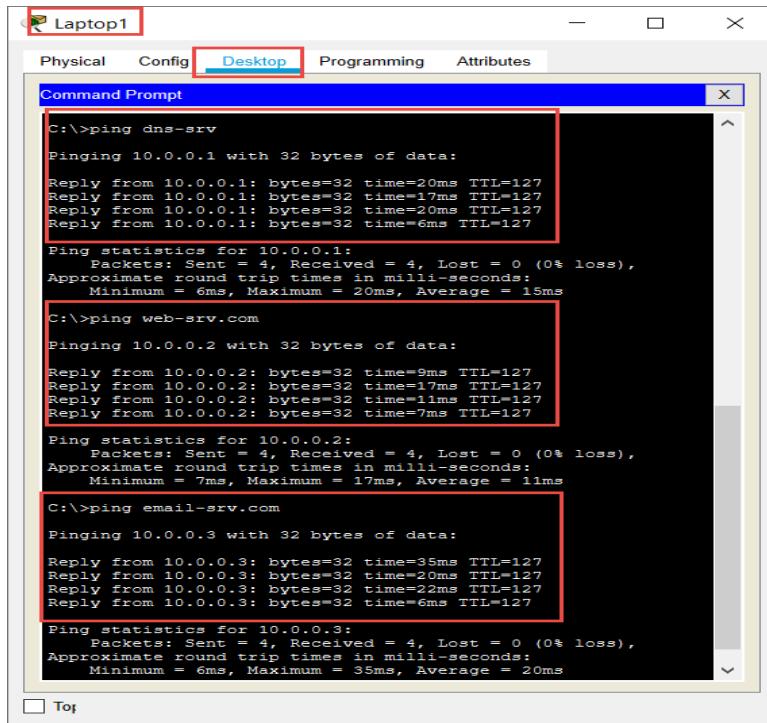
Setelah konfigurasi DNS server selesai dilakukan, untuk memastikan apakah berhasil atau tidak dengan cara : i)Pastikan



konfigurasi pada setiap pc, laptop dan server ditambahkan isian IP DNS Server yaitu IP address 10.0.0.1, seperti terlihat pada capture berikut ini:

Gambar 82. Pengisian IP DNS server pada pc dan server

ii) Tes koneksi dengan perintah ping, misalnya dari pc atau laptop ditujukan ke 3 server yaitu DNS server, web server dan email server. Seperti pada capture gambar berikut ini:



```
C:\>ping dns-srv
Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time=20ms TTL=127
Reply from 10.0.0.1: bytes=32 time=17ms TTL=127
Reply from 10.0.0.1: bytes=32 time=20ms TTL=127
Reply from 10.0.0.1: bytes=32 time=6ms TTL=127

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 20ms, Average = 15ms

C:\>ping web-srv.com
Pinging 10.0.0.2 with 32 bytes of data:
Reply from 10.0.0.2: bytes=32 time=9ms TTL=127
Reply from 10.0.0.2: bytes=32 time=17ms TTL=127
Reply from 10.0.0.2: bytes=32 time=11ms TTL=127
Reply from 10.0.0.2: bytes=32 time=7ms TTL=127

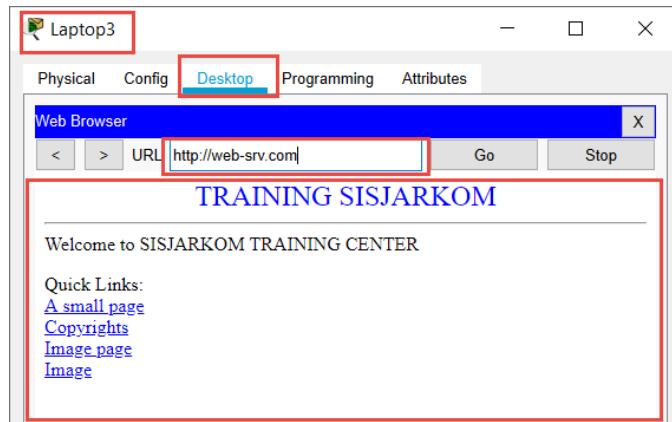
Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 17ms, Average = 11ms

C:\>ping email-srv.com
Pinging 10.0.0.3 with 32 bytes of data:
Reply from 10.0.0.3: bytes=32 time=35ms TTL=127
Reply from 10.0.0.3: bytes=32 time=20ms TTL=127
Reply from 10.0.0.3: bytes=32 time=22ms TTL=127
Reply from 10.0.0.3: bytes=32 time=6ms TTL=127

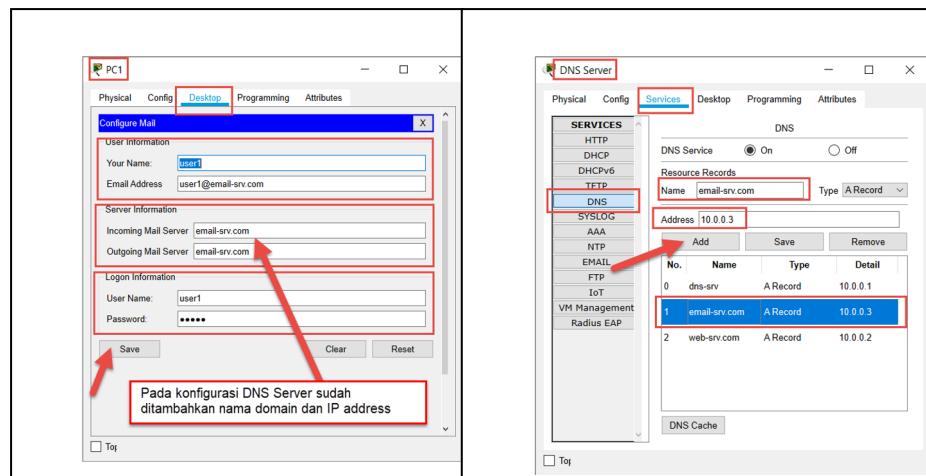
Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 35ms, Average = 20ms
```

Gambar 83. Status hasil tes koneksi dari laptop1 menuju ke 3 server

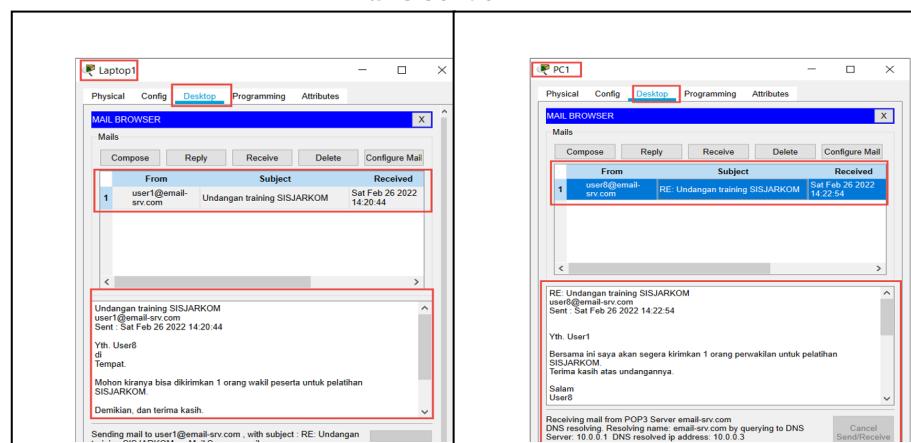
iii) Mengakses web server dan email server pada browser dengan alamat domainnya. Misalnya untuk IP address 10.0.0.2 domainnya adalah web-srv.com, sedang IP address 10.0.0.3 domainnya adalah email-srv.com. Berikut ini capture gambar akses web server domain web-srv.com.



Gambar 84. Status akses web-srv.com



Gambar 85. Konfigurasi pop3 dan smtp pada pc klien dan konfigurasi dns server



Gambar 86. Status hasil “send” dan “reply” email antara pc1 dan laptop1

Berdasarkan hasil pengujian tes fungsionalitas terhadap DNS server diatas, baik tes koneksi dari pc ke server dengan melakukan ping nama domain, akses web server dengan nama domain dan akses email dalam mengirim dan membalas email, semuanya bisa berjalan dengan baik. Maka dapat disimpulkan bahwa fungsionalitas DNS server sudah berfungsi dengan benar.

4.2. Contoh Kasus

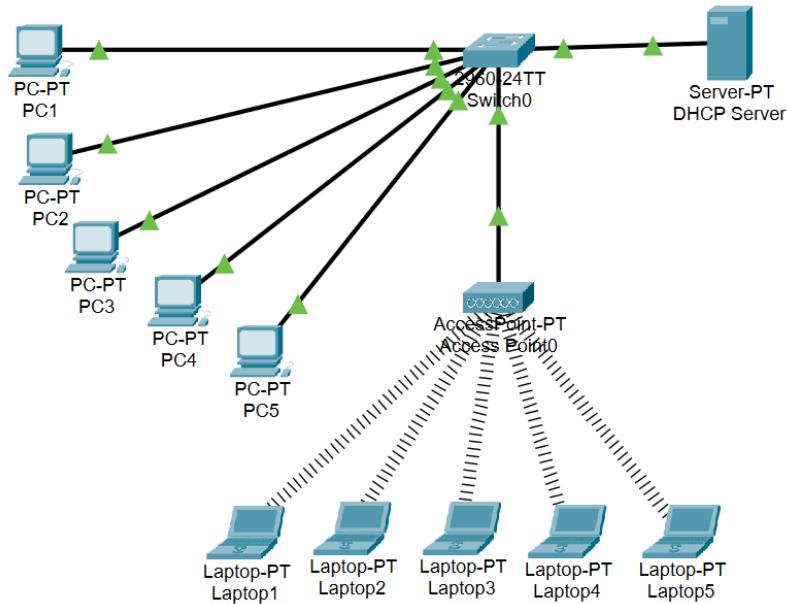
Pada sebuah perkantoran SOHO, ingin dibangun jaringan LAN dengan spesifikasi kebutuhan sebagai berikut:

Tersedia :

- 1 server, 1 AP, 1 switch, 5 pc dan 5 laptop;
- 1 server utk DHCP server dengan IP static 192.168.1.100, 5 pc dan 5 laptop akan menggunakan IP private dengan network 192.168.1.0 dengan ketentuan: 5 pc koneksinya menggunakan kabel sedangkan 5 laptop koneksinya menggunakan wireless.(nirkabel). Baik pc maupun laptop metode ip nya dilakukan secara random/ auto detect (DHCP);
- Jaringan LAN ini koneksinya menggunakan media nirkabel (wireless).

