EFFAN NAJWAINI

JARINGAN KOMPUTER

JARINGAN KOMPUTER

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).

JARINGAN KOMPUTER

Effan Najwaini

Poliban Press

JARINGAN KOMPUTER

Penulis :
Effan Najwaini

ISBN :
978-623-7694-64-9

ISBN Elektronik :
978-623-7694-65-6 (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

Alhamdulillah penulis panjatkan ke hadirat Allah SWT atas selesainya penulisan buku ajar Jaringan Komputer ini. Buku ajar ini ditulis dengan tujuan untuk membantu para mahasiswa dalam mempelajari mata kuliah Jaringan Komputer. Dengan adanya buku ajar ini diharapkan mahasiswa dapat lebih memahami materi perkuliahan sehingga capaian pembelajaran perkuliahan Jaringan Komputer dapat tercapai.

Buku ajar ini dapat selesai berkat bantuan dari berbagai pihak terutama dari P3M Poliban, Tim Poliban Press serta dosen-dosen jurusan Administrasi Bisnis. Untuk itu penulis menyampaikan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu dalam menyelesaikan buku ajar ini.

Penulis mohon maaf jika dalam penulisan buku ajar ini terdapat kesalahan maupun kekeliruan dalam menyampaikan ide. Untuk itu penulis sangat mengharapkan saran, kritik dan koreksi. Semoga buku ini dapat bermanfaat bagi kita semua.

Banjarmasin, November 2021

Penulis,

Effan Najwaini

DAFTAR ISI

BAB 1
Dasar Jaringan Komputer

Capaian Pembelajaran:

1. Memahami cara kerja jaringan secara umum.
2. Memahami perbedaan model jaringan.

1.1 Pendahuluan Jaringan

Jaringan komputer merupakan sebuah sistem yang terdiri atas komputer/laptop/smartphone atau yang sering disebut sebagai end device serta perangkat jaringan yang saling bekerja sama untuk melakukan pertukaran data. Keuntungan penggunaan jaringan komputer yaitu sebagai berikut.

a. Hardware Sharing

Penggunaan jaringan komputer memungkinkan untuk berbagi penggunaan perangkat keras secara bersama-sama. Sebuah printer dapat digunakan bersama-sama oleh banyak komputer. Begitu pula penggunaan harddisk dapat digunakan secara terpusat oleh banyak komputer.

b. Resource Sharing

Sistem jaringan komputer memungkinkan untuk berbagi data dan informasi termasuk juga berbagi koneksi internet. Sebuah komputer yang terkoneksi ke internet dapat berbagi koneksinya ke dalam jaringan lokal sehingga komputer-komputer lain pada jaringan tersebut dapat mengakses internet juga.

c. Saving Money

Manfaat lainnya yaitu penghematan biaya. Suatu perusahaan atau kantor tidak perlu membeli perangkat printer yang banyak, cukup membeli beberapa dan dihubungkan ke jaringan sehingga dapat digunakan secara bersama.

d. High Reliability

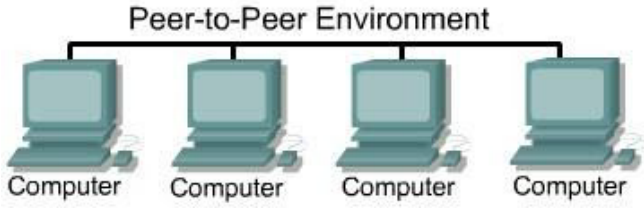
Dengan menggunakan jaringan komputer, dapat meningkatkan reliability dari data. Data yang digunakan dapat disimpan di beberapa komputer yang terhubung dengan jaringan komputer, sehingga jika salah satu komputer rusak, maka salinan data yang lain masih dapat digunakan sebagai cadangan terhadap data aslinya.

1.2 Model Jaringan

Terdapat dua model jaringan yang dapat digunakan dalam sistem jaringan komputer yaitu Peer to Peer (P2P) dan model Client-Server.

a. Peer to Peer

Pada jaringan Peer to Peer, semua komputer berperan setara. Masing-masing komputer dapat memakai atau membagikan resource nya ke komputer lain. Pada model jaringan ini tidak ada sumber daya terpusat, sehingga masing-masing komputer mempunyai kemampuan yang sama untuk memakai sumber daya jaringan. Contoh jaringan Peer to Peer dapat dilihat pada Gambar 1.1.

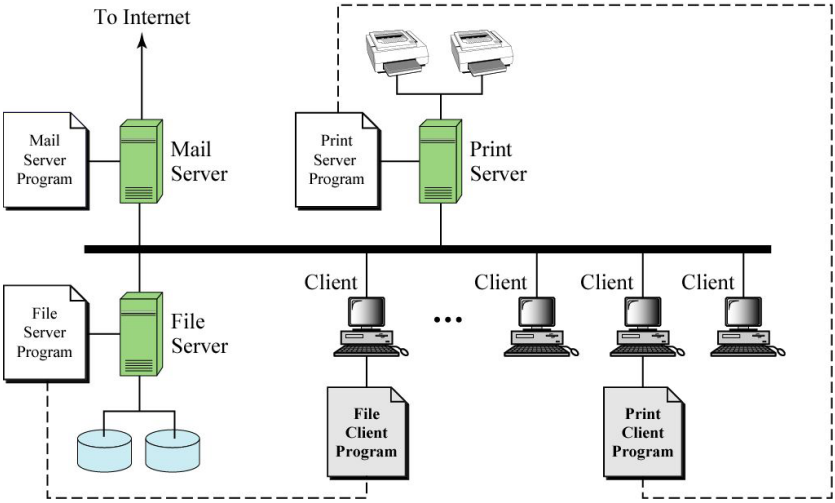


Gambar 1.1 Jaringan Peer to Peer

Sumber Gambar: www.webillian.com

b. Client Server

Model jaringan client server memungkinkan untuk memusatkan fungsi kepada satu atau beberapa komputer. Pada model ini ada komputer yang bertindak sebagai server, yaitu memberikan resource nya kepada komputer lain di jaringan. Server akan melayani permintaan dari komputer lainnya. Setiap server umumnya memiliki fungsi tertentu misal web server, DNS server, File Server dan lainnya. Contoh jaringan Peer to Peer dapat dilihat pada Gambar 1.2.



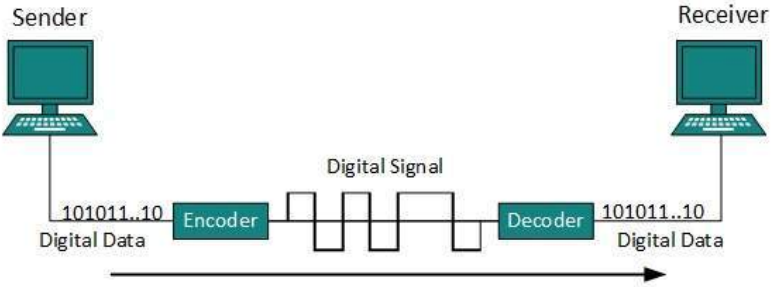
Gambar 1.2 Contoh jaringan client server

Sumber Gambar: www.webillian.com

1.3 Cara Kerja Jaringan Secara Umum

Pada teknologi digital, data disimpan dalam satuan bit (0/1). Semua data baik itu file, gambar, suara, video dikodekan ke dalam nilai binner yang kemudian data ini dapat disimpan maupun dipindahkan ke media lainnya. Pada proses komunikasi data, data berupa nilai bit ini dikirimkan melalui suatu media transmisi. Jika media transmisi yang digunakan merupakan kabel tembaga, maka data tersebut akan disimbolkan menggunakan tegangan dan arus listrik, sedangkan jika menggunakan kabel optik, maka data tersebut disimbolkan menggunakan cahaya. Hal ini mirip seperti penggunaan sandi morse yang mensimbolkan titik dan garis. Gambar 1.3 menunjukkan proses pengiriman data dimana data digital diubah ke dalam sinyal digital melalui proses *line coding*. Sinyal digital tersebut kemudian dikirimkan melalui media transmisi dan diubah kembali menjadi data digital di sisi penerima.

Pada jaringan komputer, proses pengiriman data dari suatu komputer ke komputer lain mirip seperti pengiriman paket melalui ekspedisi. Paket/data yang akan dikirim dibungkus dan diberikan alamat sumber serta alamat tujuan. Paket tersebut kemudian dikirimkan



Gambar 1.3 Proses Pengiriman Data

Sumber Gambar: https://medium.com/@chowdhuryasif

ke perangkat-perangkat jaringan yang akan membaca alamat tujuan dari paket tersebut. Berdasarkan alamat tujuan tersebut setiap perangkat jaringan dapat meneruskan paket tersebut hingga ke tujuannya. Komputer tujuan dapat memberikan balasan dengan membaca alamat Sumber dari paket yang datang. Alamat Sumber tersebut kemudian akan menjadi alamat tujuan dari paket balasan yang dikirimkan.

BAB 2
Pengenalan Jaringan Melalui Simulasi pada Packet Tracer

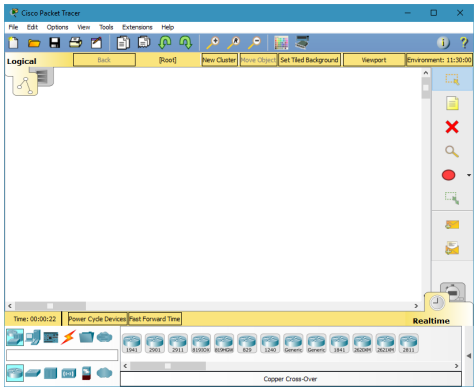
Capaian Pembelajaran:

1. Mampu membuat simulasi jaringan pada Packet Tracer.
2. Mampu menggunakan perangkat jaringan dengan tepat sesuai kebutuhan.
3. Mampu menggunakan mode simulasi untuk memahami ARP dan cara kerja Ethernet.
4. Mampu menggunakan mode simulasi untuk memahami perbedaan Switch dan Hub.

2.1 Simulasi Sederhana Pada Packet Tracer

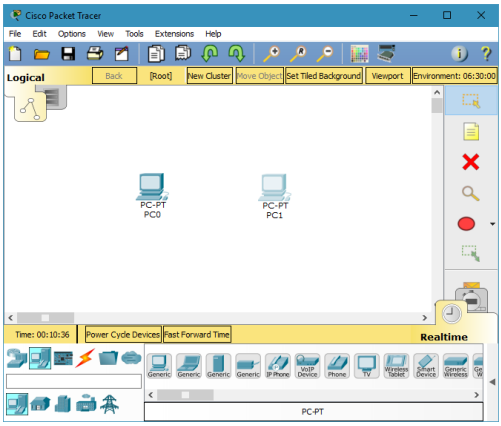
Packet Tracer merupakan *software* simulator yang dibuat oleh perusahaan Cisco System yang bertujuan untuk mensimulasikan jaringan komputer menggunakan perangkat Cisco. Packet Tracer banyak dipakai karena dapat mensimulasikan jaringan nyata yang dapat membantu pemahaman mengenai cara kerja jaringan serta konfigurasi jaringan. Berikut tahapan untuk membuat simulasi sederhana pada Packet Tracer yang menghubungkan dua buah komputer.

1. Jalankan *software* paket tracer sehingga muncul tampilan seperti pada Gambar 2.1.



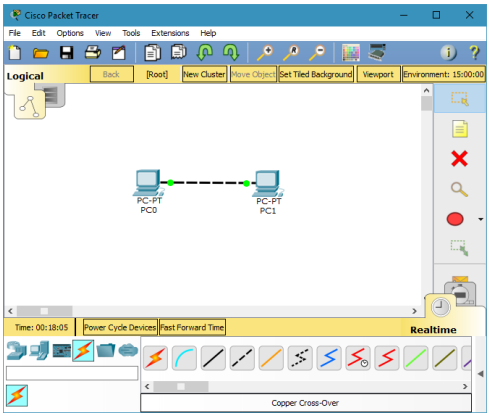
Gambar 2.1 Tampilan Awal Packet Tracer

2. Pada bagian bawah paket tracer terdapat icon-icon perangkat. Pilih End device pada bagian sebelah kiri sehingga muncul gambar perangkat seperti PC, notebook dan lainnya (atau dengan menekan ctrl+alt+v). Pilih PC dan masukkan ke dalam workspace sehingga tampilan seperti pada Gambar 2.2.



