
POLITEKNIK NEGERI BANJARMASIN
DASAR-DASAR
JARINGAN
WANVY ARIFHA SAPUTRA

DASAR-DASAR JARINGAN

Undang-Undang No. 28 Tahun 2014 Tentang Hak Cipta

Fungsi dan sifat hak cipta Pasal 4

Hak Cipta sebagaimana dimaksud dalam Pasal 3 huruf a merupakan hak eksklusif yang terdiri atas hak moral dan hak ekonomi.

Pembatasan Perlindungan Pasal 26

Ketentuan sebagaimana dimaksud dalam Pasal 23, Pasal 24, dan Pasal 25 tidak berlaku terhadap :

i. penggunaan kutipan singkat Ciptaan dan/atau produk Hak Terkait untuk pelaporan peristiwa aktual yang ditujukan hanya untuk keperluan penyediaan informasi aktual;
ii. Penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk kepentingan penelitian ilmu pengetahuan;
iii. Penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk keperluan pengajaran, kecuali pertunjukan dan Fonogram yang telah dilakukan Pengumuman sebagai bahan ajar; dan
iv. penggunaan untuk kepentingan pendidikan dan pengembangan ilmu pengetahuan yang memungkinkan suatu Ciptaan dan/atau produk Hak Terkait dapat digunakan tanpa izin Pelaku Pertunjukan, Produser Fonogram, atau Lembaga Penyiaran.

Sanksi Pelanggaran Pasal 113

1. Setiap Orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp 100.000.000 (seratus juta rupiah).
2. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp 500.000.000,00 (lima ratus juta rupiah).
3. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf a, huruf b, huruf e, dan/atau huruf g untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).
4. Setiap Orang yang memenuhi unsur sebagaimana dimaksud pada ayat (3) yang dilakukan dalam bentuk pembajakan, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau pidana denda paling banyak Rp 4.000.000.000,00 (empat miliar rupiah).

DASAR-DASAR JARINGAN

Wanvy Arifha Saputra

Poliban Press

DASAR-DASAR JARINGAN

Penulis :
Wanvy Arifha Saputra

ISBN :
978-623-7694-93-9

ISBN Elektronik:
978-623-7694-94-6 (PDF)

Editor dan Penyunting :
Reza Fauzan

Desain Sampul dan Tata letak :
Eko Sabar Prihatin; Rahma Indera

Penerbit :
POLIBAN PRESS
Anggota APPTI (Asosiasi Penerbit Perguruan Tinggi Indonesia)
no.004.098.1.06.2019
Cetakan Pertama, 2022

Redaksi :
Politeknik Negeri Banjarmasin, Jl. Brigjen H. Hasan Basry,
Pangeran, Komp. Kampus ULM, Banjarmasin Utara
Telp : (0511)3305052
Email : press@poliban.ac.id

Diterbitkan pertama kali oleh :
Poliban Press, Banjarmasin, Januari 2022

Kata Pengantar

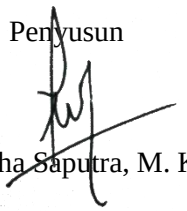
Puji Syukur kehadirat Allah Subhanahu wa Ta'ala, karena atas limpahan rahmat-Nya, sehingga kami dapat menyelesaikan bahan ajar dasar-dasar jaringan. Bahan ajar ini disusun berdasarkan topik tingkatan pemahaman khusus vokasi. Bahan ajar ini juga dilengkapi dengan latihan soal untuk menguji pemahaman mahasiswa terkait dengan materi.

Kami menyadari masih banyak kekurangan dalam penyusunan bahan ajar ini. Oleh karena itu, kami sangat mengharapkan kritik dan saran demi perbaikan dan kesempurnaan bahan ajar ini.

Kami mengucapkan terima kasih kepada berbagai pihak yang telah membantu proses penyelesaian bahan ajar ini, terutama unit P3M Politeknik Negeri Banjarmasin yang telah mendukung penuh atas penerbitan bahan ajar ini. Kemudian kepada bapak Arifin Noor Asyikin dan bapak Effan Najwaini yang telah memberikan kontribusi referensi terhadap materi di bahan ajar ini. Semoga bahan ajar ini dapat bermanfaat bagi kita semua, khususnya para mahasiswa.

Banjarmasin, 31 Agustus 2021

Penyusun



Wanvy Arifha Saputra, M. Kom

Daftar Isi

BAB 1
Konsep Dasar dan *Software Tools* Jaringan

Capaian Pembelajaran:

1. Mampu menjelaskan konsep dasar jaringan secara umum
2. Mampu menyebutkan *software tools* jaringan
3. Mampu melakukan simulasi jaringan LAN dengan Kabel

Pada bab ini membahas tentang konsep-konsep dasar jaringan, dan *software tools* pendukungnya. Konsep dasar yang dijabarkan merupakan pengertian jaringan secara umum beserta perangkat *hardware*, dan sejarah singkat terjadinya jaringan komputer. Kemudian untuk *software tools* pendukung dijabarkan meliputi spesifikasi dan kegunaannya. Pada soal latihan memuat tentang simulasi jaringan LAN dengan kabel menggunakan *packet tracert*.

1.1 Konsep Dasar

1.1.1 Jaringan Komputer

Jaringan Komputer merupakan jaringan telekomunikasi yang menghubungan antara komputer satu dengan yang lainnya, minimal 2 buah perangkat. Jaringan komputer membutuhkan *Network adapter* atau perangkat penghubung komputer seperti *Network Interface Card* (NIC) / *wireless* NIC / *modem portable*. Media koneksinya sebagai medium transmisi data pada jaringan komputer yaitu kabel maupun nirkabel (*wireless* seperti radio, microwave, satelit dan sebagainya).

Selain perangkat tersebut, diperlukan juga sistem operasi sebagai antar muka antara manusia dan mesin. Sistem operasi yang diperuntukkan khusus jaringan seperti Microsoft windows 2000 server, Microsoft windows NT, Novell netware, Linux dan sebagainya. Untuk menjembatani antara komputer atau perangkat jaringan lainnya

membutuhkan peralatan interkoneksi. Peralatan tersebut seperti Hub, Bridge, Switch, Router, dan lainnya.

Peralatan interkoneksi jaringan terbagi menjadi dua, yaitu aktif dan pasif. Perangkat aktif merupakan perangkat yang menggunakan sumberdaya listrik untuk beroperasi. Berikut beberapa perangkat aktif yang umum digunakan:

- *Repeater*

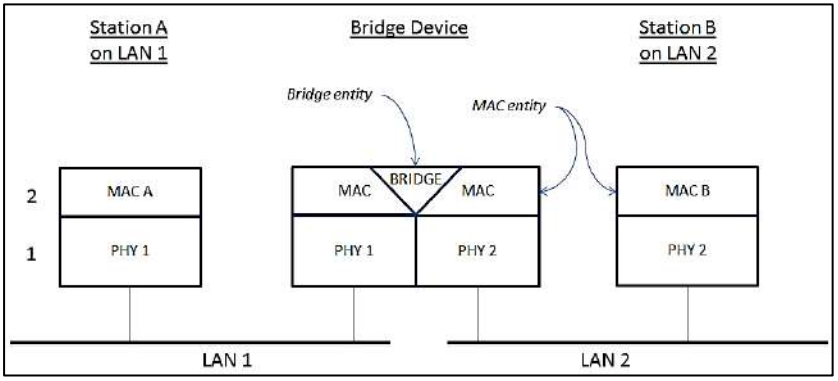
  Repeater (*Amplifier*) adalah perangkat jaringan yang digunakan untuk menguatkan sinyal data kemudian mengirimkan kembali sinyal tersebut dengan daya yang lebih tinggi sehingga dapat memperluas jangkauan sinyal. Sistem yang digunakan *repeater* untuk meningkatkan frekuensi data ada dua macam yaitu sistem analog dan sistem digital. *Repeater* bekerja pada layer ke satu (Physical layer). Pada sistem analog, data yang dikirim oleh *repeater* memiliki kualitas berbanding lurus dengan konsumsi daya listrik, sedangkan pada sistem digital data yang diterima akan diperbaiki kualitasnya sebelum data tersebu dikirim kembali.

Gambar 1.*Repeater*

- *Bridge*

  Bridge yaitu perangkat yang menghubungkan dua jaringan komputer LAN, *bridge* juga dapat menghubungkan tipe jaringan komputer yang berbeda-beda seperti *Ethernet* & *Fast Ethernet*.

Gambar 2. *Bridge*



Gambar 3. Jaringan *Bridge*

- *Server*

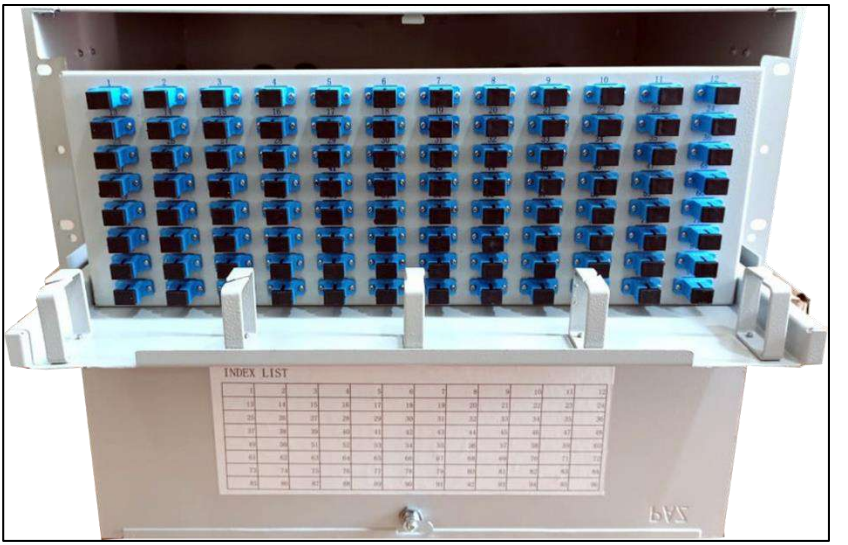
  Server bisa disebut juga perangkat yang digunakan untuk mengelola segala aktivitas yang terjadi dalam jaringan. Selain itu juga berperan sebagai pusat data informasi. Adapun aktivitas yang umumnya dikelola oleh *server* yaitu:

  ✓ Mengatur lalu lintas transfer data atau *file* yang diminta komputer *client*;
  ✓ Menyimpan data atau *file* yang dikirim oleh komputer *client*;
  ✓ Mengatur hak akses data atau file dalam sebuah jaringan;
  ✓ Melindungi komputer client dari malware dengan anti malware atau firewall;.

Sedangkan perangkat pasif merupakan perangkat yang dapat berjalan tanpa sumberdaya listrik, namun tetap dapat menghantarkan aliran data. Biasanya perangkat pasif merupakan perangkat untuk jaringan optik. Berikut beberapa perangkat pasif yang umum digunakan:

- OTB (Pasif)

  OTB (*Optical Termination Box*) adalah titik terminasi kabel serat optik outdoor dengan kabel serat optik indoor. OTB biasanya terletak di data sentral pada sebuah ISP dan berdekatan dengan perangkat aktif penting lainnya.



Gambar 4. OTB 96 *Core*

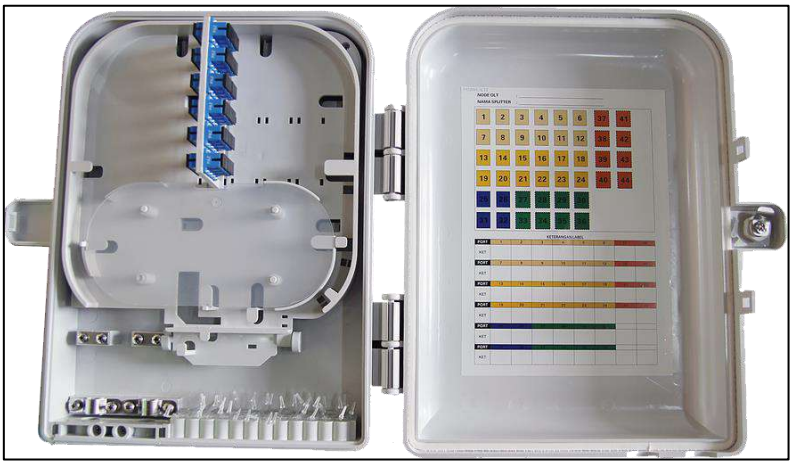
- ODC

  ODC (*Optical Ditribution Cabinet*) adalah suatu ruang yang berbentuk kotak terbuat dari material khusus yang berfungsi sebagai tempat instalasi sambungan jaringan optik single-mode untuk menghubungkan telekomunikasi. Biasanya penempatan berada di pinggir jalan atau halaman kosong rumah penduduk yang sudah terikat kontrak.

Gambar 5. ODC-C 144 *Core*

- ODP

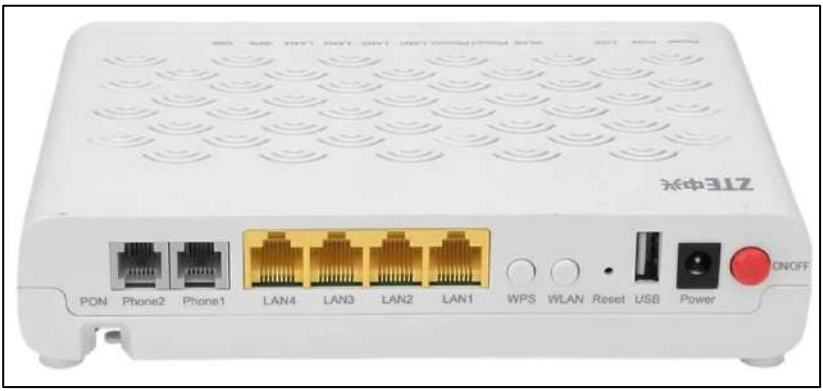
  ODP (*Optical Distribution Point*) adalah tempat *splitter* dan terminasi drop kabel. Biasanya penempatan ada di tiang teratas dan dekat dengan rumah penduduk.



Gambar 6. ODP *pole*

- ONT

  ONT (*Optical Network Termination*) menyediakan interface antara jaringan optik dengan pelanggan. Biasanya posisi ada didalam rumah pelanggan dan umumnya disebut juga *router* WLAN optik.



Gambar 7. ONT ZTE F623

1.1.2 Sejarah Jaringan

Bermula dari tahun 1937 negara menggunakan TELEX untuk mengirimkan pesan khusus militer saja, namun pada era 2000-an TELEX menjadi teknologi resmi dan komersil. Kemudian dilanjutkan tahun 1957 terbentuknya Advanced Research Projects Agency (ARPA) oleh Department of Defence (DoD) USA untuk riset komputer yang saling terhubung. Projek tersebut berhasil dan terciptalah desain awal pada tahun 1967 dan pengembangannya sampai tahun 1969. Pada tahun tersebut jaringan sudah terealisasi dan dikenal dengan ARPANET. Memasuki tahun 1970, terdapat lebih dari 10 komputer yang dapat terhubung dan saling berkomunikasi. Tahun 1972 Roy Tomlinson berhasil menyempurnakan program "e-mail" untuk ARPANET, dimana program tersebut populer dengan ikon "@" yang bearti "pada".

Tahun 1973 ARPANET berkembang luas keluar dari USA, dan pada tahun tersebut pula *University College* di London mempunyai komputer pertama yang tergabung dalam ARPANET diluar USA. Pada 1974 ini pula lah gagasan tentang "*internet*" atau protocol TCP/IP ditemukan

oleh Vincent Cerf dan Bob Kahn yang dipresentasikan di *Sussex University*. Hari bersejarah yang paling populer pada 26 Maret 1976, yaitu Ratu Inggris yang berhasil mengirim e-mail dari *royal signal and radar establishment* di Malvern sebagai bagian dari demonstrasi teknologi tercanggih saat itu. Dan pada tahun 1982 TCP/IP menjadi secara resmi menjadi protocol untuk ARPANET, karena pada waktu tersebut sudah banyak sekali komputer yang terhubung ke ARPANET.

Pada tahun 1984, komputer yang terhubung diperkirakan sebanyak 1000 unit, karena itu diperkenalkan teknologi bernama *Domain Name System* (DNS) yang merupakan sistem penamaan masing-masing komputer yang terhubung dijaringan. Dan tahun 1992 menemukan program editor dan browser ysng bisa menjelejah antar komputer oleh Tim Berners Lee. Program tersebut dinamakan *world wide web* (www) yang kemudian dikenal era sekarang yaitu *surfing* atau *browsing*.

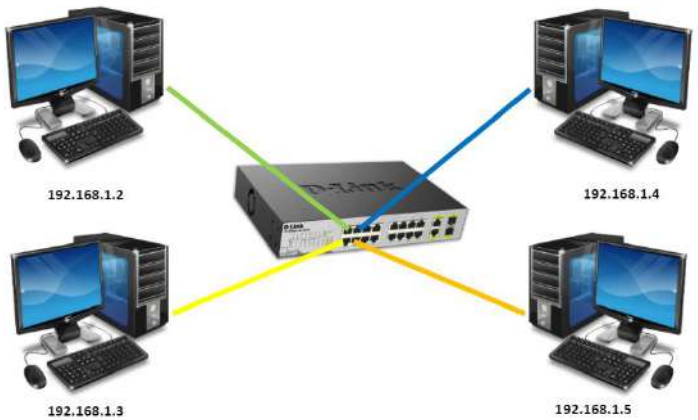
1.1.3 Pengenalan Jaringan

Pengenalan jaringan terdiri dari PAN, LAN, MAN, dan WAN.

a) PAN (*Personal Area Network*) merupakan jaringan komputer yang menghubungkan komputer satu maupun dengan perangkat lain dalam jarak sangat dekat misalnya satu ruangan, jaringan ini bisa dihubungkan dengan kabel dan internet ke printer, PDA, dan perangkat lainnya. Fungsi jaringan PAN mencakup area yang sangat dekat dan tidak sampai lintas ruangan apalagi lintas gedung sehingga menjadi media penghubung yang mudah dan juga personal.

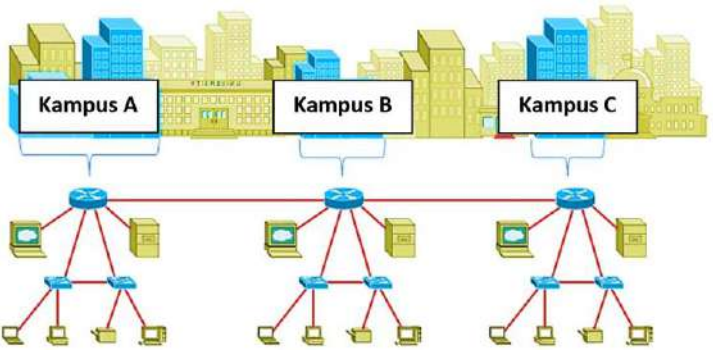
Gambar 8. *Personal Area Network* (PAN)

b) LAN (*Local Area Network*) disebut juga area komputer yang cakupannya kecil atau tidak begitu luas seperti satu ruangan, satu sekolah, satu gedung, dan lainnya. Jaringan ini hanya bisa menghubungkan antara satu komputer dengan komputer lainnya dengan jarak yang dekat. Fungsi jaringan ini membantu mempercepat informasi dari server (Komputer inti) ke komputer turunan, memudahkan proses pengecekan *database*, memudahkan komunikasi setiap karyawan, dan membantu menjaga keamanan data



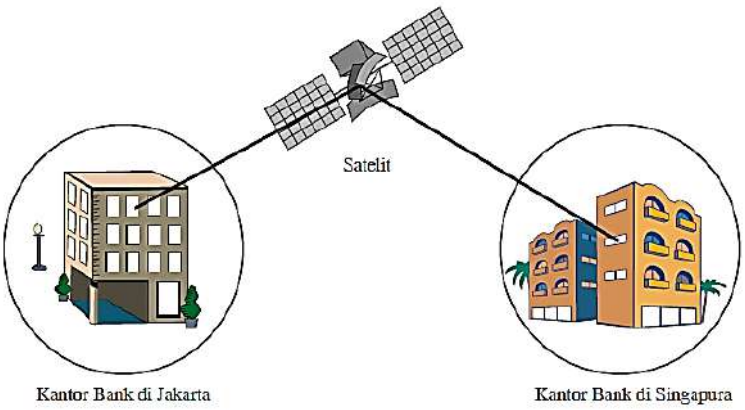
Gambar 9. Local Area Network (LAN)

c) MAN (*Metropolitan Area Network*) merupakan jaringan komputer yang areanya cukup luas bisa dalam satun kota yang sama. Jarak antara server dengan user anatara 5 - 50 KM. Jaringan ini digunakan menghubungkan server dari perusahaan pusat ke user dikantor cabang. Fungsi jaringan MAN membantu sistem jaringan mengkombinasikan dua *server*, menghubungkan komputer dari satu kota kekota lain dan meningkatkan efesiensi antara kantor pusat dengan kantor cabang.



Gambar 10. *Metropolitan Area Network* (MAN)

d) WAN (*Wide Area Network*) merupakan jenis jaringan komputer yang cakupannya paling luas tidak hanya lintas kota namun lintas pulau, lintas negara, dan lintas benua. Jaringan ini dibangun dengan menggunakan kabel fiber optik yang ditanam ditanah maupun didasar laut. Fungsi jaringan WAN menjadi penghubung antara jaringan LAN dan MAN, membantu mempercepat sharing data atau berbagai informasi, memudahkan kegiatan komunikasi yang terpisah jarak jauh, memudahkan update data karena *real time*, menjadi media menyampaikan informasi lebih cepat dan efisien.



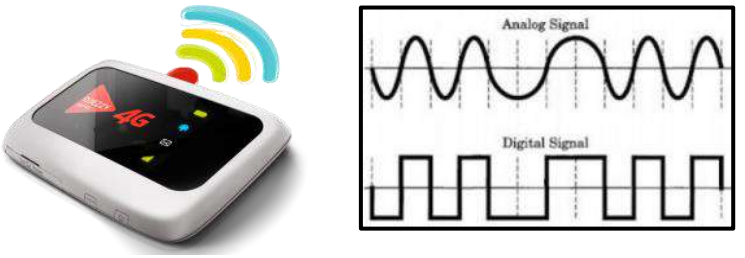
Gambar 11. *Wide Area Network*

1.1.4 Perangkat Jaringan

Perangkat jaringan telah banyak dikembangkan berbagai macam perangkat jaringan komputer untuk membantu dan mengoptimalkan kinerja sistem jaringan. Berikut ini merupakan macam perangkat yang umum dijumpai dan digunakan:

- Modem (Modulator Demodulator)

  Modem Merupakan perangkat yang digunakan untuk menghubungkan antara perangkat komputer, dengan penyedia layanan internet atau bisa disebut juga dengan *internet Service Provider* (ISP). Modem juga memiliki fungsi untuk mengubah sinyal digital dan analog, sehingga dalam menerima dan mengirim pesan bisa berjalan baik.



Gambar 12. Modem

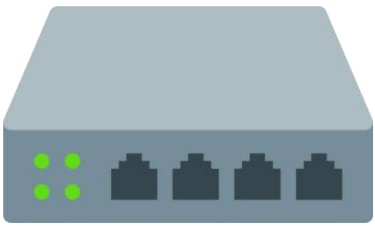
- NIC (*Network Interface Card*)

  NIC adalah sebuah komponen yang berfungsi sebagai jembatan dari komputer ke jaringan komputer lainnya. NIC dapat dipasangkan pada *motherboard* sebuah CPU. NIC dapat dipasang lebih dari satu pada sebuah komputer asalkan *motherboard* mendukung multi slot.

Gambar 13. NIC

- Hub

  Hub yaitu sebuah perangkat yang berfungsi untuk menghubungkan komputer yang satu dengan yang lainnya. Hub hanya bekerja di *layer physical*, sehingga hanya mengenal arus listrik saja tanpa mengenal *MAC ADDRESS* atau TCP/IP.



Gambar 14. *Hub*

- *Switch*

  Switch merupakan suatu jenis perangkat jaringan pada komputer yang digunakan untu menghubungkan beberapa hub dengan membentuk jaringan yang lebih besar atau menghubungkan komputer yg memiliki kebutuhan akan *bandwidth* yang lebih besar. *Switch* bekerja pada *layer Data Link*, sehingga mampu mengenali MAC ADDRESS.

Gambar 15. *Switch*

- *Router*

  Router adalah sebuah alat yang mengirimkan paket data melalui sebuah jaringan atau internet untuk mencapai tujuannya melalui sebuah proses yang dikenl dengan istilah *routing*. Perangkat ini bekerja pada layer Network, sehingga mengenali MAC ADDRESS dan TCP/IP.

Gambar 16. *Router*

- *Access Point*

  Access point merupakan perangkat jaringan nirkabel yang berisi sebuah *tranceiver* dan antena. Fungsinya yaitu untuk melakukan *bridge* dari 802.11 WLAN ke 802.3 *Ethernet*. Layer yang bekerja pada perangkat ini yaitu *data link*.

Gambar 17. *Access Point*

1.2 *Software Tools* Jaringan

Dalam pekerjaan yang berhubungan dengan jaringan diperlukan sebuah *tools* berupa *software* yang dapat mendukung. Berikut beberapa tools yang umumnya digunakan:

- Packet Tracer merupakan simulator jaringan berbasis cross-platform yang dirancang oleh Cisco System. Kemampuannya memungkin pengguna untuk membuat topologi jaringan dan meniru jaringan komputer modern. *Sofware* ini dapat diinstalasi pada sistem operasi windows x86, windows x64, dan Mac OS. Versi terbaru saat ini yaitu Tracer 7.3.0
- VMWare *workstation player* merupakan implementasi perangkat lunak dari sebuah mesin komputer yang dapat menjalankan program yang sama seperti layaknya komputer asli. Kemampuannya dapat merasakan system operasi selain yang

digunakan sehari-hari, VMWare ini dapat dipasang pada windows dan linux.

- *Wireshark* adalah penganalisis aliran paket data dari suatu perangkat dan sifatnya *freeware*. Perangkat ini digunakan untuk pemecahan masalah jaringan, analisis, perangkat lunak dan pengembangan protokol komunikasi, dan pendidikan.
- Nmap (*The network Mapper*) merupakan tool yang berfungsi untuk melakukan *port scanning*. Aplikasi ini digunakan untuk mengaudit jaringan yang ada, dan jaringan ini juga *freeware*.
- *Angry IP Scanner* merupakan *tools* untuk mendapatkan alamat IP dari komputer yang berada di jaringan komputer tertentu dan juga *freeware*.
- NetCut merupakan tools *yang* digunakan untuk berbagai hal yang berkaitan dengan protokol TCP atau UDP. Terkenal akan memutuskan koneksi *host* lain dalam satu jaringan, *freeware* oleh Arcai.com dan biasaya disalahgunakan oleh oknum tertentu.

1.3 Sertifikasi Jaringan

Untuk mendapatkan pengakuan secara nasional dan internasional dibidang jaringan diperlukanlah sertifikasi. Di Indonesia terdapat sertifikasi yang diakui oleh nasional melalui BNSP yang dibantu oleh Lembaga Sertifikasi Profesi (LSP) sebagai pihak ketiga. Beberapa skema yang populer yaitu skema *Junior Network Administrator*, *Network Administrator*, *Junior Networking*, dan *Networking*.

Sedangkan untuk sertifikasi internasional dapat melalui CISCO. CISCO merupakan produsen *Network Equipment* terbesar di dunia. Dan diakui sebagai produsen terbaik didunia.