Rancangan jaringan digambarkan sebagai berikut ini:

RANCANGAN JARINGAN LAN PERKANTORAN SOHO

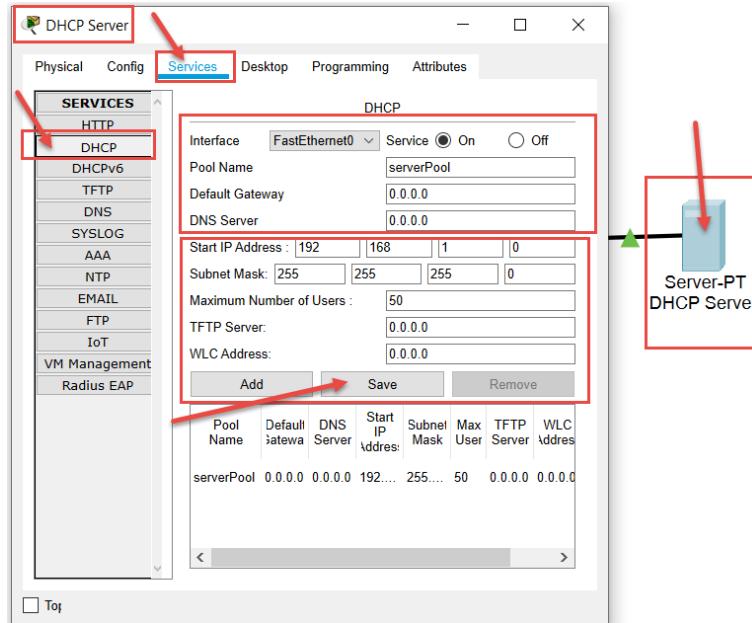


Penugasan:

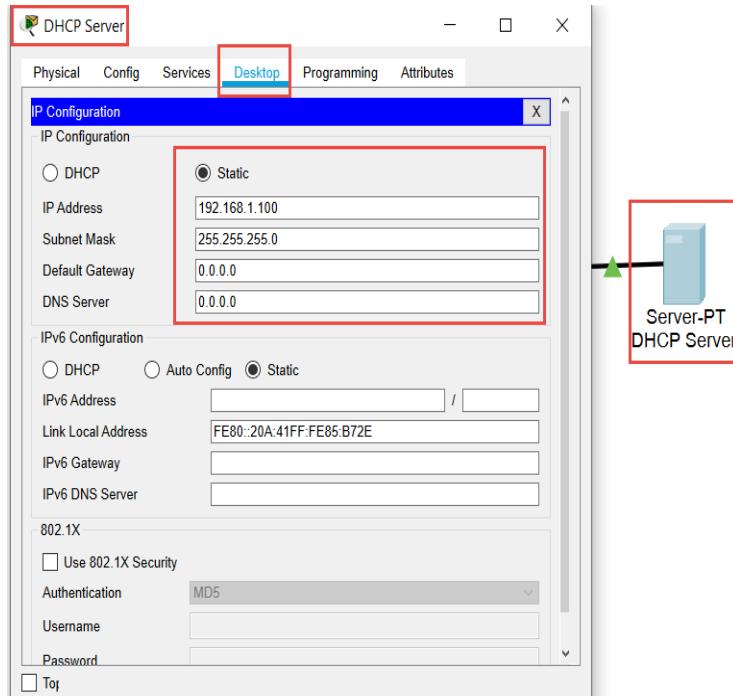
Dari rancangan jaringan tersebut, lakukan konfigurasinya serta, koneksi masing masing pc, laptop dan server tersebut melalui switch dan laptop melalui AP, sehingga semuanya berfungsi dengan benar!

Pemecahan:

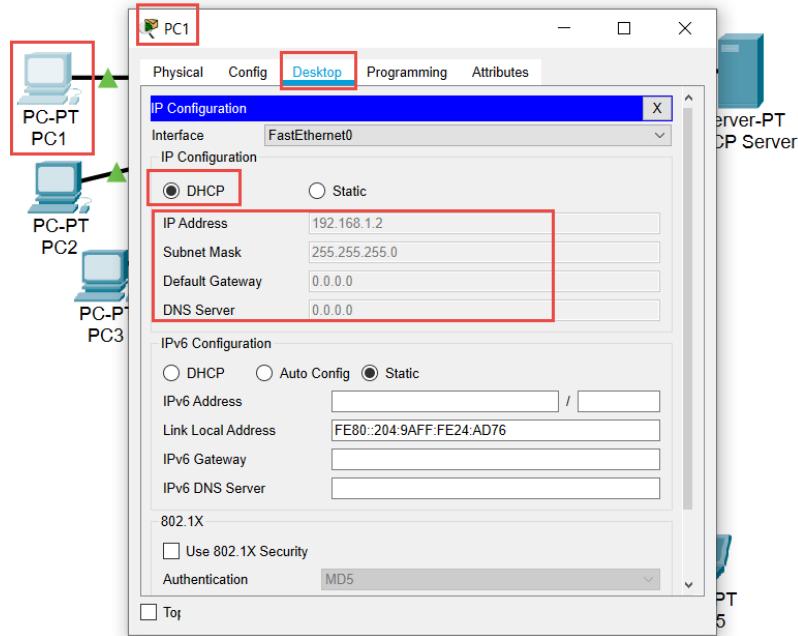
1. Konfigurasi pada server DHCP, seperti capture pada gambar berikut:



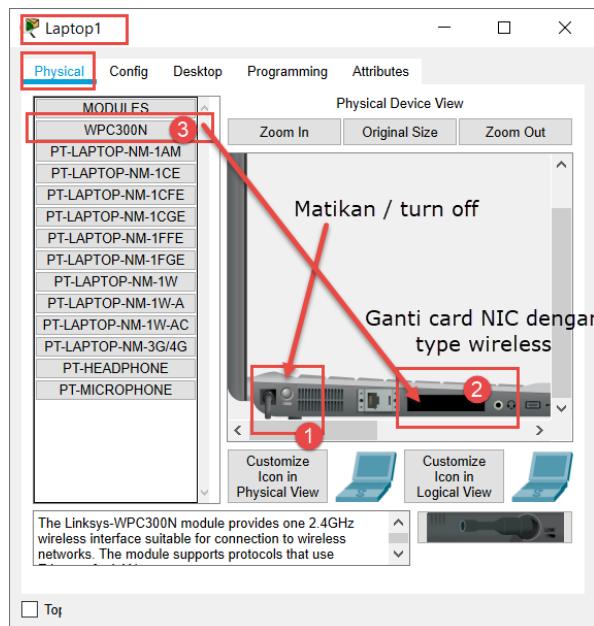
- Menambahkan alamat IP address static pada DHCP server, misalnya IP addressnya 192.168.1.100

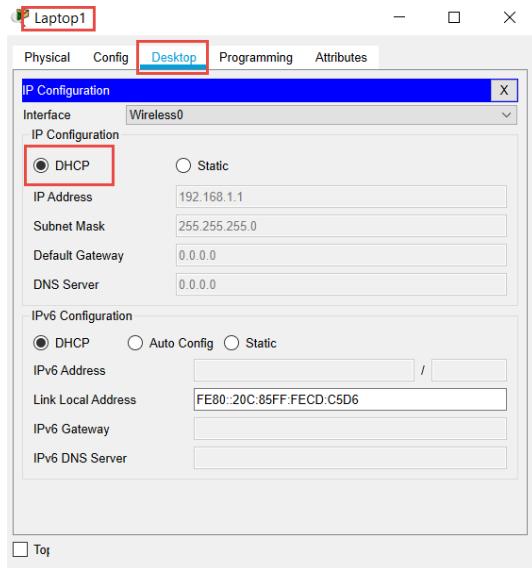


- Konfigurasi pada ke 5 pc, dengan pengisiannya sebagai berikut

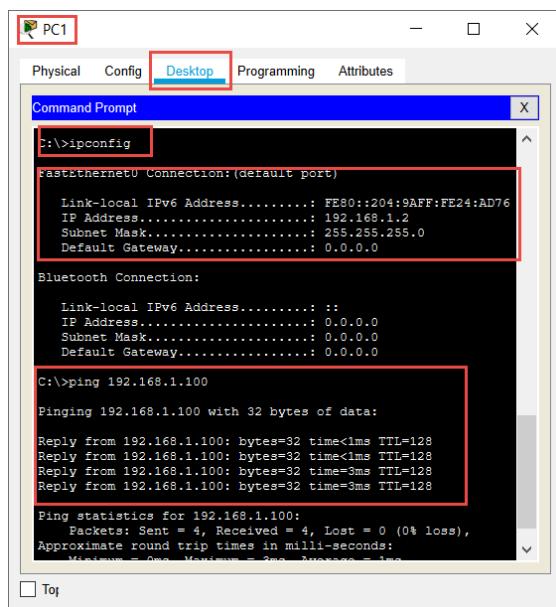


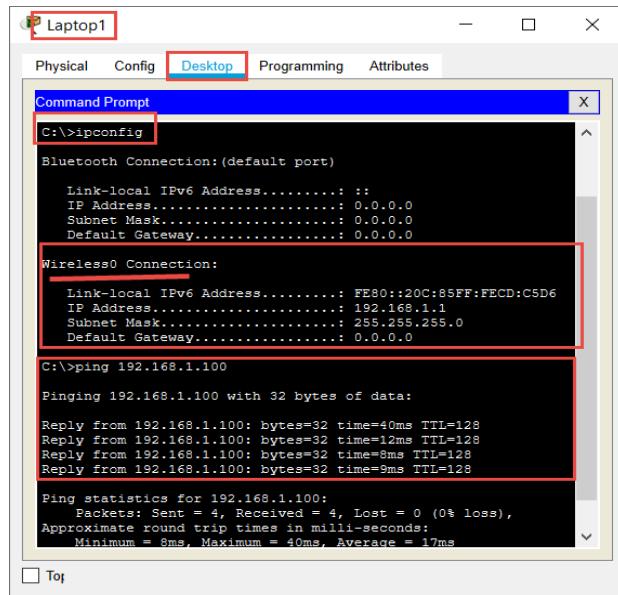
4. Konfigurasi pada ke 5 laptop, dengan pengisiannya sebagai berikut:





5. Lakukan tes koneksi antar device pc, laptop dan DHCP Server, sebagai berikut:





Laptop1

Physical Config Desktop Programming Attributes

Command Prompt

C:\>ipconfig

Bluetooth Connection: (default port)

Link-local IPv6 Address..... ::
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0

Wireless0 Connection:

Link-local IPv6 Address.....: FE80::20C:85FF:FECD:C5D6
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 0.0.0.0

C:\>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.1.100: bytes=32 time=40ms TTL=128
Reply from 192.168.1.100: bytes=32 time=12ms TTL=128
Reply from 192.168.1.100: bytes=32 time=9ms TTL=128
Reply from 192.168.1.100: bytes=32 time=9ms TTL=128

Ping statistics for 192.168.1.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 8ms, Maximum = 40ms, Average = 17ms

Berdasarkan 5 tahapan diatas dengan berpatokan pada desain/rancangan jaringan LAN Perkantoran SOHO yang dibuat, dapat disimpulkan bahwa : Secara operasional hasil simulasinya berfungsi dan berjalan dengan benar.