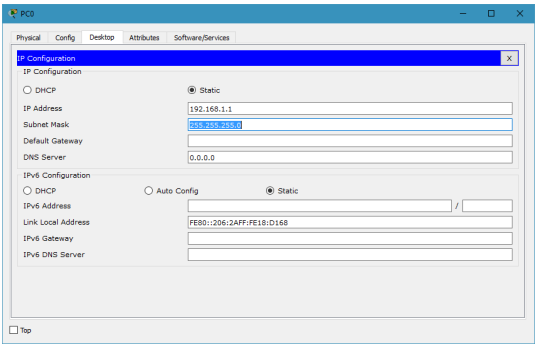
Gambar 2.2 Pemilihan PC

3. Hubungkan kedua PC tersebut dengan memilih bagian Connection atau dengan menekan ctrl+alt+o sehingga muncul gambar-gambar jenis koneksi. Pilih kabel copper cross-over dan kemudian klik pada salah satu PC di workspace sehingga menampilkan pilihan port yang akan dikoneksikan. Pilih FastEthernet0. Kemudian klik pada komputer lainnya dan pilih FastEthernet0 sehingga tampilannya seperti Gambar 2.3.



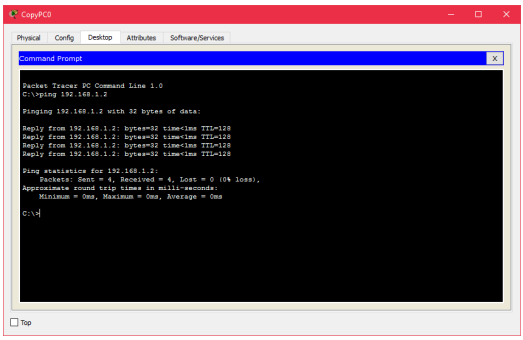
Gambar 2.3 Menyambungkan PC Menggunakan Kabel Cross

4. Klik pada salah satu PC untuk melakukan konfigurasi alamat IP. Konfigurasi IP ada dua cara, pertama bisa masuk ke bagian config pilih FastEthernet0, masukkan alamat IP pada bagian IP Address. Cara kedua yaitu dengan masuk ke tab Desktop (Gambar 2.4) kemudian pilih IP Configuration. Untuk PC pertama masukkan IP Address 192.168.1.1 dengan Subnet Mask 255.255.255.0, sedangkan PC kedua gunakan IP Address 192.168.1.2 dengan Subnet Mask 255.255.255.0



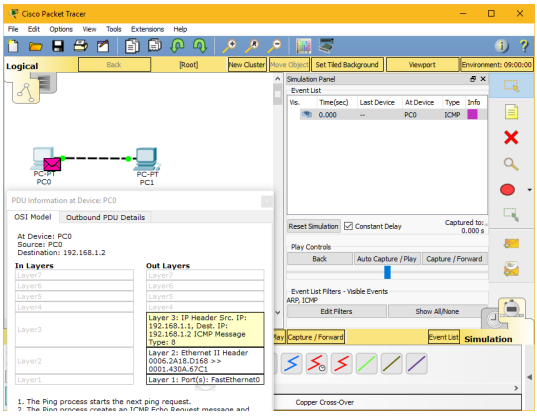
Gambar 2.4 Pemberian Alamat IP

5. Jika kedua PC telah dikonfigurasi, lakukan tes koneksi dengan perintah ping. Klik pada salah satu PC, masuk pada bagian Desktop, pilih Command Prompt kemudian ketik perintah “ping <ip komputer tujuan>” contoh “ping 192.168.1.2”. Jika memunculkan tampilan Reply from 192.168.1.2 seperti pada Gambar 2.5 maka kedua komputer tersebut sudah terhubung melalui jaringan.



Gambar 2.5 Proses Ping

6. Selain mode realtime, pada software ini juga terdapat mode simulation. Pada mode simulation dapat dilihat setiap paket yang beredar di jaringan. Untuk mencoba mode simulation dapat dilakukan dengan langkah sebagai berikut.
   a) Masuk ke mode simulation dengan menekan shortcut shift+s pada keyboard atau dengan memilih mode simulation yang terletak di sebelah kanan bawah.
   b) Jika sudah berada pada mode simulation, maka akan muncul simulation panel. Pada bagian Event List Filters, klik Show All/None kemudian klik Edit Filters, centang ICMP. Pada simulasi yang akan dicoba hanya akan menampilkan paket-paket protocol ICMP.
   c) Sama seperti langkah 5, lakukan ping dari satu PC ke PC lainnya.
   d) Kembali ke workspace, maka akan muncul gambar amplop yang menunjukkan paket dengan protocol ICMP hendak dikirim. Untuk menjalankan simulasi dapat dilakukan dengan menekan tombol Capture/Forward atau Auto Capture/Play.
   e) Pada mode simulasi terlihat paket-paket yang dikirim dari satu PC ke PC lainnya. Isi dari paket tersebut juga dapat dilihat dengan mengklik gambar amplop atau warna pada kolom info di bagian Event List. Tampilan mode simulasi dapat dilihat pada Gambar 2.6.



Gambar 2.6 Mode Simulasi

2.2 Memahami Konsep ARP (Address Resolution Protocol)

Address Resulution Protocol (ARP) merupakan sebuah protokol yang bertanggung jawab mencari alamat MAC Address dari suatu host. Pada jaringan LAN (Local Area Network) yang terhubung menggunakan perangkat layer 1 dan 2 (Switch, HUB, repeater, Access Point) setiap host saling berkomunikasi dengan menggunakan alamat MAC sehingga ketika akan mengirimkan data, setiap host harus mengetahui alamat MAC tujuannya. Ketika paket akan dikirimkan ke tujuan, paket tersebut akan diberikan alamat IP sumber dan tujuan (layer 3) setelah itu baru kemudian diberikan alamat MAC sumber dan tujuan (layer 2). Jika komputer yang ingin mengirimkan pesan tersebut belum mengetahui alamat MAC dari tujuannya, maka komputer tersebut terlebih dahulu mencari alamat MAC tersebut berdasarkan alamat IP. Caranya yaitu dengan mengirimkan satu paket ARP yang sifatnya broadcast ke seluruh host yang ada di jaringan tersebut. Paket broadcast ini akan diteruskan oleh perangkat layer 1 dan 2 ke seluruh host. Komputer yang menerima paket ARP yang sesuai dengan alamat IP yang dicari selanjutnya akan membalas paket ARP tersebut, sehingga komputer yang akan mengirimkan pesan mengetahui alamat MAC komputer tujuannya.

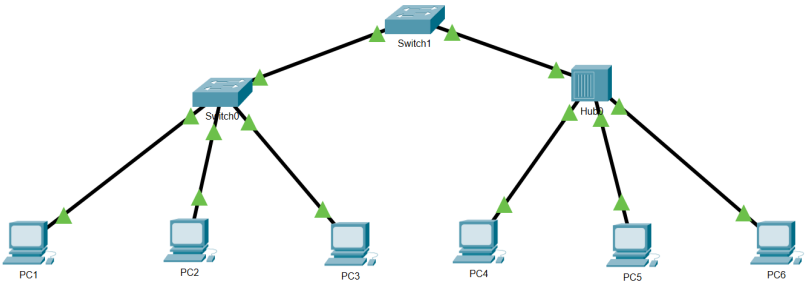
Konsep ARP ini sering dianalogikan dengan nama dan bentuk fisik muka seseorang. Nama dianalogikan sebagai alamat IP, sedangkan fisik muka dianalogikan sebagai alamat MAC. Misal dalam suatu ruangan kelas yang terdiri dari 30 siswa dan seorang guru, pada saat pertama kali masuk kelas guru tidak mengenal satupun siswanya. Guru memiliki daftar nama siswa tetapi tidak mengetahui fisik muka siswanya. Sang guru kemudian ingin bertanya ke seseorang yang bernama Budi (analogi guru ingin mengirim pesan ke Budi). Jika guru tersebut hanya mengetahui nama tanpa mengetahui yang mana dari 30 siswanya yang bernama Budi, maka guru tersebut tidak bisa bertanya langsung ke Budi. Guru tersebut harus memanggil nama Budi di depan kelas agar terdengar oleh seluruh siswa (mengirim paket broadcast). Dari 30 siswa tersebut hanya 1 orang yang menjawab panggilan guru yaitu si Budi,

siswa yang lain hanya mendengar panggilan tersebut tanpa menjawab. Setelah si Budi menjawab, maka Guru sudah mengetahui fisik muka dari siswa yang bernama Budi. Jika kemudian siswa ingin bertanya atau mengirim pesan langsung ke Budi maka Guru tidak perlu lagi memanggil di depan kelas, karena sudah mengetahui fisik dari Budi. Konsep inilah yang digunakan pengiriman data pada jaringan LAN (layer 2). Gambar 2.7 menunjukkan analogi ARP dengan lingkungan kelas.

Gambar 2.7 Gambar Analogi ARP

Sumber Gambar: http://unycommunity.com/

Untuk mempraktekkan konsep ARP pada jaringan menggunakan Packet Tracer dapat dilakukan dengan membuat jaringan sederhana layer 1 dan 2 dengan perangkat switch atau hub. Contoh jaringan yang dapat dibuat dapat dilihat pada Gambar 2.8.



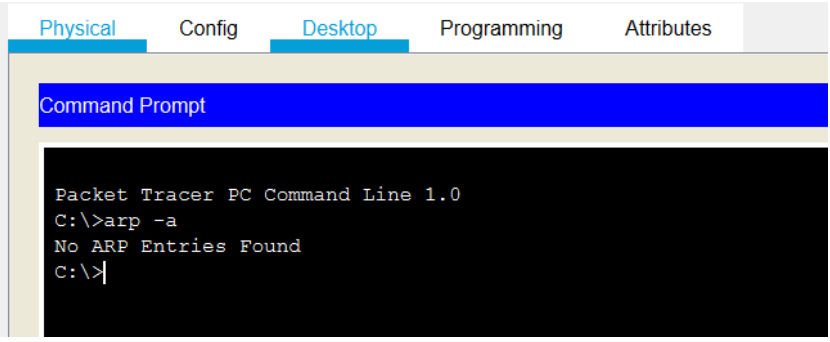
Gambar 2.8 Topologi simulasi ARP

Buatlah topologi seperti gambar diatas dengan alamat IP untuk masing-masing PC yaitu:

- PC 1: IP Address 192.168.1.1 Subnetmask 255.255.255.0
- PC 2: IP Address 192.168.1.2 Subnetmask 255.255.255.0
- PC 3: IP Address 192.168.1.3 Subnetmask 255.255.255.0

- PC 4: IP Address 192.168.1.4 Subnetmask 255.255.255.0
- PC 5: IP Address 192.168.1.5 Subnetmask 255.255.255.0
- PC 6: IP Address 192.168.1.6 Subnetmask 255.255.255.0

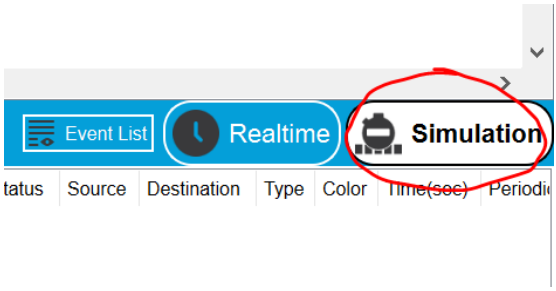
Untuk melihat daftar alamat MAC yang diketahui oleh tiap komputer dapat dilakukan melalui command prompt pada masing-masing PC dengan perintah 'arp -a'. Jika ada tulisan No ARP Entries Found seperti pada Gambar 2.9 berarti belum ada alamat MAC yang dikenali oleh komputer tersebut.