Secara Umum tingkatan sertifikasi dari CISCO sebagai berikut:

- CCT (Cisco Certification Technique) untuk *Entry level*
- CCNA (*Networking Associate*) untuk *associate level*
- CCNP (*Networking Professional*) untuk profesional *level*
- CCIE (*Infrastructure Enterprise*) untuk *expert level*

1.4 Instalasi Packet Tracer

Sebelum melakukan instalasi, siapkan *setup packet tracer* / 64 bit (sesuaikan dengan tipe pada sistem operasi yang digunakan). Dan Requirement khusus Packet tracer versi 7.1 adalah sebagai berikut:

- ✓ Microsoft Windows (7 / 8.1 / 10) atau Linux Ubuntu (14.04 64-bits)
- ✓ *Processor* Pentium 4 (2.5 GHz)
- ✓ Minimum 2GB RAM (4GB *recommended*)
- ✓ 700 MB kesediaan kapasitas *hard disk*
- ✓ Minimum resolusi layar 1024 x 768

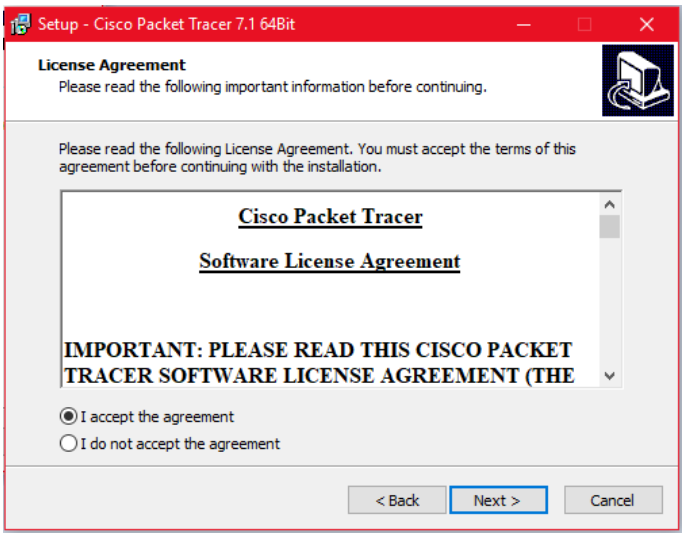
Bila tidak memenuhi *requirement* tersebut, silahkan instalasi menggunakan versi yang lebih rendah

Berikut langkah instalasinya:

1) Klik *Next* pada *welcome screen*

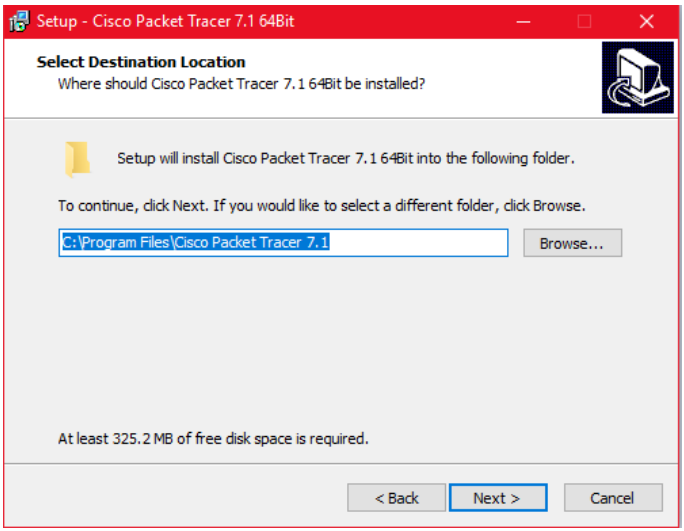
Gambar 18. Langkah 1 Instalasi

2) Pilih "*I Accept the agreement*", kemudian *Next*



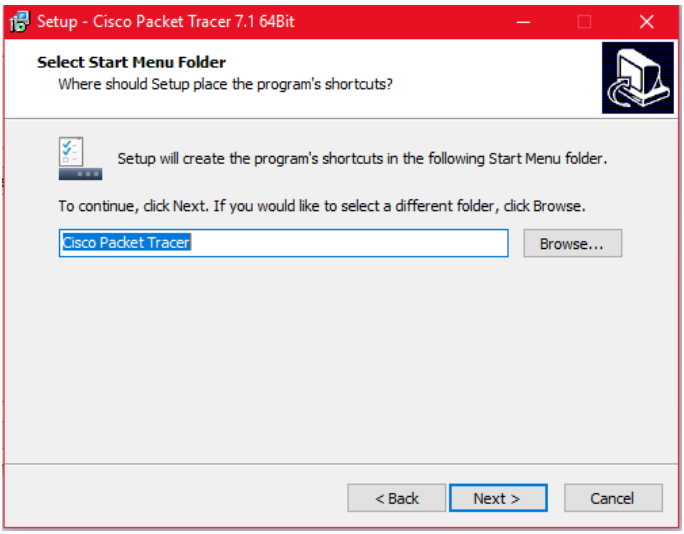
Gambar 19. Langkah 2 Instalasi

3) Biarkan saja lokasi intalasi di *program files*, Kemudian klik *Next*



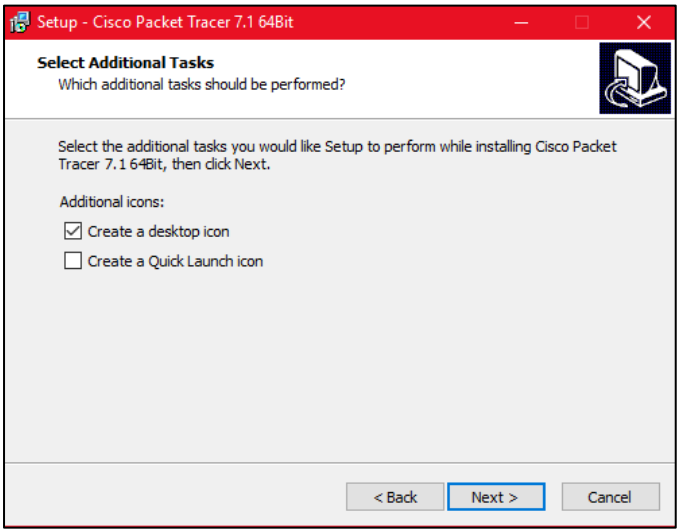
Gambar 20. Langkah 3 Instalasi

4) Biarkan saja nama *folder* yang *start menu*, Kemudian klik *Next*



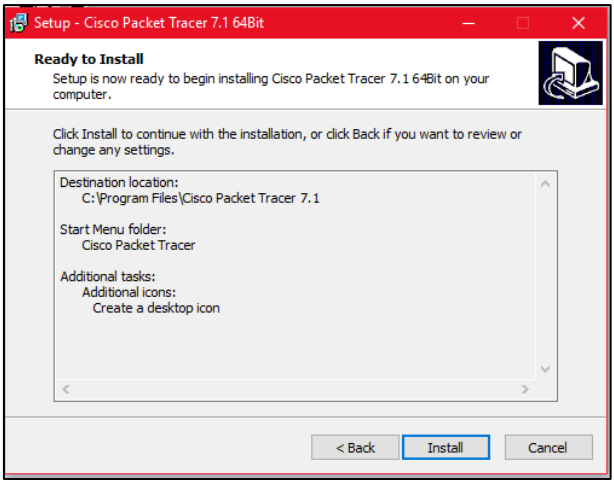
Gambar 21. Langkah 4 Instalasi

5) Centang "*create desktop icon*", Kemudian klik *Next*



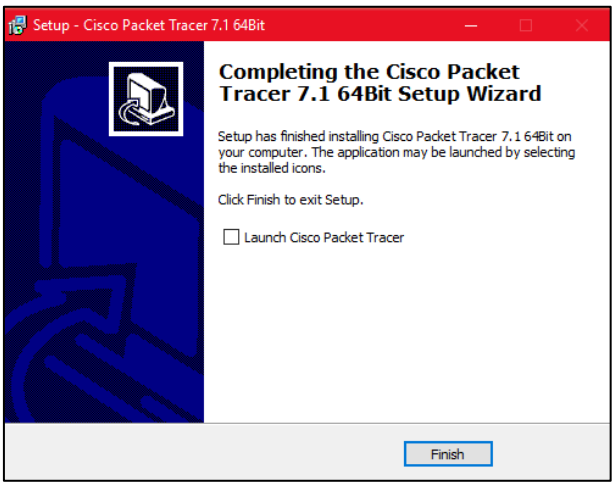
Gambar 22. Langkah 5 Instalasi

6) Klik tombol "*install*"



Gambar 23. Langkah 6 Instalasi

7) Klik *Finish*, dan jalankan aplikasinya



Gambar 24. Langkah 7 Instalasi

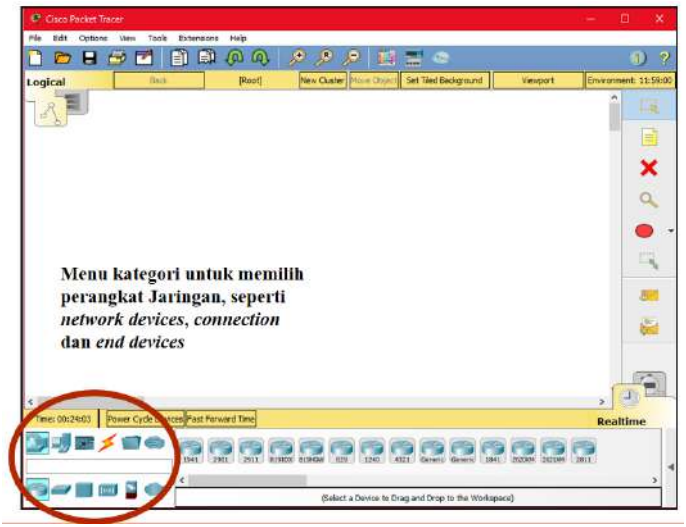
8) Tidak usah diisikan apa pun, langsung saja Pilih "*Guest Login*"

Gambar 25. Langkah 8 Instalasi

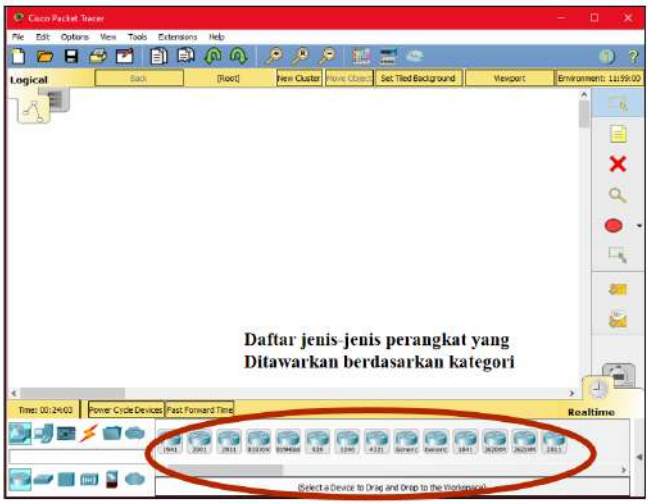
9) Tunggu *Countdown* pada *guest*, jika sudah sampai ke angka 0, tekan tombol *guest* lagi

1.5 Penjelasan Fitur Packet Tracer

Setelah melakukan instalasi packet tracert, berikut dijelaskan fitur-fitur yang secara umum digunakan pada simulasi jaringan.



Gambar 26. Penjelasan Fitur 1



Gambar 27. Penjelasan Fitur 2

Gambar 28. Penjelasan Fitur 3

1.6 Latihan Simulasi Jaringan LAN dengan Kabel

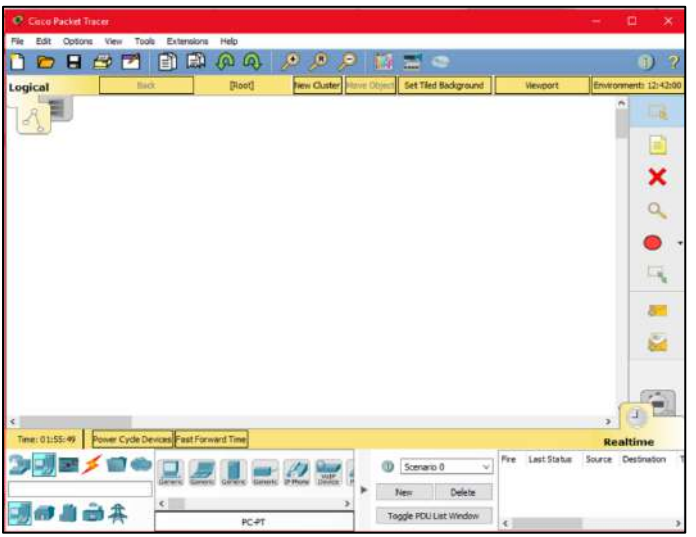
1.6.1 Percobaan Pertama (latihan1.pkt)

- Buatlah 1 buah jaringan sederhana (LAN) menggunakan 2 buah PC dan kabel jaringan cross dengan ketentuan berikut:

Nama PC	IP Address	Subnet Mask
PC0	192.168.0.2	255.255.255.0
PC1	192.168.0.3	255.255.255.0

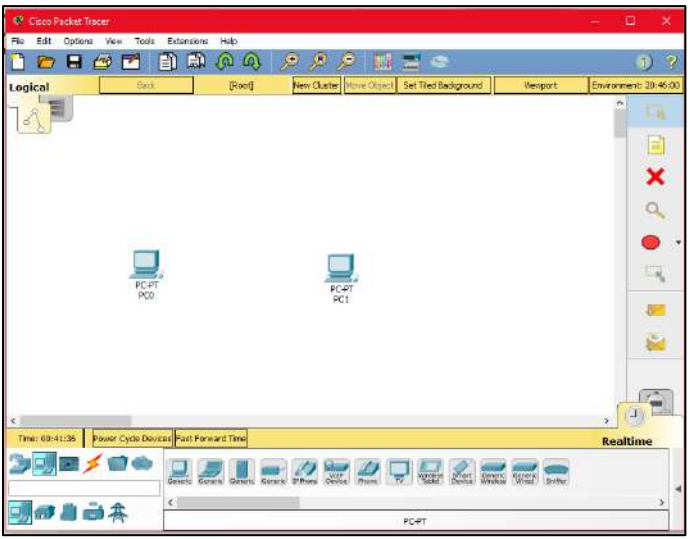
Untuk membantu proses latihan, silahkan ikuti langkah berikut:

1) Pilih *End Devices*, Kemudian pilih PC-PT *Generic*, Tarik ke dalam layar *Logical*



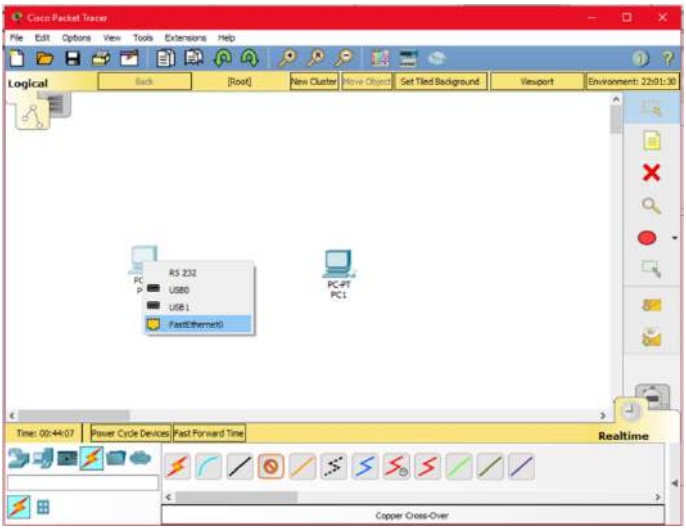
Gambar 29. Latihan 1 (1)

2) Sesuaikan perangkat dengan gambar setelah ini



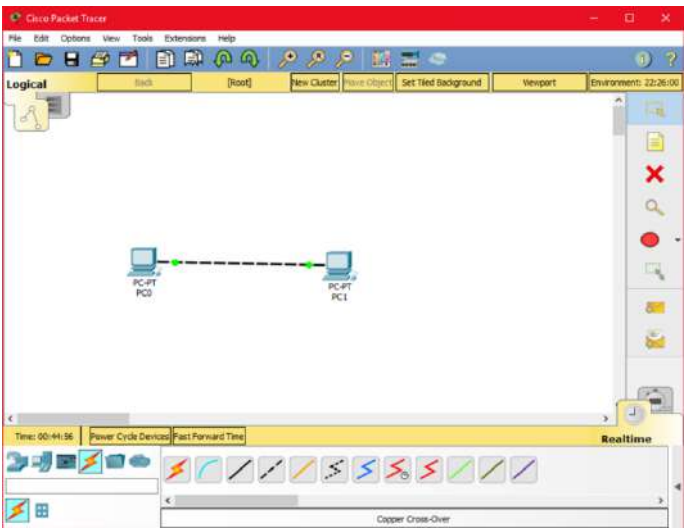
Gambar 30. Latihan 1 (2)

3) Kemudian pilih *Connection*, Dan Klik *Copper Cross-Over*, Arahkan *mouse* ke PC0, dan pilih *Fast Ethernet0*, Kemudian arahkan lagi PC1, dan pilih *Fast Ethernet0* juga,



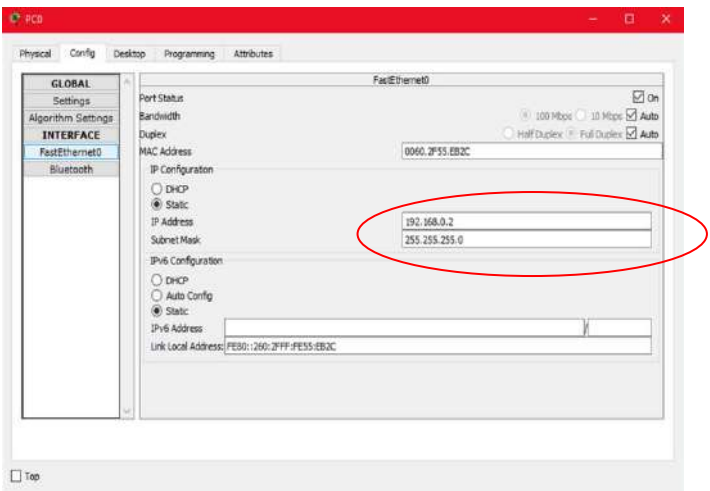
Gambar 31. Latihan 1 (3)

4) Kemudian klik kiri pada PC0, Dan lakukan setting *IP Address* dan *Subnet Mask*



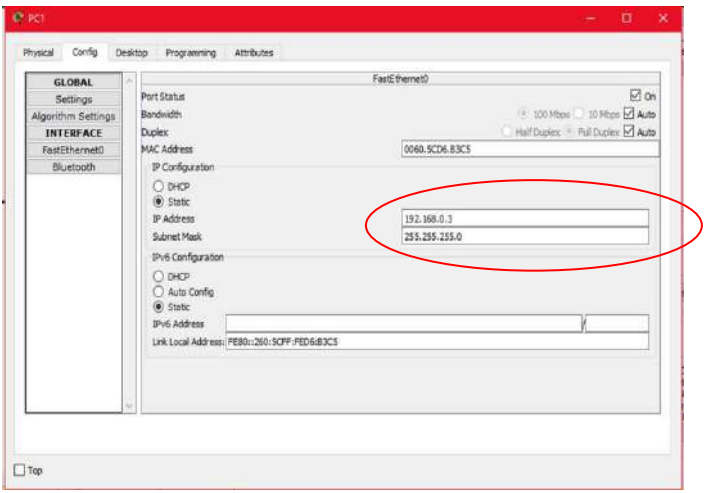
Gambar 32. Latihan 1 (4)

5) Untuk melakukan setting IP, pilih tab config →FastEhernet0
6) Untuk PC0, masukkan IP 192.168.0.2
7) Kemudian Subnetmask 255.255.255.0



Gambar 33. Latihan 1 (5)

8) Untuk PC1, masukkan IP 192.168.0.3
9) Kemudian Subnetmask 255.255.255.0

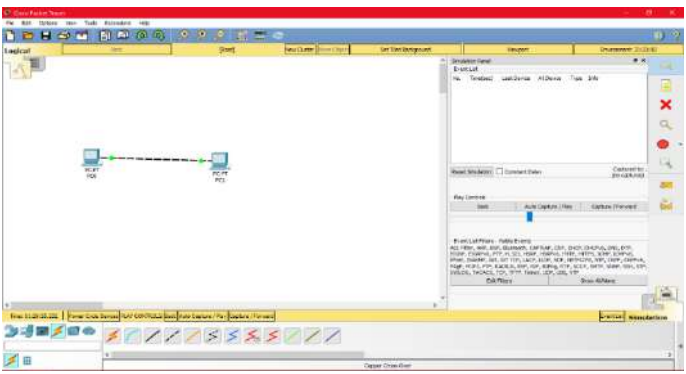


Gambar 34. Latihan 1 (6)

10) Kemudian, Klik PC0, Pilih Tap *Dekstop*, Kemudian Pilih *Command Prompt*
11) Ketikkan perintah berikut:
    - Ping 192.168.0.3
    - Ping 192.168.0.4
12) Amati pesan dari terminal tersebut

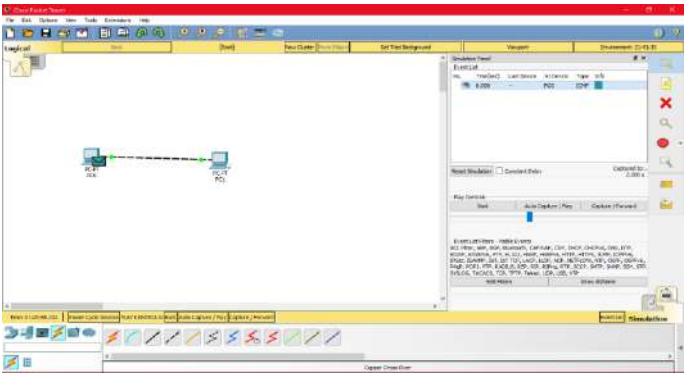
Gambar 35. Latihan 1 (7)

13) Untuk masuk ke simulasi, Pindah dari Realtime ke simulation,
14) Hasil akhir harus sesuai dengan gambar setelah ini



Gambar 36. Latihan 1 (8)

15) Kemudian klik add simple PDU, arahkan ke PC0 →PC1



Gambar 37. Latihan 1 (9)

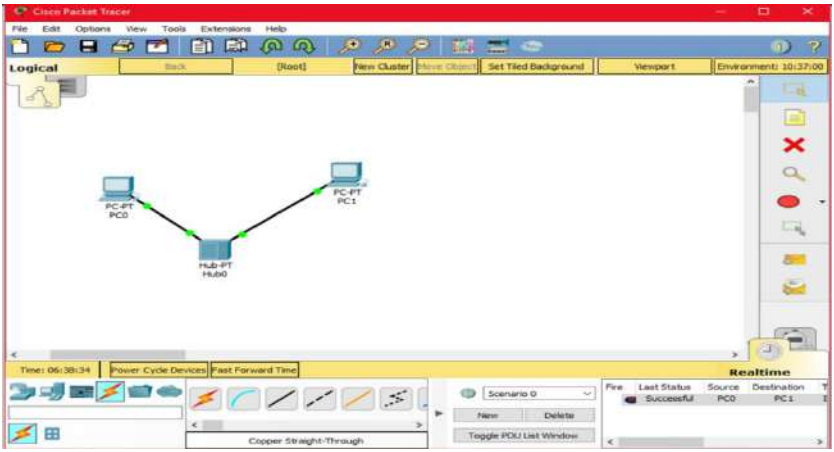
Dari percobaan tersebut:

- Dari PC0, Lakukan ping ke 192.168.0.3, jelaskan balasan pesan yang didapatkan
- Dari PC0, Lakukan ping ke 192.168.0.4, jelaskan balasan pesan yang didapatkan
- Dari Animasi yang dihasilkan, apakah paket data terkirimkan dengan baik? jelaskan

1.6.2 Percobaan Kedua (latihan2.pkt)

- Buatlah 1 buah jaringan sederhana (LAN) menggunakan 2 buah PC, 1 buah hub, 2 kabel jaringan straight dengan ketentuan berikut (Skema sesuai gambar setelah ini):

Nama PC	IP Address	Subnet Mask
PC0	192.168.0.2	255.255.255.0
PC1	192.168.0.3	255.255.255.0



Gambar 38. Latihan 2

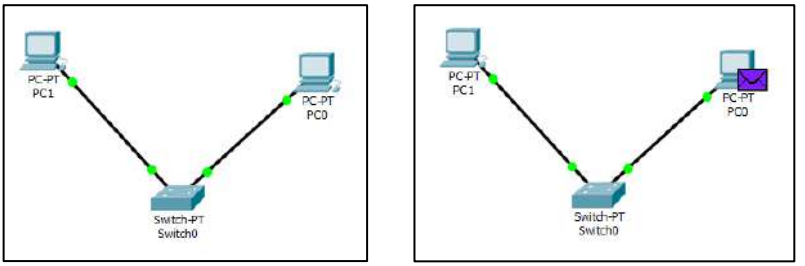
Dari percobaan tersebut:

- Dari PC0, Lakukan ping ke 192.168.0.3, jelaskan balasan pesan yang didapatkan
- Dari PC0, Lakukan ping ke 192.168.0.4, jelaskan balasan pesan yang didapatkan
- Dari Animasi yang dihasilkan, apakah paket data terkirimkan dengan baik? Jelaskan

1.6.3 Percobaan Ketiga (latihan3.pkt)

- Buatlah 1 buah jaringan sederhana (LAN) menggunakan 2 buah PC, 2 kabel jaringan straight dan 1 switch dengan ketentuan berikut:

Nama PC	IP Address	Subnet Mask
PC0	192.168.0.2	255.255.255.0
PC1	192.168.0.3	255.255.255.0



Gambar 39. Latihan 3

Dari percobaan tersebut:

- Dari PC0, Lakukan ping ke 192.168.0.3, jelaskan balasan pesan yang didapatkan
- Dari PC0, Lakukan ping ke 192.168.0.4, jelaskan balasan pesan yang didapatkan
- Dari Animasi yang dihasilkan, apakah paket data terkirimkan dengan baik? Jelaskan

BAB 2
Topologi Jaringan, IP *Address*, dan *Subnetmask*

Capaian Pembelajaran:

1. Mampu menjelaskan topologi jaringan
2. Mampu menjelaskan IP *Address*
3. Mampu menjelaskan subnetmask
4. Mampu melakukan simulasi jaringan WLAN

Pada bab ini membahas tentang topologi jaringan, IP *Address*, dan *subnetmask* pada sebuah jaringan. Topologi yang dijabarkan merupakan topologi jaringan yang sering digunakan beserta perbandingan antara *internet*, *intranet*, dan *ekstranet*. Kemudian untuk IP *address* dijabarkan meliputi IPV4 dan IPV6. Dan terakhir *subnetmask* menjabarkan tentang pembagian kelas jaringan. Pada soal latihan memuat tentang simulasi jaringan WLAN menggunakan *packet tracert*.

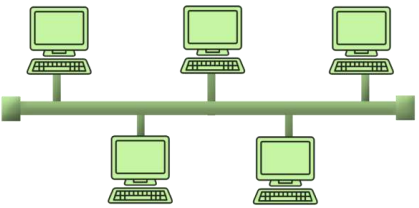
2.1 Topologi Jaringan

Topologi jaringan adalah suatu cara untuk membuat sejumlah komputer saling berhubungan satu sama lain, baik menggunakan kabel maupun yang secara nirkabel. Biasanya, tujuan topologi jaringan adalah demi kemudahan pertukaran informasi. Topologi jaringan ini sering kali dipakai di suatu perusahaan, lembaga, atau pun badan institusi agar antar anggotanya bisa saling melakukan komunikasi dengan cepat dan aman. Berikut jenis - jenis topologi jaringan:

- Topologi Jaringan BUS

  Topologi BUS adalah topologi jaringan yang lebih sederhana, masing-masing komputer (BNC Ethernet Card) terhubung ke satu kabel panjang (Coaxial) dengan beberapa terminal (Tconnector), dan pada akhir ujung kabel harus menggunakan terminator.

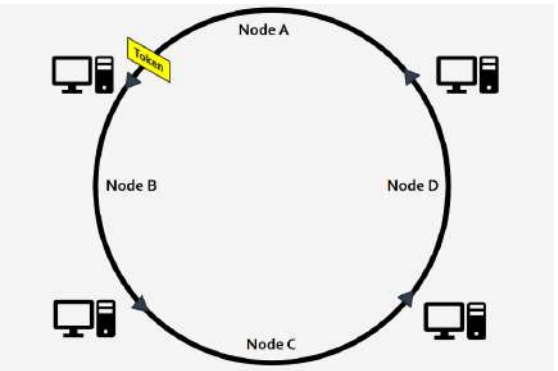
Topologi ini sudah sangat jarang ditemukan dimasa sekarang dan kabel yang digunakan saat itu adalah Coaxial RJ 58, menggunakan topologi ini jika salah satu node rusak maka jaringan seluruh node mengalami gangguan dan resiko tabrakan aliran data juga sangat besar.



Gambar 40. Topologi jaringan BUS

- Topologi Jaringan RING

  Topologi ini menggunakan Patch Cord Cable jenis UTP untuk membentuk jaringan menyerupai lingkaran sederhana yang terdiri dari beberapa node disusun secara seri. Topologi ini juga sangat jarang sekali digunakan, dan membutuhkan dua LAN Card yang terpasang pada setiap komputer. Pergerakan data melalui mekanisme token dengan berjalan satu arah, sehingga tidak ada kemungkinan untuk bertabrakan. jika salah satu node rusak, maka data yang melewati node jaringan tersebut mengalami gangguan sama seperti topologi BUS.



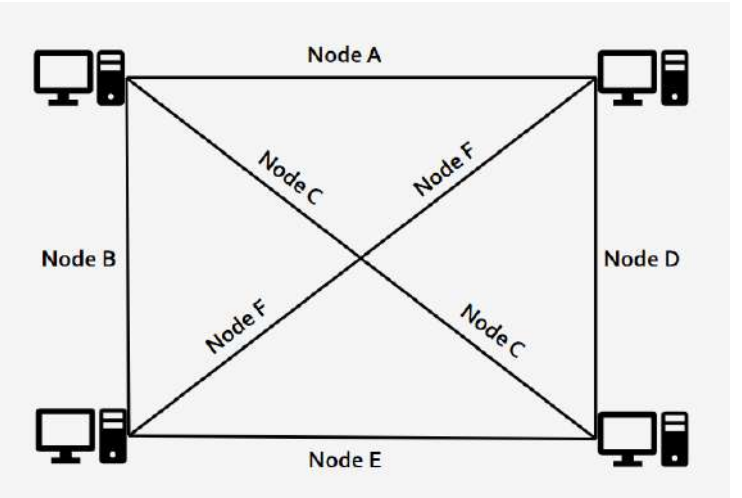
Gambar 41. Topologi Jaringan Ring

- Topologi Jaringan MESH

  Sistem topologi mesh ini di mana koneksi antar komputer saling terhubung secara langsung satu sama lain (dedicated link). Topologi ini juga membutuhkan banyak LAN Card yang terpasang pada setiap komputer dengan rumus:

  LAN Card per Komputer = Total Komputer dalam satu jaringan - 1

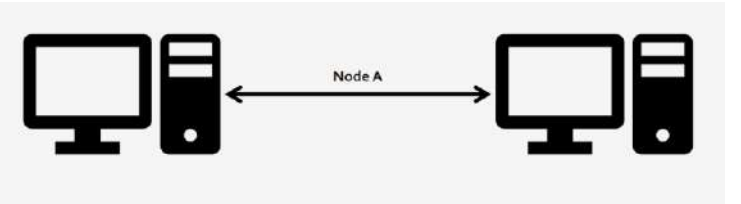
  Pergerakan data pada topologi ini berjalan langsung ke komputer yang dituju, sehingga tidak ada kemungkinan untuk bertabrakan, dan jika salah satu node rusak maka tidak mempengaruhi node lain.