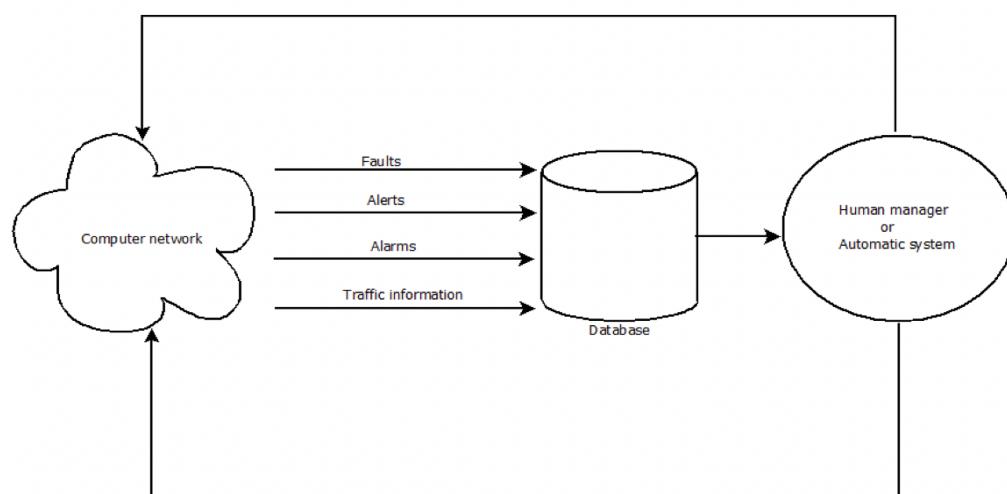
BAB V EVALUASI SISTEM JARINGAN KOMPUTER

4.1. Uraian Materi

Evaluasi sistem jaringan komputer ditujukan untuk memastikan sistem jaringan komputer dapat berjalan sesuai yang diharapkan dan sesuai dengan kebutuhan organisasi. Evaluasi erat kaitannya dengan pengelolaan jaringan komputer (*Network Management*).

Network Management adalah *service* yang menggunakan berbagai macam protokol, alat, aplikasi, dan perangkat yang membantu administrator jaringan dalam memonitor dan mengontrol sumber daya jaringan baik perangkat keras maupun lunak, untuk memenuhi kebutuhan.

Network Management dapat menggunakan dua pandangan. Pertama sebagai alat untuk membantu memonitor aktivitas jaringan untuk memperlihatkan gambaran dari kondisi jaringan sehingga dapat melakukan peningkatan dari sisi operasional maupun performa. Kedua sebagai alat yang mampu mengotomasi proses pada pemantauan jaringan, dimana informasi yang diperoleh dapat menjadi dasar dalam penyesuaian dan adaptasi jaringan oleh perangkat secara otomatis sehingga memenuhi operasional dan kinerja yang diinginkan.



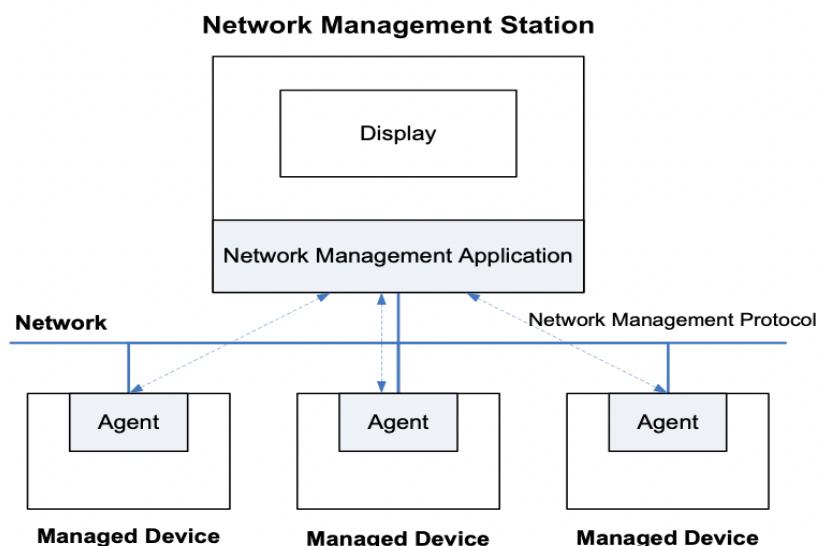
Gambar 87. *Network Management*

Contoh aktivitas pengelolaan jaringan:

1. Monitoring komputer dan jalur jaringan untuk mendeteksi *fault* yang mungkin muncul.
2. Monitoring antrian *message* pada tiap komputer untuk memastikan penggunaan sumber daya jaringan secara efisien dan mencegah *message loss*.
3. Mengontrol *routing message* yang melalui jaringan. Dapat digunakan untuk *routing fault* yang dideteksi di jaringan. Juga menyediakan jalan untuk menghindari jalur sibuk dimana *message* dapat tertunda.
4. Mendeteksi *network intrusion* dan memberikan *alarm*/peringatan pada administrator terkait trafik jaringan yang dicurigai.

Network Management System (NMS)

Network Management System (NMS) merujuk pada sekumpulan aplikasi yang memungkinkan komponen jaringan untuk dimonitor dan dikontrol. Secara umum, NMS mempunyai arsitektur dasar seperti pada Gambar berikut.



Gambar 88. Arsitektur NMS

Arsitektur memiliki dua elemen : perangkat pengelola (*management station*) sebagai manajer dan perangkat yang dikelola (*managed device*) sebagai agen. Selain itu terdapat *platform* yang digunakan aplikasi manajer untuk melakukan fungsi pengelolaan melalui interaksi dengan agen. Agen merespon dengan memberikan informasi yang diperlukan.

Adanya berbagai macam perangkat yang dikelola seperti *router*, *bridge*, *switch*, *hub*, dan perangkat lain serta berbagai macam sistem operasi dan antarmuka pemrograman, protokol pengelolaan menjadi penting untuk *management station* untuk berkomunikasi dengan *management agent* secara efektif. Protokol network management yang banyak dikenal yaitu SNMP dan CMIP. NMS secara umum dijelaskan menggunakan model *OSI network management*.

Tujuan utama dari *network management* adalah untuk memastikan sumber daya jaringan tersedia untuk pengguna yang memerlukan. Untuk memastikan kemajuan yang cepat dan konsisten dalam fungsi *network management*, ISO mengelompokkan fungsi pengelolaan ke dalam lima area yaitu:

1. Configuration Management

Configuration management fokus pada inisialisasi jaringan, penyediaan sumber daya jaringan dan layanan, serta monitoring dan pengontrolan jaringan. Lebih khususnya pada pengelolaan konfigurasi meliputi: pengaturan, pemeliharaan, penambahan, dan pembaruan hubungan antar komponen dan kondisi komponen selama jaringan berjalan.

Configuration Management terdiri dari konfigurasi perangkat dan konfigurasi jaringan. Konfigurasi perangkat dapat dilakukan langsung atau secara remote. Konfigurasi jaringan secara otomatis seperti *Dynamic Host Configuration Protocol* (DHCP) dan *Domain Name Services* (DNS) memiliki peran penting dalam *network management*.

2. Fault Management

Fault Management meliputi deteksi, isolasi, dan perbaikan dari anomali jaringan yang mungkin menyebabkan kegagalan OSI network. Tujuan utamanya untuk memastikan jaringan selalu tersedia dan saat terjadi kesalahan (*fault*) dapat segera mungkin diperbaiki.

Fault harus dibedakan dengan *error*. Error merupakan single event, sedangkan fault merupakan kondisi abnormal yang memerlukan perbaikan. Contohnya, jalur komunikasi yang terpotong adalah fault, dan single bit error pada komunikasi adalah error.

3. Accounting Management

Accounting management memungkinkan perangkat yang dikelola untuk diukur penggunaannya dan ditentukan biaya dari penggunaan tersebut. Pengukuran dapat termasuk sumber daya yang digunakan, fasilitas yang digunakan untuk mengumpulkan data penghitungan dan pengaturan parameter pembiayaan layanan yang digunakan pengguna, pemeliharaan *database* yang digunakan untuk *billing*, dan persiapan dari pemanfaatan sumber daya dan laporan *billing*.

4. Security Management

Security management melindungi jaringan dan sistem dari akses yang tidak terautentikasi dan serangan keamanan. Mekanisme untuk *security management* meliputi autentikasi, enkripsi, dan otorisasi. *Security management* juga terkait dengan pembuatan, pendistribusian, dan penyimpanan *encryption key* dan informasi keamanan lain yang terkait. Selain itu, *security management* dapat juga mencakup sistem keamanan seperti *firewall* dan *intrusion detection system* yang menyediakan monitoring yang *realtime* dan *event log*.

5. Performance Management

Performance management menyangkut evaluasi dan pelaporan aktivitas dan keefektifan perangkat jaringan yang dikelola. NMS dapat mengukur dan menampilkan status dari jaringan seperti mengumpulkan

informasi statistik dari banyaknya trafik, ketersediaan jaringan, *response time*, dan *throughput*.

Network Management Protocols

Pada November 1987 perangkat *network management* diperkenalkan yaitu *Simple Gateway Monitoring Protocol* (SGMP). Selanjutnya pada 1988 *Internet Architecture Board* (IAB) menyetujui *Simple Network Management Protocol* (SNMP). Protokol standar seperti SNMP dan Common Management Information Protocol (CMIP) menjadi dasar pengembangan perangkat dan aplikasi *network management* lainnya.

SNMP merupakan protokol yang digunakan untuk pertukaran *management information* antara perangkat jaringan. SNMP merupakan protokol *network management* yang paling banyak digunakan. Sebagian besar perangkat jaringan yang digunakan dalam sistem jaringan perusahaan memiliki *built in network agents* yang dapat merespon SNMP. Ini memungkinkan perangkat yang baru dapat dimonitor secara otomatis. Di sisi lain, RMON merupakan tambahan penting untuk standar dasar SNMP. MIB mendefinisikan *remote network monitoring* MIB yang menambahkan MIB-2 dan menyediakan *network manager* dengan informasi penting mengenai *internetwork*. Protokol SNMP berkembang dari SNMP/SNMPv1, SNMP2, dan SNMPv3.