Gambar 2.9 Tabel ARP pada PC1

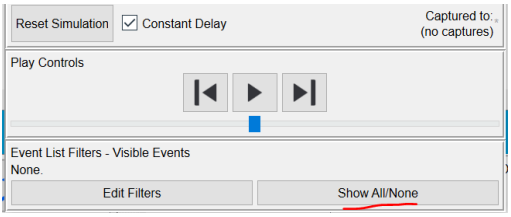
Untuk melihat cara kerja ARP dapat dilakukan dengan langkah berikut:

1. Masuk ke mode simulasi seperti pada Gambar 2.10.



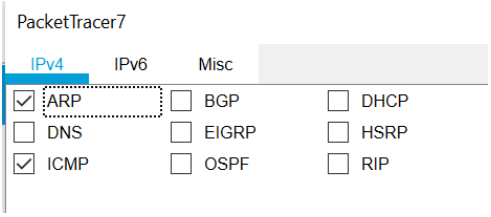
Gambar 2.10 Proses Masuk ke Mode Simulasi

2. Klik Show All / None untuk mematikan semua protocol filter sehingga pada Event List Filters tertulis None yang dapat dilihat pada Gambar 2.11.



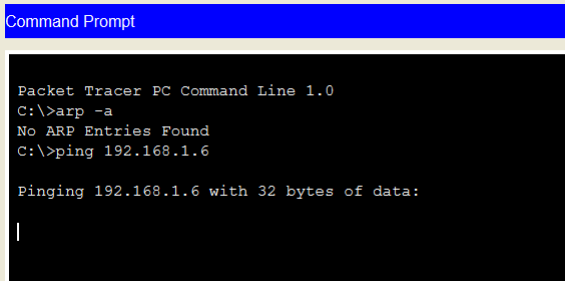
Gambar 2.11 Mematikan Semua Protokol

3. Klik Edit Filters, aktifkan ARP dan ICMP seperti terlihat pada Gambar 2.12.



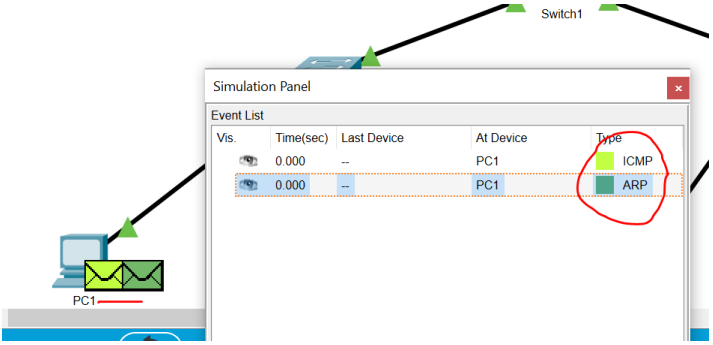
Gambar 2.12 Memilih Protokol ARP dan ICMP untuk Simulasi

4. Setelah itu lakukan Ping dari komputer PC1 ke PC6. Proses ping dapat dilihat pada Gambar 2.13.



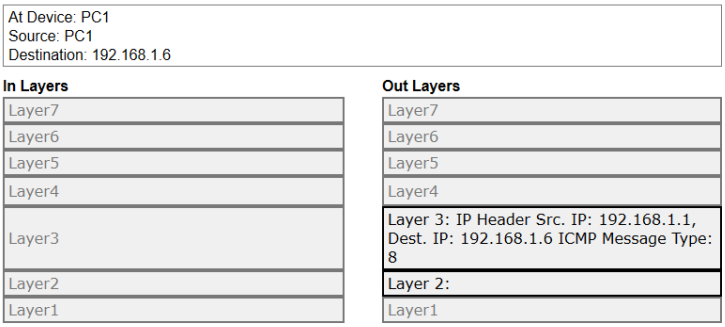
Gambar 2.13 Proses Ping dari PC1 ke PC6

5. Karena masuk di dalam folder simulasi, proses ping tidak berlanjut hingga ditekan tombol play atau forward pada simulation panel. Pada simulation panel dan workspace (Gambar 2.14) terlihat ada dua paket yang akan dikirimkan oleh PC 1, yaitu paket ICMP dan ARP.



Gambar 2.14 Paket ARP sebelum ICMP dikirim

6. Jika diklik paket ICMP maka akan terlihat pada bagian Out Layers (atau paket yang akan keluar) pada bagian layer 3 sudah terdapat IP address Sumber Gambar dan tujuan. Tetapi pada layer 2 belum ada MAC address sumber dan tujuan. Hal ini karena PC 1 belum mengetahui alamat fisik (MAC) dari PC 6 sehingga belum bisa menuliskan alamat MAC tersebut di paket ICMP nya. PC 1 perlu mengirimkan paket ARP terlebih dahulu agar mengetahui alamat MAC PC 6. Isi paket ICMP dapat dilihat pada Gambar 2.15.

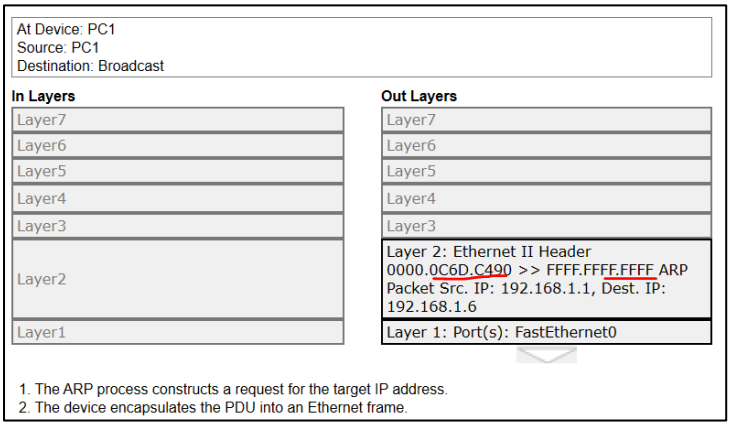


Gambar 2.15 Isi Paket ICMP

7. Jika paket ARP di klik maka akan terlihat alamat MAC sumber yaitu MAC PC 1 (C490) dan alamat MAC tujuan (FFFF). Tujuan FFFF berarti paket yang dikirim tersebut bertujuan ke seluruh host yang ada di jaringan. Jika perangkat switch menerima paket dengan tujuan FFFF maka akan meneruskan ke seluruh port yang aktif

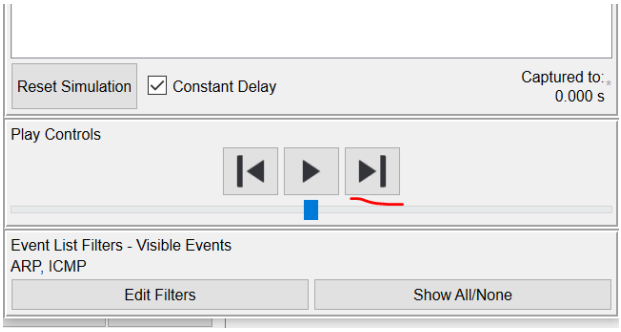
selain port sumbernya. Dest IP pada layer 2 berarti paket tersebut merupakan paket ARP dengan maksud mencari alamat MAC dari komputer dengan alamat IP 192.168.1.6. Isi paket ARP dapat dilihat pada Gambar 2.16

Catatan: Nilai MAC Address dapat berbeda-beda, belum tentu sama seperti contoh.



Gambar 2.16 Isi Paket ARP

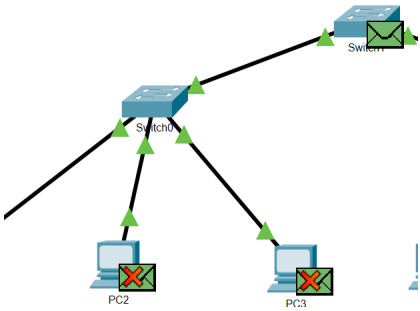
8. Untuk melihat proses selanjutnya dapat dilakukan dengan menekan tombol forward seperti pada Gambar 2.17.



Gambar 2.17 Tombol Forward simulasi

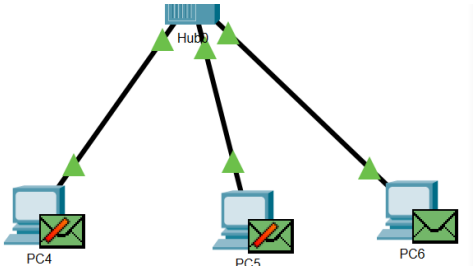
9. Proses selanjutnya yaitu paket ARP dari PC1 akan dikirimkan ke switch 0. Switch 0 yang menerima paket dengan alamat MAC tujuan FFFF maka akan meneruskan paket tersebut ke semua port yang aktif di switch tersebut sehingga meneruskan juga ke PC2, PC3 dan

Switch 1. PC2 dan PC3 menerima paket ARP tersebut, tetapi tidak memprosesnya karena paket tersebut ditujukan untuk alamat IP 192.168.1.6. Gambar 2.18 menunjukkan paket ARP pada PC2 dan PC3.



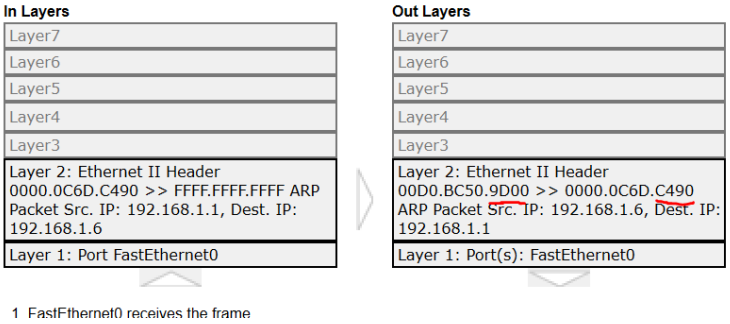
Gambar 2.18 Paket ARP di PC2 dan PC3

10. Switch1 meneruskan kembali paket tersebut ke Hub0 dan selanjutnya diteruskan ke PC4, PC5, dan PC6. Sama seperti PC2 dan PC3, PC4 dan PC5 tidak memproses paket tersebut seperti pada Gambar 2.19. Sedangkan PC6 memproses paket tersebut dan menyiapkan paket balasannya.



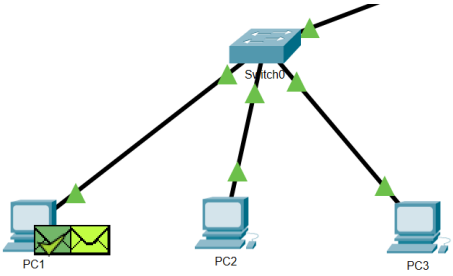
Gambar 2.19 Paket ARP di PC4, PC5 dan PC6

11. Jika paket yang sampai di PC6 di klik, maka akan terlihat pada bagian In Layers sama persis seperti Out Layers dari PC1 sebelumnya seperti pada Gambar 2.20. Pada bagian Out Layers merupakan paket balasan dari PC6 ke PC1 dimana pada Layers 2 MAC Address sumber (9D00) merupakan MAC Address PC6 dan MAC Address tujuan (C490) merupakan MAC Address PC1 yang didapat dari paket ARP yang diterima.