Gambar 42. Topologi Jaringan Mesh

- Topologi Jaringan P2P

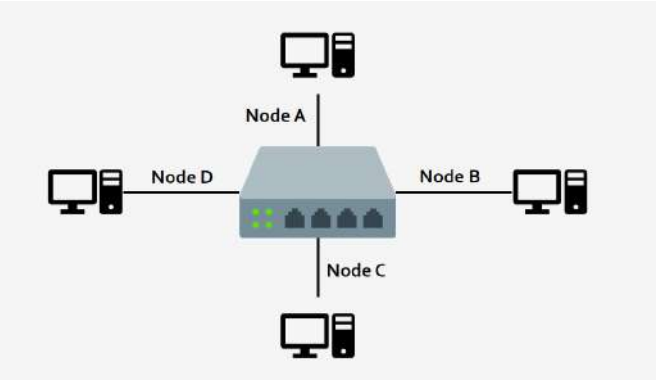
  Topologi jaringan P2P merupakan topologi yang menghubungkan dua buah komputer dengan satu kabel (umumnya UTP RJ 45) dan hanya membutuhkan 1 Lan Card, pergerakan data langsung berjalan ke komputer yang dituju, jika salah satu node rusak dapat dipastikan akan mengalami gangguan.



Gambar 43. Topologi Jaringan P2P

- Topologi Jaringan Star

  Topologi Star merupakan topologi jaringan dari beberapa komputer yang memiliki koneksi dengan node pada jaringan pusat. Topologi ini juga sangat sering digunakan, dan membutuhkan minimal 1 perangkat jaringan penghubung (Hub / Switch / Router). Pergerakan data pada topologi ini melalui mekanisme terpusat atau sentral, sehingga alur data diatur oleh perangkat sentral untuk meminimalisir kemungkinan terjadinya tabrakan data, dan jika salah satu node rusak tidak mempengaruhi node lain.

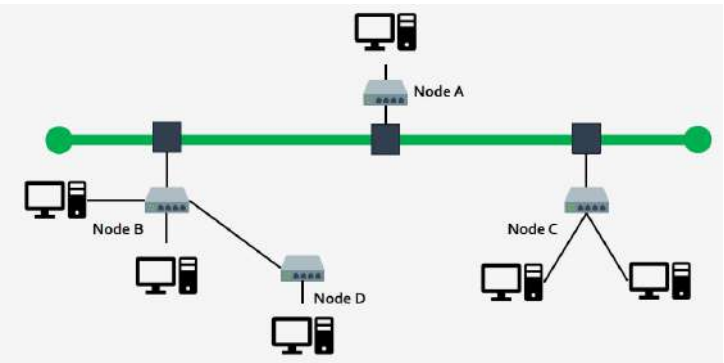


Gambar 44. Topologi Jaringan Star

- Topologi Jaringan TREE

  Topologi jaringan berbentuk TREE (pohon) merupakan bentuk gabungan dari sistem topologi BUS dan STAR, di mana jaringan topologi BUS menjadi konektor utama beberapa topologi STAR Jika diibaratkan dengan bentuk seperti pohon, topologi BUS adalah batang utama yang menghubungkan beberapa topologi STAR

sebagai rantingnya. Ciri-ciri topologi jaringan TREE adalah memiliki kabel utama sebagai penghubung beberapa jaringan star, dan memiliki tingkatan jaringan atau hierarki. Jika salah satu stasiun sekunder mengalami kerusakan, tidak akan mengganggu keseluruhan sistem.

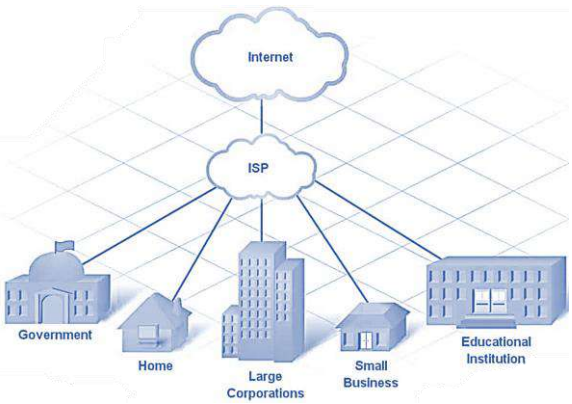


Gambar 45. Topologi Jaringan Tree

2.2 *Internet, Intranet,* dan *Ekstranet*

2.2.1 Internet

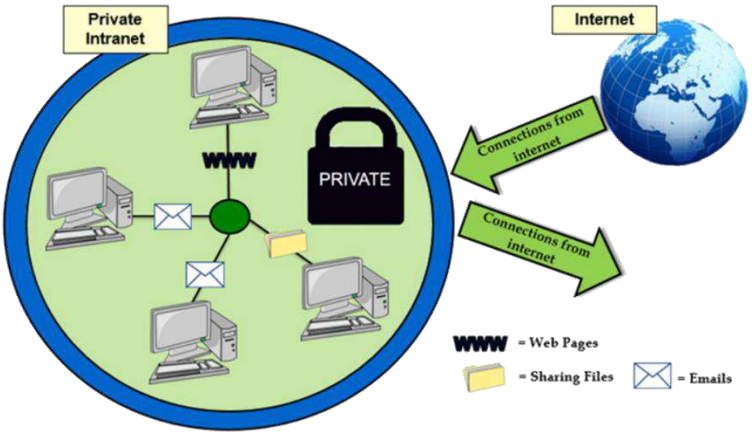
Internet adalah sebuah jaringan yang menghubungkan komputer satu dengan komputer lainnya yang menggunakan Transmission Control Protocol atau Internet Protocol Suite (TCP/IP) sebagai protokol sehingga dapat berkomunikasi, berinteraksi, dan saling bertukar informasi meski dalam jarak yang jauh.



Gambar 46. Internet

2.2.2 Intranet

Intranet adalah jaringan pribadi (Private Network) untuk bertukar informasi di dalam jaringan lokal (LAN / MAN / WAN) dan tidak bisa diakses melalui jaringan luar.



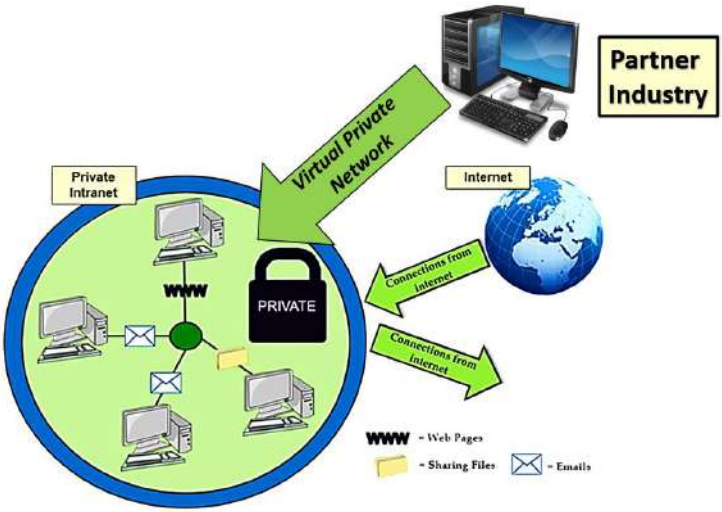
Gambar 47. Intranet

Intranet dapat digunakan dengan jaringan internet sebagai jembatan untuk koneksi ke jaringan lokal dengan menggunakan VPN (Virtual Private Network), contoh lingkungan yang menggunakannya adalah sekolah, kantor, perusahaan, dan universitas. Perbedaan antara internet dan intranet dapat dilihat pada tabel dibawah ini:

Parameter	**Internet**	**Intranet**
Penggunaan	Public / Umum	Private / Terbatas
Koneksi	User menggunakan dial-up melalui ISP secara mandiri	User tinggal menikmati, karena dilakukan oleh organisasi atau instansi
Informasi	Semua informasi	Terbatas hanya pada informasi internal
Cakupan	Sangat Luas	Kecil
Akses User	Sangat banyak	Sedikit
Maintenance Sistem	Tidak dapat diprediksi	Dilakukan mandiri oleh organisasi atau instansi

2.2.3 Ekstranet

Jaringan intranet organisasi yang ingin mengekspose informasi yang mereka miliki ke jaringan luar. Umumnya terkait mitra sebagai pihak ke-2 yang telah dipercaya oleh pihak ke-1, dan memberikan akun untuk mengakses informasi didalam jaringan intranet pihak ke-1.



Gambar 48. Ekstranet

2.3 IP *Address*

IP address adalah protokol yang memberikan alamat atau identitas untuk peralatan di dalam jaringan. IP Address (*internet protocol address*) merupakan deretan angka biner antara 32 bit sampai dengan 128 bit yang digunakan sebagai alamat identifikasi untuk tiap komputer host dalam jaringan internet. Angka 32 bit digunakan untuk alamat IP Address versi IPv4 dan angka 128 bit digunakan untuk IP Address versi IPv6 untuk menunjukkan alamat dari komputer pada jaringan internet berbasis TCP/IP.

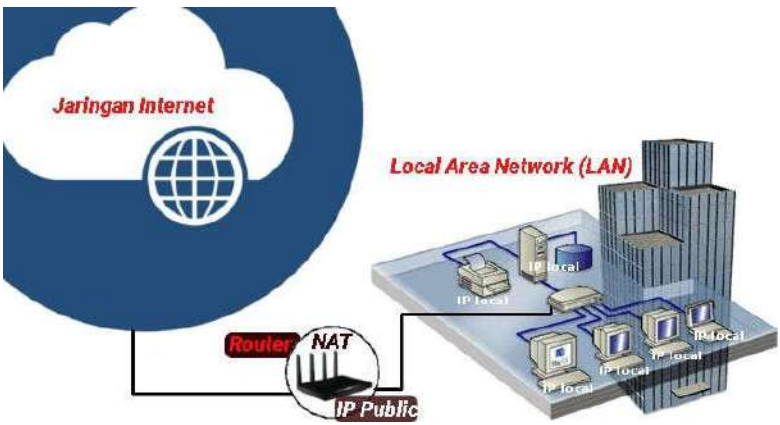
IP Address tersebut memiliki identitas numerik yang akan dilabelkan kepada suatu device seperti komputer, router atau printer yang terdapat dalam suatu jaringan komputer yang menggunakan internet protocol sebagai sarana komunikasi.

Fungsi IP Address:

- IP Address sebagai alat identifikasi host atau antarmuka pada jaringan. Fungsi ini diilustrasikan seperti Nama Orang sebagai suatu metode untuk mengenali siapa orang tersebut. Dalam jaringan komputer pun berlaku hal yang sama yaitu alamat IP Address yang unik tersebut akan digunakan untuk mengenali sebuah komputer atau device pada jaringan.
- IP Address sebagai alamat lokasi jaringan. Fungsi ini diilustrasikan seperti Alamat Rumah yang menunjukkan lokasi kita berada. Untuk memudahkan pengiriman paket data, maka IP Address memuat informasi keberadaannya. Ada rute yang harus dilalui agar data dapat sampai ke komputer yang dituju.

2.3.1 IP *Private* dan IP *Public*

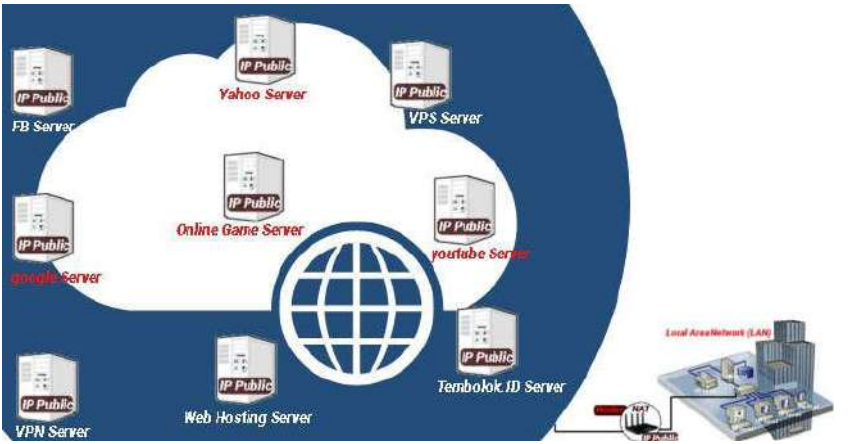
Pembagian dalam *IP Address* dibagi kedalam dua kategori yaitu IP private dan IP Publik. IP private adalah hanya bisa diakses dari jaringan lokal saja dan tidak bisa diakses melalui jaringan internet secara langsung tanpa bantuan router (NAT). IP private digunakan untuk jaringan lokal (LAN) agar sesama komputer dapat saling berkomunikasi.



Gambar 49. IP *Private*

Sedangkan dalam IP *public* 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 50. IP *Public*

2.3.2 IPV4

IPv4 adalah sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP menggunakan protokol IP versi 4. Total panjangnya adalah 32-bit. Alamat IP versi 4 umumnya diekspresikan dalam notasi desimal bertitik (*dotted-decimal notation*) yang dibagi ke dalam empat buah oktet berukuran 8-bit. Karena setiap oktet berukuran 8-bit, maka nilainya berkisar antara 0 hingga 255. Alamat IP yang dimiliki oleh sebuah *host* dapat dibagi dengan menggunakan *subnet mask* jaringan ke dalam dua bagian, yaitu:

- *Network Identifier* (NetID) atau *Network Address* yang digunakan khusus untuk mengidentifikasikan alamat jaringan di mana host berada.
- *Host Identifier* (HostID) adalah alamat yang digunakan khusus untuk mengidentifikasikan alamat host di dalam jaringan. Nilai hostID tidak boleh bernilai 0 atau 255 dan harus bersifat unik di dalam segmen jaringan.

Alamat IPv4 terbagi menjadi 3 jenis:

1) Alamat *Unicast*

   Merupakan alamat IPv4 yang ditentukan untuk sebuah antarmuka jaringan yang dihubungkan ke sebuah *Internetwork* IP. Alamat *unicast* digunakan dalam komunikasi *point-to-point* atau *one-to-one*.

2) Alamat *Broadcast*

   Merupakan alamat IPv4 yang didesain agar diproses oleh setiap *node* IP dalam segmen jaringan yang sama. Alamat *broadcast* digunakan dalam komunikasi *one-to-everyone*.

3) Alamat *Multicast*

   Merupakan alamat IPv4 yang didesain agar diproses oleh satu atau beberapa node dalam segmen jaringan yang sama atau berbeda. Alamat *multicast* digunakan dalam komunikasi *one-to-many.*

Pembagian kelas IP *Address* versi 4:

1) 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.

2) 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.

3) 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*. Seabagai

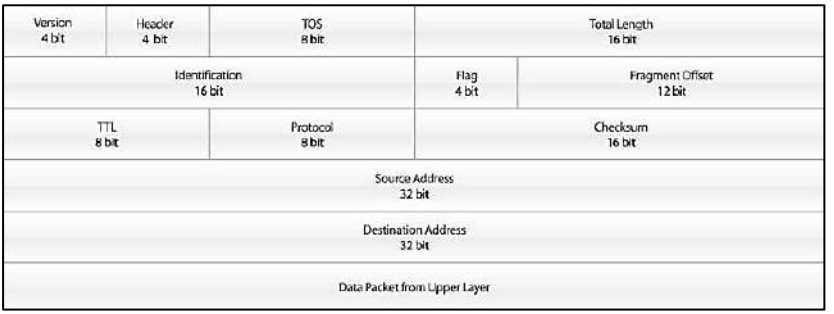
contoh penggunaan IP Address Kelas C adalah: 192.168.1.2, 192.168.1 merupakan *network* ID dan 2 merupakan *host* ID-nya

4) IP *Address* Kelas D

   Alamat IP kelas D 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*.

5) IP *Address* Kelas E

   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*.



Gambar 51. Struktur Paket IPv4

Berikut penjelasan setiap *tag* dari Gambar diatas:

- *Version* mengindentifikasi versi IP, yang dimana untuk IPV4 nilai diset menjadi 4
- *Header* (IHL) berfungsi mengidentifikasi ukuran header IP.
- TOS (*Type of service*) digunakan untuk menentukan kualitas transmisi dari sebuah datagram IP.
- *Total Length* dapat didefinisikan panjang keseluruhan dari datagram IP, dimana mencakup *header* IP dan muatan yang didalamnya dalam bentuk *byte*. Minimum-panjang datagram adalah 20 *byte* (*header* 20-*byte* + 0 *byte* data) dan maksimal adalah 65.535 *byte*

- *Indetification* merupakan bagian yang digunakan mengindentifikasi sebuah paket IP yang tertentu yang akan difregmentasikan.
- *Flag* digunakan untuk mengontrol apakah *router* diperbolehkan untuk fragmen dan untuk menunjukkan bagian-bagian dari sebuah paket ke *receiver*.
- *Fragment Offset* merupakan jumlah byte dari awal paket yang dikirim. Selain itu *Fragment Offset* digunakan untuk mengidentifikasikan *offset* di mana fragmen yang dimulai.
- *Time to Live* digunakan untuk mengidentifikasikan berapa banyak saluran jaringan di mana sebuah datagram IP dapat berjalan.
- *Protocol* mendefinisikan protokol yang digunakan dalam bagian data dari datagram IP.
- *Header Checksum* berguna untuk melakukan pengecekan integritas terhadap header IP. *Header Checksum* berisi nilai *checksum* yang dihitung dari seluruh *field* dari *header* paket IP.
- *Source address* adalah sebuah alamat IPv4 yang menunjukkan pengirim paket.
- *Destination address* adalah sebuah alamat IPv4 yang menunjukkan penerima paket

2.3.3 IPV6

Alamat IP versi 6 (IPv6) adalah sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol Internet versi 6. Panjang totalnya adalah 128-bit, dan secara teoritis dapat mengalamati hingga 2^{128} = 3,4 x 10^{38} *host* komputer di seluruh dunia.

21da:00d3:0000:2f3b:02aa:00ff:fe28:9c5a

Gambar 52. Contoh IPv6

IPv6 juga mengizinkan adanya DHCPv6 Server sebagai pengelola alamat. Jika dalam IPv4 terdapat *dynamic address* dan *static address*, maka dalam IPv6, konfigurasi alamat dengan menggunakan DHCP Server dinamakan dengan *stateful address configuration*, sementara

jika konfigurasi alamat IPv6 tanpa DHCP Server dinamakan dengan *stateless address configuration*.

Pada IPv6 terdapat 3 jenis tipe alamat IP yaitu:

1) Alamat *Unicast*, yang menyediakan komunikasi secara *point-to-point*, secara langsung antara dua *host* dalam sebuah jaringan.
2) Alamat *Multicast*, yang menyediakan metode untuk mengirimkan sebuah paket data ke banyak *host* yang berada dalam group yang sama. Alamat *multicast*digunakan dalam komunikasi *one-to-many*.
3) Alamat *Anycast*, yang menyediakan metode penyampaian paket data kepada anggota terdekat dari sebuah group. Alamat ini digunakan dalam komunikasi *one-to-one-ofmany*. Alamat ini juga digunakan hanya sebagai alamat tujuan (*destination address*) dan diberikan hanya kepada *router*, bukan kepada *host-host* biasa.

Dalam IPv6, alamat 128-bit akan dibagi ke dalam 8 blok berukuran 16-bit, yang dapat dikonversikan ke dalam bilangan heksadesimal berukuran 4-digit. Setiap blok bilangan heksadesimal tersebut dipisahkan dengan tanda titik dua (:). Karenanya, format notasi yang digunakan oleh IPv6 juga sering disebut dengan *colon-hexadecimal format*, berbeda dengan IPv4 yang menggunakan *dotted-decimal format***.**

Berikut ini adalah contoh alamat IPv6 dalam bentuk bilangan biner:

0010000111011010000000001101001100000000000000000001011
11001110110000001010101010000000001111111111111100010
10001001110001011010

Gambar 53. IPv6 dalam biner 128-bit

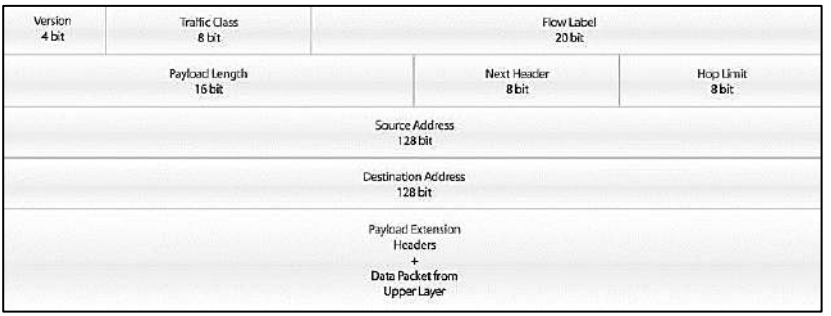
Untuk menerjemahkannya ke dalam bentuk notasi *colon-hexadecimal format*, angka-angka biner di atas dibagi ke dalam 8 buah blok berukuran 16-bit:

- Blok 1: 0010000111011010
- Blok 2: 0000000011010011

- Blok 3: 0000000000000000
- Blok 4: 0010111100111011
- Blok 5: 0000001010101010
- Blok 6: 0000000011111111
- Blok 7: 1111111000101000
- Blok 8: 1001110001011010

Lalu, setiap blok berukuran 16-bit tersebut dikonversikan ke dalam bilangan heksadesimal dan setiap bilangan heksadesimal tersebut dipisahkan dengan menggunakan tanda titik dua. Hasil konversinya adalah sebagai berikut:

21da:00d3:0000:2f3b:02aa:00ff:fe28:9c5a



Gambar 54. Struktur Paket IPv6

Berikut penjelasan setiap *tag* dari Gambar diatas:

- *Version:* field yang menunjukkan versi Internet Protokol, yaitu 6.
- *Prior:* field yang menunjukkan nilai prioritas. *Field* ini memungkinkan pengirim paket mengidentifikasi prioritas yang diinginkan untuk paket yang dikirimkan.
- *Flow Label:* digunakan oleh pengirim untuk memberi label pada paket-paket yang membutuhkan penanganan khusus dari *router* IPv6, seperti *quality of service* yang bukan *default*, misalnya *service-service* yang bersifat *real-time*.
- *Payload Length: field* berisi 16 bit yang menunjukkan panjang *payload*, yaitu sisa paket yang mengikuti *header* IP, dalam oktet.

- *Next Header:* field 8 bit yang berfungsi mengidentifikasi *header* yang mengikuti *header* IPv6 utama.
- *Hop Limit:* field berisi 8 bit *unsigned integer*. Menunjukkan jumlah *link* maksimum yang akan dilewati paket sebelum dibuang. Paket akan dibuang bila *Hop Limit* bernilai nol.
- *Source Address:* field 128 bit, menunjukkan alamat pengirim paket.
- *Destination Address:* field 128 bit, menunjukkan alamat penerima paket.

2.3.4 Perbedaan IPV4 dan IPV6

- Kelas Pengalamatan

  Di dalam IPV4 dikenal dengan kelas pengalamatan, yang terdiri dari 5 kelas yaitu Kelas A, Kelas B, Kelas C, Kelas D dan kelas E. Biasanya yang dipakai oleh umum ada di kelas A, B, dan C, sedangkan Kelas D untuk *multicast* dan Kelas E untuk penelitian. Namun terdapat pendapat Kelas D dan E menjadi satu. Sedangkan di dalam IPV6, tidak dikenal penamaan kelas-kelas tersebut. Tetapi di dalam IPV6 dikenal jenis pengalamatan, yaitu Pengalamatan *Unicast*, Pengalamatan *Multicast*, dan pengalamatan *Anycast*. Alamat Unicast dibagi lagi menjadi 3 bagian, yaitu Alamat *Link Local*, Alamat *Site Local*, dan Alamat Global.
- *Routing*

  Di IPV4, memiliki jalur yang lebih lambat dalam melakukan *routing*, hal ini dikarenakan adanya pemeriksaan *header* MTU di setiap *routing* dan *switching*. Sedangkan di IPV6, proses *routing* menjadi lebih sederhana. Dengan begini proses *routing* di IPV6 menjadi lebih cepat.
- *Mobile* IP

  Dukungan IPV4 terhadap perangkat *mobile* sangat kurang. Karena IPV4 tidak diperuntukkan untuk sebuah perangkat *mobile*. Karena itu sering terjadi *roaming*. Sedangkan pada IPV6 mendukung perangkat *mobile* di dalam desain IP.

- Keamanan

  Untuk menjaga keamanan IPV4 mengggunakan Ipsec sebagai fitur keamanan tambahan. Sedangkan IPV6, IPsec secara *default* telah digunakan. Jadi setiap proses akan melewati IPsec terlebih dahulu.

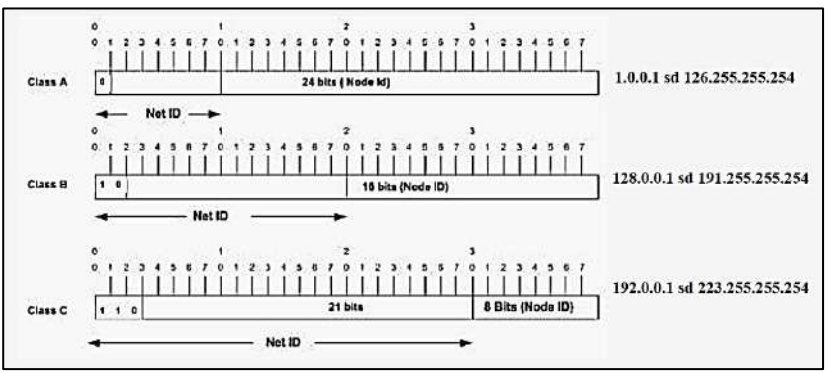
2.4 *Subnetmask*

Subnetmask merupakan teknik khusus untuk membagi jaringan komputer menjadi *subnetwork* dengan ukuran yang lebih kecil dan bisa dilakukan terhadap IPV4 yang terdiri dari kelas A, B dan C. IPv4 terdiri atas 4 oktet, nilai 1 oktet adalah 255. Karena ada 4 oktet maka jumlah IP Address yang tersedia adalah 255 x 255 x 255 x 255. Untuk penjelasasn tentang kelas IPV4 sudah dibahas sebelumnya. Fungsi Subnetmask:

- Efisiensi alokasi IP Address pada suatu jaringan

  Penggunaan IP Address yang dimaksud bisa dijalankan secara lebih optimal terhadap jumlah IP dengan jumlah pengguna yang aktif. Sehingga mengurangi resiko berupa ketidakstabilan jaringan akibat dari jumlah host yang terlalu banyak di suatu jaringan komputer.
- Mengatasi masalah yang berkaitan dengan perbedaan media fisik dan hardware yang digunakan dalam suatu *network*.

  Karena secara umum, Router IP itu hanya bisa dipakai untuk mengintegrasikan network-network yang media fisiknya berbeda dan mempunyai IP Address unik.