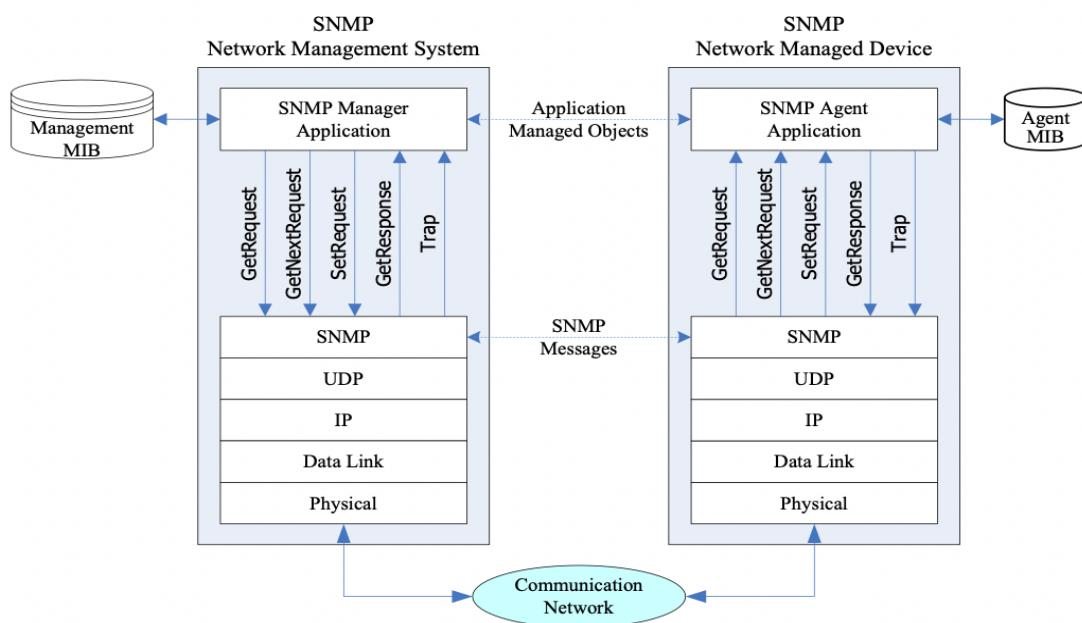
SNMP

Model dari SNMP yang digunakan untuk TCP/IP mencakup beberapa elemen:

- *Management station*: host dari aplikasi network management
- *Management agent*: menyediakan informasi yang terdapat di MIB untuk pengelolaan aplikasi dan menerima informasi kontrol dari *management station*
- *Management information base (MIB)*: mendefinisikan informasi yang dapat dikumpulkan dan dikontrol oleh aplikasi pengelolaan

- *Network management protocol* mendefinisikan protokol yang digunakan untuk menghubungkan *management station* dan *management agent*.

Arsitektur SNMP yang terdapat pada Gambar menunjukkan elemen dari lingkungan network management. SNMP didesain sederhana dengan protokol yang berbasis pesan. *Manager process* memperoleh *network management* menggunakan SNMP, yang digunakan di atas UDP. SNMP *agent* juga menggunakan protokol SNMP dan UDP. SNMP merupakan protokol *connectionless* dimana setiap pertukaran antara *management station* dan *agent* merupakan transaksi terpisah. Desain ini meminimalkan kompleksitas dari *management agent*. SNMP mendukung lima tipe PDU. Manager dapat menerbitkan tiga tipe PDU sebagai bagian dari *management application*: *GetRequest*, *GetNextRequest*, dan *SetRequest*. Tiga pesan tersebut dikenali oleh *agent* dengan pesan *GetResponse* yang disampaikan ke *management application*. Pesan lain yang dihasilkan *agent* yaitu *trap*. *Trap* merupakan pesan yang dikirimkan saat operasi MIB terganggu



Gambar 89. Arsitektur SNMP Network Management

RMON

Perangkat RMON disebut *monitors* atau *probes* merupakan perangkat yang digunakan untuk memonitor jaringan. RMON dapat menghasilkan ringkasan informasi mengenai perangkat yang dikelola termasuk statistik dari error, kinerja, dan traffic. Berdasarkan informasi statistik tersebut, kondisi dari perangkat dapat diamati dan dianalisis. Pada tabel meringkas sembilan grup monitoring. Terdapat dua versi RMON yaitu RMON 1 dan RMON 2.

Tabel 7. Tabel RMON 1 MIB

RMON Group	Function
Statistics	Contains statistics measured by the probe for each monitored interface on this device
History	Records periodic statistical samples from a network and stores them for later retrieval
Alarm	Takes statistical samples periodically from variables in the probe and compares them with previously configured thresholds. If the monitored variable crosses a threshold, an event is generated
Host	Contains statistics associated with each host discovered on the network
HostTopN	Prepares statistics about the top N hosts on a subnetwork based on the available parameters
Matrix	Stores statistics for conversations between sets of two addresses. As the device detects a new conversation, it creates a new entry in its table
Filters	Enables packets to be matched by a filter equation. These matched packets form a data stream that may be captured or may generate events
Packet Capture	Enables packets to be captured after they flow through a channel
Events	Controls the generation and notification of events from a device
Token Ring Extensions	Contains four groups to define some additional monitoring functions specified for Token Ring. They are the Ring Station Group, the Ring Station Order Group, the Ring Station Configuration Group, and the Source Routing Statistics Group

Directory-Enable Networking Management

SNMP menyimpan *dynamic state* dari perangkat jaringan, sedangkan DEN menyimpan *persistent state*. DEN mendefinisikan skema standar untuk menyimpan *persistent state* dari perangkat jaringan dan model yang menjelaskan hubungan antar objek mewakili pengguna, aplikasi, perangkat jaringan, dan layanan jaringan. SNMP berkomunikasi dengan perangkat jaringan, sementara DEN berkomunikasi dengan perangkat jaringan dan

service. DEN menggunakan direktori untuk mengelola keseluruhan jaringan komputer. Direktori digunakan untuk merekam pengguna, aplikasi, dan sumber daya jaringan seperti *file server* dan *printer*.

Keuntungan menggunakan DEN sebagai berikut:

- Menyederhanakan konfigurasi perangkat. Perangkat jaringan menyediakan lebih banyak fungsionalitas yang berdampak pada konfigurasi perangkat yang semakin kompleks.
- Mengontrol pengelolaan dan penyediaan perangkat jaringan melalui *policy*. DEN dapat memetakan SLA dan aturan organisasi melalui kumpulan *policy*. Dengan *policy* dapat diatur alokasi sumber daya jaringan berdasarkan pengguna, *subnet*, waktu, dan faktor lain.
- Menjadi alat yang membuat aplikasi lebih *network-aware* dan menjadikan jaringan lebih *application-aware*

Perangkat *Network Management*

Pertumbuhan pesat jaringan komputer dalam skala dan variasinya menyebabkan pengelolaan jaringan menjadi kompleks dan menantang. Untuk mengelola jaringan komputer secara jelas dan efisien, perangkat khusus dapat digunakan untuk memonitor aktivitas jaringan dan menentukan perilaku jaringan terlebih dahulu.

Perangkat *network management* digunakan berdasarkan protokol yang digunakan dalam pengelolaan jaringan. Sebagian besar sistem menggunakan *open protocol*, tetapi sebagian yang lain menggunakan protokol *proprietary*. Kemampuan perangkat pengelolaan jaringan berdasarkan fungsi yang didudukung oleh *protocol*.

Fungsi-fungsi pada *network management*:

- Pemantauan jaringan (*monitoring*)

Tanggung jawab mendasar dari pengelola jaringan adalah pemantauan jaringan. Perangkat monitoring jaringan harus memiliki kemampuan mengumpulkan dan menganalisis trafik jaringan. Sistem pemantauan yang

baik memungkinkan untuk menghasilkan *file log* dan grafik yang menunjukkan kemampuan dan respon sistem. Dengan data tersebut dapat dilakukan optimasi pada konfigurasi jaringan dan persiapan terhadap *fault*. Beberapa perangkat monitoring didesain dengan SNMP untuk menampilkan isu dasar jaringan. Untuk meminimumkan waktu *downtime*, perangkat pemantauan akan memberikan *alert* peringatan jika terdapat anomali jaringan.

- **Pemindai Jaringan (*scanning*)**

Kerentanan pada kemanana jaringan dideteksi setiap harinya. Pemindai jaringan merupakan perangkat yang penting untuk keamanan jaringan. Perangkat ini melakukan pengecekan pada sistem jaringan, sistem operasi, dan aplikasi yang berjalan di jaringan untuk mengidentifikasi kerentanan dan celah keamanan yang dapat mengekspos jaringan. Untuk melindungi aset digital dan mengilangkan risiko, beberapa perangkat pemindai jaringan juga mengotomatiskan pegecekan kerentanan.

- ***Packet Filter***

Packet filter mengontrol akses terhadap paket data pada jaringan dengan melakukan pemindaian pada konten dari *packet header*. *Packet filter* selanjutnya menentukan paket yang diperbolehkan melewati jaringan atau diterapkan kebijakan akses kontrol lainnya. *Packet filter* paling sering digunakan sebagai perlindungan pertama pada jaringan dari serangan luar. *Packet filter* dapat menjamin keamanan jaringan dan data internal.

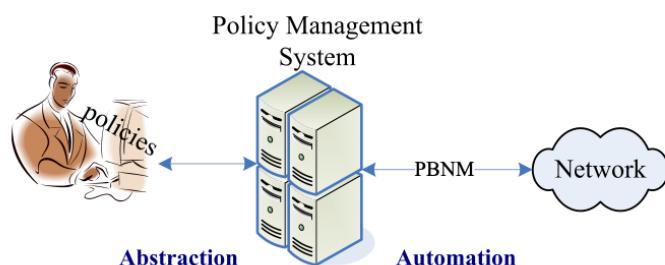
Dynamic packet filtering merujuk pada *stateful inspection*, yaitu arsitektur *firewall* yang berjalan pada layer jaringan. *Stateful inspection* melacak setiap koneksi yang melintasi setiap *interface firewall* dan memastikan koneksi tersebut valid. *Statefull firewall* dapat memeriksa konten dari paket melalui layer aplikasi untuk memperoleh informasi lebih lanjut selain *source* dan *destination*. *Stateful inspection firewall* juga memonitor status koneksi dan mengkompilasi informasi dalam *state table*. Dengan

demikian, keputusan *filtering* berdasarkan pada rule yang ditentukan administrator jaringan dan juga konteks yang dibuat paket sebelumnya yang telah melalui *firewall*.

Policy based Network Management (PBNM)- Solusi untuk Next Generation

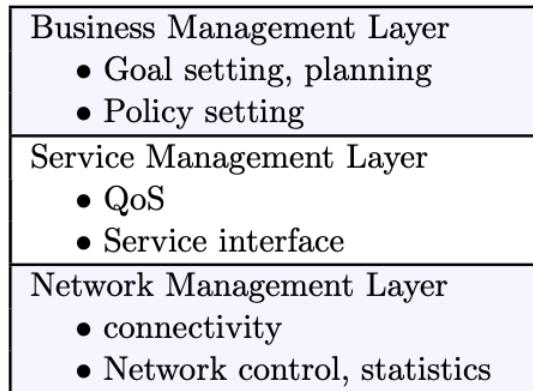
PBNM merupakan cara untuk mengelola konfigurasi dan perilaku pada satu atau lebih perangkat berdasarkan kebutuhan bisnis dan kebijakan. PBNM memungkinkan aturan dan prosedur bisnis ditranslasikan ke kebijakan yang mengkonfigurasi dan mengontrol jaringan dan layanannya. PBNM dapat didefinisikan dalam mekanisme *condition-action*.

```
ON <event>
IF <conditions>
THEN <actions>
```



Gambar 90. Model Policy based Network Management

PBNM meng-*enable* respon otomatis dan merapkannya pada jaringan berdasarkan policy yang telah ditentukan sebelumnya. Dengan mengotomatisasikan pengelolaan jaringan, keseluruhan jaringan dapat dikelola sebagai kesatuan.