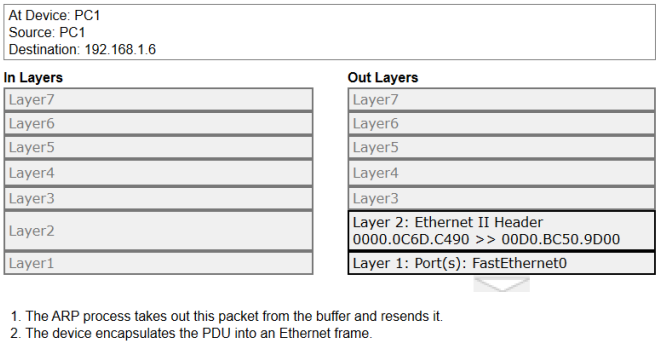
Gambar 2.20 Isi Paket ARP di PC6

12. Selanjutnya paket balasan dikirimkan ke PC1 melalui HUB0, Switch1 dan Switch0. Switch 1 dan Switch 0 tidak meneruskan paket tersebut ke seluruh port, tetapi hanya ke port tujuan saja. Hal ini dikarenakan alamat MAC address tujuan sudah jelas, bukan FFFF lagi.



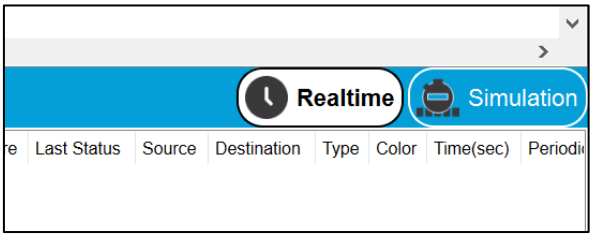
Gambar 2.21 Paket ICMP dapat Dikirim Setelah PC 1 Mendapat Balasan ARP

13. Ketika sampai di PC1, PC1 kemudian membaca paket ARP tersebut dan dapat mengetahui alamat MAC Address dari PC6 sehingga paket ICMP yang sebelumnya belum dapat dikirim karena belum ada alamat MAC tujuan sudah dapat dikirim seperti terlihat pada Gambar 2.21. Jika diklik paket ICMP maka akan terlihat seperti Gambar 2.22.

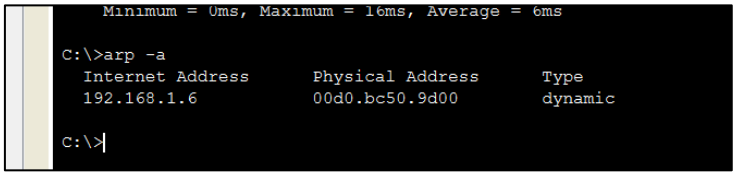


Gambar 2.22 Isi Paket ICMP setelah ARP

14. Pada Out Layers paket ICMP terlihat paket dikirim dari MAC C490 (PC1) ke 9D00 (PC6). Paket yang dikirim dari PC1 diteruskan ke Switch0 dan Switch1 langsung ke port tujuan tanpa broadcast ke semua port. Pada proses selanjutnya pengiriman dari PC1 ke PC6 sudah dapat dilakukan langsung tanpa adanya pengiriman paket ICMP terlebih dahulu lagi. Pada Command Prompt di PC1 dapat terlihat ARP tabel yang memetakan IP Address PC 6 (192.168.1.6) ke MAC Address PC6 (9D00) seperti terlihat pada Gambar 2.24. Untuk melihat tabel ARP dapat dilakukan dengan masuk ke mode Realtime (Gambar 2.23) terlebih dahulu agar proses Ping sebelumnya bisa selesai.

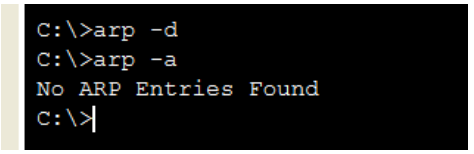


Gambar 2.23 Masuk ke mode Realtime



Gambar 2.24 Tabel ARP dari PC1

15. Proses pengiriman paket dari PC1 ke PC6 maupun sebaliknya tanpa melalui proses ARP lagi, karena MAC address tujuan sudah dapat dilihat melalui ARP tabel. Jika PC tersebut di restart maka tabel ARP yang sudah tersimpan sebelumnya menjadi hilang sehingga perlu dilakukan proses ARP lagi untuk pengiriman paket. Untuk menghilangkan tabel ARP juga bisa dilakukan dengan perintah 'arp -d' seperti pada Gambar 2.25. Setelah perintah tersebut dimasukkan maka tabel ARP menjadi kosong kembali.



Gambar 2.25 Menghapus Table ARP

2.3 Perbedaan Switch dan Hub

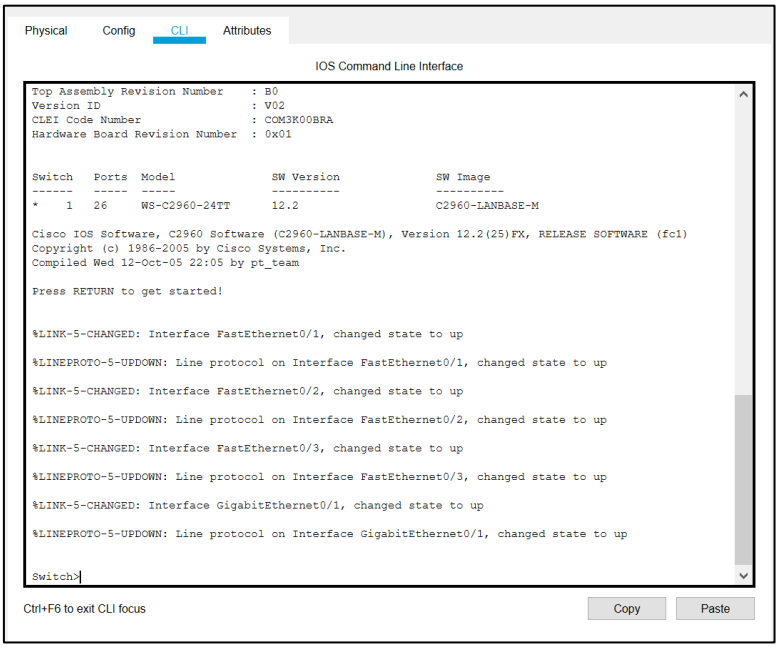
Switch dan Hub memiliki perbedaan dari cara menangani paket yang masuk untuk diteruskan ke port tujuan. Switch dan Hub sama-sama membuat topologi Star secara fisik. Dalam penanganan paket, Hub memiliki cara meneruskan paket seperti pada topologi bus, dimana paket yang dikirimkan akan diteruskan ke semua port lainnya. Hub memiliki kerja pada layer 1, dimana pada layer ini hanya berfungsi sebagai penerus sinyal yang diterima. Switch bekerja pada layer 2, dimana pada layer ini terdapat informasi MAC address sumber dan tujuan dari paket tersebut. Karena switch bekerja di layer 2, maka switch meneruskan paketnya berdasarkan MAC Address tujuan, sehingga jika alamat MAC address tujuan diketahui berada di port mana, switch tidak melakukan broadcast (mengirim ke semua port) dalam mengirim paketnya.

Switch memiliki MAC Address tabel yang memetakan alamat MAC tertentu berada di port mana dari switch tersebut. Tabel ini dibentuk dengan mempelajari setiap paket yang melewati switch. Jika MAC Address tujuan tidak ada di dalam MAC Address tabel, maka switch akan melakukan broadcast terhadap paket tersebut, tetapi jika sudah ada

di dalam MAC Address tabel, maka switch dapat langsung mengirimkan ke port tujuannya tanpa broadcast. Switch juga akan tetap melakukan broadcast jika paket yang dikirimkan dengan tujuan MAC FFFF.FFFF.FFFF.FFFF seperti pada paket ARP.

Untuk melakukan simulasi perbedaan switch dan hub bisa dilakukan dengan cara berikut:

1. Buat topologi seperti pada latihan sebelumnya dengan alamat IP PC yang sama seperti pada Gambar 2.8.
2. Masuk ke CLI switch0 dengan mengklik Switch tersebut dan masuk ke tab CLI, kemudian tekan enter. Tampilan CLI dapat terlihat pada Gambar 2.26.



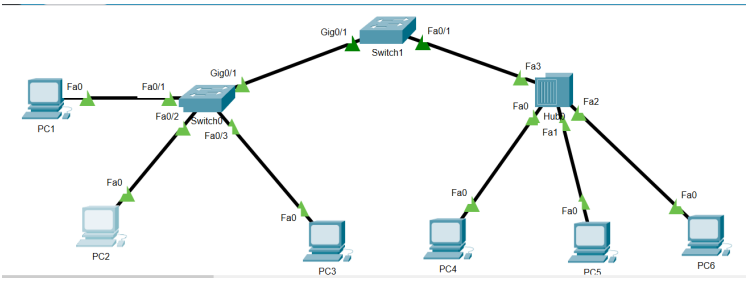
Gambar 2.26 CLI pada Switch0

3. Ketikan perintah ‘show mac-address-table’ untuk melihat MAC Address Table di Switch 0 sepert pada Gambar 2.27. Switch akan mempelajari paket yang lewat sehingga terbentuk tabel yang memetakan antara MAC Address dan Port lokasi MAC address tersebut.

```
Switch>show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0000.0c6d.c490    DYNAMIC     Fa0/1
   1    0090.21e3.3a19    DYNAMIC     Gig0/1
   1    00d0.bc50.9d00    DYNAMIC     Gig0/1
Switch>
```

Gambar 2.27 MAC Address Tabel Pada Switch0

4. Pada Gambar 2.27, Switch mempelajari bahwa MAC Address 9D00 (PC6) ada di port G0/1 dan C490 (PC1) ada di Port Fa0/1 dari switch0. MAC 3A19 merupakan MAC dari Switch1 yang juga berada pada port G0/1 dari switch0. Port pada setiap switch dapat dilihat pada Gambar 2.28.



Gambar 2.28 Port pada Switch

5. Selanjutnya coba lakukan Ping dari PC1 ke PC5 (192.168.1.5), setelah ping dilakukan cek kembali MAC Address Tabel pada Switch0. Setelah dilakukan ping, maka MAC Address Tabel pada Switch0 menjadi seperti pada Gambar 2.29.

```
Switch>show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0000.0c6d.c490    DYNAMIC     Fa0/1
   1    0060.476b.033a    DYNAMIC     Gig0/1
   1    0090.21e3.3a19    DYNAMIC     Gig0/1
   1    00d0.bc50.9d00    DYNAMIC     Gig0/1
Switch>
```

Gambar 2.29 MAC Address Tabel Setelah Ping PC5

6. Pada Gambar 2.29, terlihat terdapat penambahan MAC Address 033A yang mana merupakan MAC Address dari PC5. MAC Address PC5 berada diarah port Gig0/1 sehingga jika ada paket dengan tujuan MAC tersebut, Switch akan langsung mengirimkan ke port Gig0/1.

Dari simulasi diatas, mungkin akan timbul pertanyaan dari manakah Switch0 bisa mendapatkan alamat MAC PC5 yang sebelumnya tidak ada di MAC Address Tabel Switch0? Ketika PC1 akan melakukan Ping ke PC5, PC1 harus mengetahui alamat MAC PC5 terlebih dahulu, jika belum maka PC1 harus mengirimkan ARP ke jaringan yang nanti akan dibalas oleh PC5. Ketika PC5 membalas paket ARP dari PC1, Switch0 akan mempelajari paket tersebut dan menyimpan informasi *source* MAC Address yang ada di dalam paket tersebut ke dalam memory nya dan disesuaikan dengan asal paket tersebut masuk ke Switch0. Paket jawaban ARP dari PC5 pasti akan masuk ke Switch0 melalui port Gig0/1.