Gambar 55. Subnetmask IPV4

2.5 Latihan Simulasi Jaringan WLAN dengan Kabel

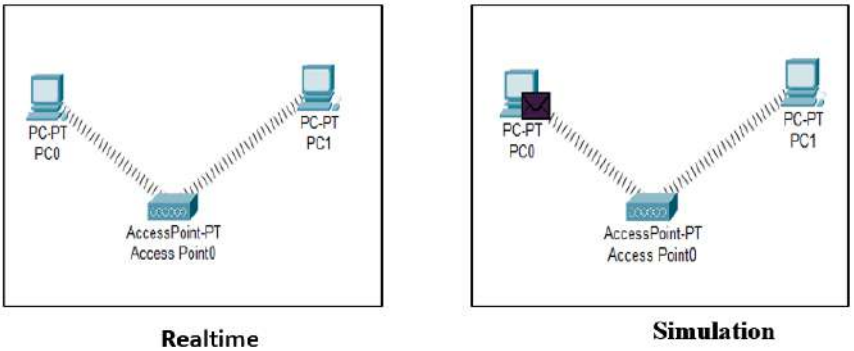
2.5.1 Percobaan Pertama (latihan1.pkt)

- Buatlah 1 buah jaringan wireless sederhana (WLAN) menggunakan 2 buah PC, 1 buah Access Point-PT dengan ketentuan berikut:

Nama PC	IP Address	Subnet Mask	Perangkat
PC0	192.168.0.2	255.255.255.0	WMP300N
PC1	192.168.0.3	255.255.255.0	WMP300N

- Konfigurasi access point:
  - ✓ Duplex setting auto pada interface port 0
  - ✓ Bandwidth setting auto pada interface port 0
  - ✓ Pastikan port status ON pada interface port 0
  - ✓ Channel bebas saja pada interface port 1
  - ✓ SSID dengan nama “Lab RPL” pada interface port 1
  - ✓ Authentication disabled pada interface port 1
- Rubah Perangkat Kartu Jaringan Menjadi *Wireless* (WMP300N)

Gambar 56. Latihan 1



Gambar 57. Latihan 1

Dari percobaan tersebut:

- Dari PC0, Lakukan ping ke 192.168.0.3, jelaskan balasan pesan yang didapatkan
- Dari PC1, Lakukan ping ke 192.168.0.4, jelaskan balasan pesan yang didapatkan
- Kirimkan paket data PC0→ PC1. Dari Animasi yang dihasilkan, apakah paket data terkirimkan dengan baik? Jelaskan

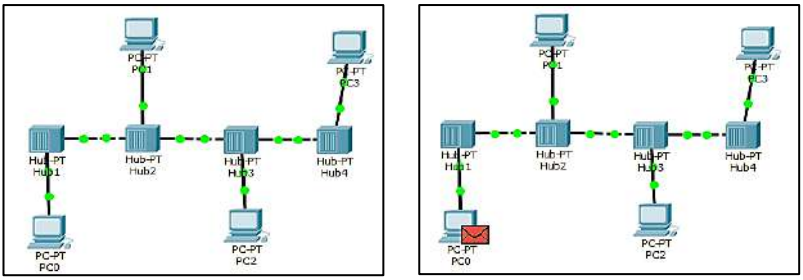
2.5.2 Percobaan Kedua (latihan2.pkt)

- Buatlah topologi jaringan BUS (Logical) dimana terdapat 4 buah PC, 4 buah Hub, 3 buah kabel cross, dan 4 buah kabel straight dengan ketentuan sebagai berikut:

Nama PC	IP Address	Subnet Mask
PC0	192.168.0.2	255.255.255.0
PC1	192.168.0.3	255.255.255.0
PC2	192.168.0.4	255.255.255.0
PC3	192.168.0.5	255.255.255.0

- Perangkat (Hub-PT) atau Modules pada semua hub:
  - ✓ 6 PT-REPEATER-NM-1CFE

Gambar 58. Latihan 2



Realtime **Simulation**

Gambar 59. Latihan 2

Dari percobaan tersebut:

- Dari PC1, Lakukan ping ke 192.168.0.3, jelaskan balasan pesan yang didapatkan
- Kirimkan paket data PC0→ PC3. Dari simulasi yang dihasilkan, Bagaimana paket data yang dikirimkan?
- Kenapa terdapat tanda X pada beberapa PC?
- Potonglah kabel antara Hub 2 dan Hub 3 dengan menggunakan delete, kemudian jalankan lagi simulasinya, bagaimana paket data yang dikirimkan?

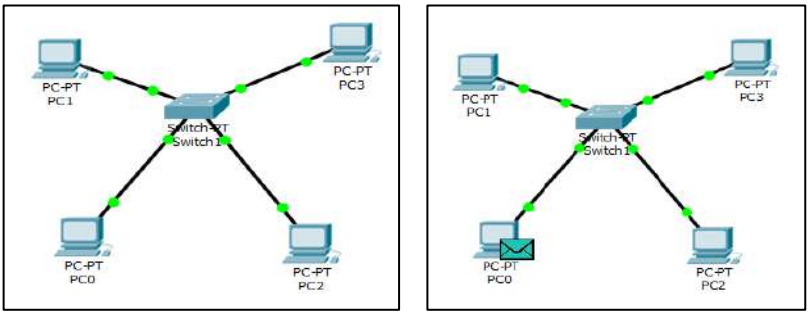
2.5.3 Percobaan Ketiga (latihan3.pkt)

- Buatlah topologi jaringan STAR (Physical) dimana terdapat 4 buah PC, 1 Switch dan 4 buah kabel straight dengan ketentuan sebagai berikut:

Nama PC	**IP Address**	**Subnet Mask**
PC0	192.168.0.2	255.255.255.0
PC1	192.168.0.3	255.255.255.0
PC2	192.168.0.4	255.255.255.0
PC3	192.168.0.5	255.255.255.0

- Perangkat (Switch-PT) atau Modules pada switch0:
  - ✓ 4 PT-REPEATER-SWITCH-1CFE
  - ✓ 2 PT-REPEATER-SWITCH-1FFE

Gambar 60. Latihan 3



Realtime **Simulation**

Gambar 61. Latihan 3

Dari percobaan tersebut:

- Dari PC2, Lakukan ping ke 192.168.0.3, jelaskan balasan pesan yang didapatkan
- Kirimkan paket data PC0→PC3. Dari simulasi yang dihasilkan, Bagaimana paket data yang dikirimkan?

- Potonglah kabel antara PC2 dan Switch dengan menggunakan delete, kemudian jalankan lagi simulasinya, bagaimana paket data tersebut?
- Dari PC0, lakukan ping ke 192.168.0.4, jelaskan balasan pesan tersebut

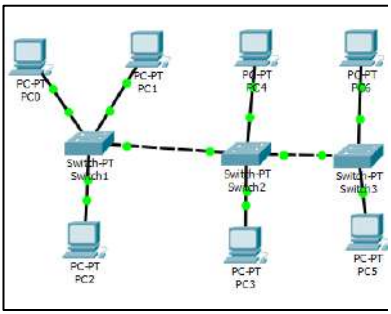
2.5.4 Percobaan Keempat (latihan4.pkt)

- Buatlah topologi jaringan STAR-BUS (Physical-Logical) dimana terdapat 7 PC, 3 Switch, 7 kabel straight dan 2 kabel cross dengan ketentuan sebagai berikut:

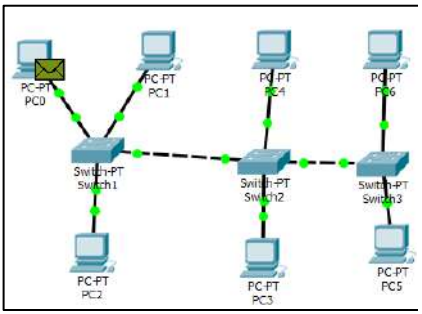
Nama PC	IP Address	Subnet Mask
PC0	192.168.0.2	255.255.255.0
PC1	192.168.0.3	255.255.255.0
PC2	192.168.0.4	255.255.255.0
PC3	192.168.0.5	255.255.255.0
PC4	192.168.0.6	255.255.255.0
PC5	192.168.0.7	255.255.255.0
PC6	192.168.0.8	255.255.255.0

- Perangkat (Switch-PT) atau Modules pada semua switch:
  - ✓ 4 PT-REPEATER-SWITCH-1CFE
  - ✓ 2 PT-REPEATER-SWITCH-1FFE

Gambar 62. Latihan 4



Realtime



Simulation

Gambar 63. Latihan 4

Dari percobaan tersebut:

- Dari PC4, Lakukan ping ke 192.168.0.8, jelaskan balasan pesan yang didapatkan
- Kirimkan paket data PC0→PC6. Dari simulasi yang dihasilkan, Bagaimana paket data yang dikirimkan?
- Potonglah kabel antara Switch1 dan Switch2 dengan menggunakan delete, kemudian jalankan lagi simulasinya, bagaimana paket data yang dikirimkan?
- Dari PC0, lakukan ping ke 192.168.0.10, jelaskan balasan pesannya!

2.5.5 Percobaan Kelima (latihan5.pkt)

- Buatlah 2 buah jaringan wireless sederhana (WLAN) menggunakan 6 buah PC, 2 buah Access Point-PT dengan ketentuan berikut:

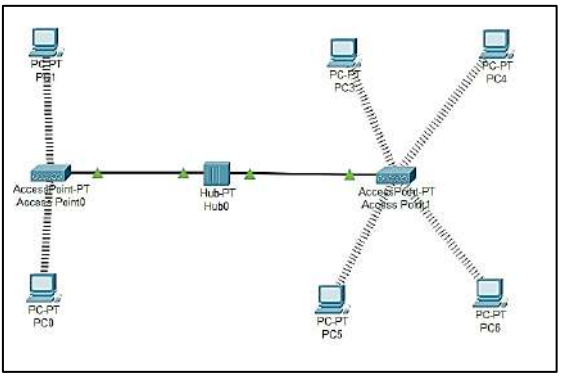
Nama PC	**IP Address**	**Subnet Mask**
PC0	192.168.0.2	255.255.255.0
PC1	192.168.0.3	255.255.255.0
PC2	192.168.0.4	255.255.255.0
PC3	192.168.0.5	255.255.255.0
PC4	192.168.0.6	255.255.255.0
PC5	192.168.0.7	255.255.255.0

- Konfigurasi access point 0:
  - ✓ Duplex setting auto
  - ✓ Bandwidth setting auto
  - ✓ Channel 1
  - ✓ SSID dengan nama “Lab RPL”
  - ✓ Tanpa security
- Konfigurasi access point 1:
  - ✓ Duplex setting auto
  - ✓ Bandwidth setting auto
  - ✓ Channel 11
  - ✓ SSID dengan nama “Lab Komdas”

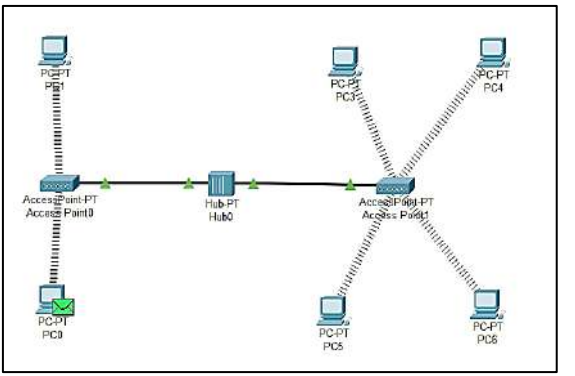
- ✓ Tanpa security

- Perangkat (Hub-PT) atau Modules pada hub0:
  - ✓ 6 PT-REPEATER-NM-1CFE

Gambar 64. Latihan 5



Realtime



Simulation

Gambar 65. Latihan 5

Dari percobaan tersebut:

- Dari PC0, Lakukan ping ke 192.168.0.3, jelaskan balasan pesan yang didapatkan
- Dari PC1, Lakukan ping ke 192.168.0.7, jelaskan balasan pesan yang didapatkan
- Dari PC3, Lakukan ping ke 192.168.0.10, jelaskan balasan pesan yang didapatkan
- Kirimkan paket data PC0→PC4. Dari Animasi yang dihasilkan, apakah paket data terkirimkan dengan baik? jelaskan

2.5.6 Percobaan Keenam (latihan6.pkt)

- Buatlah 2 buah jaringan wireless sederhana (WLAN) menggunakan 6 buah PC, 2 buah Access Point-PT dengan ketentuan berikut:

Nama PC	IP Address	Subnet Mask	Perangkat
PC0	192.168.0.2	255.255.255.0	WMP300N
PC1	192.168.0.3	255.255.255.0	WMP300N
PC2	192.168.0.4	255.255.255.0	WMP300N
PC3	192.168.0.5	255.255.255.0	WMP300N
PC4	192.168.0.6	255.255.255.0	PT-HOST-NM-1CFE
PC5	192.168.0.7	255.255.255.0	PT-HOST-NM-1CFE
PC6	192.168.0.8	255.255.255.0	PT-HOST-NM-1CFE
PC7	192.168.0.9	255.255.255.0	PT-HOST-NM-1CFE

- Konfigurasi access point 0:
  - ✓ Duplex setting auto
  - ✓ Bandwidth setting auto
  - ✓ Channel 1
  - ✓ SSID dengan nama “Lab RPL”
  - ✓ Tanpa security
- Konfigurasi access point 2:
  - ✓ Duplex setting auto

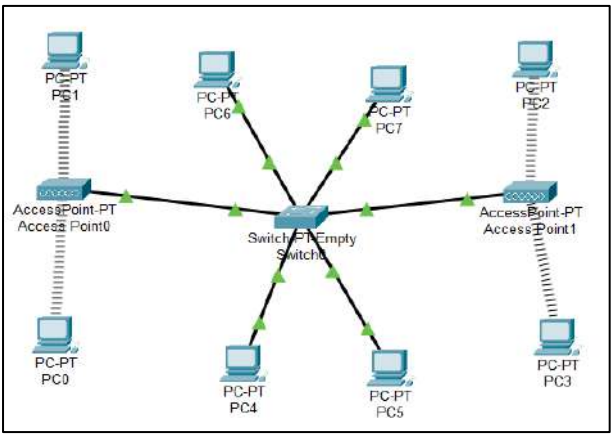
- ✓ Bandwidth setting auto
- ✓ Channel 11
- ✓ SSID dengan nama “Lab Komdas”
- ✓ Tanpa security

- Perangkat (Switch-PT-Empty) atau Modules pada switch 0:
  - ✓ 8 PT-SWITCH-NM-1CFE
  - ✓ 2 PT-SWITCH-COVER
- Konfigurasi Access point 0:
  - ✓ Duplex setting auto
  - ✓ Bandwidth setting auto
  - ✓ Channel 1
  - ✓ SSID dengan nama “Lab RPL”
  - ✓ Tanpa security
- Konfigurasi access point 1:
  - ✓ Duplex setting auto
  - ✓ Bandwidth setting auto
  - ✓ Channel 11
  - ✓ SSID dengan nama “Lab Komdas”
  - ✓ Tanpa security

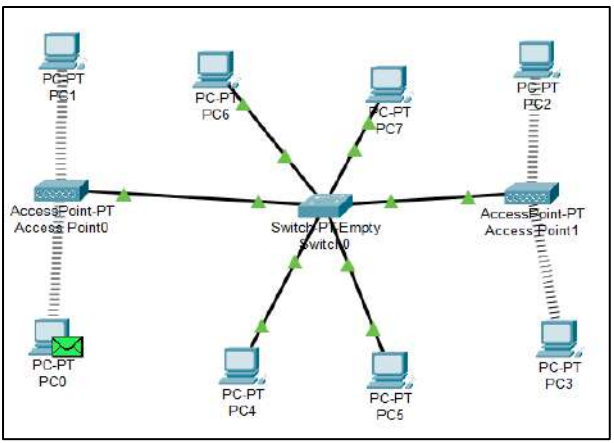
Gambar 66. Latihan 6

Dari percobaan tersebut**:**

- Dari PC2, Lakukan ping ke 192.168.0.2, jelaskan balasan pesan yang didapatkan
- Dari PC4, Lakukan ping ke 192.168.0.8, jelaskan balasan pesan yang didapatkan
- Dari PC5, Lakukan ping ke 192.168.0.1, jelaskan balasan pesan yang didapatkan
- Kirimkan paket data PC0→PC5. Dari Animasi yang dihasilkan, apakah paket data terkirimkan dengan baik? Jelaskan



Realtime



Simulation

Gambar 67. Latihan 6

BAB 3
Protocol Jaringan

Capaian Pembelajaran:

1. Mampu menjelaskan protocol jaringan OSI 7 *Layer*
2. Mampu menjelaskan protocol jaringan TCP 4 *Layer*
3. Mampu melakukan simulasi jaringan lalu lintas data melalui protocol

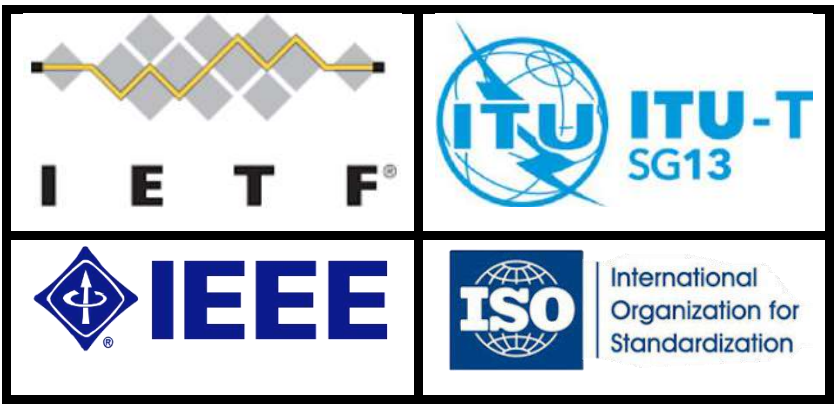
Pada bab ini membahas tentang *protocol* pada sebuah jaringan. *Protocol* dijabarkan meliputi protocol OSI 7 *Layer* dan TCP 4 *Layer*. Pada soal latihan memuat tentang simulasi jaringan lalu lintas data melalui *protocol* menggunakan *packet tracert*.

3.1 Standar *Protocol*

Standar suatu komunikasi diperlukan agar terdapat keseragaman, sehingga komunikasi memungkinkan untuk dilakukan. Dalam penetapan standarnya terdapat beberapa organisasi internasional yang mengatur. Berikut beberapa organisasi internasional yang berpengaruh:

- *Internet Engineering Task Force* (IETF)
  Merupakan sebuah organisasi yang menjaring banyak pihak dalam pengembangan jaringan komputer dan Internet. IETF merupakan pihak yang mempublikasikan spesifikasi yang membuat standar protokol TCP/IP
- *International Telecommunication Union Telecommunication Standarization Sector* (ITU-T)
  Standar internasional dibidang Telekomunikasi baik itu telepon dan data. Adapun standar yang terlahir yaitu JPEG (*Joint Photographic Expert Group*) merupakan standar kompresi file, MPEG (*Motion Picture Expert Group*) merupakan standar pengkodean layanan video, H.323 untuk pengembangan layanan VoIP, dan G.709 untuk mengimplementasikan penggunaan kabel fiber optik

- *Institute of Electrical and Electronics Engineers* (IEEE)
  IEEE adalah organisasi profesi yang membuat berbagai standar termasuk dalam bidang jaringan komunikasi data. Contohnya adalah IEEE 802.3 and IEEE 802.5 standar yang digunakan pada LAN
- *The International Organization for Standardization* (ISO)
  ISO adalah organisasi standarisasi internasional yang bertugas membuat standar dari berbagai bidang termasuk jaringan komunikasi data. Salah satu standar yang terkenal adalah model OSI (*Open System Interconnection*).



Gambar 68. Logo Organisasi Internasional

3.2 Arsitektur *Protocol*

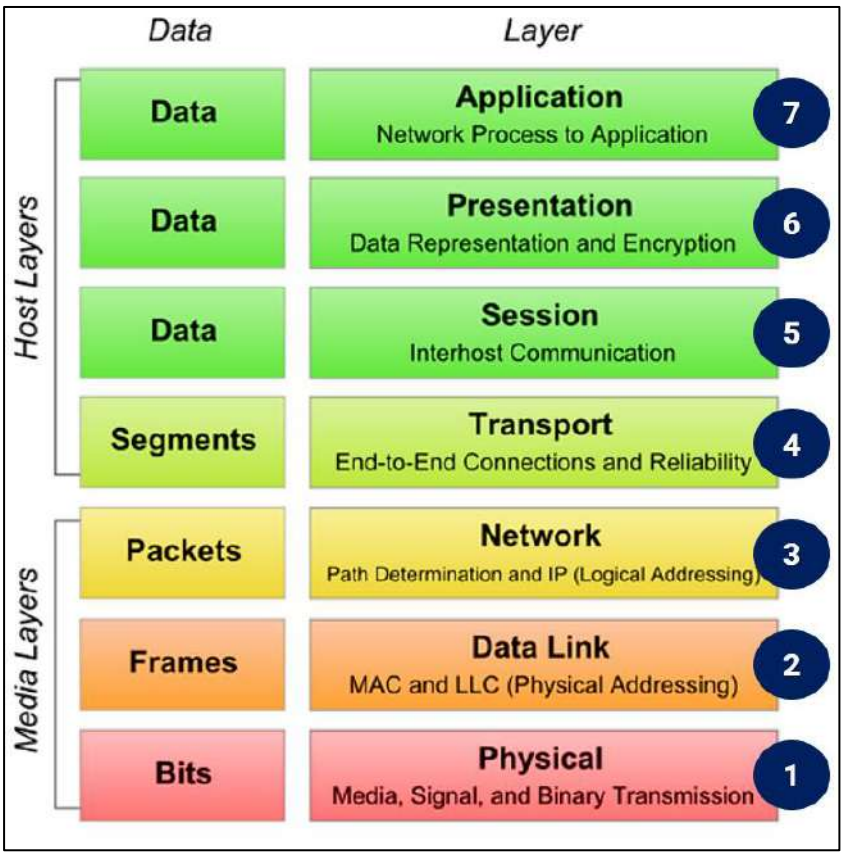
Diperlukan sebuah arsitektur terhadap protokol-protokol yang akan digunakan. Arsitektur protokol dapat diartikan sebagai struktur urutan dari *hardware* dan *sotfware* yang mendukung pertukaran data diantara sistem serta mendukung aplikasi terdistribusi. Berikut arsitektur protokol secara umum:

- Perangkat lunak dari jaringan komunikasi data
- Terdiri dari layer, protokol dan interface
  - ✓ Jaringan diorganisasikan menjadi sejumlah level (*layer*) untuk mengurangi kerumitannya
  - ✓ Setiap *layer* dibuat berdasarkan *layer* dibawahnya

- ✓ Antar layer terdapat sebuah *interface* yang menentukan operasi dan layanan yang diberikan *layer* terbawah untuk layer diatasnya
- ✓ Layer pada level yang sama di dua *host* yang berbeda dapat saling berkomunikasi dengan mengikuti sejumlah aturan dan ketetapan yang disebut sebagai protokol

3.3 OSI 7 *Layer*

OSI 7 *Layer* (*Open Source Interconnection*) merupakan standar protokol jaringan komunikasi data yang ditetapkan oleh OSI. Model referensi OSI adalah model komunikasi jaringan yang paling banyak digunakan oleh vendor (pembuat) sistem jaringan. Model OSI membantu melihat fungsi jaringan yang terjadi pada setiap *layer*.



Gambar 69. ISO 7 Layer

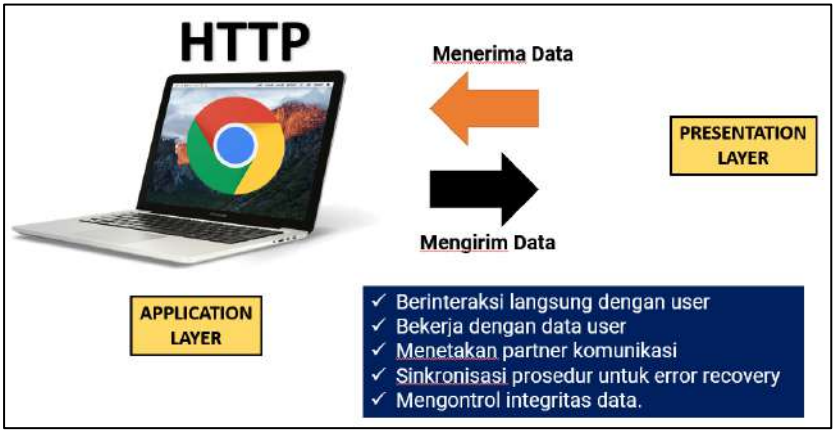
Tabel 1. Komponen *Network* dan *Protocol*

Layer	***Network***	***Protocol***
Application	✓ *Gateway*	✓ *DNS;* ✓ *FTP TFTP;* ✓ *BOOTP;* ✓ *SNMP; SMTP;* ✓ *RLOGIN* ✓ *MIME;* ✓ *NFS;* ✓ *FINGER TELNET;* ✓ *NCP APPC;* ✓ *AFP SMB*
Presentation	✓ *Gateway* ✓ *Redirector*	✓ Tidak Ada
Session	✓ *Gateway*	✓ *NetBIOS* ✓ *Names Pipes* ✓ *Mail Slots* ✓ *RPC*
Transport	✓ *Gateway* ✓ *Advanced Cable Tester* ✓ *Brouter*	✓ *TCP, ARP, RARP;* ✓ *SPX* ✓ *NWLink* ✓ *NetBIOS / NetBEUI* ✓ *ATP*
Network	✓ *Brouter* ✓ *Router* ✓ *Frame Relay Device* ✓ *ATM Switch* ✓ *Advanced Cable Tester*	✓ *IP; ARP; RARP, ICMP; RIP; OSFP;* ✓ *IGMP;* ✓ *IPX* ✓ *NWLink* ✓ *NetBEUI* ✓ *OSI* ✓ *DDP* ✓ *DECnet*
Datalink	✓ *Bridge,* ✓ *Switch* ✓ *ISDN Router*	✓ *Media Access Control (MAC)* ✓ *802.3 CSMA/CD (Ethernet)*

	✓ *Intelligent Hub* ✓ *NIC* ✓ *Advanced Cable Tester*	✓ *802.4 Token Bus (ARCnet)* ✓ *802.5 Token Ring* ✓ *802.12 Demand Priority* ✓ *Logical Link Control (LLC)* ✓ *802.2 Logical Link Control*
Physical	✓ *Repeater* ✓ *Multiplexer* ✓ *Hubs* (Pasif dan Aktif) ✓ *TDR* ✓ *Oscilloscope* ✓ *Amplifier*	✓ *IEEE 802 (Ethernet standard)* ✓ *IEEE 802.2 (Ethernet standard)* ✓ *ISO 2110* ✓ *ISDN*

3.3.1 *Application* Layer

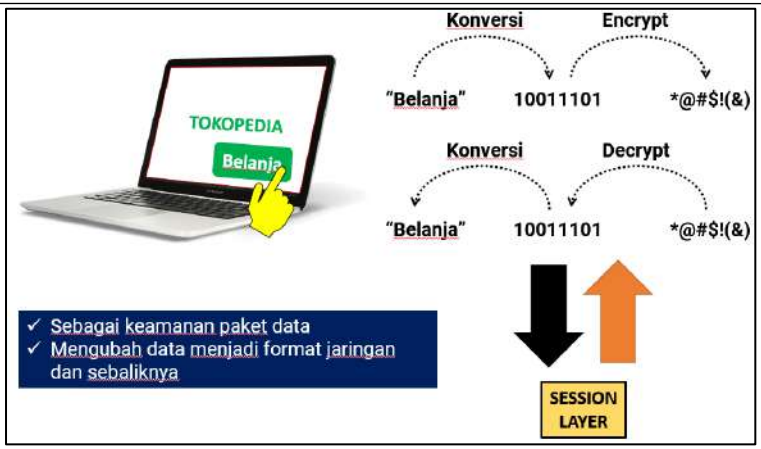
Application layer (Layer 7) menyediakan akses ke lingkungan OSI bagi user serta menyediakan layanan informasi terdistribusi.



Gambar 70. Application Layer

3.3.2 *Presentation* Layer

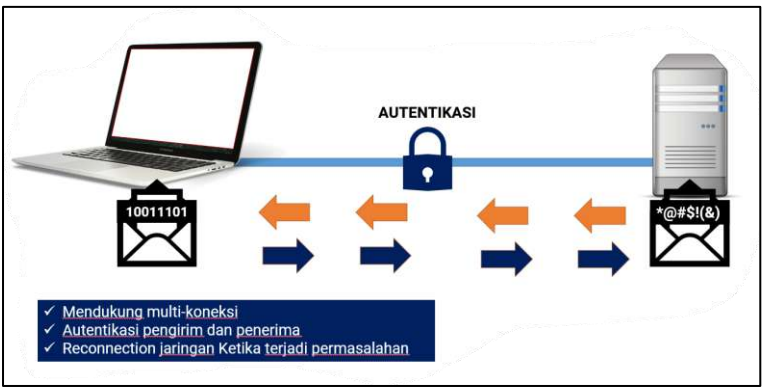
Presentation layer (Layer 6) menyediakan keleluasaan terhadap proses aplikasi untuk bermacam representasi data (*syntax*).



Gambar 71. *Presentation* Layer

3.3.3 *Session* Layer

Session layer (Layer 5) menyediakan struktur kontrol untuk komunikasi diantara aplikasi-aplikasi; menentukan, menyusun, mengatur, dan mengakhiri koneksi sesi diantara aplikasi-aplikasi yang sedang beroperasi.



Gambar 72. *Session* Layer

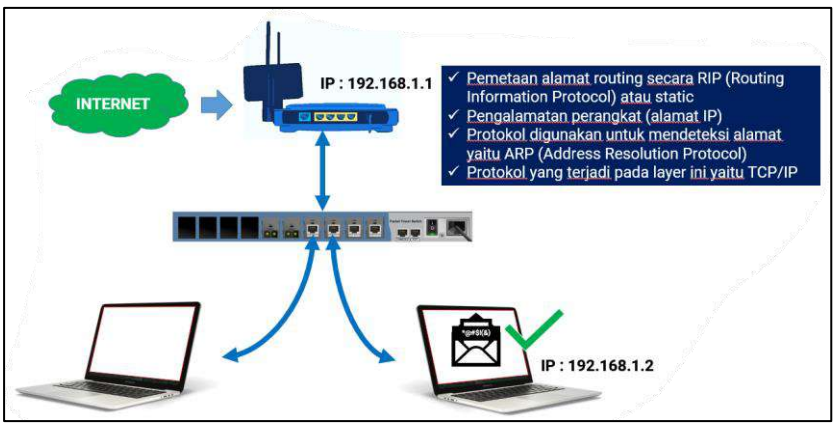
3.3.4 *Transport* Layer

Transport layer (Layer 4) menyediakan transfer data yang handal dan transparan diantara titik ujung; menyediakan perbaikan *end-to-end error* dan *flow control*.