Gambar 91. Network Management Layered View

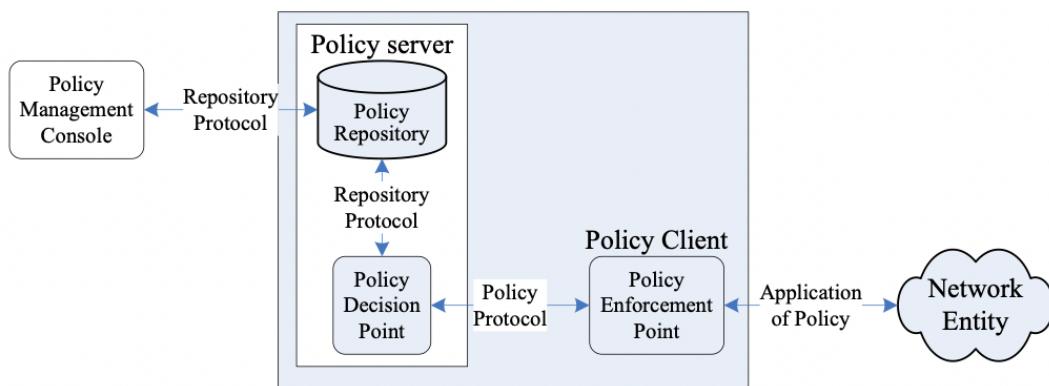
Policy didefinisikan sebagai kumpulan dari rule yang mengelola dan mengontrol akses ke sumber daya jaringan. Jaringan dapat dikelola melalui *descriptive language*. *Policy* dapat ditunjukkan pada level yang berbeda, bervariasi pada tujuan organisasi dan konfigurasi spesifik pada perangkat.

Tujuan dan kebijakan organisasi dapat didefinisikan sebagai layer terpisah (business management) di atas layer pengelolaan aplikasi (service management) yang disisipkan layanan seperti Quality of Service (QoS). Dengan pertumbuhan dan kompleksitas jaringan computer, QoS dan keamanan menjadi isu yang harus diperhatikan. PBNM sebagai solusi dalam menyederhanakan pengelolaan QoS dan keamanan.

Dengan PBNM, pengelolaan QoS dan mekanisme keamanan jaringan dapat disederhanakan sehingga pengelolaan jaringan menjadi lebih mudah. PBNM memungkinkan perilaku sistem diubah tanpa memodifikasi implementasi. Keuntungan PBNM dapat diringkas sebagai berikut:

- Mengoptimalkan sumber daya jaringan. Pengelolaan secara otomatis mengoptimalkan penggunaan infrastruktur dan *policy* jaringan. PBNM mengurangi kebutuhan *bandwidth* tambahan pada jalur yang padat.
- Menyederhanakan jaringan dan pengelolaan layanan. Untuk menggunakan PBNM tidak diperlukan keahlian khusus. Perubahan pada kebijakan organisasi tidak membutuhkan pembangunan pada *layer* bawah, dimana proses *update* menyusahkan.

- Mengelola trafik dan layanan yang kompleks dengan baik. PBNM dapat mengelola aplikasi dengan sumber daya bersama menggunakan informasi trafik yang telah diprediksi sebelumnya. Aplikasi yang tidak terotentikasi dapat dikontrol dan dibuang, sedangkan aplikasi penting dapat diberikan prioritas khusus.
- Melakukan fungsi pengaturan waktu dengan efisien. PBNM dapat menyederhanakan dan mengimplementasikan dengan baik fungsi yang memerlukan pengaturan waktu kritis, seperti perubahan konfigurasi perangkat pada waktu tertentu dan menjalankan fungsi tertentu yang telah dijadwalkan
- Menyediakan keamanan yang lebih baik. PBNM dapat mengkategorisasikan trafik dalam tipe '*expected*' dan '*unexpected*' dan menerapkan rule pada setiap tipe tersebut. PBNM dapat digunakan untuk menentukan sebuah pengguna dapat memperoleh akses atau tidak.



Gambar 92. Arsitektur PBNM

PBNM memiliki empat komponen utama yaitu:

- *Policy Management Console*: user interface untuk membuat *policy*, membangun *policy*, dan memonitor status *policy-managed environment*.
- *Policy Repository*: database yang menyimpan *rule* dari *policy*, *condition* and *action*, dan data terkait *policy*.

- *Policy Decision Point* (PDP); proses logikal yang membuat ketentuan berdasarkan *policy rule* dan kondisi dimana *policy* tersebut diterapkan.

- *Policy Enforcement Point* (PEP): entitas logikal yang menjalankan ketentuan dari *policy* dan atau membuat perubahan pada konfigurasi.

Policy communication protocol: dibutuhkan untuk pertukaran data antar entitas dalam sistem pengelolaan *policy*. *The Common Object Policy Service Protocol* (COPS) sering disebutkan untuk mendukung komunikasi antara PDP dan PEP.

a. Monitoring dan Evaluasi Sistem Jaringan Komputer

Monitoring jaringan merupakan penggunaan log dan perangkat analisis untuk secara akurat menentukan trafik, utilisasi, dan indikator performa lainnya pada jaringan. Perangkat monitoring memberikan angka maupun grafik yang menunjukkan kondisi jaringan sehingga membantu memvisualisasikan secara tepat apa yang terjadi sehingga dapat diambil tindakan yang diperlukan.

Perangkat monitoring dapat menjawab pertanyaan berikut:

- Layanan apa yang paling banyak digunakan dalam jaringan?
- Siapa pengguna yang paling banyak membebani jaringan?
- Apakah terdapat *wireless channels* lain dalam area kerja?
- Apakah terdapat *access point* yang dipasang pada area LAN dengan kabel jaringan?
- Pada jam berapa jaringan banyak digunakan?
- *Site* apa yang sering diakses pengguna?
- Apakah trafik inbound dan outbound mendekati kapasitas jaringan yang tersedia?
- Apakah terdapat indikasi keanehan kondisi jaringan yang menghabiskan *bandwidth* atau menyebabkan masalah lain?
- Apakah ISP yang menyediakan layanan internet memberikan SLA yang semestinya?

- Apakah trafik jaringan sudah sesuai ekspektasi

Maupun pertanyaan lain untuk pengelolaan jaringan. Berbagai pertanyaan tersebut merupakan bentuk evaluasi terhadap operasional sistem jaringan komputer di organisasi. Hal ini dapat dijawab dengan adanya perangkat monitoring dan pengukuran. Perangkat ini diperlukan untuk memeriksa kondisi jaringan, mendiagnosa maupun *troubleshoot* masalah.

a.1. Monitoring LAN

Monitoring pada trafik LAN merupakan tahap pertama dalam mendiagnosa permasalahan. Beberapa keuntungan dalam monitoring LAN yaitu:

- *Troubleshoot* dapat lebih mudah, virus dapat dideteksi dan ditangani
- Pengguna yang bermasalah dapat dideteksi dan diatasi
- Sumber daya dan perangkat jaringan dapat dilihat berdasarkan statistik aslinya.

Diasumsikan semua *switch* mendukung protokol SNMP. Dengan memberikan sebuah IP pada tiap *switch* maka monitoring dapat dilakukan pada seluruh interface *switch* sehingga keseluruhan network dapat diobservasi dari satu titik.

Dengan menggunakan perangkat gratis seperti MRTG, setiap *port* pada *switch* dapat dimonitor dan data ditampilkan dalam bentuk grafik sebagai rata-rata agregat dari waktu ke waktu. Grafik dapat diakses dari web, sehingga dapat dilihat kapan saja.

a.2. Monitoring WAN

Monitoring WAN dilakukan untuk memantau trafik di luar LAN. Monitoring WAN dapat berupa trafik VPN ke kantor cabang atau koneksi untuk pertukaran data termasuk juga koneksi internet.

Keuntungan dari monitoring WAN:

- Menunjukkan kesesuaian SLA koneksi VPN, koneksi Internet yang diberikan ISP
- Penentuan kapasitas selanjutnya dapat diestimasi dari trafik penggunaan internet
- Penyusup dari internet juga dapat dideteksi dan difilter sebelum menimbulkan masalah

Monitoring trafik dapat dilakukan menggunakan MRTG pada perangkat yang meng-enable SNMP seperti *router*. Jika *router* tidak support SNMP dapat menggunakan *switch* yang diletakkan diantara *router* dan ISP.

a.3. Monitoring Jaringan

Beberapa keuntungan dengan penerapan sistem monitoring *network*:

- Biaya dan sumber daya jaringan yang digunakan dapat dijustifikasi. Infrastruktur jaringan yang digunakan (*bandwidth, hardware* dan *software*) dapat dilihat apakah sudah dapat memenuhi kebutuhan pengguna.
- Penyusup jaringan dapat diditeksi dan difilter sehingga tidak menganggu jaringan komputer
- Virus pada jaringan dapat dengan mudah dideteksi
- Menyederhanakan *troubleshooting* jika terdapat masalah pada jaringan.
- Performa jaringan dapat dioptimasi.
- Perencanaan kapasitas dapat dengan mudah dilakukan
- Penggunaan jaringan dapat dipaksakan sesuai dengan kebijakan yang ditentukan. Misalnya terkait pengaturan bandwith yang diberikan kepada pengguna.