Sama seperti ARP Tabel pada PC, MAC Address Tabel pada Switch0 juga akan hilang begitu Switch nya restart. Bagaimana jika PC5 yang sudah mengetahui alamat MAC PC1, sedangkan Switch baru saja restart, sehingga MAC Address tabel nya hilang? Untuk kasus tersebut dapat kita simulasikan dengan langkah sebagai berikut:

1. Pastikan PC5 sudah memiliki alamat MAC dari PC1 dengan melihat menggunakan perintah ‘arp -a’ pada PC5. Jika sudah ada akan terlihat seperti Gambar 2.30. Jika belum maka lakukan ping terlebih dahulu ke PC1. Pastikan ping dilakukan pada mode realtime.

```
Packet Tracer PC Command Line 1.0
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.1           0000.0c6d.c490        dynamic
```

Gambar 2.30 MAC Address PC1 yang tersimpan di PC5

2. Langkah berikutnya yaitu restart switch0 dengan memasukkan perintah enable dan reload pada CLI. Tekan enter jika ada konfirmasi seperti Gambar 2.31.

```
Switch>enable
Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 00D0.BCA5.996E
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
```

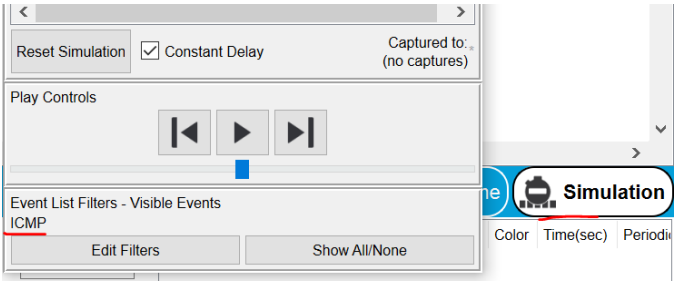
Gambar 2.31 Restart Switch0

3. Setelah restart, pastikan kembali tidak ada MAC Address PC1 pada MAC Address Tabel Switch0 dengan perintah ‘show mac-address-table’ seperti pada Gambar 2.32.

```
Switch>show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0090.21e3.3a19    DYNAMIC     Gig0/1
Switch>
```

Gambar 2.32 MAC Address Tabel Switch0 setelah restart

4. Masuk ke mode simulasi untuk memulai proses simulasi dan melihat cara switch0 meneruskan paket. Aktifkan hanya protokol ICMP pada Event List Filter sehingga terlihat seperti Gambar 2.33.



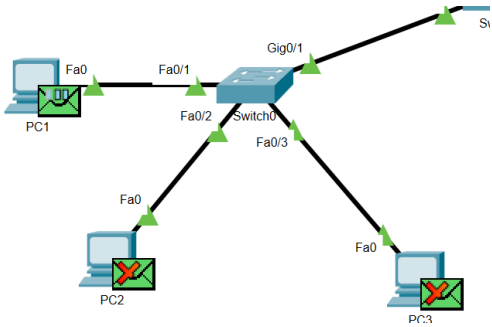
Gambar 2.33 Mode Simulasi

5. Tetap di mode simulasi, lakukan ping dari PC5 ke PC1 (192.168.1.1) seperti Gambar 2.34, sehingga pada workspace dan event list terdapat paket ICMP yang keluar dari PC5.