Gambar 73. *Transport* Layer

3.3.5 *Network* Layer

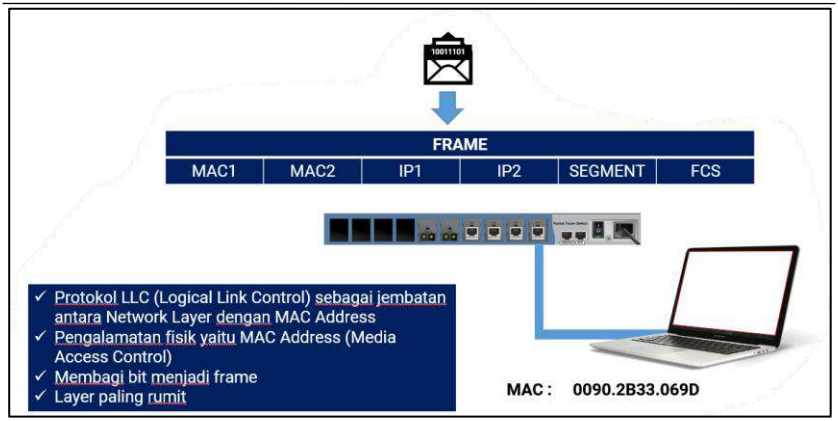
Network layer (Layer 3) melengkapi lapisan yang lebih tinggi dengan keleluasaan dan transmisi data dan teknologi-teknologi *switching* yang dipergunakan untuk menghubungkan sistem; bertugas menyusun, mempertahankan, serta megakhiri koneksi.



Gambar 74. *Network* Layer

3.3.6 *Data Link* Layer

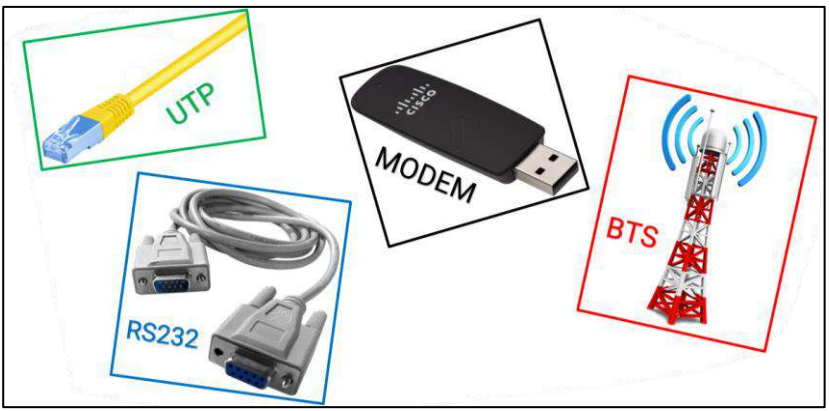
Data link layer (Layer 2) menyediakan transfer informasi yang reliabel melewati link fisik; mengirim blok (*frame* dengan sinkronisasi yang diperlukan, kontrol *error*, dan *flow control*.



Gambar 75. *Data Link* Layer

3.3.7 *Physical* Layer

Physical layer (Layer 1) berkaitan dengan transmisi bit stream yang tidak terstruktur sepanjang media *physical* (*Physical* Medium), berhubungan dengan karakteristik prosedural, fungsi, elektris, dan mekanis untuk mengakses media fisikal.

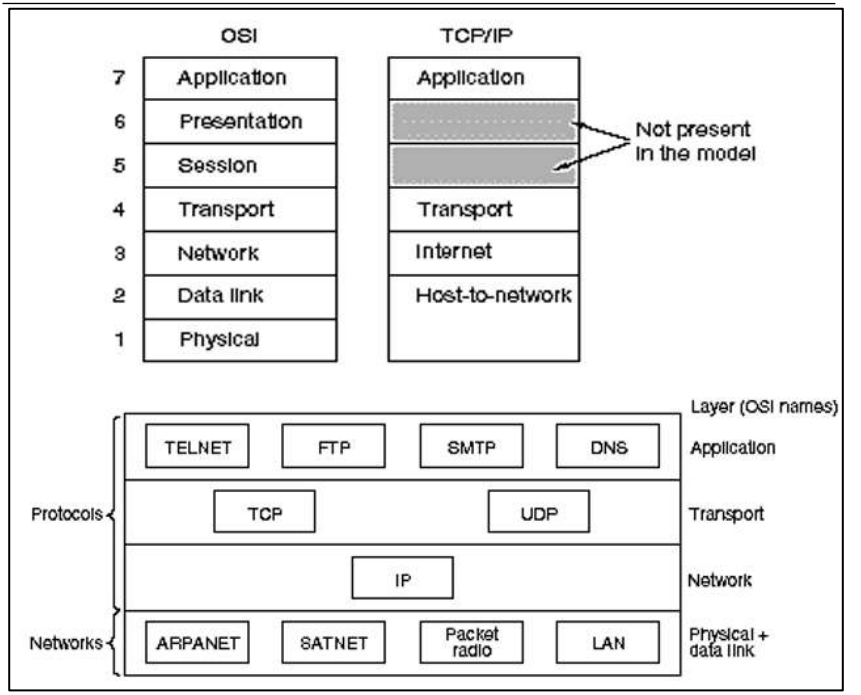


Gambar 76. *Physical* Layer

3.4 TCP 4 *Layer*

Meski model referensi OSI lebih umum digunakan tapi secara teknis dan historis, model referensi standar internet adalah *Transmission Control Protocol/Internet Protocol* (TCP/IP). Model ini memiliki 4 layer:

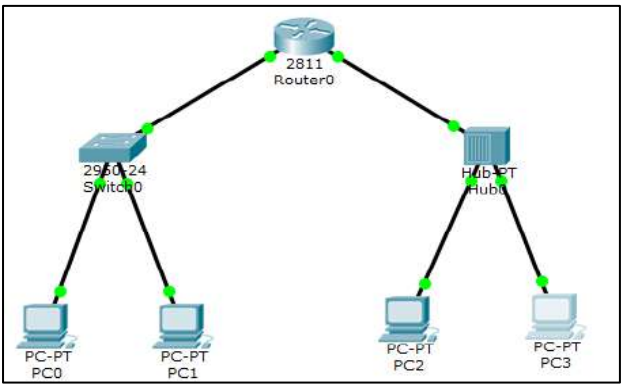
1. *Application layer* (*layer* 4) model TCP/IP berkutat dengan urusan presentasi, *encoding*, dan *dialog control*. TCP/IP mengkombinasikan *session*, *presentation* dan *application* dalam satu *layer* dan mengasumsikan data telah siap dienkapsulasi pada layer berikutnya.
2. *Transport layer* (*layer* 3 TCP/IP) berkutat dengan urusan *quality of service* dari *reliability*, *flow control* dan *error corection*. Salah satu dari protokolnya, *transmission control protocol* (TCP), menyediakan cara yang fleksibel dan sempurna untuk komunikasi jaringan yang *reliable*, *well-flowing*, *low-error*. TCP berdialog antara pengirim dan penerima ketika melakukan enkapsulasi data ke dalam segment. TCP adalah protokol *connection-oriented*, artinya segment bergerak bolak balik antara dua *host* untuk memberitahukan bahwa koneksi terjadi selama waktu tertentu (*packet switching*).
3. *Internet* layer (*layer* 2 TCP/IP) berfungsi mengirim paket antara jaringan yang berbeda dan menentukan lintasan yang ditempuh. Protokol spesifik layer ini adalah *Internet protocol* (IP). Jalan terbaik tekad dan packet *switching* terjadi pada lapisan ini. Pikirkan hal ini dalam hal sistem pos. Bila seseorang mengirim surat, tentunya orang tersebut tidak tahu bagaimana sampai disana (ada rute berbagai kemungkinan).
4. *Network* layer (*layer* 1 TCP/IP) juga disebut layer *host-to-network*. *Layer* ini menyediakan segala sesuatu yang dibutuhkan paket data untuk membuat sambungan langsung (*physical link*) termasuk detil teknologi LAN dan WAN dan seluruh detil dalam *Physical* dan *Data link layer* (*Layer* 1 dan *layer* 2 OSI).



Gambar 77. TCP 4 *Layer*

3.5 Latihan Simulasi Jaringan Lalu Lintas Data melalui *Protocol*

Buat jaringan dengan topologi star menggunakan *switch* dan hub serta hubungkan antar *switch* dan hub tersebut menggunakan *router*. Gunakan *router* seri 2811. Pada *Router*, hubungkan port FastEthernet0/0 ke *Switch* dan FastEthernet0/1 ke Hub.



Gambar 78. Latihan 1

Setting *IP address* PC sebagai berikut:

- PC0:
  - ✓ IP Address 192.168.1.2,
  - ✓ Subnet Mask 255.255.255.0,
  - ✓ Default Gateway 192.168.1.1.
- PC1:
  - ✓ IP Address 192.168.1.3,
  - ✓ Subnet Mask 255.255.255.0,
  - ✓ Default Gateway 192.168.1.1.
- PC2:
  - ✓ IP Address 192.168.2.2,
  - ✓ Subnet Mask 255.255.255.0,
  - ✓ Default Gateway 192.168.2.1.
- PC3:
  - ✓ IP Address 192.168.2.3,
  - ✓ Subnet Mask 255.255.255.0,
  - ✓ Default Gateway 192.168.2.1.

Pada Router setiap port yang terhubung harus dikonfigurasi IP Address nya. Berikut konfigurasi pada router:

- FastEthernet0/0:
  - ✓ IP Address 192.168.1.1,
  - ✓ Subnet Mask 255.255.255.0
- FastEthernet0/1:
  - ✓ IP Address 192.168.2.1,
  - ✓ Subnet Mask 255.255.255.0

Dari percobaan tersebut:

- Lakukan simulasi dengan filter ARP dan ICMP. Pada Command Prompt PC0 ketik perintah “arp -a” (seharusnya muncul tulisan “No ARP Entries Found”, jika tidak ketik perintah “arp -d”). Kemudian lakukan ping dari PC0 ke PC1, amati paket yang keluar dari PC0. Setelah selesai ketik kembali “arp -a”. Lakukan ping kembali dari PC0 ke PC1, amati perbedaan paket yang keluar dari PC0.

- Jelaskan fungsi dari perintah ARP?
- Jelaskan perintah arp -a?
- Kenapa pada saat ping pertama muncul paket ARP diawal, sedangkan pada saat ping kedua tidak muncul paket ARP?

- Lakukan simulasi dengan filter ICMP. Lakukan ping dari PC0 ke PC1. Kemudian lakukan ping dari PC2 ke PC3, amati perbedaan aliran datanya. Bagaimanakah perbedaan Switch dan Hub dalam menangani paket?
- Jika PC1 diganti IP Address nya menjadi 192.168.3.2, Bisakah PC0 terhubung ke PC1 (tes dengan perintah ping)? Kenapa?
- Jika IP Address pada port FastEthernet0/0 di router diganti dengan 192.168.1.5 bisakah PC0 terhubung ke PC3 (tes dengan perintah ping)? Jika tidak, apa yang harus diubah agar PC0 terhubung ke PC3 (tanpa mengubah lagi IP Address pada port router).
- Jika IP Address pada port FastEthernet0/1 di router diganti dengan 192.168.3.1 bisakah PC3 terhubung ke PC0 (tes dengan perintah ping)? Jika tidak, apa yang harus diubah agar PC3 terhubung ke PC0 (tanpa mengubah lagi IP Address pada port router).

BAB 4
Jaringan Lokal *Ethernet*

Capaian Pembelajaran:

1. Mampu melakukan implementasi jaringan lokal *ethernet*
2. Mampu melakukan konfigurasi jaringan lokal *ethernet*

Pada bab ini membahas tentang implementasi jaringan lokal *ethernet* dan konfigurasinya. Implementasi jaringan lokal *ethernet* yang dijabarkan meliputi perakitan kabel UTP dan pengujian, teori jenis kabel beserta alat pendukung perakitan. Kemudian untuk konfigurasi jaringan lokal *ethernet* dijabarkan meliputi konfigurasi *firewall*, konfigurasi IP *Address* dan *subnetmask*, pengecekan paket data melalui terminal, dan konfigurasi data *sharing*.

4.1 Jenis Kabel

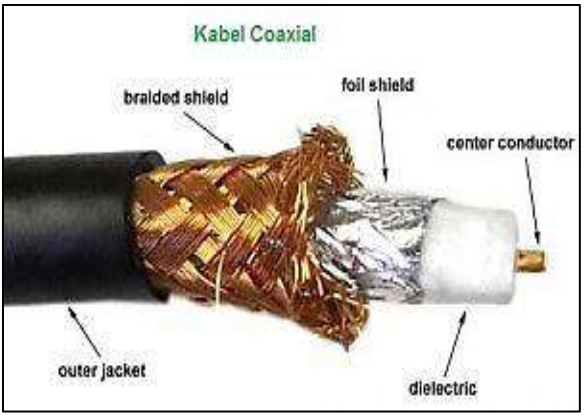
Media transmisi adalah media yang menghubungkan antara pengiriman dan penerima data. Oleh karena jaraknya yang jauh, maka data terlebih dahulu diubah menjadi kode-kode, dan kode inilah yang akan dimanipulasi dengan berbagai macam cara untuk diubah kembali menjadi data. Jenis media transmisi ada dua, yaitu *Guided* dan *Unguided*. *Guided transmission* media atau media transmisi terpadu merupakan jaringan yang menggunakan sistem kabel. *Unguided transmission* media atau media transmisi tidak terpadu merupakan jaringan yang menggunakan sistem gelombang.

4.1.1 *Guided* Media (Media dengan Kabel)

Guided media menyediakan jalur transmisi sinyal yang terbatas secara fisik, meliputi *twisted-pair cable*, *coaxial cable* (kabel koaksial) dan *fiber-optic cable*. Sinyal yang melewati media-media tersebut diarahkan dan dibatasi oleh batas fisik media.

- Kabel Coaxial

  Biasanya, digunakan pada jenis jaringan yang memilki topologi jaringan bus dan juga topologi ring. Kabel coaxial merupakan jenis kabel yang terdiri dari kawat tembaga, yang dilapisi oleh isolator, konduktor, dan kemudian pada bagian luar dari kabel coaxial ini dilindungi dengan menggunakan bahan PVC.



Gambar 79. Kabel Coaxial

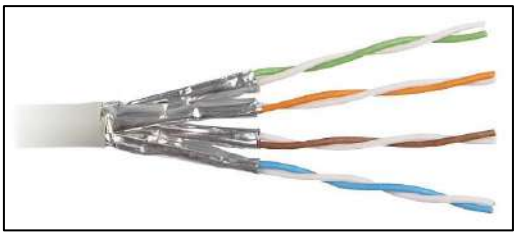
- Kabel UTP (*Unshielded Twisted Pair*)

  Kabel UTP dalam aplikasinya tidak mendukung sebuah perlindungan atau proteksi dari kumpulan spiralnya. Karena tidak memilki perlindungan apapun pada bagian kabelnya, maka kabel jenis UTP ini memiliki kelemahan utama, yaitu sangat rentan dan juga sensitif terhadap voltase tinggi dan juga medan magnet. Kabel UTP banyak digunakan pada kabel jaringan telepon, dan juga jaringan LAN kecil.

Gambar 80. Kabel UTP

- Kabel FTP (*Foiled Twisted Pair*)

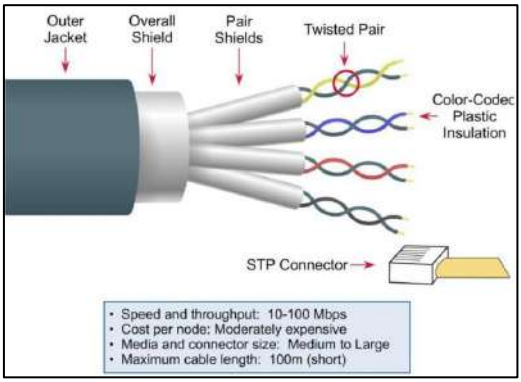
  FTP memiliki spesifikasi yang lebih baik dibandingkan dengan kabel UTP, karena lapisan kabelnya dilindungi oleh semacam foil kabel jenis FTP memiliiki ketahanan yang lebih baik terhadap noise dan gangguan magnetic dibandingkan dengan kabel UTP



Gambar 81. Kabel FTP

- Kabel STP (*Shielded Twisted Pair*)

  Hampir sama dengan kabel FTP, kabel STP juga memiliki perlindungan di dalam lapisan kabelnya. Yang membedakan hanyalah bahan yang digunakan untuk melapisi susunan kabel twisted pairnya. STP juga memiliki kemampuan yang baik dalam menangkal noise dan gangguan magnetic.

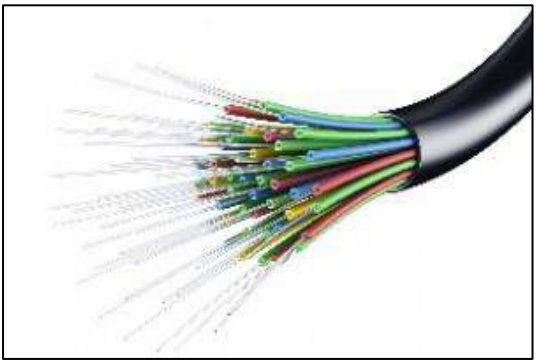


Gambar 82. Kabel STP

- Fiber Optik

  Kabel fiber optic ini merupakan jenis kabel yang terdiri atas kumpulan serat – serat fiber, dengan ukuran yang lebih kecil dan

juga lebih fleksibel dibandingkan dengan kabel twisted pair. Mampu mentransmisikan sinyal dengan kecepatan tinggi Dapat mentransmisikan sinyal cahaya Tahan terhadap gelombang radio.



Gambar 83. Kabel Fiber Optik

4.1.2 *Unguided* Media (Tanpa Kabel)

Unguided Media merupakan jaringan yang menggunakan sistem gelombang. Pada unguided media, disediakan alat untuk mentransmisikan data namun tidak mengendalikannya, yang termasuk *unguided transmission* media diantaranyanya: inframerah, *Bluetooth*, dan Wi-fi.

- Inframerah

  Inframerah merupakah radiasi elektromagnetik yang memiliki panjang gelombang antara 700 nanometer (frekuensi 430 THz) hingga 1 milimeter (frekuensi 300 GHz). Gelombang ini dapat digunakan sebagai media transmisi jarak dekat. Inframerah terbagi menjadi 3 jenis berdasarkan ISO 20473, yaitu inframerah jarak dekat dengan panjang gelombang 0.78 hingga 3 μm, inframerah jarak menengah dengan panjang gelombang 3 hingga 50 μm, dan inframerah jarak jauh dengan panjang gelombang 50 hingga 1000 μm.

- *Bluetooth*

  Biuetooth merupakan salah satu standar teknologi nirkabel untuk jarak dekat yang digunakan sebagai media transmisi dalam

pertukaran data antara perangkat menggunakan gelombang radio UHF pada ISM bands dari 2.402 GHz hingga 2.48 GHz, dan membentuk jaringan lokal skala pribadi atau dikenal dengan istilah *personal area network* (PAN). Untuk standar organisasi ditetapkan oleh IEEE saat ini dan belum ada pembaharuan yaitu 802.15.1.

- Wi-Fi

  Wi-Fi termasuk dalam protokol jaringan nirkabel berbasis IEEE 802.11. Jaringan ini seringkali dipakai jaringan lokal rumahan / kantoran untuk mengakses internet, sehingga bisa bertukar data antar perangkat menggunakan gelombang radio. Wi-Fi merupakan merek dagang non-profit dari Wi-Fi Alliance.

4.2 Alat Pendukung Perakitan Kabel *Twisted Pair*

Sebelum melakukan perakitan kabel jaringan twisted pair, sebaiknya menyiapkan alat pendukungnya terlebih dahulu. Berikut alat pendukung perakitan kabel *twisted pair*:

1) Kabel *Tester*

   Kabel *tester* digunakan untuk mengetahui apakah kabel telah berhasil disambungkan. Sebagai alat yang mendeteksi terputus atau tidaknya kabel yang digunakan pada jaringan.

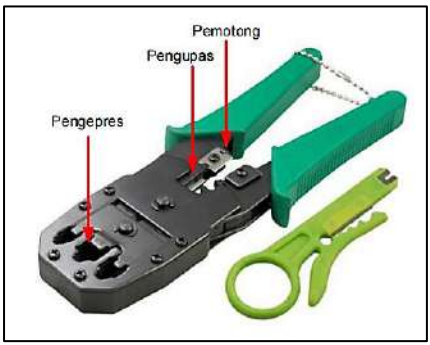
Gambar 84. Kabel *Tester*

2) Tang *Crimper*

   Tang *Crimper* merupakan alat yang mempunyai berbagai fungsi untuk keperluan pemasangan kabel jaringan. Alat ini biasanya mempunyai tiga bagian yaitu:

   ✓ *Cutter* atau pemotong

- ✓ *Nipper* atau pengupas
- ✓ *Crimpe* atau pengepres/penjepit



Gambar 85. Tang *Crimper*

3) Wire Strippers

Wire Strippers digunakan untuk mengupas selimut kabel dan menyisakan urat kabelnya saja, namun penggunaan yang tidak berhati-hati dapat membuat luka pada urat kabel, sehingga menyebabkan *noise* saat instalasi selesai.

Gambar 86. *Wire Stripper*

4) Wire Cutter

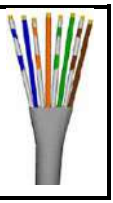
Wire Cutter digunakan untuk memotong kabel tembaga dan menghasilkan potongan yang rapi dan tidak menyebabkan luka pada kabel.

Gambar 87. *Wire Cutter*

4.3 Susunan Warna Kabel *Twisted Pair*

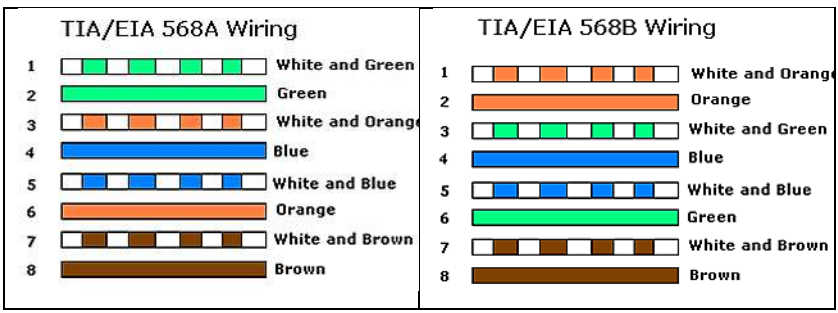
Kabel *Twisted Pair* (TP) atau yang biasa disebut sebagai kabel LAN, merupakan kabel yang digunakan untuk membangun jaringan LAN. Kabel ini mempunyai dua jenis yaitu STP (*Shielded Twisted Pair*) dan UTP (*Unshielded Twisted Pair*). Perbedaan kedua jenis kabel tersebut hanya pada pelindung (*Shielded*) yang berupa alumunium foil yang melindungi serat kabelnya dari gangguan gelombang elektromagnetik dari luar ataupun dari pasangan kabel lainnya.

Kabel TP mempunyai 4 pasang serat kabel di dalamnya, dan masing-masing pasang dibedakan berdasarkan warna kabel. Pasangan kabelnya yaitu pasangan kabel warna Oranye, Hijau, Biru dan Cokelat. Kabel Oranye berpasangan atau berlilitan (*Twisted*) dengan kabel warna belang Putih-Oranye, begitu pula dengan kabel Hijau, berpasangan dengan kabel warna belang Putih-Hijau.

Pasangan 1	Biru & Biru-Putih	
Pasangan 2	Oranye & Oranye-Putih	
Pasangan 3	Hijau & Hijau-Putih	
Pasangan 4	Coklat & Coklat-Putih	

Gambar 88. Kabel TP Susunan Kabel

Untuk pemasangan kabel ada dua jenis urutan warna yang umum digunakan yaitu 568A dan 568B. Standar urutan warna ini selain bertujuan untuk memudahkan teknisi juga untuk menghindari terjadinya crosstalk. Berikut urutan warna pemasangan kabel TP.



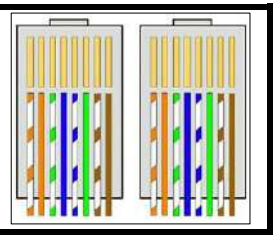
Gambar 89. Standar Urutan Kabel

Ada dua jenis pemasangan kabel TP yang umum digunakan, ditambah satu jenis pemasangan khusus untuk cisco router, yaitu: *Straight Through Cable*, *Cross Over Cable*, dan *Roll Over Cable*.

1) *Straight Through Cable*

Digunakan untuk menghubungkan beberapa unit komputer melalui perantara HUB/Switch, yang berfungsi sebagai konsetrator maupun repeater (*PC/Router to Hub/Switch*). Untuk membuat kabel Straight, susunan warna dikedua ujung kabel sama, yaitu menggunakan susunan 568B. Berikut gambar sambungan kabel Straight.

Ujung A		Ujung B	
OP	TX+	OP	TX+
O	TX-	O	TX-
HP	RX+	HP	RX+
B	Voice	B	Voice
BP	Voice	BP	Voice
H	RX-	H	RX-
CP	PoE	CP	PoE
C	PoE	C	PoE

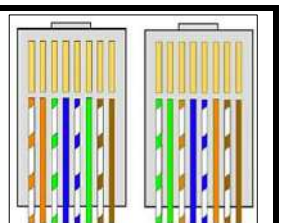


Gambar 90. Susunan *Straight Through*

2) *Cross Over Cable*

Kabel *Cross Over* digunakan untuk menghubungkan PC ke PC atau Hub/Switch ke Hub/Switch. Untuk membuat kabel Cross, ujung satu menggunakan urutan 568B dan ujung satunya menggunakan urutan 568A. Kabel Cross akan menghubungkan pin 1 ke pin 3 dan pin 2 ke pin 6. Untuk lebih jelasnya dapat melihat gambar berikut.

Ujung A		Ujung B	
OP	TX+	HP	TX+
O	TX-	H	TX-
HP	RX+	OP	RX+
B	Voice	B	Voice
BP	Voice	BP	Voice
H	RX-	O	RX-
CP	PoE	CP	PoE
C	PoE	C	PoE

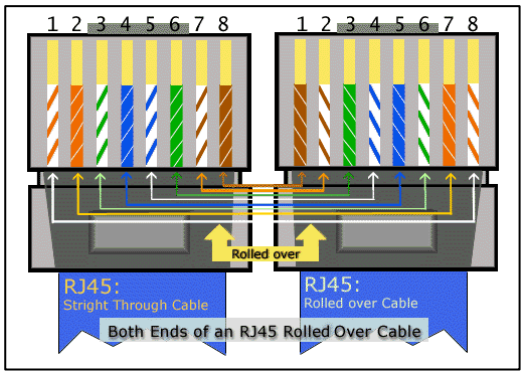


Gambar 91. Susunan *Cross Over*

3) *Roll Over Cable*

Roll Over Cable digunakan untuk menghubungkan terminal komputer ke port console router untuk keperluan konfigurasi router.

Untuk melakukan konfigurasi router cisco, port console pada router akan dihubungkan ke port serial atau USB pada komputer. Urutan kabel Roll over dan gambar kabel *console* dapat dilihat pada gambar berikut.

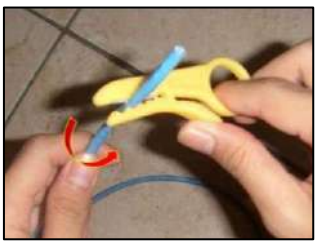


Gambar 92. Susunan *Roll Over*

4.4 Perakitan Kabel UTP dan Pengujian

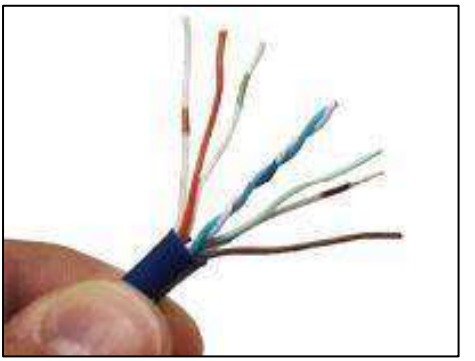
Langkah yang dilakukan untuk memasang konektor RJ-45 pada kabel UTP/STP yaitu:

1) Kupas pelindung luar dari kabel, sehingga terlihat 8 serat kabel. Untuk mengupas kabel dapat memanfaatkan alat bantu pengupas kabel, atau dengan menggunakan tang krimping. Umumnya pada tang crimping terdapat lekukan setengah lingkaran seukuran kabel, disertai dengan pisau. Ketika kabel diletakan pada tempat tersebut, rapatkan tang sehingga pisau menggores luaran kabel, putar kabel atau tang nya sehingga membuat goresan di sekeliling kabel.



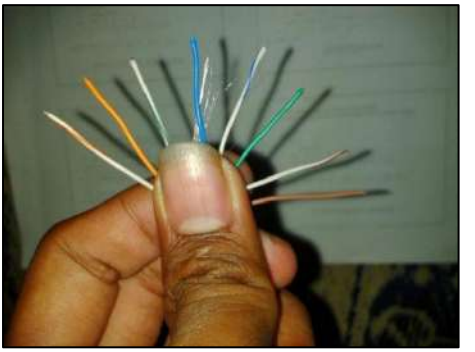
Gambar 93. Pengupasan Kabel dengan *Stripper*

Gambar 94. Pengupasan Kabel dengan *Crimper*



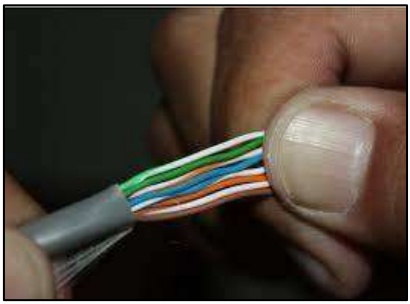
Gambar 95. Hasil Kupasan Kabel UTP

2) Setelah pelindung luar kabel dikupas, kemudian urutkan serat kabel berdasarkan urutan warna yang diinginkan. Untuk mempermudah, urutkan dari kiri ke kanan (pin 1 di kiri).