Perangkat yang dapat digunakan untuk monitoring jaringan salah satunya berupa *monitoring server*. Aplikasi monitoring dapat ditambahkan pada server yang sudah ada, dengan hanya menggunakan satu server atau

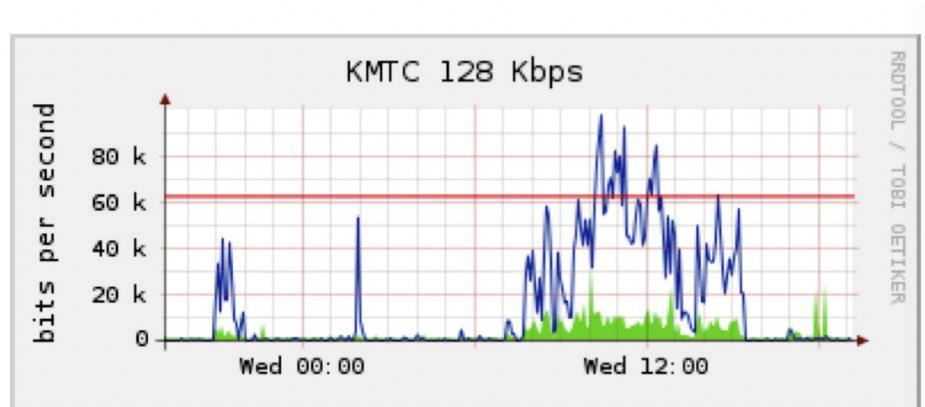
lebih jika diperlukan. Beberapa aplikasi memerlukan *resource* yang besar untuk dijalankan seperti ntop, tetapi terdapat juga aplikasi yang memerlukan RAM dan storage rendah dengan sedikit CPU. Sistem operasi *open source* menggunakan sumber daya secara efisien sehingga memungkinkan untuk membangun monitoring server menggunakan resource yang ada.

Kecuali jika monitoring yang dilakukan pada skala besar misalnya dengan node lebih dari beberapa ratus dan bandwidth lebih dari 50 Mbps maka perlu dilakukan pemisahan monitoring jaringan pada beberapa server. Selain itu juga bergantung pada apa saja yang ingin dimonitor, jika seluruh aplikasi pada tiap *IP address* maka akan memerlukan *resource* lebih besar dibanding hanya memonitor lalu lintas jaringan pada *port switch*.

Sebagian besar instalasi monitoring cukup dipenuhi dengan satu dedicated server. Di sisi lain menggabungkan *monitoring* pada satu server akan menyederhanakan *upgrade* dan pengelolaan serta memastikan monitoring yang lebih baik. Bagi administrator jaringan, data yang dikumpulkan terkait performa jaringan sangat penting sehingga dapat memberikan gambaran jaringan yang dikelola. Monitoring harus mencakup semua perangkat dan sedapat mungkin melindungi dari terhentinya layanan.

Jika hanya data lalu lintas jaringan yang dikumpulkan dari *router*, maka *monitoring server* dapat diletakkan di dalam LAN. Dapat diperoleh data terkait utilisasi tetapi tidak dapat dilihat lebih jauh informasi mengenai komputer, pengguna atau protokol apa yang menggunakan *bandwidth*.

Monitoring server juga harus dapat mengakses semua node yang perlu dimonitor. Koneksi ke semua node dapat berupa koneksi fisik (kabel) atau koneksi virtual dengan mendefinisikan VLAN yang dikhususkan untuk monitoring.



Gambar 93. Utilisasi Bandwidth

a.4. Indikator Monitoring Jaringan

Informasi yang dikumpulkan dapat berbeda-beda bergantung pada jaringan yang dimonitor. Indikator yang akan dimonitor harus dapat menggambarkan performa dari jaringan. Beberapa contoh indikator yang dapat dikumpulkan administrator jaringan yaitu pada beberapa jenis jaringan berikut:

1) *Wireless statistics*

- a. *Received signal and noise from all backbone nodes*
- b. *Number of associated stations*
- c. *Detected adjacent networks and channels*
- d. *Excessive retransmissions*
- e. *Radio data rate*, jika menggunakan *automatic rate scaling*

2) *Switch statistics*

- a. *Bandwidth usage per switch port*
- b. *Bandwidth usage broken down by protocol*
- c. *Bandwidth usage broken down by MAC address*
- d. *Broadcasts as a percentage of total packets*
- e. *Packet loss and error rate*

3) *Internet statistics*

- a. *Internet bandwidth use by host and protocol*
- b. *Proxy server cache hits*
- c. *Top 100 sites accessed*
- d. *DNS requests*
- e. *Number of inbound emails / spam emails / email bounces*
- f. *Outbound email queue size*
- g. *Availability of critical services (web servers, email servers, etc.).*
- h. *Ping times and packet loss rates to your ISP*
- i. *Status of backups*

4) *System health statistics*

- a. *Memory usage*
- b. *Swap file usage*
- c. *Process count / zombie processes*
- d. *System load*
- e. *Uninterruptible Power Supply (UPS) voltage and load*
- f. *Temperature, fan speed, and system voltages*
- g. *Disk SMART status*
- h. *RAID array status*

Indikator tersebut dapat dijadikan pertimbangan untuk monitoring jaringan. Dengan semakin berkembangnya jaringan akan diperlukan indikator baru untuk dimonitor. Banyak *tool* gratis yang dapat digunakan untuk memonitor jaringan secara detail sesuai dengan kebutuhan. Selain itu *monitoring server* yang digunakan juga perlu dimonitor.

a.5. Tipe-tipe perangkat monitoring

Terdapat beberapa tipe perangkat monitoring diantaranya:

1) *Network detection tool*

Digunakan untuk wireless access point untuk menampilkan informasi nama network, kekuatan signal, dan channel. Dapat digunakan untuk mendeteksi jaringan terdekat, menentukan jaringan tersebut masuk dalam jangkauan atau memberikan interfensi.

Sistem operasi pada perangkat jaringan menyediakan *built-in support* untuk jaringan *wireless*. Diantaranya digunakan untuk *scan* jaringan *wireless* yang tersedia dan memilih jaringan yang akan digunakan. Netstumbler merupakan aplikasi yang paling popular untuk mendeteksi jaringan *wireless* menggunakan *Microsoft Windows*. Aplikasi ini mudah digunakan, dapat mendeteksi *open and encrypted network*, menggambarkan grafik *radio receiver*, dan terintegrasi dengan berbagai macam GPS. Sedangkan *Mactumbler* digunakan pada perangkat Mac.

2) *Spot check tool*

Digunakan untuk *troubleshooting* pada titik tertentu jika terdapat masalah. Contohnya program *ping* yang dapat menunjukkan trafik pada node tertentu dan dapat digunakan di semua jenis OS. *Ping* menggunakan paket ICMP untuk mengkontak *host* tertentu dan berapa lama waktu yang diperlukan untuk respon. *Traceroute* digunakan untuk menemukan lokasi masalah dari komputer ke berbagai node di jaringan. *My TraceRoute* (mtr) yang mengkombinasikan *ping* dan *traceroute* dalam satu *tool*, dapat diperoleh informasi rata-rata *latency* sekaligus *packet loss*.

3) *Passive spot check tool (Protocol Analyser)*

menganalisis protokol dengan melakukan pengecekan pada setiap paket jaringan dan memberikan informasi lengkap komunikasi jaringan (*source and destination addresses, protocol information, and application data*).

Tool dapat memberikan informasi detail mengenai lalu lintas data di jaringan dengan melakukan inspeksi pada *individual packet*. Pada *wired network*, dapat diinspeksi paket pada *data-link layer* dan *layer* di atasnya. Untuk jaringan *wireless*, dapat diinspeksi informasi pada *802.11 frames*. Beberapa tools yang dapat digunakan secara gratis yaitu: *Kismet*, *KisMAC*, *Tcpdump*, dan *Wireshark*.

4) *Trending tools*

Tools memonitor dalam jangka waktu lama sehingga dapat menghasilkan grafik dari jaringan. *Tool* memonitoring node secara periodik dan menampilkan ringkasan dalam bentuk grafik. Contoh perangkat: *MRTG*, *RRDTool*, *Ntop*, *cacti*, *netflow*, *flowc*, *SmokePing*, dan lainnya

5) *Throughput testing*

Perangkat dapat menunjukkan *bandwidth* aktual yang tersedia antara dua *node* dalam jaringan. Hal ini dapat diketahui dengan membanjiri koneksi dengan trafik dan mengukur waktu yang diperlukan untuk transfer data. *Tool* yang dapat digunakan seperti *Speedtest* yang dapat diakses dari *browser*. *Tool* lain yang dapat digunakan langsung pada jaringan kita yaitu: *ttcp*, *iperf*, dan *bing*

6) *Realtime monitoring tool*

Tool ini dapat memberikan *alert* jika terdeteksi adanya masalah sehingga tindakan perbaikan dapat dilakukan lebih awal. Selain itu dapat bertindak sebagai *intrusion detection* dengan mengawasi trafik yang tidak diinginkan dan mengambil tindakan yang tepat misal dengan menolak akses atau memberi peringatan pada administrator. Beberapa tool yang dapat digunakan yaitu: *Snort*, *Apache: mod_security*, *Nagios*, *Zabbix*,

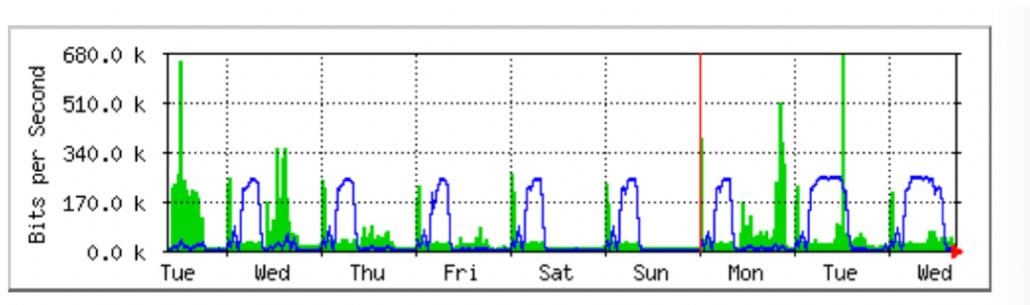
Beberapa perangkat lain yang bermanfaat untuk kebutuhan khusus yaitu: *ngrep* (digunakan untuk mencari paket terkait menggunakan *keyword* tertentu) dan *nmap* (*diagnostic tool* yang menunjukkan kondisi dan

ketersediaan port jaringan pada *interface* jaringan, seringkali digunakan untuk *scan port* yang dapat digunakan).

a.6. Menentukan *baseline*

Dalam monitoring jaringan perlu ditentukan *baseline* yang menunjukkan normalnya kondisi jaringan kita. *Baseline* dapat digunakan sebagai dasar dalam penentuan apakah terdapat permasalahan pada jaringan dari hasil monitoring yang diperoleh.

a.7. Cara menginterpretasi Grafik monitoring



Gambar 94. Contoh Grafik Monitoring

Grafik standar menggambarkan garis hijau menunjukkan *inbound traffic* dan garis biru menunjukkan *outbound traffic*. *Inbound traffic* menunjukkan trafik yang masuk dari luar ke jaringan kita. Sedangkan *Outbound traffic* menunjukkan trafik yang keluar dari jaringan kita ke jaringan luar. Dengan grafik akan memudahkan kita dalam mengenali bagaimana jaringan kita digunakan. Misalnya pada *server*, biasanya memiliki *outbound traffic* lebih besar untuk merespon pengguna, sedangkan pada perangkat *client* menunjukkan *inbound traffic* lebih besar karena memperoleh data dari *server*.