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
```

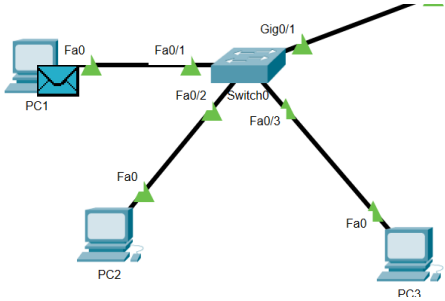
Gambar 2.34 Ping PC1

6. Klik tombol forward sehingga paket berpindah dari PC5 ke Hub0, selanjutnya ke switch1 dan kemudian ke switch0. Setelah sampai di Switch0, Switch0 akan melihat alamat MAC tujuan dan mencocokkannya pada MAC Address tabel yang ada. Karena pada MAC Address Tabel tidak terdapat alamat MAC Address tujuan (PC1) maka switch0 akan membroadcast paket yang diterima ke seluruh port yang aktif seperti pada Gambar 2.35, kecuali port asal sehingga perilakunya mirip dengan Hub.



Gambar 2.35 Broadcast Switch0

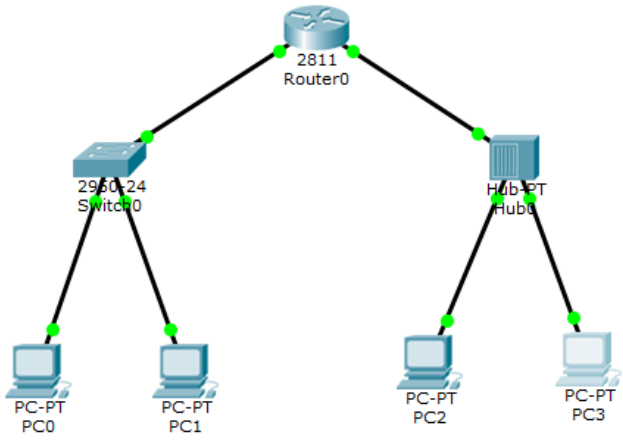
7. Tetapi pada paket ping berikutnya, switch0 sudah memiliki informasi port lokasi dari PC1 sehingga paket berikutnya switch0 tidak melakukan broadcast lagi seperti pada Gambar 2.36.



Gambar 2.36 Paket Ping Berikutnya dari PC5

2.4 Tugas

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 sehingga jaringannya seperti terlihat pada Gambar 2.37.



Gambar 2.37 Tugas BAB 2

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

1. 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.
   a. Apa itu ARP dan gunanya untuk apa?
   b. Apa gunanya perintah arp -a?
   c. Kenapa pada saat ping pertama muncul paket ARP diawal sedangkan pada saat ping kedua tidak muncul paket ARP?
2. 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?
3. Jika PC1 diganti IP Address nya menjadi 192.168.3.2, Bisakah PC0 terhubung ke PC1 (tes dengan perintah ping)? Kenapa?
4. 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).
5. 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 3
Pengkabelan Twisted Pair

Capaian Pembelajaran:

1. Memahami fungsi lilitan, dan shielded serta warna dalam kabel twisted pair
2. Memahami konsep MDI dan MDIX (pin transmit dan receive)
3. Memahami perbedaan kabel straight, cross dan roll over
4. Mampu membuat kabel straight atau cross.

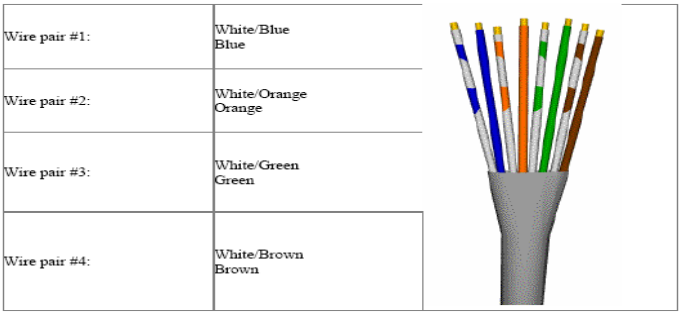
3.1 Mengenal Kabel Twisted Pair

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 kabel TP 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. Untuk lebih jelasnya dapat dilihat pada Gambar 3.1.

Lilitan pada kabel TP mempunyai fungsi yaitu untuk mengurangi gangguan atau interferensi gelombang elektromagnetik yang diakibatkan oleh adanya aliran listrik di kabel yang lain. Adanya aliran listrik yang mengalir di kabel akan menyebabkan munculnya gelombang elektromagnetik disekitarnya. Gelombang elektromagnetik ini dapat mengakibatkan munculnya arus listrik di kabel lainnya sehingga seolah-olah ada loncatan aliran listri ke kabel lain. Loncatan

aliran listrik ini disebut dengan cross-talk yang akan mengganggu komunikasi data yang mengalir di kabel tersebut.

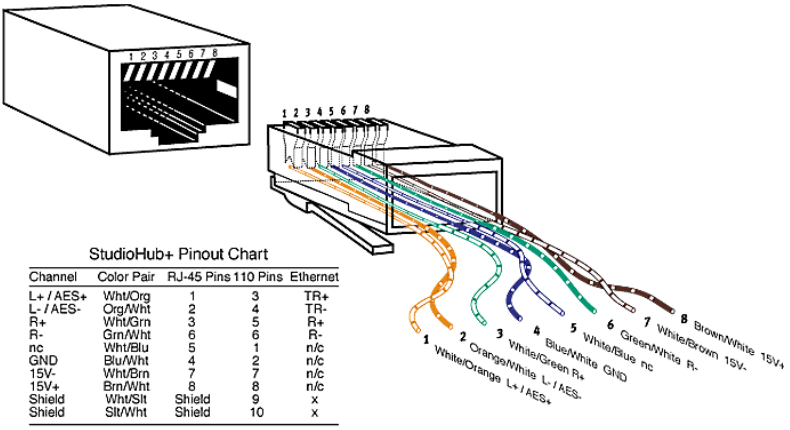


Gambar 3.1 Gambar Kabel Twisted Pair

Sumber Gambar: https://stephel.tilobert.ru/

3.2 Konsep MDI dan MDI-X

Pada NIC atau port di perangkat jaringan (switch/hub/router) terdapat 8 pin yang setiap pin nya akan terhubung ke kabel melalui konektor RJ-45. Masing-masing Pin memiliki fungsi yang berbeda, tetapi umumnya untuk komunikasi data digunakan 4 Pin yaitu 2 pin untuk transmit (mengirim data) dan 2 pin untuk receive (menerima data). Fungsi setiap pin pada NIC dapat dilihat pada Gambar 3.2.



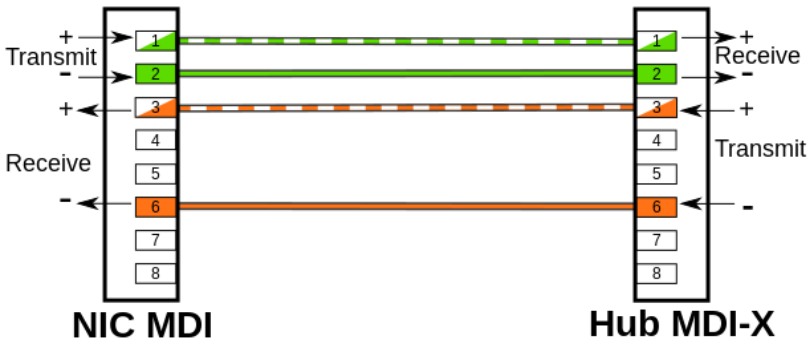
StudioHub+ Pinout Chart

Channel	Color Pair	RJ-45 Pins	110 Pins	Ethernet
L+ / AES+	Wht/Org	1	3	TR+
L- / AES-	Org/Wht	2	4	TR-
R+	Wht/Grn	3	5	R+
R-	Grn/Wht	6	6	R-
nc	Wht/Blu	5	1	n/c
GND	Blu/Wht	4	2	n/c
15V-	Wht/Brn	7	7	n/c
15V+	Brn/Wht	8	8	n/c
Shield	Wht/Slt	Shield	9	x
Shield	Slt/Wht	Shield	10	x

Gambar 3.2 Pinout pada NIC

Sumber Gambar: https://www.electronicshub.org/types-of-computer-ports/

Ada dua tipe Pinout yang berbeda yang digunakan pada perangkat jaringan yaitu MDI (Medium Dependent Interface) dan MDI-X (Medium Dependent Interface Crossover). MDI biasa digunakan pada end device (perangkat akhir) misal komputer atau printer, sedangkan MDI-X biasa digunakan pada perangkat Switch dan Hub. Pada pinout MDI, pin nomor 1 dan 2 berfungsi sebagai transmit, sedangkan pin 3 dan 6 berfungsi untuk receive. Sebaliknya, pada MDI-X, Pin 1 dan 2 berfungsi sebagai receive dan pin 3 dan 6 berfungsi sebagai transmit.



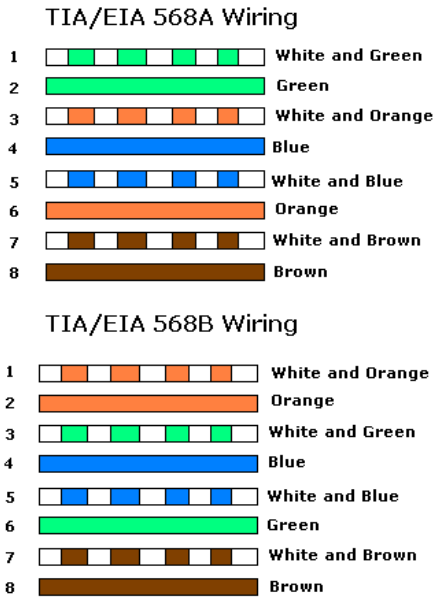
Gambar 3.3 Pinout MDI dan MDI-X

Sumber Gambar : https://en.wikipedia.org/wiki/Medium-dependent_interface

Untuk menghubungkan dua interface jaringan, perlu menghubungkan pin yang berfungsi sebagai transmit ke pin yang berfungsi sebagai receive dari perangkat lainnya, begitu juga sebaliknya. Jika ingin menghubungkan perangkat yang bertipe MDI dengan perangkat MDI-X maka perlu menghubungkan pin 1 dan 2 MDI yang berfungsi sebagai transmit (pengirim) dengan pin 1 dan 2 MDI-X yang berfungsi sebagai receive (penerima) serta pin 3 dan 6 MDI yang berfungsi sebagai receive dengan 3 dan 6 MDI-X yang berfungsi sebagai transmit. Sehingga untuk menghubungkan MDI ke MDI-X perlu menggunakan kabel lurus (straight), dimana akan menghubungkan pin 1-8 dari satu sisi ke pin 1-8 sisi lainnya seperti pada Gambar 3.3.

3.3 Perbedaan Kabel Straight, Cross dan Roll Over

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*. Urutan warna pemasangan kabel TP dapat dilihat pada Gambar 3.4.



Gambar 3.4 Urutan Warna Kabel TP

Sumber Gambar: https://zho.amuddycup.com/

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.

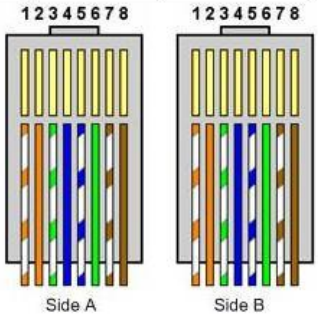
1. Straight Through Cable

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. Gambar 3.5 menunjukkan sambungan kabel Straight.

2. Cross Over Cable

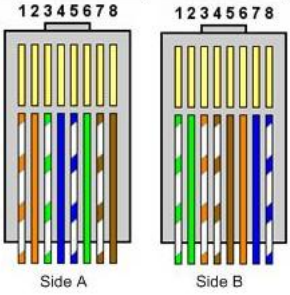
Kabel Cross Over digunakan untuk menghubungkan PC ke PC atau Hub/Switch ke Hub/Switch. Untuk membuat kabel Cross, ujung satu menggunakan urutan 568B dan ujung satunya menggunakan urutan 568A. Kabel Cross akan menghubungkan pin 1 ke pin 3 dan pin 2 ke pin 6. Untuk lebih jelasnya dapat melihat Gambar 3.6 dan Gambar 3.7.

Pin ID	Side A	Side B
1	Orange-white	Orange-white
2	Orange	Orange
3	Green-white	Green-white
4	Blue	Blue
5	Blue-white	Blue-white
6	Green	Green
7	Brown-white	Brown-white
8	Brown	Brown



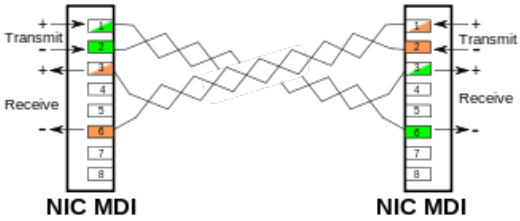
Gambar 3.5 Urutan Warna kabel Straight

Pin ID	side A	side B
1	Orange-white	green-white
2	Orange	green
3	green-white	orange-white
4	blue	brown-white
5	blue-white	Brown
6	green	orange
7	brown-white	Blue
8	brown	blue-white



Gambar 3.6 Urutan Warna Kabel Cross Over

Sumber Gambar: https://www.home-network-help.com/

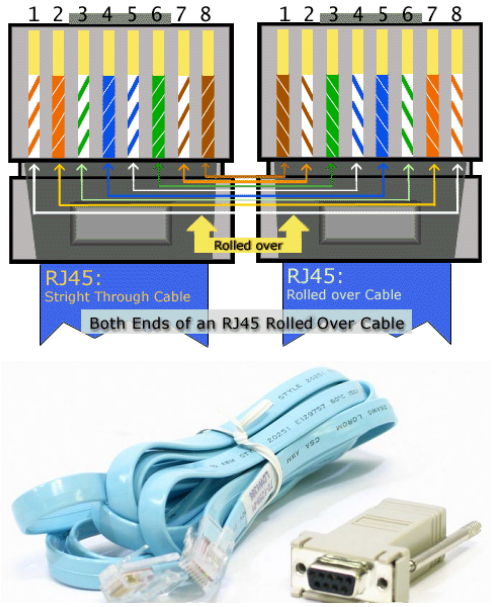


Gambar 3.7 Penggunaan Kabel Cross Over

Sumber Gambar : https://en.wikipedia.org/wiki/Medium-dependent_interface

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 3.8.



Gambar 3.8 Kabel Roll Over untuk Console Cisco

Sumber Gambar: https://www.ciscozine.com/ dan https://blog.router-switch.com/