Gambar 96. Cara Memegang Serat Kabel

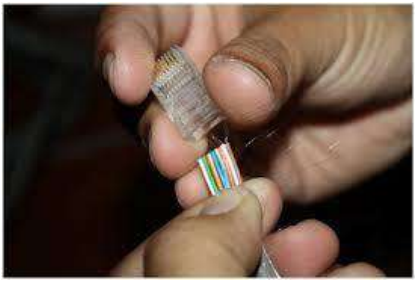
3) Setelah diurutkan, rapatkan seluruh kabel dan rapikan agar tidak bergelombang. Kemudian potong ujung kabel menggunakan tang krimping dengan panjang yang sesuai dengan konektor.



Gambar 97. Hasil Penyusunan Serat Kabel

Gambar 98. Pemotongan Serat Kabel dengan *Crimper*

4) Setelah memotong ujung kabel, tetap pegang kabelnya dan kemudian langsung masukkan ke dalam konektor. Posisi memasukkan konektor yaitu pin konektor yang berwarna kuning menghadap keatas.

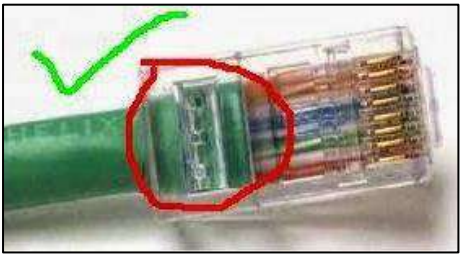


Gambar 99. Pemasangan Konektor

5) Masukkan kabel hingga setiap serat kabel benar-benar berada dibawah pin, atau sampai ujung konektor. Setelah dipastikan setiap serat kabel sampai menyentuh ujung konektor, lakukan krimping yaitu dengan meletakkan konektor yang telah terpasang kabel pada tang krimping kemudian tekan tang dengan kuat.

Gambar 100. Proses *Crimping*

6) Hasil krimping yang baik, kulit kabel masuk kedalam konektor, sehingga konektor akan mengunci kabel dengan kuat. Pemasangan konektor yang buruk akan menyebabkan serat kabel mudah terlepas dari konektor. Selain itu juga dapat menyebabkan adanya interferensi listrik dari luar yang dapat mengganggu transfer data dikarenakan adanya bagian serat yang tidak terlindung oleh kulit kabel (terutama pada kabel STP yang kulit kabelnya dilapisi lagi oleh alumunium).



Gambar 101. Hasil *Crimping* yang Bagus

Gambar 102. Hasil *Crimping* yang Jelek

7) Setelah selesai dipasang, lakukan tes kabel menggunakan kabel tester. Pengetesan dilakukan untuk memastikan setiap pin terhubung (terutama pin 1,2,3 dan 6) serta urutan kabel sudah benar.

Gambar 103. Penggunaan *Tester*

8) Lampu *tester* akan menyala berurutan, jika ada lampu yang tidak menyala berarti kabel tidak tersambung atau konektor tidak terpasang dengan benar. Untuk mengatasi ini, jangan langsung memutus kabel (memasang ulang konektor) tetapi tekan kembali konektor menggunakan tang krimping dengan kuat. Sebagian kasus terjadi karena kurang kuat pada saat menekan tang krimping.
9) Konektor sekali dilakukan krimping tidak dapat digunakan lagi. Jika salah memasang kabel atau posisi serat kabel tidak pas berada dibawah pin akan menyebabkan pin tidak terhubung. Untuk mengatasi masalah ini, harus dilakukan krimping ulang dengan konektor yang baru. Potong kabel dibawah konektor yang dirasa bermasalah, kemudian lakukan krimping ulang.

4.4 Konfigurasi Jaringan dan Pengecekan Paket Data

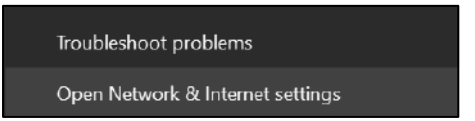
Langkah-langkahnya:

1) setting IP ADDRESS (IPV4)

a. klik kanan pada logo jaringan

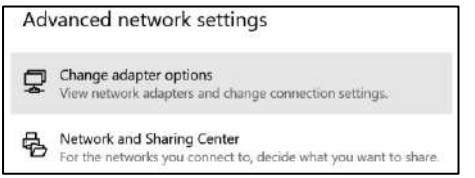
Gambar 104. Langkah 1

b. open *network & internet settings*



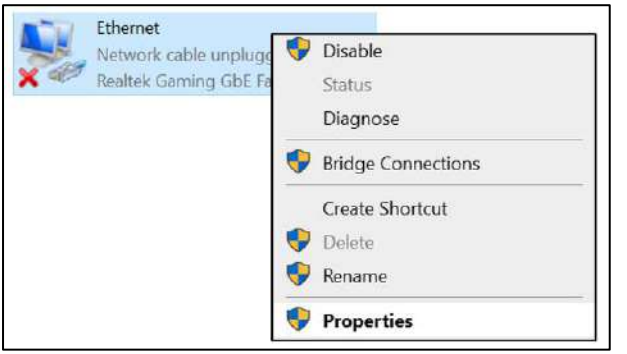
Gambar 105. Langkah 2

c. klik *change adapter options*



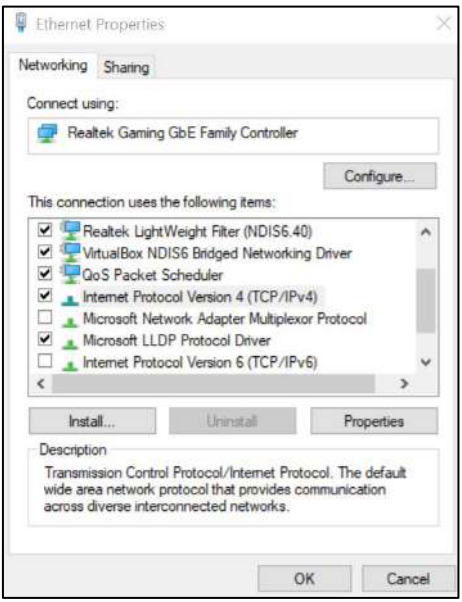
Gambar 106. Langkah 3

d. klik kanan *ethernet* masing-masing, pilih properties



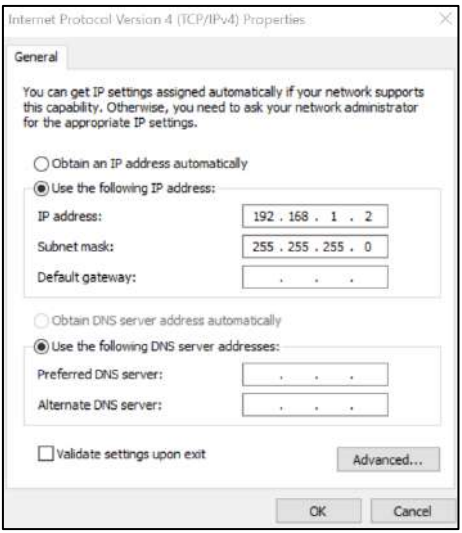
Gambar 107. Langkah 4

e. pilih IPV4, kemudian klik properties



Gambar 108. Langkah 5

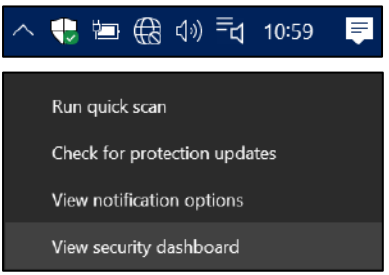
f. masukkan *ip address* dan *subnetmask*, dan klik ok sampai tuntas



Gambar 109. Langkah 6

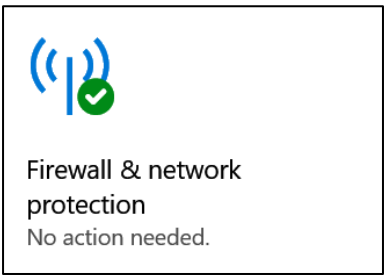
2) Mematikan *firewall public* sementara

a. Klik logo perisai, kemudian pilih *view security dashboard*



Gambar 110. Langkah 7

b. Klik *firewall and network protection*

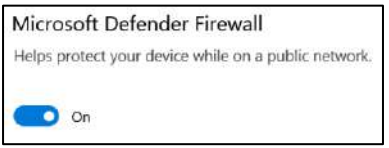


Gambar 111. Langkah 8

c. Kemudian pilih *public network*

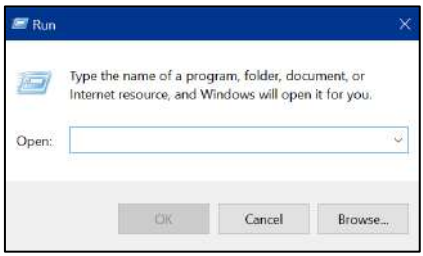
Gambar 112. Langkah 9

d. Kemudian geser *slider* ke *off* dengan cara di klik



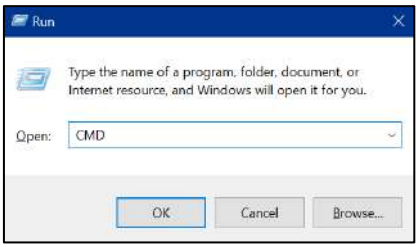
Gambar 113. Langkah 10

3) Membuka terminal atau command prompt
   a. bagi *windows*, tekan tombol *windows* + R



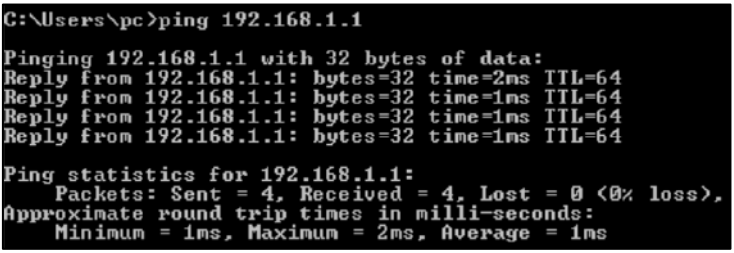
Gambar 114. Langkah 11

   b. ketikkan cmd



Gambar 115. Langkah 12

4) perintah terminal
   a. ketikkan *ipconfig* untuk mengetahui *ip address* masing-masing
   b. lakukan perintah *ping ip address* selain komputer sendiri



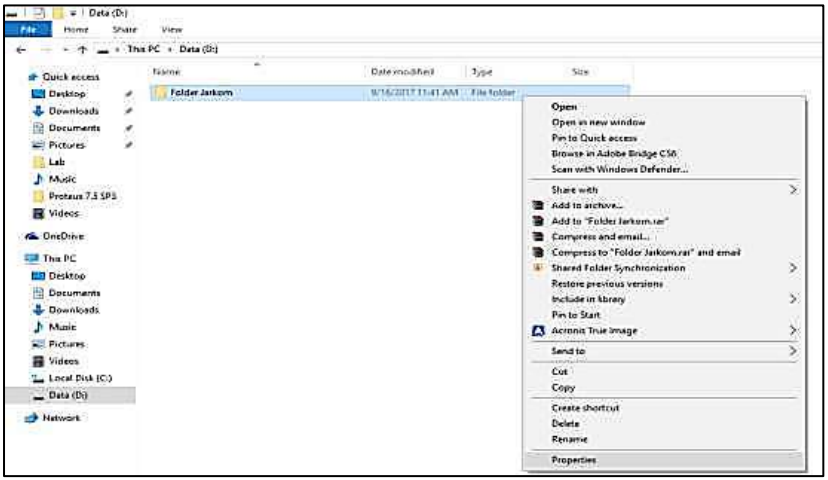
Gambar 116. Langkah 14

4.7 Data *Sharing*

Sharing resources bertujuan agar seluruh program, peralatan atau peripheral lainnya dapat dimanfaatkan oleh setiap orang yang ada pada

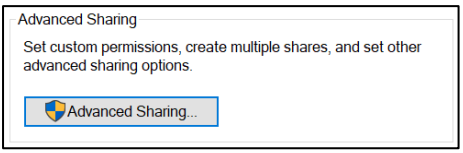
jaringan komputer tersebut tanpa terpengaruh oleh lokasi maupun pengaruh dari pemakai lainnya. Syarat yang harus dipenuhi dalam *sharing resource* atau file adalah IP Address. IP Address ini berfungsi sebagai penghubung antara PC yang memberikan *resource/file* dan PC yang menerima *resource/file* tersebut. Langkah langkah Sharing *resource/file* pada PC yang menggunakan Sistem Operasi windows sebagai berikut:

1) Pilih folder / file yang ingin dishare, Klik kanan dan masuk ke properties



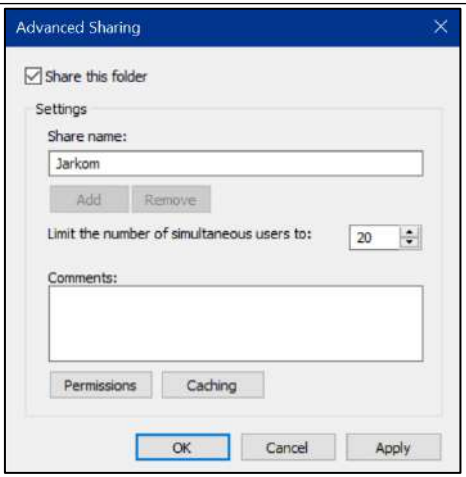
Gambar 117. *Data Sharing* 1

2) Klik tab *sharing*, dan pilih *Advance Sharing*



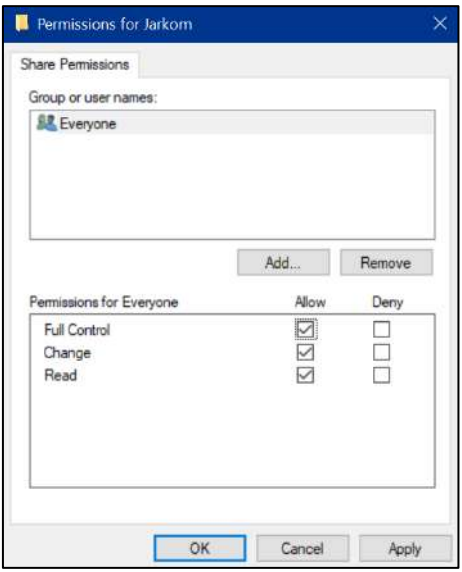
Gambar 118. *Data Sharing* 2

3) Masuk ke *Advance Sharing* dan centang pada kolom *Share This Folder*



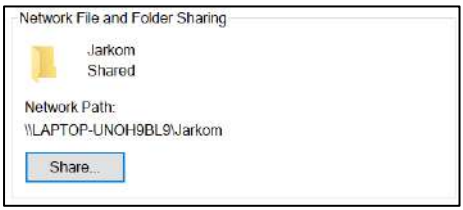
Gambar 119. *Data Sharing* 3

4) Untuk Mengatur apa saja yang client boleh lakukan terhadap file yang disharing, masuk ke Permission, dan centang pada *ALLOW* untuk semua perintah yang ada, lalu *APPLY*.

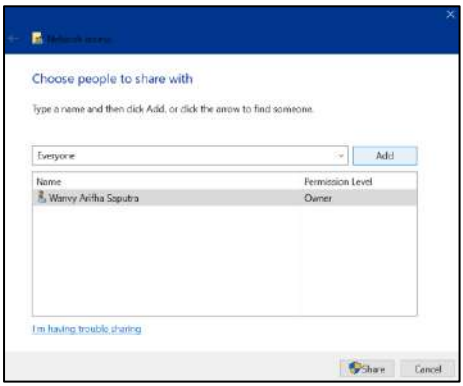


Gambar 120. *Data Sharing* 4

5) Kita juga bisa memilih kepada siapa saja kita bisa membagikan file kita dengan cara klik SHARE → Everyone lalu klik add → SHARE.

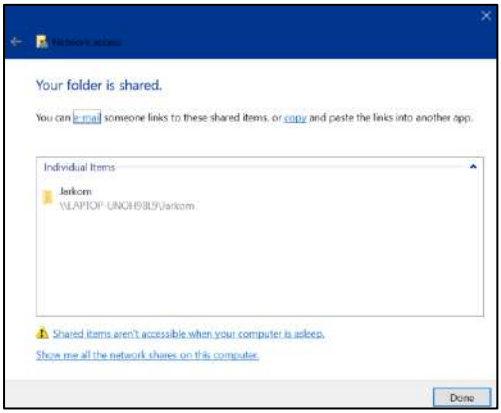


Gambar 121. *Data Sharing* 5



Gambar 122. *Data Sharing* 6

6) Setelah selesai, akan muncul pemberitahuan bahwa file kita sudah bisa share, lalu Klik *DONE*.



Gambar 123. *Data Sharing* 7

BAB 5
VLAN, CIDR, dan VLSM

Capaian Pembelajaran:

1. Mampu menjelaskan VLAN
2. Mampu menjelaskan CIDR
3. Mampu menjelaskan VLSM
4. Mampu melakukan simulasi VLAN, CIDR, dan VLSM menggunakan packet tracert.

Pada bab ini membahas tentang VLAN pada Switch *Managable*, *Classless Inter-Domain Routing* (CIDR), dan teknik subnet VLSM. VLAN yang dijabarkan meliputi teori *access* dan *trunk*. Kemudian untuk CIDR dijabarkan meliputi teknik penghitungan biner pada IPV4. Kemudian untuk *Variable Length Subnet Mask* (VLSM) dijabarkan meliputi teknik subnet pada IPV4. Pada soal latihan memuat tentang simulasi VLAN, CIDR, dan VLSM menggunakan *packet tracert*.

5.1 VLAN

Kumpulan perangkat di satu atau lebih jaringan LAN yang dikonfigurasikan oleh suatu perangkat lunak. Bertujuan agar perangkat dapat berkomunikasi satu sama lain seolah-olah perangkat tersebut terpasang pada saluran yang sama, di mana Perangkat sebenarnya menaungi sejumlah segmen LAN yang berbeda. VLAN dibuat dalam jaringan pihak ketiga, tetapi VLAN hanya sebagian kecil dari jaringan IP yang terisolasi secara logis.

Untuk jenis VLAN terbagi menjadi 5, yaitu:

- *Default* VLAN

  VLAN yang sudah ada sejak pertama kali switch dihidupkan. sebelum dikonfigurasi, semua port yang ada pada switch akan

tergabung ke dalam *default* VLAN dan dapat tergabung pada masing-masing VLAN. Pada Cisco, default VLAN adalah VLAN 1.

- Data VLAN
  VLAN yang hanya mengatur trafik data pada VLAN.
- Native VLAN
  VLAN yang dikembalikan ke suatu port apabila tidak dalam bentuk *tagged* dan *untagged*.
- Voice VLAN
  VLAN yang mendukung VoIP dan dikhususkan untuk komunikasi data suara pada VLAN.
- Management VLAN
  VLAN yang di konfigurasi untuk management switch.

Berdasarkan hal tersebut, maka keuntungan VLAN yaitu:

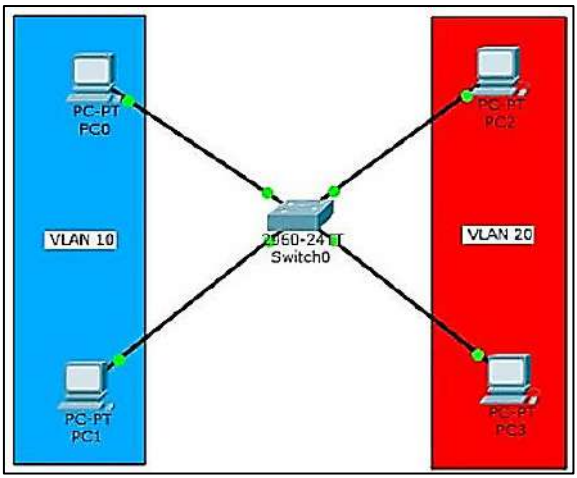
- Semua data sensitif dipisahkan dari jaringan yang ada, sehingga pelanggaran terhadap akses ke informasi rahasia dan penting dapat dikurangi.
- Menghemat biaya dengan menekan biaya upgrade jaringan seperti penggunaan bandwidth dan uplink.
- Kinerja yang lebih tinggi dapat mengurangi tingkat kepadatan lalu lintas suatu jaringan.
- Broadcast Storm Mitigation yang dapat mengontrol jumlah perangkat pengguna dalam jaringan.
- Efisiensi staf TI dalam manajemen jaringan, karena pengguna dengan kebutuhan jaringan yang sama menggunakan VLAN yang sama.

5.1.1 Mode *Access*

Mode *access* pada VLAN memiliki fungsi sebagai berikut:

- Port yang dikonfigurasi hanya untuk satu vlan pada *switch* tersebut
- Satu port yang bisa terdaftar disatu vlan dan tidak bisa didaftarkan lebih dari satu vlan.

- Mode ini biasanya hanya di set di port switch yang terhubung ke *endpoint* seperti PC, Server, dan *endpoint* yang lainnya.
- Anggota suatu vlan tidak bisa berkomunikasi dengan anggota vlan yang lain, kecuali jika dihubungkan dengan router mode access link mendukung teknologi ethernet biasa (10 mbps) hingga fast ethernet (100 mbps).
- Mode access link sering disebut dengan untagged vlan.

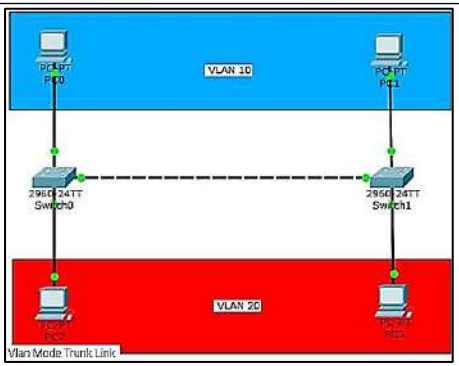


Gambar 124. *Mode Access*

5.1.2 Mode *Trunk*

Mode *trunk* pada VLAN memiliki fungsi sebagai berikut:

- Port yang dikonfigurasi untuk dilalui berbagai vlan.
- Port switch pada mode trunk link bisa untuk membawa banyak vlan.
- Port mode ini akan menjadi trunk link jika port pada switch lawan di set ke mode trunk atau Dynamic trunking protocol.
- Mode ini biasa digunakan untuk menghubungkan switch dengan switch, switch dengan router atau switch dengan server.
- Mode trunk link mendukung teknologi fast ethernet (100Mbps) dan gigabit(1000Mbps),
- Mode trunk link sering disebut dengan tagged vlan.



Gambar 125. *Mode Trunk*

5.2 *Classless Inter-Domain Routing* (CIDR)

Diperkenalkan oleh lembaga IETF pada tahun 1992, merupakan konsep baru untuk mengembangkan *Supernetting* dengan *Classless Inter-Domain Routing*. CIDR menghindari cara pemberian IP Address tradisional menggunakan klas A, B dan C. CIDR menggunakan "*network prefix*" dengan panjang tertentu. Prefix-length menentukan jumlah "bit sebelah kiri" yang akan dipergunakan sebagai network ID.

Jika suatu IP Address memiliki 16 bit sebagai network ID, maka IP address tersebut akan diberikan prefix-length 16 bit yang umumnya ditulis sebagai /16 dibelakang IP Address, contoh: 202.152.0.1/18. Oleh karena tidak mengenal kelas, CIDR dapat mengalokasikan kelompok IP address dengan lebih efektif.

Seperti contoh, jika satu blok IP address (192.168.1.0/26) dialokasikan untuk 62 host dengan subnetmask 255.255.255.192. Maka pembagian IP networknya sebagai berikut:

Subnet 1 = 62 host → network address = 192.168.1.0/26
Subnet 2 = 62 host → network address = 192.168.1.64/26
Subnet 3 = 62 host → network address = 192.168.1.128/26
Subnet 4 = 62 host → network address = 192.168.1.192/26

Bila salah satu subnet masih ingin memecah jaringannya menjadi beberapa bagian, misal subnet 4 masih akan dibagi menjadi 2 jaringan (subnet 4.1 dan subnet 4.2), maka 62 IP yang sebelumnya akan

dialokasikan buat host subnet 4 akan dipecah menjadi 2 subnet lagi dengan jumlah host yang sama.

Subnet 4.1 = 30 host → network address = 192.168.1.192/27
Subnet 4.2 = 30 host → network address = 192.168.1.224/27
Subnet Mask = 255.255.255.224

Sisa host masing-masing subnet yang baru hanya 30 host, dikarenakan perlu satu IP sebagai identitas alamat Network. dan satu IP lainya (yang terakhir) digunakan sebagai IP broadcast subnet tersebut.

5.3 *Variable Length Subnet Mask* (VLSM)

Jika pada pengalokasian IP address classfull, suatu network ID hanya memiliki satu subnetmask, maka VLSM menggunakan metode yang berbeda, yakni dengan memberikan suatu network address lebih dari satu subnetmask.Perhatikan contoh berikut:

Satu blok IP address (128.64.0.0/20) dibagi menjadi 16.

Subnet 1 = 4094 host → Net address = 128.64.0.0/20
Subnet 2 = 4094 host → Net address = 128.64.16.0/20
Subnet 3 = 4094 host → Net address = 128.64.32.0/20
Subnet 4 = 4094 host → Net address = 128.64.48.0/20
…
Subnet 16= 4094 host → Net address = 128.64.240.0/20
Subnet Mask = 255.255.240.0

Berikutnya Subnet 2 akan dipecah menjadi 16 subnet lagi yang lebih kecil.

Subnet 2.1 = 254 host → Net address = 128.64.16.0/24
Subnet 2.2 = 254 host → Net address = 128.64.17.0/24
Subnet 2.3 = 254 host → Net address = 128.64.18.0/24
…
Subnet 2.16 = 254 host → Net address = 128.64.31.0/24
Subnet Mask = 255.255.255.0

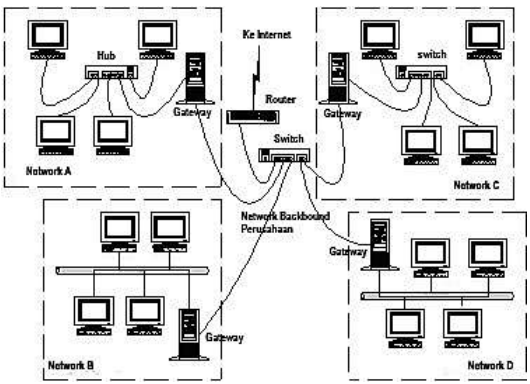
Bila subnet 2.1 akan dipecah lagi menjadi beberapa subnet, misal 4 subnet, maka:

Subnet 2.1.1 = 62 host → Net address = 128.64.16.0/26
Subnet 2.1.2 = 62 host → Net address = 128.64.16.64/26
Subnet 2.1.3 = 62 host → Net address = 128.64.16.128/26
Subnet 2.1.4 = 62 host → Net address = 128.64.16.192/26
Subnet Mask = 255.255.255.192

Pada Subnet 2 (Net address 128.64.16.0) dapat memecah jaringannya menjadi beberapa subnet lagi dengan mengganti Subnetmask-nya menjadi: 255.255.240.0, 255.255.255.0 dan 255.255.255.192. Jika diperhatikan, CIDR dan metode VLSM mirip satu sama lain, yaitu blok *network address* dapat dibagi lebih lanjut menjadi sejumlah blok IP address yang lebih kecil.

Perbedaannya adalah CIDR merupakan sebuah konsep untuk pembagian blok IP Public yang telah didistribusikan dari IANA, sedangkan VLSM merupakan implementasi pengalokasian blok IP yang dilakukan oleh pemilik network (*network administrator*) dari blok IP yang telah diberikan padanya (sifatnya local dan tidak dikenal di internet).

Misalkan suatu perusahaan yang terdiri dari 4 departemen ingin memiliki LAN yang dapat mengintegrasikan seluruh departemen. Masing-masing departemen memiliki server sendiri-sendiri (bisa Novell Server, Windows Server, Linux atau UNIX). Cara yang sederhana adalah membuat topologi network perusahaan tersebut seperti ditampilkan pada gambar berikut.



Gambar 126. *Subnetting* Fisik

Kita membuat 5 buah physical network (sekaligus logical network), yakni 4 buah pada masing-masing departemen, dan satu buah lagi sebagai jaringan backbone antar departemen. Dengan kata lain, kita membuat beberapa subnetwork (melakukan subnetting). Keseluruhan komputer tetap dapat saling berhubungan karena server juga berfungsi sebagai router. Pada server terdapat dua network interface, masing-masing tersambung ke jaringan backbone dan jaringan departemennya sendiri.

Setelah membuat subnet secara fisik, kita juga harus membuat subnet logic. Masing-masing subnet fisik setiap departemen harus mendapat subnet logic (IP Address) yang berbeda, yang merupakan bagian dari network address perusahaan. Dengan mengetahui dan menetapkan subnetmask, kita dapat memperkirakan jumlah host maksimal masing-masing subnet pada jaringan tersebut. Berikut ini daftar subnetting yang bisa dihapal dan diterapkan untuk membuat subnet.