Dari hasil monitoring menggunakan berbagai perangkat yang disesuaikan dengan kebutuhan organisasi, selanjutnya dapat dilakukan

evaluasi. Evaluasi dilakukan untuk mengetahui bagaimana operasional sistem jaringan komputer di organisasi. Misalnya untuk mengetahui apakah pemanfaatan jaringan sudah merata untuk semua pengguna, apakah bandwidth sudah mencukupi kebutuhan pengguna, apakah SLA yang dijanjikan dapat terpenuhi, apakah trafik jaringan normal, dan sebagainya. Dari hasil evaluasi selanjutnya dapat dilakukan berbagai macam tindakan yang diperlukan termasuk jika terdapat permasalahan agar sistem jaringan komputer dapat terjamin ketersediaannya.

b. Analisis Permasalahan Sistem Jaringan Komputer

Setelah dilakukan evaluasi, apabila ditemukan permasalahan pada sistem jaringan komputer maka perlu dilakukan analisis permasalahan untuk mengetahui sebab terjadinya permasalahan untuk dilakukan perbaikan.

Permasalahan di jaringan dapat ditemukan dengan dua cara yaitu:

- Jaringan dimonitor secara aktif pada keseleruhan komponennya
- Komponen pada jaringan mengirimkan *error report* saat terdeteksi masalah pada komponennya sendiri atau komponen lain.

Cara kedua lebih sering digunakan karena kompleksitas jaringan saat ini.

Apabila terjadi permasalahan dapat dilakukan beberapa prosedur berikut:

- Menentukan letak masalah, pemantauan jaringan diperlukan untuk mengetahui apakah komponen jaringan beroperasi secara benar. Komponen dapat mengirimkan peringatan apabila mendeteksi masalah pada fungsi komponen tersebut
- Mendiagnosa masalah, menemukan secara tepat apa permasalahannya, dan jika memungkinkan mengumpulkan bukti dan menyimpulkan permasalahan.
- *By-pass* masalah, memeriksa kembali masalah untuk memastikan jaringan lain tidak terdampak.

- Menyelesaikan masalah, memperbaiki masalah dan mengembalikan jaringan ke kondisi semula
- Membuat dokumentasi dengan menyimpan catatan permasalahan. Log lengkap dari permasalahan dapat berisi informasi penting tentang jaringan yang sudah operasional, masalah yang sering muncul, cara untuk menyelesaikan masalah, dan lainnya.

Problem management sering dilakukan dengan penggunaan ‘*alert*’ (peringatan). *Alert* merupakan pesan yang dihasilkan dalam jaringan dan dikirimkan ke *Network Management Center* untuk memberikan peringatan bahwa terdapat komponen yang perlu mendapatkan perhatian.

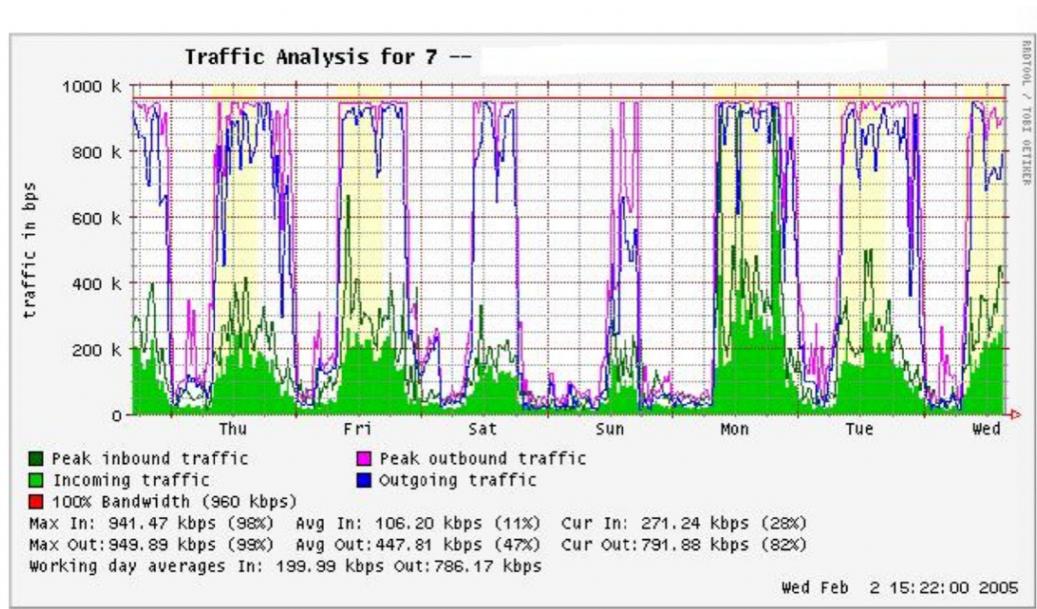
Beberapa contoh analisis permasalahan yang dilakukan pada sistem jaringan komputer:

1) Permasalahan 1:

Di sebuah kantor dibangun jaringan yang sudah berjalan 3 bulan, dengan 50 komputer dan tiga *server*: *email server*, *web server*, dan *proxy server*. Pengguna mulai mengeluh lambatnya kecepatan jaringan dan meningkatnya spam email. Di sisi lain, pengguna juga mengeluh lambatnya komputer yang digunakan.

Analisis Permasalahan 1:

Dilakukan pengecekan pada perangkat monitoring dan ditemukan grafik trafik sebagai berikut:



Gambar 95. Grafik *Flat Top* menunjukkan *Over Utilisation*

Grafik flat top menunjukkan *bandwidth* yang digunakan mencapai kapasitas maksimal. Grafik juga dapat menunjukkan *throughput* aktual koneksi jika digunakan hingga mendekati kapasitas yang tersedia pada waktu sibuk (*peak time*). Grafik *flat top* adalah indikasi yang cukup jelas bahwa bandwidth jaringan digunakan dengan kapasitas penuh. Koneksi internet terutilisasi maksimal sehingga menyebabkan *lag* jaringan.

Dengan MRTG dapat dilihat jelas bahwa jaringan LAN dipenuhi trafik yang lebih besar dari trafik koneksi internet yang dapat digunakan, bahkan saat komputer tidak digunakan. Ini menunjukkan adanya akses jaringan tanpa adanya campur tangan pengguna. Kemungkinan besar disebabkan adanya virus yang membanjiri jaringan.

Selanjutnya dilakukan pengecekan pada salah satu komputer pengguna menggunakan anti virus yang update ditemukan virus. Setelah instalasi anti virus dan anti spyware di seluruh komputer, trafik LAN kembali normal.

2) Permasalahan 2:

Pengguna di beberapa ruangan mengeluhkan tidak bisa mengakses internet.

Analisis Permasalahan 2:

Dilakukan pengecekan pada perangkat monitoring yang dapat menunjukkan status perangkat.



Gambar 96. Monitoring menggunakan Cacti

Dari gambar dapat dilihat bahwa beberapa perangkat mati (indikator merah) dan terdapat perangkat yang masih hidup (indikator hijau). Kemudian dilakukan pengecekan langsung ke *switch*. Ternyata ditemukan UPS pada *switch* tersebut tidak berfungsi, sehingga saat mati listrik (*trip*) perangkat tidak *switch* hidup. Kemudian dilakukan restart pada *switch* dan jaringan internet dapat diakses kembali.

3) Permasalahan 3:

Pengguna tidak dapat mengakses jaringan LAN

Analisis Permasalahan 3:

Dilakukan pengecekan pada dashboard monitoring perangkat, semua perangkat jaringan menunjukkan indikator hijau (hidup). Untuk mengetahui dimana koneksi terhenti dapat dilakukan tes *ping*.

Beberapa kemungkinan yang terjadi dari tes *ping*

1. Paket memerlukan waktu lama untuk direspon, maka kemungkinan terjadi *congestion*.
2. Paket memiliki *Time To Live* (TTL) rendah maka kemungkinan terdapat masalah pada *routing*.
3. *Ping name* bukan *IP Address* maka kemungkinan terdapat masalah pada DNS.
4. Tidak dapat *Ping default router* maka tidak dapat terhubung dalam jaringan internet.
5. Tidak dapat *Ping IP* pada lokal LAN, maka koneksi pada PC perlu diperiksa sesuai dengan koneksi yang digunakan *wired* atau *wireless*.
6. Paket *Ping* tidak mendapat jawaban, kemungkinan *node* mati atau *node* melakukan blok terhadap akses ping. Dapat dicoba menggunakan service lain seperti *ssh* atau *http*.

Debug jaringan menggunakan Ping dapat memberikan berbagai kemungkinan, tetapi tetap dapat bermanfaat dalam deteksi kondisi jaringan. Penambahan command -n dapat mempercepat *trace* tanpa perlu resolving DNS.

Dilakukan ping ke *default router*, tetapi tidak mendapat jawaban. PC menggunakan koneksi wired LAN. Selanjutnya dilakukan pengecekan pada kabel jaringan menggunakan alat penguji kabel, ditemukan bahwa kabel tidak stabil sehingga perlu dilakukan penggantian kabel LAN.

4) Permasalahan 4:

Pengguna tidak bisa mengakses internet.

Analisis Permasalahan 4:

Perangkat monitoring menunjukkan jaringan LAN dalam kondisi normal. Selanjutnya dilakukan *traceroute* untuk melacak di hop mana koneksi terhenti

```
$ traceroute -n google.com
traceroute to google.com (72.14.207.99), 64 hops max, 40 byte packets

 1 10.15.6.1 4.322 ms 1.763 ms 1.731 ms
 2 216.231.38.1 36.187 ms 14.648 ms 13.561 ms
 3 69.17.83.233 14.197 ms 13.256 ms 13.267 ms
 4 69.17.83.150 32.478 ms 29.545 ms 27.494 ms
 5 198.32.176.31 40.788 ms 28.160 ms 28.115 ms
 6 66.249.94.14 28.601 ms 29.913 ms 28.811 ms
 7 172.16.236.8 2328.809 ms 2528.944 ms 2428.719 ms
 8 * * *
```

Gambar. Contoh traceroute

Pada gambar saat *hop* ke 7 waktu yang diperlukan lebih dari 2 detik, dan paket berhenti pada *hop* ke 8. Ini mungkin menunjukkan permasalahan terjadi pada perangkat tersebut sehingga *troubleshooting* dapat dimulai dari node tersebut.

c. Optimalisasi Sistem Jaringan Komputer

Dari hasil monitoring dan evaluasi sistem jaringan komputer, selanjutnya dapat dilakukan optimalisasi sistem jaringan komputer. Optimalisasi dapat diartikan memberikan solusi-solusi terbaik atas permasalahan-permasalahan yang ada. Sedangkan optimalisasi jaringan komputer yaitu suatu cara untuk mempercepat berbagai aplikasi yang diakses oleh pengguna perusahaan yang menggunakan jaringan LAN/WAN yang didistribusikan dengan cara menghilangkan kelebihan transmisi, pengiriman data dalam cache lokal, penekanan dan memprioritaskan data, dan perampingan sejumlah protokol. Dengan optimalisasi diharapkan kinerja sistem jaringan komputer meningkat.