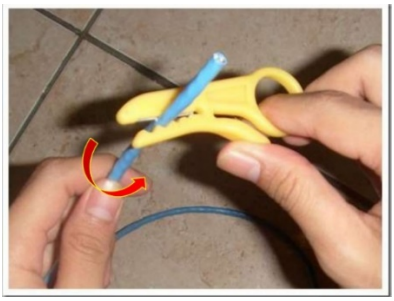
3.4 Pemasangan Konektor RJ 45 ke Kabel UTP

Untuk memasang konektor pada kabel UTP/STP diperlukan alat yang bernama *crimping tool* atau sering juga disebut dengan tang crimping (Gambar 3.9).

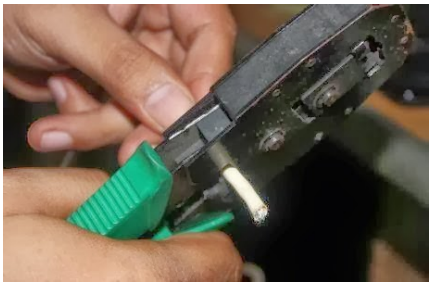
Gambar 3.9 Tang Crimping

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

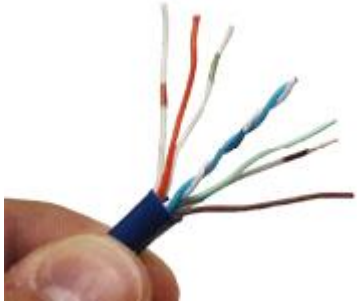
1. Kupas pelindung luar dari kabel, sehingga terlihat 8 serat kabel. Untuk mengupas kabel dapat memanfaatkan alat bantu pengupas kabel (Gambar 3.10), atau dengan menggunakan tang crimping (Gambar 3.11). Umumnya pada tang crimping terdapat lekukan setengah lingkaran seukuran kabel, disertai dengan pisau. Ketika kabel diletakan pada tempat tersebut, rapatkan tang sehingga pisau menggores luaran kabel, putar kabel atau tang nya sehingga membuat goresan di sekeliling kabel. Setelah pelindung luar kabel dikupas, terlihat 8 serat kabel seperti pada Gambar 3.12.



Gambar 3.10 Mengupas kabel dengan alat khusus pengupas

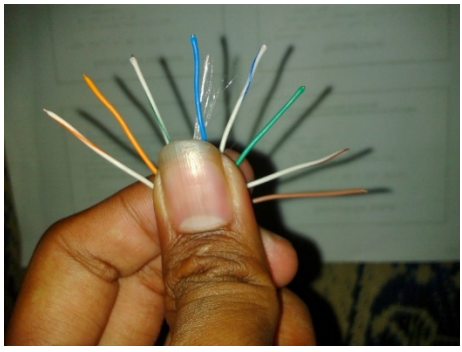


Gambar 3.11 Mengupas kabel dengan tang krimping



Gambar 3.12 Kabel setelah dikupas bagian luar

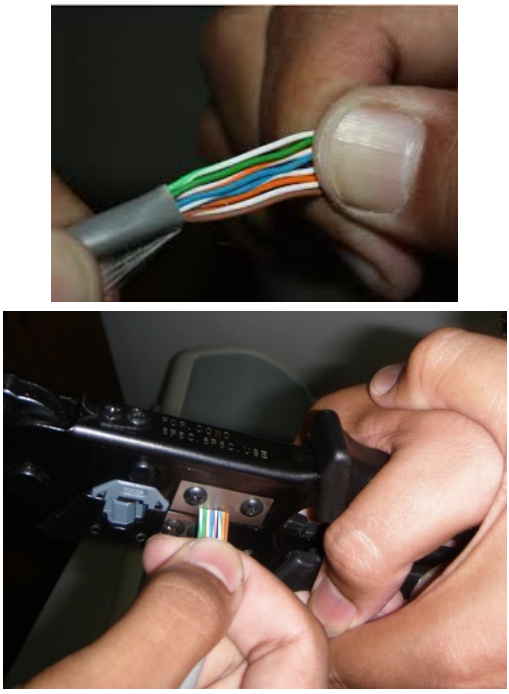
2. Setelah pelindung luar kabel dikupas, kemudian urutkan serat kabel berdasarkan urutan warna yang diinginkan. Untuk mempermudah, urutkan dari kiri ke kanan (pin 1 di kiri) seperti pada Gambar 3.13.



Gambar 3.13 Kabel TP setelah dikupas

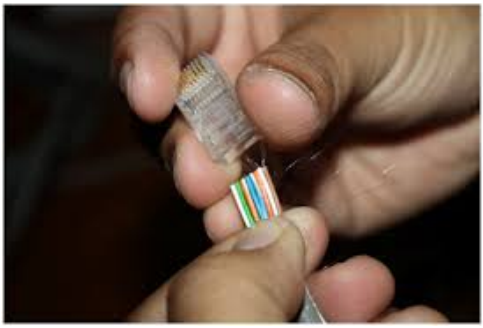
3. Setelah diurutkan, rapatkan seluruh kabel dan rapikan agar tidak bergelombang. Kemudian potong ujung kabel menggunakan tang

krimping dengan panjang yang sesuai dengan konektor seperti pada Gambar 3.14.



Gambar 3.14 Proses mengurutkan dan merapikan

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 seperti pada Gambar 3.15.

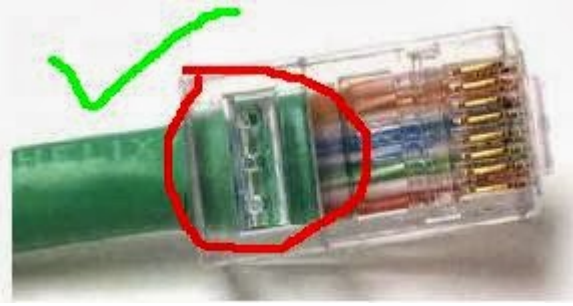


Gambar 3.15 Proses Memasukan Kabel ke Konektor

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 seperti terlihat pada Gambar 3.16.

Gambar 3.16 Proses Krimping

6. Hasil krimping yang baik (Gambar 3.17), kulit kabel masuk kedalam konektor, sehingga konektor akan mengunci kabel dengan kuat.



Gambar 3.17 Contoh pemasangan konektor yang baik

Gambar 3.18 Contoh pemasangan yang buruk

Pemasangan konektor yang buruk (Gambar 3.18) 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).

7. Setelah selesai dipasang, lakukan tes kabel menggunakan kabel tester seperti pada Gambar 3.19. Pengetesan dilakukan untuk memastikan setiap pin terhubung (terutama pin 1,2,3 dan 6) serta urutan kabel sudah benar (Straight atau Cross).

Gambar 3.19 Tes Hasil Pemasangan Konektor

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.

3.5 Tugas

Buat sebuah kabel Cross Over kemudian tes hasil pemasangan konektor tersebut dengan menggunakan tester. Kemudian buat koneksi antar PC menggunakan kabel tersebut. Pastikan antar PC dapat saling berkomunikasi melalui kabel tersebut.

BAB 4
Wireless

Capaian Pembelajaran:

1. Memahami konsep wireless secara umum
2. Mampu merancang dan membuat jaringan wireless dengan tepat

4.1 Konsep *Wireless*

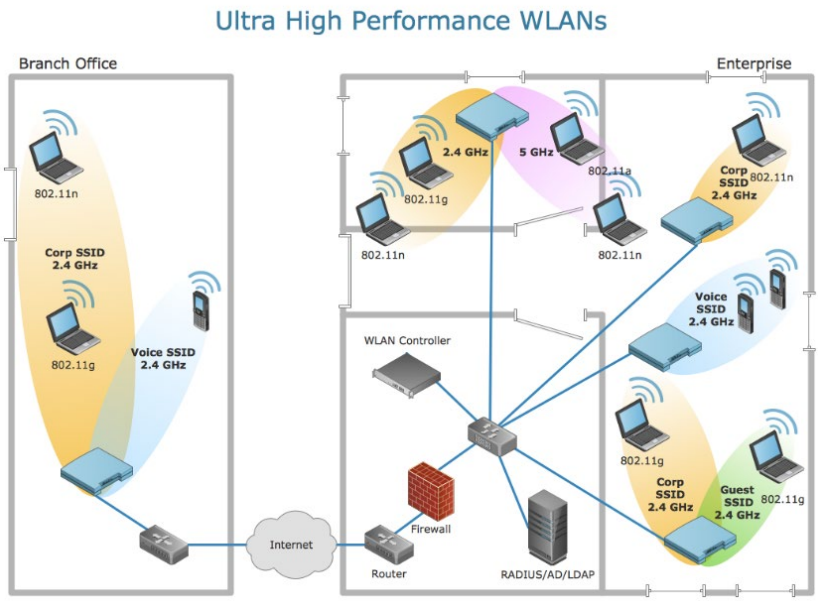
Jaringan wireless atau nirkabel sering juga disebut dengan WLAN (Wireless Local Area Network). Wlan merupakan jaringan komputer yang menggunakan gelombang radio sebagai media transmisinya. Data ditransfer dari satu perangkat ke perangkat lainnya tanpa menggunakan kabel. Keuntungan dari jaringan ini yaitu:

1. Hemat biaya instalasi
2. Fleksibilitas dan kemudahan instalasi
3. Kemampuan jangkauan
4. Mobilitas yang tinggi

Selain keuntungan diatas, komunikasi wlan juga memiliki kelemahan, yaitu:

1. Komunikasi data dari komputer berbeda dapat saling mengganggu.
2. Adanya resiko gangguan koneksi akibat interferensi.
3. Keamanan tidak terjamin karena menggunakan gelombang radio yang dapat diakses setiap orang.
4. Kecepatan koneksi bergantung pada cuaca dan wilayah.

Komunikasi Wlan umumnya digunakan sebagai komunikasi ke client (laptop, handphone atau PC) dimana komunikasi backbone nya masih menggunakan kabel. Perpaduan jaringan kabel dan wlan ini, seperti telihat pada Gambar 4.1, bertujuan untuk memanfaatkan kelebihan masing-masing dan mengurangi kelemahannya.



Gambar 4.1 Perpaduan jaringan kabel dan wireless

Sumber Gambar: https://www.conceptdraw.com/

Komunikasi WLAN umumnya menggunakan frekuensi 2.4 dan 5.8 GHz, dimana frekuensi ini sering disebut dengan frekuensi ISM (Industrial, Scientific and Medical). Frekuensi ISM merupakan frekuensi yang dapat digunakan secara bebas tanpa memerlukan izin dan sewa melalui pemerintah. Saat ini, penggunaan frekuensi 2.4 biasanya digunakan untuk komunikasi dari perangkat client (PC, Smartphone atau notebook) ke perangkat wireless access point. Sedangkan frekuensi 5.8 umumnya digunakan untuk komunikasi antar site (antar dua buah wireless access point atau wireless router).

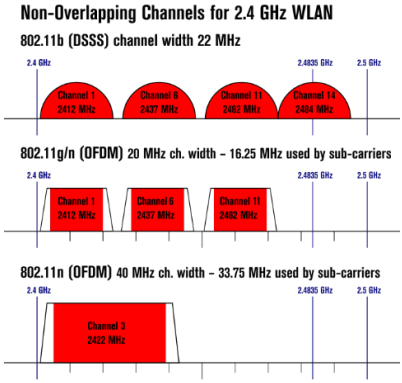
Untuk dapat berkomunikasi, setiap perangkat harus menggunakan protokol yang sama. Komunikasi WLAN menggunakan protokol 802.11 dari IEEE. Protokol ini bekerja pada layer data link. Protokol 802.11 terus berkembang untuk membuat komunikasi lebih cepat dengan jangkauan yang lebih luas. Standar 802.11 dapat dilihat pada Gambar 4.2.

V • T • E	802.11 network PHY standards									[hide]
802.11 protocol	Release date[6]	Frequency	Bandwidth	Stream data rate[7]	Allowable MIMO streams	Modulation	Approximate range[citation needed]			
							Indoor		Outdoor	
		(GHz)	(MHz)	(Mbit/s)			(m)	(ft)	(m)	(ft)
802.11-1997	Jun 1997	2.4	22	1, 2	N/A	DSSS, FHSS	20	66	100	330
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	35	115	120	390
		3.7[A]					—	—	5,000	16,000[A]
b	Sep 1999	2.4	22	1, 2, 5.5, 11	N/A	DSSS	35	115	140	460
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	38	125	140	460
n	Oct 2009	2.4/5	20	400 ns GI : 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2 [B] 800 ns GI : 6.5, 13, 19.5, 26, 39, 52, 58.5, 65 [C]	4	MIMO-OFDM	70	230	250	820[8]
			40	400 ns GI : 15, 30, 45, 60, 90, 120, 135, 150 [B] 800 ns GI : 13.5, 27, 40.5, 54, 81, 108, 121.5, 135 [C]			70	230	250	820[8]
ac	Dec 2013	5	20	400 ns GI : 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3 [B] 800 ns GI : 6.5, 13, 19.5, 26, 39, 52, 58.5, 65, 78, 86.7 [C]	8		35	115[9]		
			40	400 ns GI : 15, 30, 45, 60, 90, 120, 135, 150, 180, 200 [B] 800 ns GI : 13.5, 27, 40.5, 54, 81, 108, 121.5, 135, 162, 180 [C]			35	115[9]		
			80	400 ns GI : 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3 [B] 800 ns GI : 29.2, 58.5, 87.8, 117, 175.5, 234, 263.2, 292.5, 351, 390 [C]			35	115[9]		
			160	400 ns GI : 65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7 [B] 800 ns GI : 58.5, 117, 175.5, 234, 351, 468, 702, 780 [C]			35	115[9]		

Gambar 4.2 802.11 Standards

Sumber Gambar: https://en.wikipedia.org/wiki/IEEE_802.11