Tabel 2. Tabel *Subnet*

Bit Host	CIDR	Subnet	Net Mask	Host
0	/8	1	255.0.0.0	16.777.214
1	/9	2	255.128.0.0	8.388.606
2	/10	4	255.192.0.0	4.194.302
3	/11	8	255.224.0.0	2.097.150
4	/12	16	255.240.0.0	1.048.574
5	/13	32	255.248.0.0	524.286
6	/14	64	255.252.0.0	262.142
7	/15	128	255.254.0.0	131.070
8	/16	256	255.255.0.0	65.534
9	/17	512	255.255.128.0	32.766
10	/18	1.024	255.255.192.0	16.382
11	/19	2.048	255.255.224.0	8.910
12	/20	4.096	255.255.240.0	4.094
13	/21	8.912	255.255.248.0	2.046
14	/22	16.384	255.255.252.0	1.022
15	/23	32.768	255.255.254.0	510
16	/24	65.536	255.255.255.0	254
17	/25	131.072	255.255.255.128	126

18	/26	262.144	255.255.255.192	62
19	/27	524.288	255.255.255.224	30
20	/28	1.048.576	225.255.255.240	14
21	/29	2.097.152	255.255.255.248	6
22	/30	4.194.304	255.255.255.252	2
23	/31	Salah	255.255.255.254	Salah

Dapat juga mempelajari cara menghitung dengan mempergunakan rumus:

Jumlah Host per Network = $2^{n} - 2$

Dimana *n* adalah jumlah bit tersisa yang belum diselubungi, misal *Network Prefix* /10, maka bit tersisa **(n)** adalah 32 –10 = 22,

Kemudian $2^{22} - 2 = 4194302$

Sedangkan untuk mencari jumlah subnet sebgai berikut:

Jumlah Subnet = 2^{N}

Dimana *N* adalah jumlah bit yang dipergunakan (diselubungi) *atau N = Network Prefix* – 8

Seperti contoh, bila network prefix /10, maka N = 10 – 8 = 2 → $2^{2} = 4$

Untuk menyusun tabel diatas, sebenarnya cukup mudah dilakukan, yang perlu diperhatikan bahwa, nilai jumlah host per network ternyata tersusun terbalik dengan jumlah subnet, Host/network dapat dengan gampang disusun dengan rumus lain, seperti:

$A \times 2 + 2 = A_n$

Dimana *A* adalah jumlah host sebelumnya, dan A_n adalah jumlah host yang didapatkan.

Seperti contoh, 2 x 2 + 2 = 6, 6 x 2 + 2 = 14, 14 x 2 + 2 = 30 dst.

Subnet: 1 x 2 = 2, 2 x 2 = 4, 4 x 2 = 8, 8 x 2 = 16, dst.

5.4 Latihan *Subnetting*

Bila suatu jaringan memiliki IP address dari kelas C seperti 192.168.0.1, Tentukan berapa jumlah host maksimal yang bisa disusun dalam satu network dan berapa jumlah network (subnet) yang bisa dibentuk (1 network atau lebih)

Cara Penyelesaian:

Net Address	: 192.168.0.0/24
	11000000.10101000.00000000.00000000
Netmask	: 255.255.255.0
	11111111.11111111.11111111.00000000
Wildcard	: 0.0.0.255
	00000000.00000000.00000000.11111111
IP Host Awal	: 192.168.0.1
	11000000.10101000.00000000.00000001
IP Host Akhir	: 192.168.0.254
	11000000.10101000.00000000.11111110
Broadcast	: 192.168.0.255
	11000000.10101000.00000000.11111111
Hosts/Net	: 254 (1 Network)

Network	: 192.168.0.0/25
	11000000.10101000.00000000.00000000
Netmask	: 255.255.255.128
	11111111.11111111.11111111.10000000
Wildcard	: 0.0.0.127
	00000000.00000000.00000000.01111111
IP Host Awal	: 192.168.0.1
	11000000.10101000.00000000.00000001
IP Hos tAkhir	: 192.168.0.126
	11000000.10101000.00000000.01111110
Broadcast	: 192.168.0.127
	11000000.10101000.00000000.01111111
Hosts/Net	: 126 (1 Network)

Network	: 192.168.0.128
	11000000.10101000.00000000.10000000
IP Host Awal	: 192.168.0.129
	11000000.10101000.00000000.10000001
IP HostAkhir	: 192.168.0.254
	11000000.10101000.00000000.11111110
Broadcast	: 192.168.0.255
	11000000.10101000.00000000.11111111
Hosts/Net	: 126 (1 Network)
Subnets	: 2 Network
Hosts Max	: 252

Net Add : 192.168.0.0/26
11000000.10101000.00000000.00000001
Netmask : 255.255.255.192
11111111.11111111.11111111.11000000
Wildcard : 0.0.0.63
00000000.00000000.00000000.00111111

Network : 192.168.0.0/26
11000000.10101000.00000000.00000000
HostMin : 192.168.0.1
11000000.10101000.00000000.00000001
HostMax : 192.168.0.62
11000000.10101000.00000000.00111110
Broadcast : 192.168.0.63
11000000.10101000.00000000.00111111
Hosts/Net : 62

Network : 192.168.0.64/26
11000000.10101000.00000000.01 000000
HostMin : 192.168.0.65
11000000.10101000.00000000.01 000001
HostMax : 192.168.0.126
11000000.10101000.00000000.01 111110
Broadcast : 192.168.0.127
11000000.10101000.00000000.01 111111
Hosts/Net : 62

Network : 192.168.0.128/26
11000000.10101000.00000000.10 000000
HostMin : 192.168.0.129
11000000.10101000.00000000.10 000001
HostMax : 192.168.0.190
11000000.10101000.00000000.10 111110
Broadcast : 192.168.0.191
11000000.10101000.00000000.10 111111
Hosts/Net : 62

Network : 192.168.0.192/26
11000000.10101000.00000000.11 000000
HostMin : 192.168.0.193
11000000.10101000.00000000.11 000001
HostMax : 192.168.0.254

11000000.10101000.00000000.11 111110
Broadcast : 192.168.0.255
11000000.10101000.00000000.11 111111
Hosts/Net : 62

Subnets	: 4
Hosts	: 248

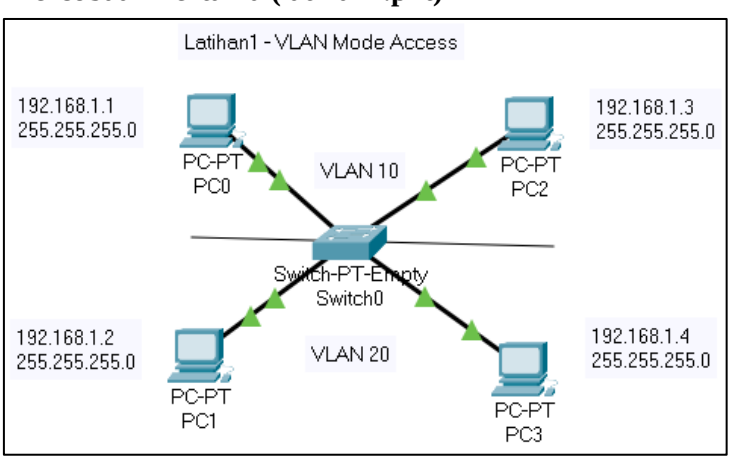
Untuk lebih rinci dapat dilihat pada tabel berikut:

Tabel 3. Rincian Latihan *Subnetting*

Bit Masked	Bit Host ID	CIDR	Subnet	Net Mask	Host Max	Host per Network
0	8	/24	1	255.255.255.0	254	254
1	7	/25	2	255.255.255.128	252	126
2	6	/26	4	255.255.255.192	248	62
3	5	/27	8	255.255.255.224	240	30
4	4	/28	16	255.255.255.240	224	14
5	3	/29	32	255.255.255.248	192	6
6	2	/30	64	255.255.255.252	128	2

5.5 Latihan Simulasi VLAN, CIDR, dan VLSM

5.5.1 Percobaan Pertama (latihan1.pkt)

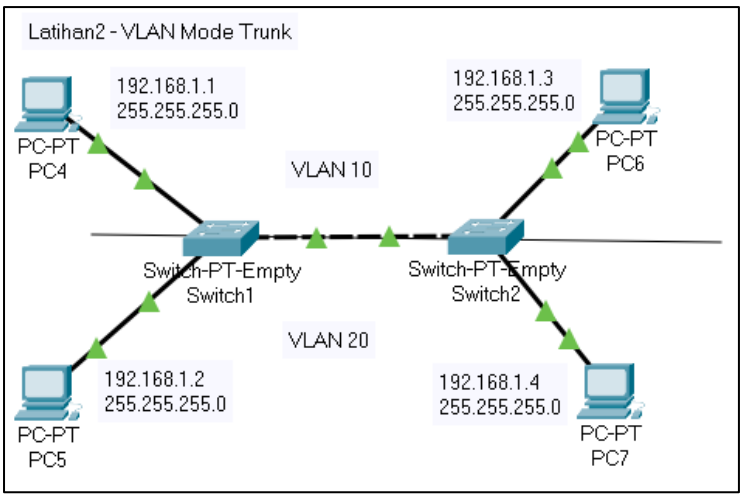


Gambar 127. Latihan 1

Gambar 128. Latihan 1

- Soal 1:
  Sebelum melakukan VLAN ACCESS, Lakukanlah perintah PING dari 192.168.1.1 ke 192.168.1.3, Jelaskan hasilnya !
- Soal 2:
  Sebelum melakukan VLAN ACCESS, Lakukanlah perintah PING dari 192.168.1.1 ke 192.168.1.4, Jelaskan hasilnya !
- Soal 3:
  Setelah melakukan VLAN ACCESS, Lakukanlah perintah PING dari 192.168.1.3 ke 192.168.1.2, Jelaskan hasilnya !
- Soal 4:
  Setelah melakukan VLAN ACCESS, Lakukanlah perintah PING dari 192.168.1.3 ke 192.168.1.1, Jelaskan hasilnya !

5.5.2 Percobaan Kedua (latihan2.pkt)

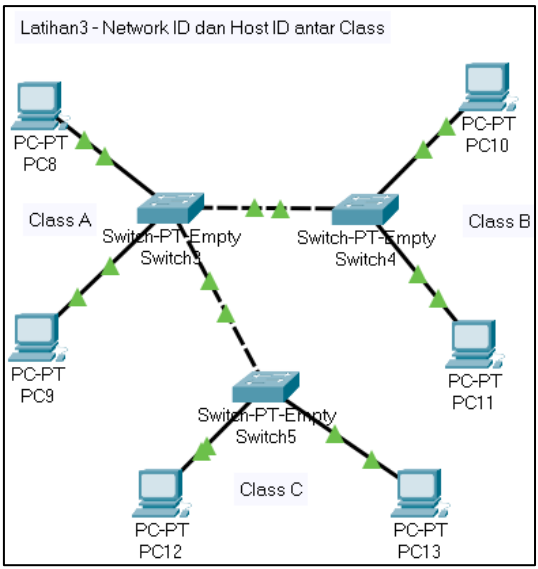


Gambar 129. Latihan 2

Gambar 130. Latihan 2

- Soal 1:
  Sebelum melakukan VLAN ACCESS dan TRUNK, Lakukanlah perintah PING dari PC4 ke PC6, Jelaskan hasilnya !
- Soal 2:
  Setelah melakukan VLAN ACCESS dan belum TRUNK, Lakukanlah perintah PING dari PC4 ke PC5, Jelaskan hasilnya !
- Soal 3:
  Setelah melakukan VLAN ACCESS dan TRUNK, Lakukanlah perintah PING dari PC4 ke PC6, Jelaskan hasilnya !
- Soal 4:
  Setelah melakukan VLAN ACCESS dan TRUNK, Lakukanlah perintah PING dari PC6 ke PC7, Jelaskan hasilnya !

5.5.3 Percobaan Ketiga (latihan3.pkt)



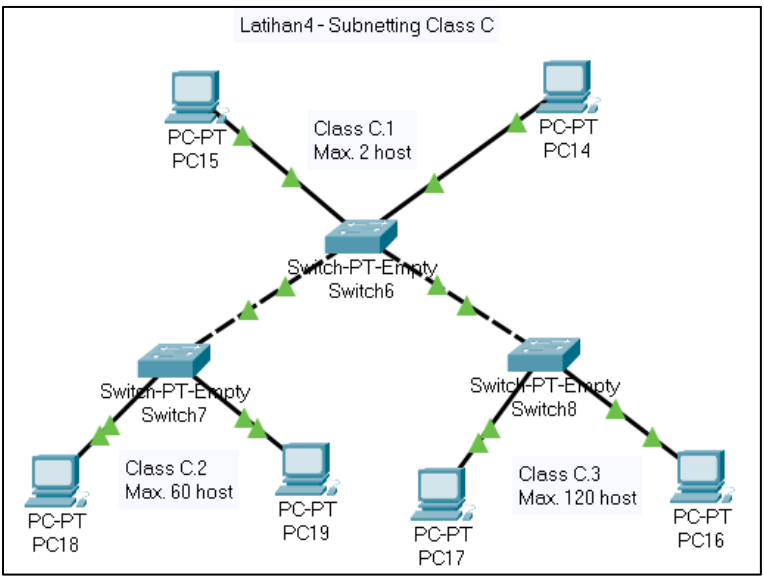
Gambar 131. Latihan 3

Gambar 132. Latihan 3

Gambar 133. Latihan 3

- Soal 1:
  Tentukan IP CLASS A pada PC8 dan PC9, kemudian Lakukanlah perintah PING dari PC8 ke PC9, Jelaskan hasilnya !
- Soal 2:
  Tentukan IP CLASS B pada PC10 dan PC11, kemudian Lakukanlah perintah PING dari PC10 ke PC11, Jelaskan hasilnya !
- Soal 3:
  Tentukan IP CLASS C pada PC12 dan PC13, kemudian Lakukanlah perintah PING dari PC12 ke PC13, Jelaskan hasilnya !
- Soal 4:
  Lakukanlah perintah PING antar CLASS dari PC8 ke PC13, kemudian PC10 ke PC 13. Jelaskan hasilnya !

5.5.4 Percobaan Keempat (latihan4.pkt)



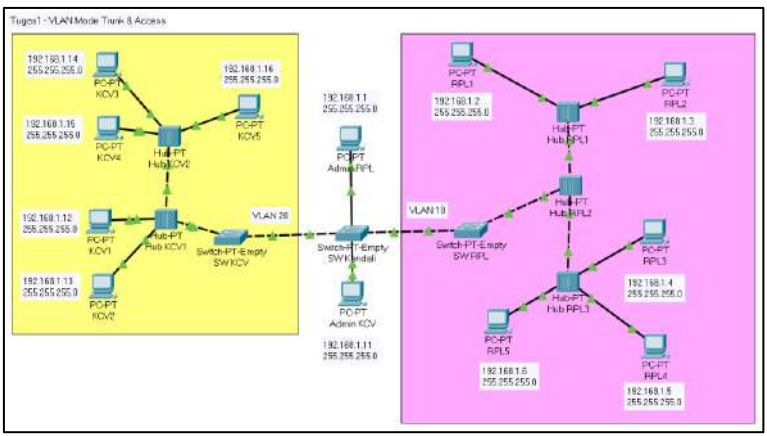
Gambar 134. Latihan 4

Gambar 135. Latihan 4

Gambar 136. Latihan 4

- Soal 1:
  Tentukan IP dan subnetmask PC16 dan PC17 dengan ketentuan 120 host
- Soal 2:
  Tentukan IP dan subnetmask PC16 dan PC17 dengan ketentuan 120 host
- Soal 3:
  Tentukan IP dan subnetmask PC16 dan PC17 dengan ketentuan 120 host
- Soal 4:
  Lakukan ping dari PC Class C.1 ke PC Class C.3, Jelaskan !

5.5.5 Percobaan Kelima (latihan5.pkt)



Gambar 137. Latihan 5

Buatlah simulasi persis seperti pada gambar sebelumnya, simulasi tersebut terdapat:

- Perangkat Aktif
- Komputer
- Kabel Jaringan
- Ruangan
- IP Address
- Subnet Mask
- VLAN

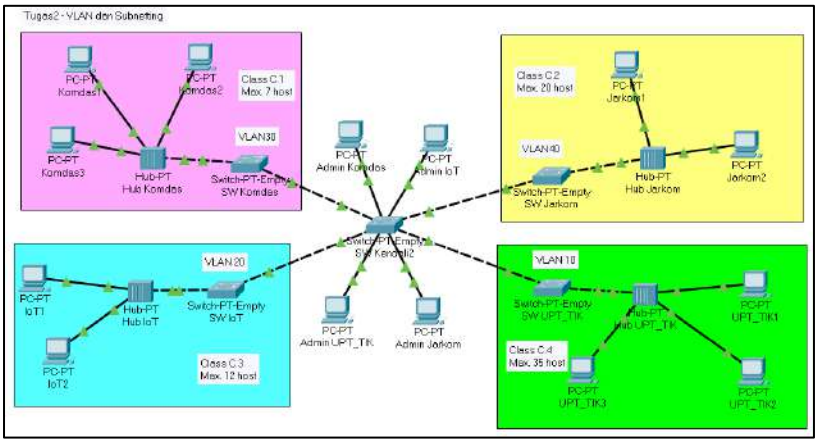
Ketentuan wajib simulasi:

- PC pada Lab KCV hanya dapat berinteraksi antar lab KCV dan Admin lab KCV
- PC pada Lab RPL hanya dapat berinteraksi antar lab RPL dan admin lab RPL

Petunjuk:

- Buktikan dengan memasukkan gambar *port* berapa saja yang memerlukan akses VLAN RPL dan KCV pada setiap switch terkait
- Buktikan dengan memasukkan gambar VLAN Databases setiap Switch terkait

5.5.6 Percobaan Keenam (latihan6.pkt)



Gambar 138. Latihan 6

Buatlah simulasi persis seperti pada gambar sebelumnya, simulasi tersebut terdapat:

- Perangkat Aktif
- Komputer
- Kabel Jaringan
- Ruangan
- IP Address
- Subnet Mask
- VLAN

Ketentuan wajib simulasi:

- PC pada Lab KCV hanya dapat berinteraksi antar lab KCV dan Admin lab KCV
- PC pada Lab RPL hanya dapat berinteraksi antar lab RPL dan admin lab RPL
- PC pada Lab Komdas hanya dapat berinteraksi antar lab Komdas dan Admin lab Komdas
- PC pada Lab IoT hanya dapat berinteraksi antar lab IoT dan admin lab IoT

Petunjuk:

- Buktikan dengan memasukkan gambar *port* berapa saja yang memerlukan akses VLAN RPL dan KCV pada setiap *switch* terkait.
- Buktikan dengan memasukkan gambar VLAN *Databases* setiap Switch terkait.
- Buktikan dengan memasukkan gambar screenshot dari spreadsheet / excel / metode hitugan lainnya.

BAB 6
Routing Statik dan Dinamik

Capaian Pembelajaran:

1. Mampu menjelaskan *routing* statik
2. Mampu menjelaskan *routing* dinamik
3. Mampu melakukan simulasi *routing* statik dan dinamik menggunakan *packet tracert*.

Pada bab ini membahas tentang *routing* statik dan *routing* dinamik. *Routing* statik yang dijabarkan meliputi teori penggunaan *routing* secara statik. Kemudian untuk *routing* dinamik dijabarkan meliputi teori penggunaan routing secara dinamik. Pada soal latihan memuat tentang simulasi *routing* statik dan dinamik menggunakan *packet tracert*.

6.1 *Routing*

Routing diharuskan memahami sistem penomoran IP, *subnetting*, *netmasking* dan lainnya. Dimana sudah dibahas pada materi sebelumnya. Untuk lebih mendalami pemahaman tersebut, maka mohon perhatikan kasus berikut.

Kasus Pertama:

Host X → 128.1.1.1 (IP Kelas B network id 128.1.x.x)

Host Y → 128.1.1.7 (IP kelas B network id 128.1.x.x)

Host Z → 128.2.2.1 (IP kelas B network id 128.2.x.x)

Pada kasus di atas, host X dan host Y dapat berkomunikasi langsung tetapi baik host X maupun Y tidak dapat berkomunikasi dengan host Z, karena mereka memiliki Network Id yang berbeda. Agar Z dapat berkomunikasi dengan X dan Y dapat menggunakan router.

Kasus Kedua:

Host A → 192.168.0.1 / subnet mask 255.255.255.240

Host B → 192.168.0.2 / subnet mask 255.255. 255.240

Host C → 192.168.0.17 / subnet mask 255.255. 255.240

Ketika *subnetting* dipergunakan, maka dua host yang terhubung ke segmen jaringan yang sama dapat berkomunikasi hanya jika baik Network ID maupun subnetID-nya sesuai. Pada kasus di atas, A dan B dapat berkomunikasi dengan langsung, C memiliki Network ID yang sama dengan A dan B tetapi memiliki subnetmask yang berbeda. Dengan demikian C tidak dapat berkomunikasi secara langsung dengan A dan B. Agar C dapat berkomunikasi dengan A dan B dapat menggunakan router.

Fungsi *router*, secara mudah dapat dikatakan, menghubungkan dua buah jaringan yang berbeda; tepatnya mengarahkan rute yang terbaik untuk mencapai network yang diharapkan. Dalam implementasinya, router sering dipakai untuk menghubungkan jaringan antar lembaga atau perusahaan yang masing-masing telah memiliki jaringan dengan Network ID yang berbeda.

Contoh lainnya yang saat ini populer adalah ketika sebuah perusahaan akan terhubung ke internet. Maka router akan berfungsi mengalirkan paket data dari perusahaan tersebut ke lembaga lain melalui internet, sudah barang tentu nomor jaringan perusahaan itu akan bereda dengan perusahaaan yang dituju.

Jika sekedar menghubungkan 2 buah jaringan, sebenarnya juga dapat menggunakan PC berbasis windows NT atau Linux, dengan memberikan 2 buah *network card* dan beberapa konfigurasi, maka anda telah membuat router praktis. Namun tentunya dengan segala keterbatasannya. Di *marketplace* sangat beragam merek *router*, antara lain baynetworks, 3com, Cisco dan lainnya.

Secara umum mekanisme koordinasi routing dapat dibagi menjadi dua, yaitu *routing* statik dan routing dinamik. Pada *routing* statik, entri-entri dalam *forwarding table router* diisi dan dihapus secara manual,

sedangkan pada *routing dinamik* perubahan dilakukan otomatis melalui protokol *routing*.

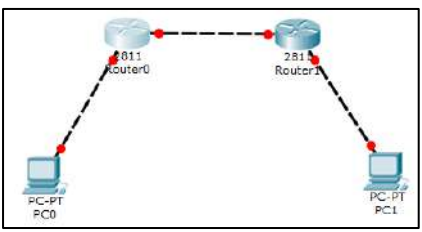
Tabel 4. Perbedaan Statik dan Dinamik

Routing Statik	Routing Dinamik
Berfungsi pada protokol IP	Berfungsi pada inter-routing protocol
Router tidak dapat membagi informasi routing	Router membagi informasi routing secara otomatis
Routing tabel dibuat dan dihapus secara manual	Routing tabel dibuat dan dihapus secara dinamis oleh router
Tidak menggunakan routing protocol	Terdapat routing protocol, seperti RIP atau OSPF
Microsoft mendukung multihomed system seperti router	Microsoft mendukung RIP untuk IP dan IPX/SPX

6.2 *Routing* Statik

Routing statik adalah pengaturan routing paling sederhana yang dapat dilakukan pada jaringan komputer. Menggunakan routing statik murni dalam sebuah jaringan berarti mengisi setiap entri dalam forwarding table di setiap router yang berada di jaringan tersebut. Penggunaan routing statik dalam sebuah jaringan yang kecil tentu bukanlah suatu masalah, hanya beberapa entri yang perlu diisikan pada forwarding table di setiap router. Namun Anda tentu dapat membayangkan bagaimana jika harus melengkapi *forwarding table* di setiap router yang jumlahnya tidak sedikit dalam jaringan yang besar. Apalagi jika Anda ditugaskan untuk mengisi entri-entri di seluruh router di Internet yang jumlahnya banyak sekali dan terus bertambah setiap hari. Untuk lebih memahami *routing*, dapat mengikuti latihan berikut:

1) Buka *Packet Tracer*, buat topologi seperti gambar berikut:

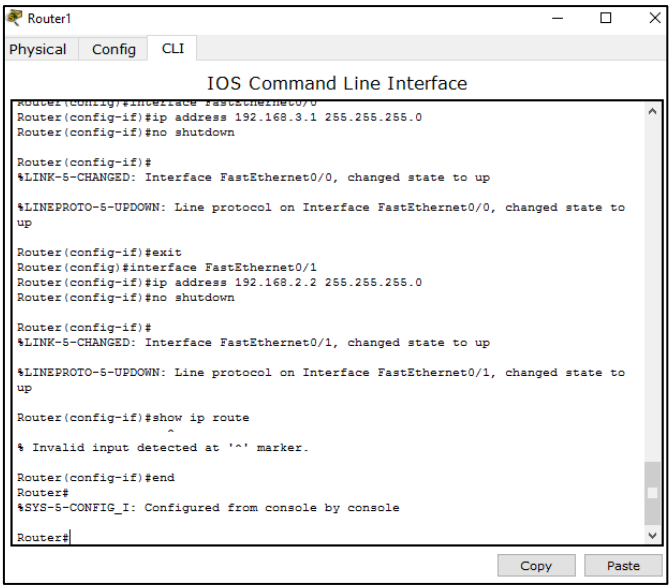


Gambar 139. *Routing* Statik 1

2) Pada router interface F0/0 terhubung ke PC, sedangkan interface F0/1 terhubung ke router tetangganya. Atur alamat IP sebagai Berikut:

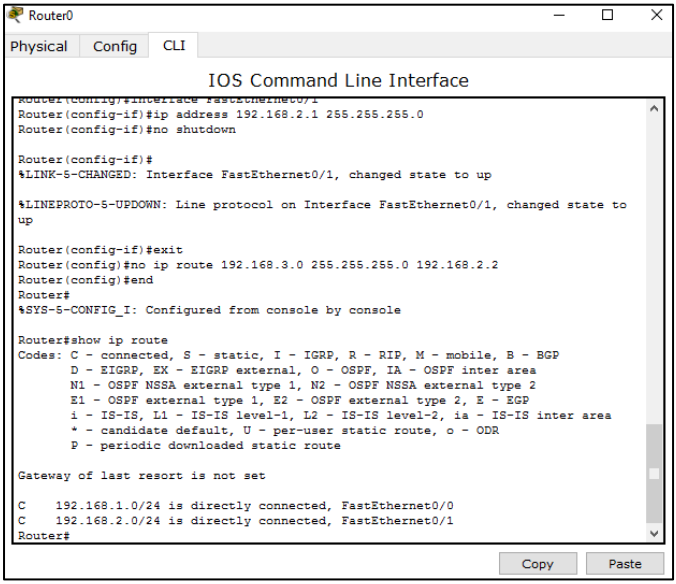
PC0: 192.168.1.2/24
Router0 F0/0: 192.168.1.1/24, F0/1: 192.168.2.1/24
Router1 F0/0: 192.168.3.1/24, F0/1: 192.168.2.2/24
PC1: 192.168.3.2/24

3) Jangan lupa untuk mengatur *gateway* pada setiap PC. IP *Gateway* adalah IP *Router* pada *interface* yang satu *network* dengan PC0.
4) Jika sudah di konfigurasi sesuai dengan konfigurasi diatas, lakukan *test* ping dari PC0 ke PC1.
5) Lakukan pada mode simulasi, kemudian amati sampai dimana paketnya terkirim dan amati pula balasan pada perintah ping di *command prompt*.
6) Cek tabel *routing* pada setiap *router*, caranya yaitu:
   - Klik 2x pada Router0
   - Masuk ke bagian CLI
   - Masukan perintah end, kemudian tekan enter 2x.



Gambar 140. *Routing* Statik 2

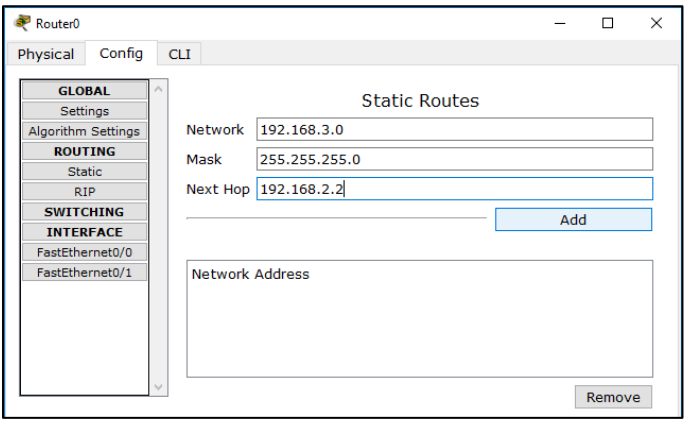
- Masukkan perintah "*show ip route*"



Gambar 141. *Routing* Statik 3

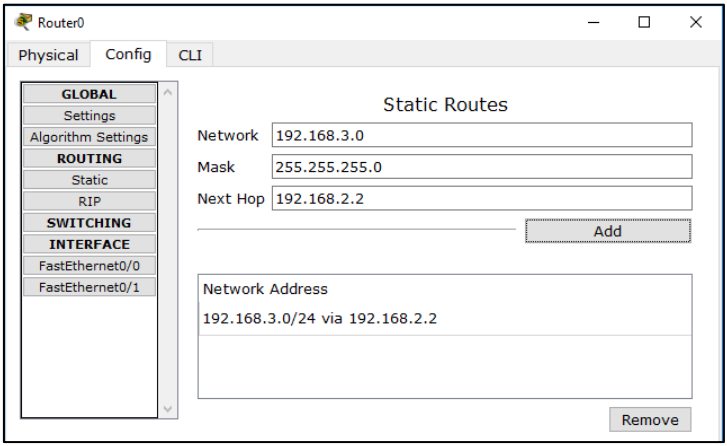
- Lakukan perintah yang sama pada Router1 kemudian catat hasilnya.