Kinerja jaringan komputer dapat diukur dari beberapa hal berikut:

- *Troughput*

Jika bandwidth adalah tingkat transmisi data maksimum yang dapat dicapai di level *hardware* ditentukan oleh laju sinyal dari jalur fisik dan

NIC. Maka throughput adalah tingkat transmisi data maksimum yang dapat dicapai di level *software*, termasuk *overhead network protocol* di dalam sistem operasi diperhitungkan. *Throughput* yang handal yaitu tingkat transmisi data maksimum yang dapat dicapai di level *software* termasuk dampak dari pemulihhan akibat kesalahan transmisi dan *packet loss* diperhitungkan. *Throughput* merupakan ukuran riil dari kecepatan komunikasi.

- *Latency*

Latency adalah waktu yang dibutuhkan untuk sebuah paket yang dikirimkan dari suatu komputer ke komputer yang dituju.

- *Delay*

Delay dalam proses transmisi paket dalam jaringan disebabkan karena adanya antrian yang panjang, atau mengambil rute lain untuk menghindari kemacetan pada *routing*. Untuk mencari *delay* pada paket yang ditransmisikan dengan membagi antara panjang paket (satuannya bit) dibagi dengan *link bandwidth* (satuannya bit/s). Untuk mengukur *delay* pada suatu jaringan komputer menggunakan perintah *ping* dimana *time* pada hasil perintah ping menunjukkan *delay* pada paket yang dikirimkan

- *Jitter*

Jitter adalah variasi dari *delay* atau selisih antara *delay* pertama dengan *delay* selanjutnya. Jika variasi *delay* dalam transmisi terlalu lebar, maka akan mempengaruhi kualitas data yang ditransmisikan. Jumlah toleransi *jitter* dalam jaringan dipengaruhi oleh kedalaman dari *buffer jitter* dalam peralatan jaringan. Jika *buffer jitter* tersedia lebih banyak, maka jaringan dapat mereduksi efek dari *jitter*. Contoh dari *jitter*, misalnya hasil ping menunjukkan *delay* dengan rentang 2ms, 4ms, 7ms. Maka *jitter* dapat dihitung dengan mengurangi *delay* akhir dengan *delay* sebelumnya, seperti contoh tersebut maka jitternya adalah $7\text{ms} - 4\text{ms} = 3\text{ms}$. Untuk

mengukur *jitter* dapat kita gunakan fasilitas *UDP test* pada perangkat lunak *iperf*.

- *Packet Loss*

Packet Loss, adalah persentase paket yang hilang selama mentransmisikan data. Hal ini disebabkan oleh banyak faktor seperti penurunan sinyal dalam media jaringan, kesalahan perangkat keras jaringan, atau juga radiasi dari lingkungan sekitar. Pada beberapa *network transfer protocol* seperti TCP yang bersifat *connection oriented*, menyediakan pengiriman kembali (*retransmission*) atau pengiriman secara otomatis (*resends*) paket yang hilang selama proses transmisi walau segmen telah tidak diakui. Walaupun TCP memiliki kelebihan tersebut, jika TCP melakukan *retransmitting* atau *resends*, *throughput* jaringan semakin menurun. Berbeda halnya dengan protokol UDP yang bersifat *connectionless*, tidak menyediakan *retransmission* maupun *Resends* jika terjadi kehilangan paket.

Untuk meningkatkan kinerja sistem jaringan komputer, dapat dilakukan beberapa hal berikut:

- Meningkatkan skala sistem jaringan komputer dengan penambahan kapasitas perangkat, penambahan *bandwidth*, penambahan perangkat jaringan, penggantian perangkat dengan teknologi yang lebih *update* dan sebagainya.
- Menambahkan konfigurasi baru atau melakukan perubahan konfigurasi pada perangkat jaringan yang digunakan untuk memaksimalkan fungsi atau fitur perangkat.
- Menyederhanakan topologi jaringan sehingga lebih efektif dan efisien.
- Peningkatan keamanan jaringan komputer dengan penggunaan *firewall* yang mampu melakukan *filtering* pada paket data, penambahan konfigurasi pada *firewall*, peningkatan *awareness* keamanan di sisi pengguna jaringan, dan lainnya.

4.2. Rangkuman

1. Evaluasi sistem jaringan komputer diperlukan untuk mengevaluasi pemanfaatan sistem jaringan komunikasi data dalam menjawab kebutuhan organisasi.
2. Evaluasi sistem jaringan erat kaitannya dengan *network management*. *Network Management* adalah *service* yang menggunakan berbagai macam protokol, alat, aplikasi, dan perangkat yang membantu administrator jaringan dalam memonitor dan mengontrol sumber daya jaringan baik perangkat keras maupun lunak, untuk memenuhi kebutuhan.
3. *Network Management System* (NMS) merujuk pada sekumpulan aplikasi yang memungkinkan komponen jaringan untuk dimonitor dan dikontrol.
4. ISO mengelompokkan fungsi *network management* ke dalam lima area yaitu: *Configuration Management*, *Fault Management*, *Accounting Management*, *Security Management*, dan *Performance Management*.
5. Dalam *network management* diperlukan protokol yang menjadi standar dalam komunikasi antar komponen *network management*.
6. Perangkat *network management* memiliki beberapa fungsi diantaranya: pemantauan, pemindaian dan packet *filtering*.
7. PBNM dimanfaatkan untuk menerapkan sejumlah *policy* pada perangkat jaringan sehingga memudahkan dalam pengelolaan sistem jaringan komputer.
8. Monitoring dan evaluasi diperlukan untuk memastikan sistem jaringan komputer berjalan sesuai dengan kebutuhan organisasi.

9. Analisis permasalahan dilakukan untuk mengetahui penyebab permasalahan yang diketahui, untuk selanjutnya dilakukan perbaikan.
10. Optimalisasi sistem jaringan komputer dimaksudkan untuk meningkatkan kinerja sistem jaringan komputer.

4.3. Soal Latihan

1. Mengapa diperlukan *network management*?
2. Apa saja komponen dalam NMS?
3. Apa saja manfaat network monitoring?
4. Jelaskan berbagai macam perangkat monitoring jaringan komputer dan contohnya!
5. Bagaimana hasil monitoring dapat membantu analisis permasalahan dan optimasi sistem jaringan komputer?

4.4. Contoh Kasus

Sebuah kantor memiliki 3 kantor cabang. Di kantor pusat terdapat data center dengan 100 komputer pengguna dan koneksi internet. Untuk menghubungkan pusat dengan kantor cabang digunakan teknologi VPN. Kantor cabang masing-masing memiliki 25 komputer.

Dari kondisi tersebut di atas:

- Jelaskan apa saja yang perlu dimonitoring dan dievaluasi!
- Jelaskan perangkat monitoring jenis apa saja yang perlu digunakan!
- Optimalisasi jaringan apa yang mungkin dilakukan?

Gunakan asumsi jika diperlukan.

BAB VI KESIMPULAN

1. Berbagai macam konsep dalam sistem jaringan komputer perlu dijadikan dasar dalam melakukan analisis, perancangan, penerapan, dan evaluasi sistem jaringan komputer.
2. Analisis kebutuhan sistem jaringan komputer dapat mencakup analisis sistem kebutuhan pengguna dan analisis sistem berjalan. Selanjutnya hasil analisis kebutuhan digunakan sebagai dasar dalam melakukan perancangan sistem jaringan komputer.
3. Perancangan jaringan dapat menggunakan topologi yang sesuai dengan kebutuhan organisasi. Terdapat dua jenis rancangan yaitu rancangan fisik dan rancangan logis.
4. Penerapan sistem jaringan komputer mengacu pada rancangan yang telah dibuat. Setelah penerapan selanjutnya dilakukan pengujian untuk memastikan penerapan sudah sesuai.
5. Monitoring dan evaluasi diperlukan ketika sistem jaringan komputer sudah berjalan. Monitoring dan evaluasi diperlukan untuk memastikan sistem jaringan komputer berjalan sesuai dengan kebutuhan organisasi.

DAFTAR PUSTAKA

Agus Siswanto dan Hetty Rohayani. Optimalisasi Kinerja Sistem Jaringan Komputer (Studi Kasus Wiltop Group Jambi). Conference Paper September 2013

Curt M. White, "Data Communications and Computer Networks, A business user's approach", 7th Edition, Course Technology, 2013

Crystal Panek, "Networking Fundamentals", Sybex A Wiley Brand, 2020

Kaveh Pahlavan and Prashant Krishnamurthy, "Networking Fundamentals, Wide, Local and Personal Area Communications", Wiley, 2009

Hasanul Fahmi. Analisis Qos (Quality Of Service) Pengukuran Delay, Jitter, Packet Lost Dan Throughput Untuk Mendapatkan Kualitas Kerja Radio Streaming Yang Baik. Jurnal Teknologi Informasi dan Komunikasi Vol 7 No 2 Desember 2018

https://www.cs.uct.ac.za/mit_notes/networks/pdfs/chp11.pdf
diakses pada 26 Februari 2022

<http://wndw.net/pdf/wndw3-en/ch16-network-monitoring.pdf>
diakses pada 26 Februari 2022

<https://www.cs.purdue.edu/homes/park/cs422/intro-2-06s.pdf>
diakses pada 28 Februari 2022

Jian Ren and Tongtong Li. Network Management. Michigan State University. Diakses pada 26 Februari 2022.
<https://www.eegr.msu.edu/~renjian/pubs/network-management.pdf>

DAFTAR LAMPIRAN

PENULIS

SINOPSIS

Modul Sistem Jaringan Komputer merupakan salah satu modul di Pranata Komputer. semoga pembaca dapat menambah ilmu dan bertambah pula wawasan system jaringan komputer.

Modul Sistem Jaringan Komputer dimaksudkan untuk meningkatkan kompetensi kerja (pengetahuan, keterampilan dan sikap) peserta dalam penggunaan analisis sampai evaluasi system jaringan computer. Serta untuk mempersiapkan dan mengkader Pranata Komputer yang lebih profesional dalam melaksanakan pekerjaan ataupun tanggap dalam menyikapi setiap proses perubahan dan perkembangan teknologi dan informasi, serta mempunyai sikap peka terhadap persoalan ketidakberdayaan yang dialami organisasi dan mempunyai ketrampilan/kemampuan untuk menyelesaiannya.

Modul Sistem Jaringan Komputer ini dimaksudkan sebagai pedoman bukan text book bagi pengajar dan peserta pelatihan dalam pelaksanaan proses belajar mengajar mata pelatihan system Jaringan komputer

COVER BELAKANG