7) Masukan *routing* statis dengan cara berikut:
   - Klik pada Router0, masuk ke bagian Config.
   - Masuk ke menu Routing Static.
   - Masukkan alamat IP sebagai berikut



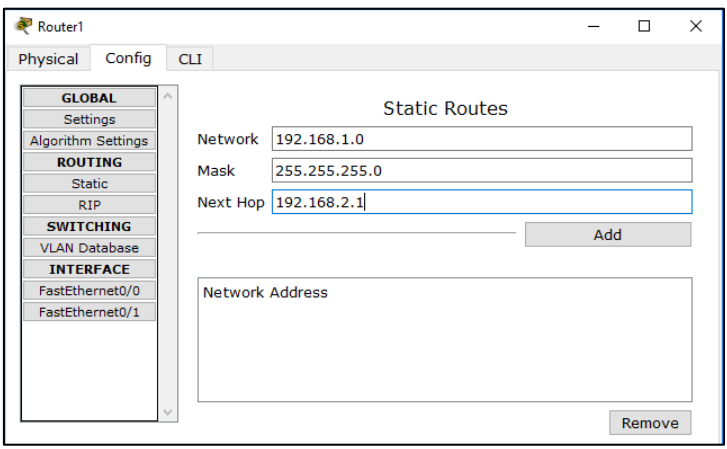
Gambar 142. *Routing* Statik 4

- Klik Tombol Add sehingga muncul seperti berikut:



Gambar 143. *Routing* Statik 5

8) Lakukan perintah "show ip route" sama seperti langkah sebelumnya pada router0 dan router1. Amati perbedaan dengan sebelumnya.
9) Lakukan Ping kembali dari PC0 ke PC1 pada mode simulasi, amati perjalanan paket yang terjadi.
10) Tambahkan *router* statis pada *router*1 dengan cara yang sama. Masukkan seperti gambar berikut:



Gambar 144. *Routing* Statik 6

11) Cek kembali "show ip route" pada kedua router, amati perbedaan dengan sebelumnya.
12) Kemudian lakukan Ping dari PC0 ke PC1 pada mode simulasi.

Konfigurasi pada langkah 7 yang tadi dilakukan bertujuan untuk mengenalkan alamat 192.168.3.0 pada router0. Sebelumnya router0 hanya mengenal alamat 192.168.1.0 dan 192.168.2.0 yang ditunjukkan pada perintah show ip *route*. Sehingga jika ada paket dengan tujuan network 192.168.3.0, maka *router* tersebut tidak dapat meneruskan paket tersebut, karena tujuan alamat belum dikenali oleh router0. 192.168.3.0/24 via 192.168.2.2 berarti kita memerintahkan pada router0 jika ada paket dengan tujuan alamat 192.168.3.0/24 maka teruskan ke alamat 192.168.2.2 (IP router1).

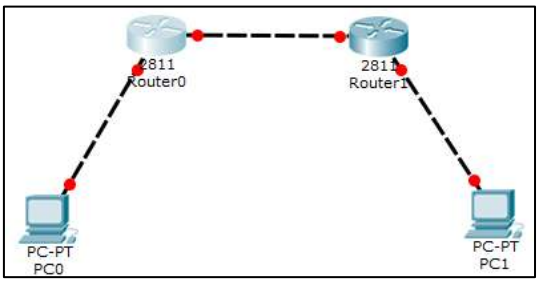
Sedangkan pada langkah 10 yang tadi dilakukan, Perintah tersebut berarti kita memerintahkan kepada router1, jika ada paket dengan tujuan 192.168.1.0/24 maka teruskan ke alamat 192.168.2.1 (ip router0). Dengan cara berikut maka PC0 dan PC1 sudah terhubung.

6.3 *Routing* Dinamik

Routing dinamik adalah cara yang digunakan untuk melepaskan kewajiban mengisi entri-entri *forwarding table* secara manual. Protokol routing mengatur *router-router* sehingga dapat berkomunikasi satu dengan yang lain dan saling memberikan informasi routing yang dapat mengubah isi *forwarding table*, tergantung keadaan jaringannya. Dengan cara ini, router-router mengetahui keadaan jaringan yang terakhir dan mampu meneruskan datagram ke arah yang benar. Dengan kata lain, routing dinamik adalah proses pengisian data *routing* di *table routing* secara otomatis.

Pada *routing* statik setiap *network* tujuan harus dikenalkan ke *router* dengan menginput secara manual. Hal ini masih mudah dilakukan untuk jaringan yang sederhana, sedangkan jika jaringannya besar maka sangat repot jika menggunakan *routing* statik. Untuk lebih memahami *routing*, dapat mengikuti latihan berikut:

1) Buat topologi sama seperti pada praktek routing statik.



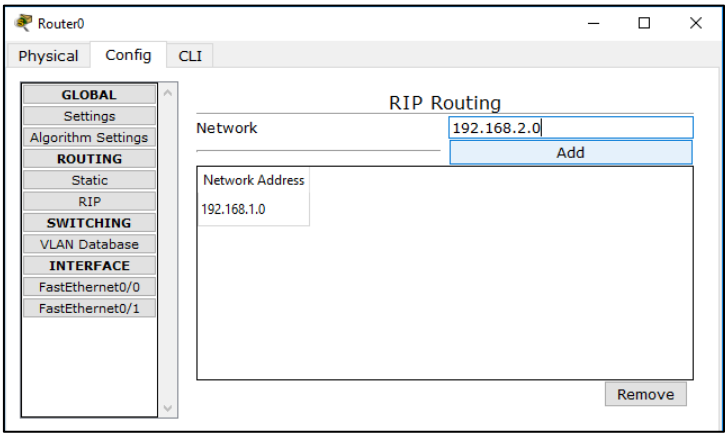
Gambar 145. *Routing* Dinamik 1

2) Konfigurasi IP interface yang sama juga seperti praktek sebelumnya.

PC0: 192.168.1.2/24
Router0 F0/0: 192.168.1.1/24, F0/1: 192.168.2.1/24
Router1 F0/0: 192.168.3.1/24, F0/1: 192.168.2.2/24
PC1: 192.168.3.2/24

3) Lakukan langkah pengamatan yang sama seperti pada praktek *routing* statik, yang berbeda hanya pada saat konfigurasi *routing*.

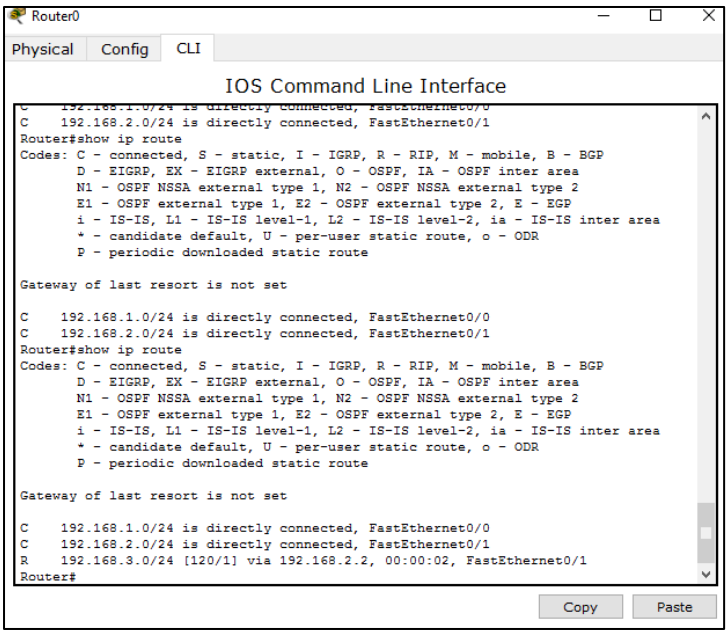
4) Lakukan konfigurasi *routing* seperti gambar dibawah:



Gambar 146. *Routing* Dinamik 2

5) Masukkan semua network yang terhubung langsung dengan router tersebut. Untuk Router0 network yang langsung terhubung langsung yaitu 192.168.1.0 dan 192.168.2.0.
6) Pada Router1 dimasukkan network 192.168.2.0 dan 192.168.3.0.
7) Lakukan tes ping dari PC0 ke PC1, amati hasilnya.

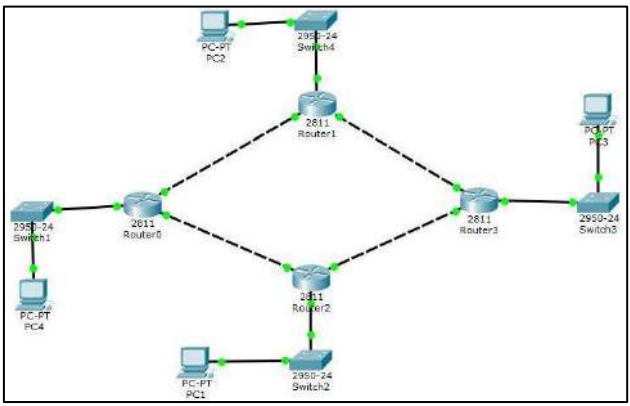
Pada Langkah 6, Kedua *Router* harus dimasukkan agar algoritma routing RIP berkerja, sehingga kedua *router* akan berbagi informasi routing. Jika hanya *Router0* yang dimasukan, maka pada tabel *routing* yang dapat dilihat dengan perintah "*show ip route*" belum menunjukkan perubahan. Jika kedua *router* sudah diaktifkan *routing* RIPnya, maka hasil tabel *routing* seperti gambar berikut.



Gambar 147. *Routing* Dinamik 3

Pada gambar terlihat terdapat routing dengan simbol R yang berisi informasi *routing* ke *network* 192.168.3.0 via 192.168.2.2, sehingga jika Router0 menerima paket dengan tujuan network 192.168.3.0 maka dilewatkan ke ip 192.168.2.2 pada *interface* FastEthernet0/1.

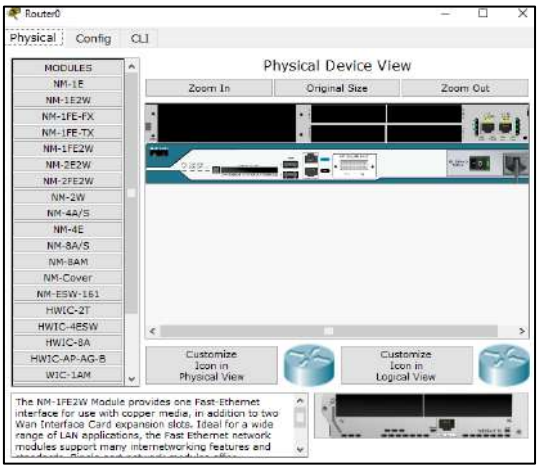
6.4 Latihan tentang Simulasi *Routing* Statik dan Dinamik



Gambar 148. Latihan Bagian 1

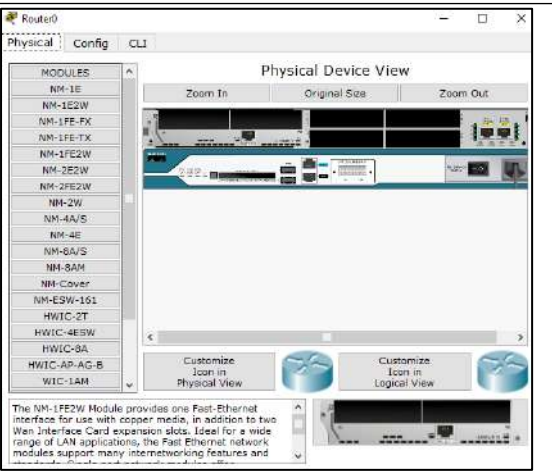
Buat jaringan seperti gambar tersebut, Setiap *router* harus mempunyai 3 interface Ethernet, secara *default Router* 2811 hanya memiliki 2 port FastEthernet sehingga perlu ditambah modul *Ethernet* lagi. Untuk menambah modul bisa dilakukan dengan langkah berikut:

- Matikan Router dengan menekan tombol power



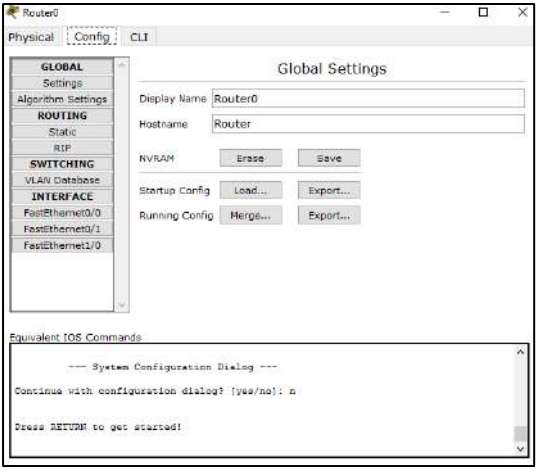
Gambar 149. Latihan Bagian 2

- Pilih NM-1FE-2W, kemudian tarik gambar modul yang terletak pada kanan bawah, ke slot Router pada gambar router di Physical Device View.



Gambar 150. Latihan Bagian 3

- Hidupkan kembali routernya dengan menekan tombol power.
- Untuk mengecek apakah interface sudah terpasang dengan benar bisa masuk ke bagian interface di tab confing, muncul 3 interface.

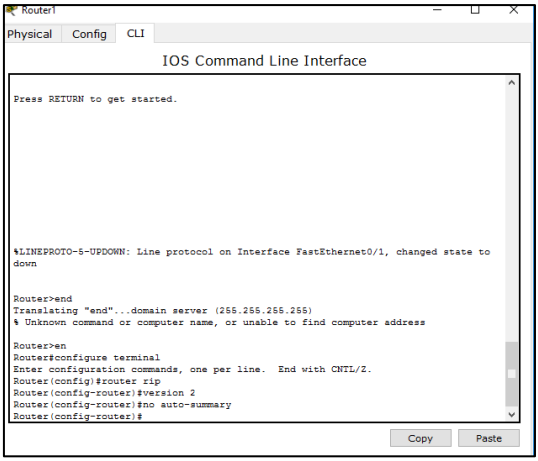


Gambar 151. Latihan Bagian 4

Konfigurasi IP address dengan blok alamat 192.168.0.0/24 yang di subnetting sesuai dengan kebutuhan (berapa jumlah host yang mungkin). Pada RIP version 1 tidak mendukung Class Less Routing Protocol, sehingga jika menggunakan subnetting untuk alamat IP, routingnya tidak berjalan karena menggunakan Class Full Routing

Protocol sehingga harus menggunakan version 2. Untuk mengaktifkan version 2 yang mendukung Class Less Routing Protocol dapat menggunakan perintah berikut:

```
#enable
#configure terminal
#router rip
#version 2
#no auto-summary
```



Gambar 152. Latihan Bagian 5

Masukkan *config router* RIP dan aktifkan *version* 2 pada semua *router*. Masukkan IP address tiap PC. Setiap PC harus dapat saling PING, jika sudah dapat saling ping, maka jaringan sudah berfungsi dengan normal.

BAB 7
Jaringan Nirkabel

Capaian Pembelajaran:

1. Mampu menjelaskan teori jaringan nirkabel
2. Mampu melakukan implementasi jaringan nirkabel

Pada bab ini membahas tentang jaringan nirkabel, dan implementasinya. Teori yang dijabarkan meliputi WLAN, *adhoc*, dan *hotspot*. Kemudian untuk implementasi jaringan nirkabel meliputi cara koneksi ke jaringan nirkabel pada *windows* 10, cara membuat jaringan *adhoc* pada *windows* 10, dan cara membuat hotspot pada *windows* 10.

7.1 Jaringan Nirkabel

Wireless LAN merupakan salah satu cara komunikasi data yang tidak menggunakan penghubung kawat melainkan melewati udara. WiFi yang merupakan singkatan dari *Wireless Fidelity* ini adalah sekumpulan standar yang digunakan untuk Jaringan Lokal Nirkabel (Wireless Local Area Networks - WLAN) yang didasari pada spesifikasi IEEE802.11. Sekarang ini ada empat variasi dari 802.11, yaitu: 802.11a, 802.11b, 802.11g dan 802.11n yang mempunyai data rate up to 300Mbps (downlink) and 150Mbps (uplink). Wireless LAN memiliki beberapa kelebihan dan juga kekurangan seperti di bawah ini.

Tabel 5. Kelebihan dan Kekurangan WLAN

Kelebihan	**Kekurangan**
✓ Mobilitas Tinggi ✓ Kemudahan dan kecepatan instalasi ✓ Menurunkan biaya kepemilikan	✓ Delay yang besar ✓ Adanya masalah propagasi radio seperti terhalang, terpantul, dan banyak sumber interferensi ✓ Kapasitas jaringan menghadapi

✓ Fleksibel ✓ Scalable	keterbatasan spektrum ✓ Keamanan / kerahasiaan data kurang terjamin

7.1.1 Jaringan Adhoc

Jaringan *wireless adhoc* sangat cocok dilakukan pada saat saat penting untuk menghubungkan dua buah laptop atau lebih secara langsung tanpa membutuhkan peralatan tambahan seperti *wireless router* atau *access point*. Tidak hanya untuk keperluan *File Sharing*, bisa juga untuk *share* koneksi internet. Jaringan WiFi Adhoc adalah mode jaringan WiFi yang memungkinkan dua atau lebih *device* (komputer atau *router*) untuk saling berkomunikasi satu sama lain secara langsung (dikenal dengan istilah *peer to peer*) tanpa melalui *Central Wireless Router* atau *Acces Point* (AP).

Gambar 153. Jaringan *Adhoc*

7.1.2 Hotspot

Hotspot adalah merupakan sebuah istilah dimana pengguna dapat membentuk area yang bisa mengakses jaringan internet, asalkan menggunakan PC, laptop atau perangkat lainnya dengan wi-fi, sehingga dapat mengakses internet tanpa media kabel dalam jangkauan radius kurang lebih beberapa ratus meteran tergantung dari kekuatan frekuensi atau signalnya. Fungsi Hotspot yaitu dapat melakukan koneksi *internet* seperti *browsing*, berkirim email, chatting, *download* / *upload.*

Kelebihan dari hotspot adalah tingginya minat masyarakat. Hal ini disebabkan jaringan nirkabel banyak terdapat di berbagai tempat umum yang sudah menyediakan Hotspot. Cara penggunaan yang gampang,

serta dapat diakses kapanpun dan dimanapun asalkan masuk kedalam radius hotspot.

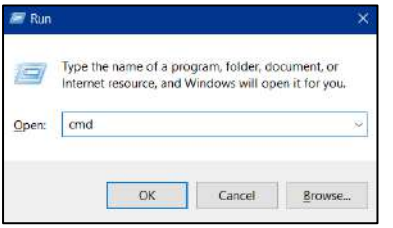
Kekurangan hotspot adalah Mudahnya diretas oleh oknum untuk mencuri *password* pengguna wi-fi. Daya tahan terhadap serangan flooding pun lemah, sehingga perlu perhatian khusus agar pengguna merasa aman. Untuk mengurangi resiko dari kekurangan hotspot tersebut, maka diperlukan beberapa cara.

Cara pertama, Jangan mengaktifkan file sharing folder atau printer pada PC / Laptop di jaringan publik, karena memungkinkan orang lain juga dapat mengakses folder yang di-*sharing*. Cara kedua, Selalu aktifkan *antivirus* dan *firewall* saat terkoneksi jaringan publik. Cara ketuga, jangan pernah bagikan *password* jaringan kita kepada orang tak dikenal.

7.2 Implementasi Jaringan Nirkabel

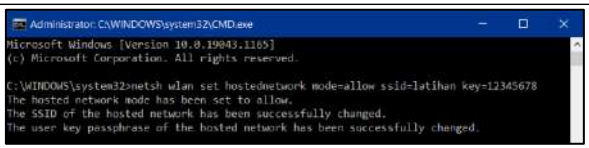
Implementasi jaringan nirkabel berikut pada sistem operasi *Windows* 10. Implementasi pertama yaitu tentang pembuatan jaringan *ad-hoc* untuk melakukan topologi P2P. Jaringan ini dapat diakses pada terminal *command prompt* saja, dan tidak memiliki user interface GUI.

1) Pertama, Buka *Command Prompt* dengan Hak Administrator melalui windows + R, ketikkan cmd, kemudian tekan CTRL + SHIFT + ENTER



Gambar 154. Langkah *adhoc* 1

2) Kemudian masukkan perintah “netsh wlan set hostednetwork mode=allow ssid=latihan key=12345678”

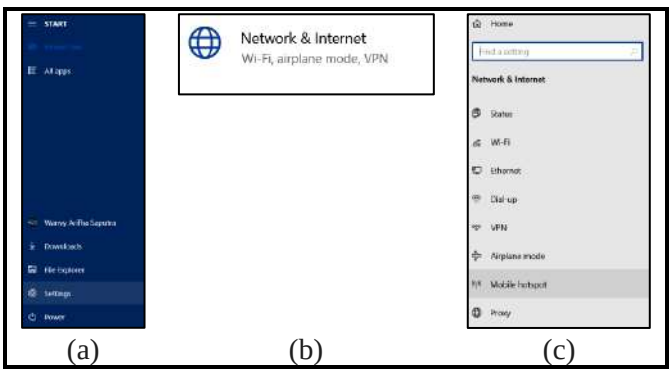


Gambar 155. Langkah *adhoc* 2

3) Jika ada pesan muncul bahwa *adhoc* berhasil dibuat. selanjutnya harus mengaktifkan adhocnya terlebih dahulu, sebelum hotspot terdeteksi. Caranya ketik "netsh wlan start hosted network" kemudian Enter.
   - Apabila terdapat pesan *error*, maka silahkan buka device manager, kemudian pilih view, dan pilih "*show hidden devices*"
   - Pada *network adapters*, silahkan enable "*Microsoft Virtual Hosted Network"*.
4) Kemudian masuk pada "*Control Panel*", pilih "*Network and Internet*", pilih "*Network Connections*", dan pada *network adapter* akan terlihat "Local Area Network * angka"
5) Kemudian pilih tab *Sharing* pada folder yang ingin berbagidata, lalu berikan ceklist pada"*Allow other network users to connect through this computer's Internet connection".*

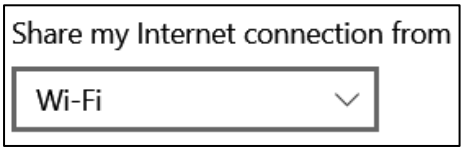
Implementasi kedua yaitu tentang pembuatan *hotspot* pada *Windows*10. Cara penggunaannya dapat menggunakan *user interface* GUI. Berikut langkah-langkah pembuatan *hotspot*:

1) Pilih tombol *Start* pada ikon , kemudian pilih *settings* → *Network & Internet* → *Mobile hotspot*.



Gambar 156. Langkah *hotspot* 1

2) Tentukan jaringan sumber untuk dijadikan *hotspot*, bila sumber *internet* menggunakan kabel jaringan, pilih *ethernet*, bila sumber menggunakan Wi-Fi, maka pilih Wi-Fi

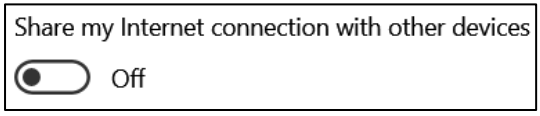


Gambar 157. Langkah *hostspot* 2

3) Pilih *Edit*, maka akan muncul gambar dibawah ini. Masukkan nama jaringan dan *password*, kemudian klik *save*

Gambar 158. Langkah *hostspot* 3

4) Geser *slider*, sehingga menjadi *on* pada *Share my Internet connection with other devices*.



Gambar 159. Langkah *hostspot* 4

Glosarium

- *Access point*:
  Sebuah piranti keras yang berfungsi untuk mengubah sinyal digital jaringan menjadi sinyal *analog*, kemudian meneruskannya dan membagi sinyal kepada berbagai piranti keras.
- Alamat IP (*IP Address*):
  Nomor yang digunakan untuk mengindentifikasi komputer, *server* atau alat lain dalam jaringan internal atau *internet* lewat TCP/IP. Terdiri dari serangkaian (empat bagian) angka yang dipisah dengan tanda titik (misalnya 123.123.123.1).
- ARP (*Address Resolution Protocol*):
  Merupakan sebuah protocol yang bertanggung jawab mencari tahu *Mac Address* atau alamat hardware dari suatu Host yang tergabung dalam sebuah jaringan LAN dengan memanfaatkan atau berdasarkan *IP Address* yang terkonfigurasi pada *Host* yang bersangkutan.
- *Bandwith*:
  Lebar jalur data yang dipergunakan untuk mengalirkan paket data yang dikirim dari satu *host* ke *host* lain, biasanya dinyatakan dalam ukuran *bit per second*(bps,Kbps, dan Mbps).
- *Bit*:
  Singkatan *binary* digit, bentuk bilangan biner yang diolah oleh komputer dalam bentuk sinyal digital.
- *Browser*:
  Program komputer untuk menampilkan file atau halaman dari sebuah situs internet. Contoh browser: Mozilla, Firefox, Safari, Opera, Internet Explorer, Konqueror, Lynx, Netscape, dsb.
- DNS (*Domain Name System*):

Servis dalam komputer yang berfungsi menerjemahkan alamat IP menjadi alamat URL atau sebaliknya.

- Dynamic:
  Suatu keadaan yang dapat berubah-ubah, biasanya dipakai dalam penerapan penggunaan IP address.
- *Firewall*:
  Sistem yang berfungsi sebagai pengatur,pengendali keamanan dan sistem transmisi data dalam jaringan. *Firewall* dirancang untuk melewatkan data yang dipercaya, menolak layanan yang mudah diserang, mencegah jaringan internal dari serangan luar yang bisa menembus *firewall* setiap waktu.
- *Gateway*:
  Sebuah perangkat yang digunakan untuk menghubungkan satu jaringan komputer dengan satu atau lebih jaringan komputer yang menggunakan protokol komunikasi yang berbeda sehingga informasi dari satu jaringan komputer dapat diberikan kepada jaringan komputer lain yang protokolnya berbeda.
- IP *Private* adalah Alamat IP yang digunakan untuk jaringan internal (intranet). IP Private tidak bisa diakses dari jaringan internet. Rentang IP yang bisa digunakan untuk jaringan internal adalah: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, dan 192.168.0.0 – 192.168.255.255.
- IP Publik
  IP Publik adalah Alamat IP yang bisa diakses secara publik lewat jaringan global (internet). Supaya nama domain, email dan web anda bisa diakses oleh pengunjung lain di internet, digunakan IP Publik.
  \
- MAC *Address*:
  Alamat unik yang diberikan oleh vendor terhadap produk piranti keras jaringan.

Daftar Pustaka

Asyikin, Arifin Noor. 2018. *Modul Jaringan Komputer*. Banjarmasin: Politeknik Negeri Banjarmasin

Lammle, Todd. 2005. *CCNA: Cisco Certified Network Associate Study Guide*. Jakarta: PT. Elex Media Komputindo

Najwaini, Effan. 2016. *Modul Jaringan Komputer*. Banjarmasin: Politeknik Negeri Banjarmasin

Pratama, I Putu Agus Eka. 2014. *Handbook Jaringan Komputer*. Bandung: Informatika

Sofana, Iwan. 2017. *Cisco CCNA-CCNP Routing dan Switching*. Bandung: Informatika

Towidjojo, Rendra. 2013. *Mikrotik Kungfu: Kitab 1*. Jasakom

Towidjojo, Rendra. 2013. *Mikrotik Kungfu: Kitab 2*. Jasakom

Towidjojo, Rendra. 2013. *Mikrotik Kungfu: Kitab 3*. Jasakom

DASAR-DASAR JARINGAN

WANVY ARIFHA SAPUTRA

Jaringan Komputer merupakan jaringan telekomunikasi yang menghubungan antara komputer satu dengan yang lainnya, minimal 2 buah perangkat. Jaringan komputer membutuhkan Network adapter atau perangkat penghubung komputer seperti Network Interface Card (NIC) / wireless NIC / modem portable. Media koneksinya sebagai medium transmisi data pada jaringan komputer yaitu kabel maupun nirkabel (wireless seperti radio, microwave, satelit dan sebagainya).

Selain perangkat tersebut, diperlukan juga sistem operasi sebagai antar muka antara manusia dan mesin. Sistem operasi yang diperuntukkan khusus jaringan seperti Microsoft windows 2000 server, Microsoft windows NT, Novell netware, Linux dan sebagainya. Untuk menjembatani antara komputer atau perangkat jaringan lainnya membutuhkan peralatan interkoneksi. Peralatan tersebut seperti Hub, Bridge, Switch, Router, dan lainnya.

ISBN 978-623-7694-94-6 (PDF)

ISBN 978-623-7694-93-9

Penerbit Poliban Press
Redaksi :
Politeknik Negeri Banjarmasin, Jl. Brigjen H. Hasan Basry, Pangeran, Komp. Kampus ULM, Banjarmasin Utara
Telp : (0511)3305052
Email : press@poliban.ac.id