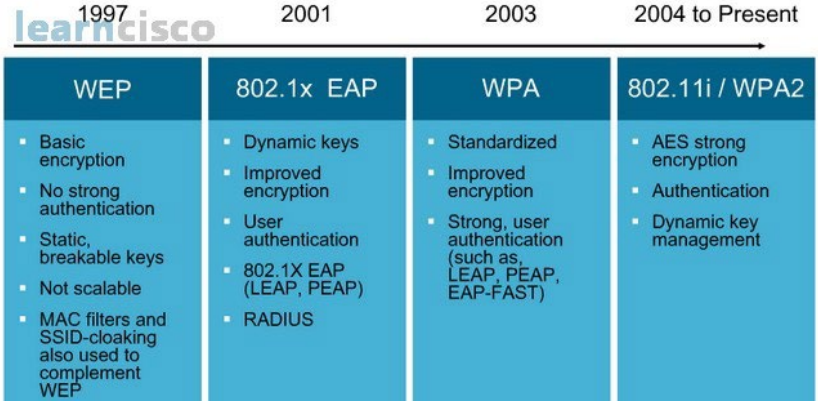
Saat ini protokol yang umumnya digunakan yaitu 802.11n dengan frekuensi 2.4 GHz. Pada frekuensi ini, komunikasi terbagi menjadi 11 channel atau sub frekuensi yang saling overlapping. Agar komunikasi WLAN tidak saling mengganggu, maka setiap perangkat pemancar (Wireless Access Point) yang berdekatan dikonfigurasi menggunakan channel yang tidak overlapping. Channel yang tidak overlapping dapat dilihat pada Gambar 4.3.



Gambar 4.3 Channel 2.4 GHz WLAN

Sumber Gambar:
https://en.wikipedia.org/wiki/List_of_WLAN_channels

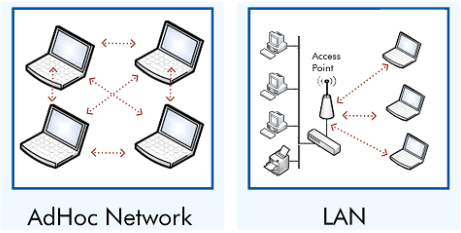
Jaringan Wireless merupakan jaringan yang tidak aman, karena komunikasi menggunakan gelombang radio, dimana dapat "didengar" oleh orang lain. Untuk mengamankan komunikasi WLAN digunakan teknologi authentikasi dan enkripsi sehingga walaupun data "didengar" oleh orang lain, tetapi arti datanya tidak dapat dimengerti, hanya pihak yang berkomunikasi yang dapat mendekripsi data komunikasinya. Saat ini metode keamaan yang paling handal untuk WLAN yaitu WPA2. Perkemabgan metode keamanan wireless dapat dilihat pada Gambar 4.4.



Gambar 4.4 Metode Keamanan Wireless

4.2 Mengenal Perangkat *Wireless*

Jaringan WLAN umumnya bekerja pada salah satu dari dua konfigurasi jaringan (kadang juga disebut dengan topologi) yaitu Ad-Hoc dan Infrastructure. Mode Ad-Hoc juga disebut sebagai jaringan peer-to-peer, dimana dua client terhubung secara langsung tanpa melalui perantara. Sedangkan mode Infrastructure, komunikasi melalui perangkat perantara yaitu Wireless Access Point.



Gambar 4.5 Konfigurasi Jaringan Wireless

Perangkat yang digunakan untuk komunikasi wlan yaitu:

1. Wireless Access Point

Wireless Access Point merupakan komponen yang berfungsi untuk mengirimkan atau menerima data yang berasal dari adapter wireless. Wireless Access Point melakukan konversi sinyal frekuensi radio menjadi sinyal digital, atau sebaliknya. Selain itu, Wireless Access Point juga sebagai jembatan dari jaringan kabel ke jaringan wireless. Access Point mengeluarkan sinyal SSID (Service Set Identifier) yang merupakan nama atau identitas sinyal radio yang diberikan pada jaringan wireless. Perangkat Wireless Access Point yang dijual saat ini umumnya juga mempunyai kemampuan menghubungkan dua jaringan yang berbeda atau biasa disebut Wireless Router. Selain itu pada Wireless Access Point juga terdapat beberapa port ethernet yang dapat difungsikan sebagai Switch.

Gambar 4.6 Wireless Router

2. Wireless Adapter

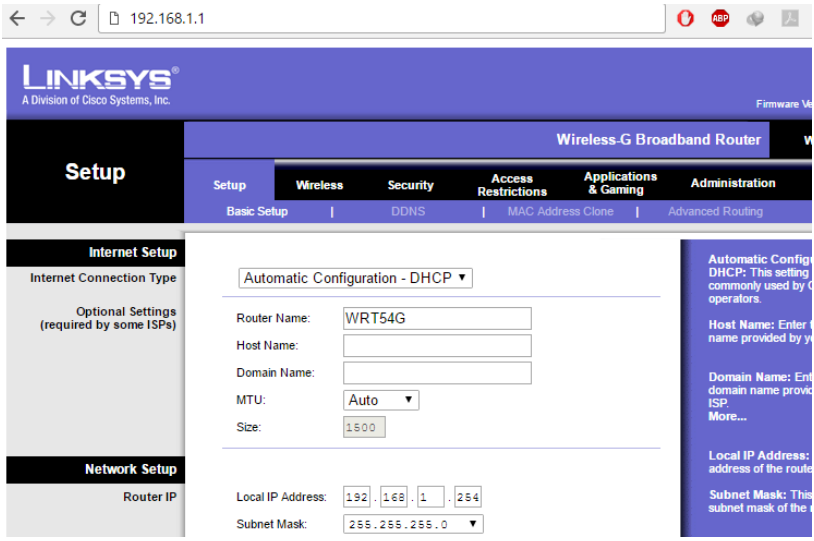
Wireless Adapter merupakan perangkat yang terdapat pada PC atau Laptop yang berfungsi mirip seperti NIC (Network Interface Card). Wireless Adapter dapat dipasang pada port PCI, USB maupun slot khusus pada laptop.

Gambar 4.7 Wireless Adapter

4.3 Konfigurasi Perangkat *Wireless*

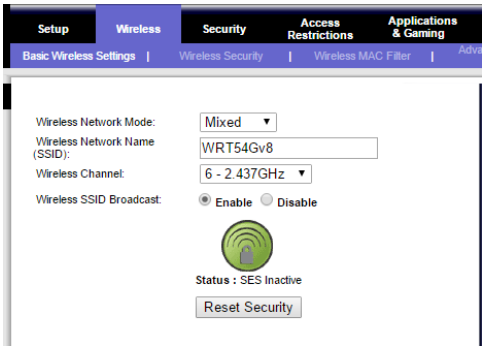
Setiap perangkat wireless access point perlu dilakukan konfigurasi melalui halaman web configuration. Untuk mengakses halaman web configuration ini berbeda-beda setiap merk dan tipe perangkat. Disarankan membaca panduan yang disertakan pada kotak perangkat atau melalui panduan dari internet. Langkah yang umum dilakukan untuk melakukan konfigurasi Wireless Access Point yaitu:

- Hidupkan wireless access point. Biasanya wireless access point baru pertama kali dihidupkan sudah memancarkan sinyal wireless. Jika sudah memancarkan sinyal, maka dapat konek langsung ke sinyal tersebut, jika dibutuhkan key untuk terhubung biasanya terdapat pada kertas panduan. Jika Wireless Access Point (WAP) tidak memancarkan sinyal maka konfigurasi dilakukan dengan menggunakan kabel UTP. Hubungkan kabel melalui port Ethernet (bukan Internet atau WAN) perangkat WAP ke komputer atau laptop.
- Jika komputer sudah terhubung ke perangkat WAP baik melalui wireless ataupun kabel, konfigurasi bisa dilakukan dengan masuk ke web configuration. Alamat default dari web configuration tiap perangkat berbeda-beda, biasanya tertulis di buku panduan. Umumnya alamat yang digunakan yaitu 192.168.1.1. Masukkan alamat tersebut ke web browser.



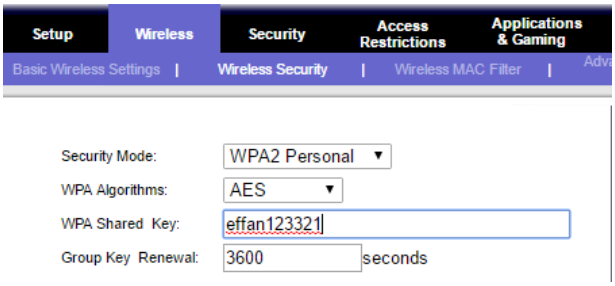
Gambar 4.8 Konfigurasi Wireless Router

- Jika pertama kali masuk diminta password login, biasanya terdapat di buku panduan, atau bisa dicari di internet dengan kata kunci "default username and password <merk dan tipe perangkat>".
- Konfigurasi yang umum dilakukan untuk membuat jaringan WLAN sederhana yaitu SSID beserta keamanan dan channel frekuensi, username dan password login web configuration.
- Pada perangkat Linksys WRT54G, konfigurasi SSID dapat dilakukan dengan masuk ke tab wireless.



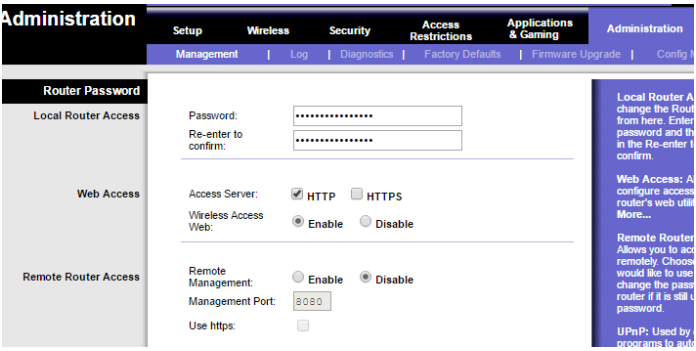
Gambar 4.9 Konfigurasi SSID

- Wireless Network Mode biasa dipilih Mixed yang berarti mendukung protokol 802.11b dan 802.11g. Pada perangkat ini hanya mendukung hingga 802.11g. SSID diisi dengan nama sinyal yang akan digunakan. Pilih Channel frekuensi yang digunakan. Pemilihan channel frekuensi sangat penting agar perangkat WAP yang berdekatan tidak menggunakan channel yang saling overlapping. Jika menggunakan channel yang overlapping maka akan saling menggangu. Pilih Enable pada Wireless SSID Broadcast agar sinyal yang dibuat terlihat. Setiap perubahan yang dilakukan, jangan lupa untuk mengklik Save pada bagian bawah.
- Untuk menambahkan keamanan, klik wireless security kemudian pilih mode security yang akan digunakan. Masukkan WPA key yang akan menjadi autentikasi setiap perangkat yang akan konek ke jaringan yang dibuat. Klik Save untuk menyimpan perubahan.



Gambar 4.10 Konfigurasi Wireless Security

- Agar tidak ada orang yang melakukan perubahan secara illegal terhadap konfigurasi perangkat, maka perlu diubah default password dari web configuration perangkat yang digunakan. Untuk mengubahnya dapat masuk ke tab Administration kemudian mengisi Password untuk mengubah password default.

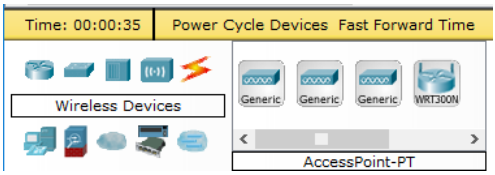


Gambar 4.11 Konfigurasi Password Administration

4.4 Simulasi *Wireless* Pada Packet Tracer

Sebagai keperluan belajar, dapat menggunakan simulator paket tracer. Paket tracer versi 6 sudah mendukung simulasi jaringan wireless. Untuk membuat jaringan wireless dapat dilakukan dengan langkah berikut:

- Pilih wireless device kemudian pilih perangkat WRT300N

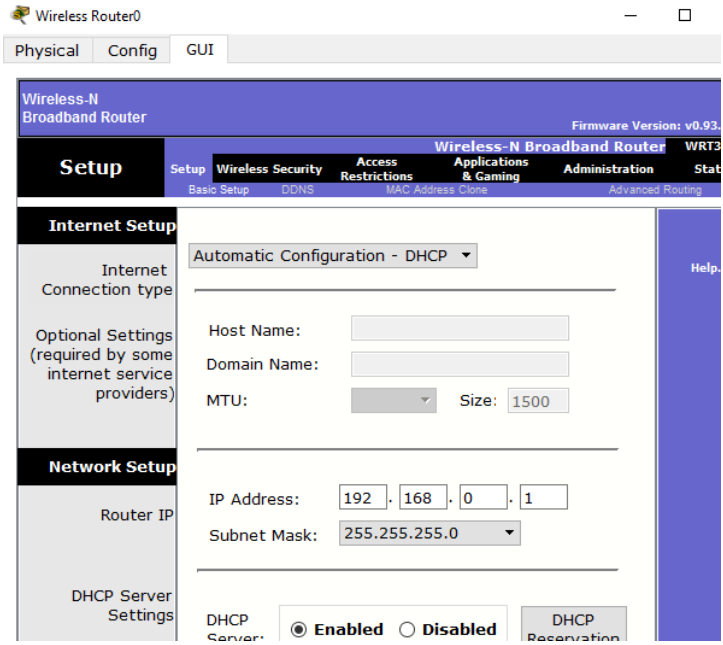


Gambar 4.12 WRT300N pada Packet Tracer

- Pilih End Device berupa Notebook yang nantinya terhubung melalui Wireless dan Komputer yang akan terhubung melalui kabel.
- Hubungkan Komputer ke WRT300N pada interface Ethernet 1.

Gambar 4.13 Hubungan PC0 ke Wireless Router

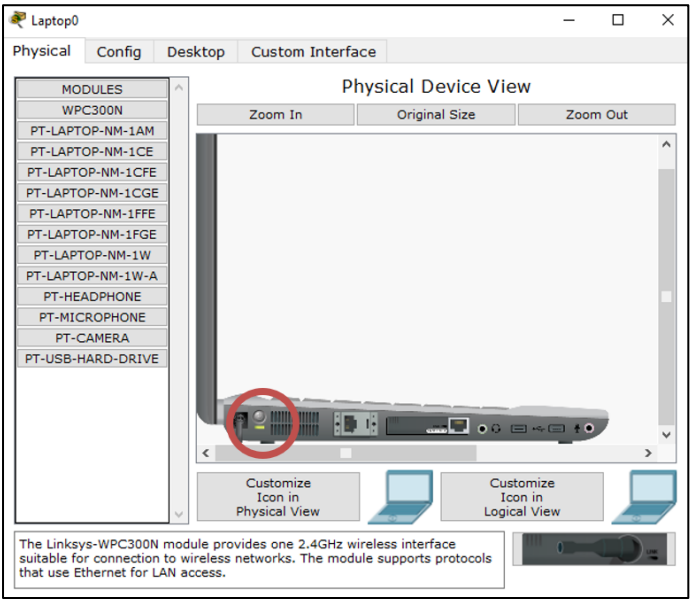
- Untuk menghubungkan Laptop ke WRT300N, maka terlebih dahulu melakukan konfigurasi perangkat WRT300N. Bisa dilakukan dengan mengklik 2x icon perangkatnya. Kemudian pilih tab GUI.



Gambar 4.14 Konfigurasi Wireless Router

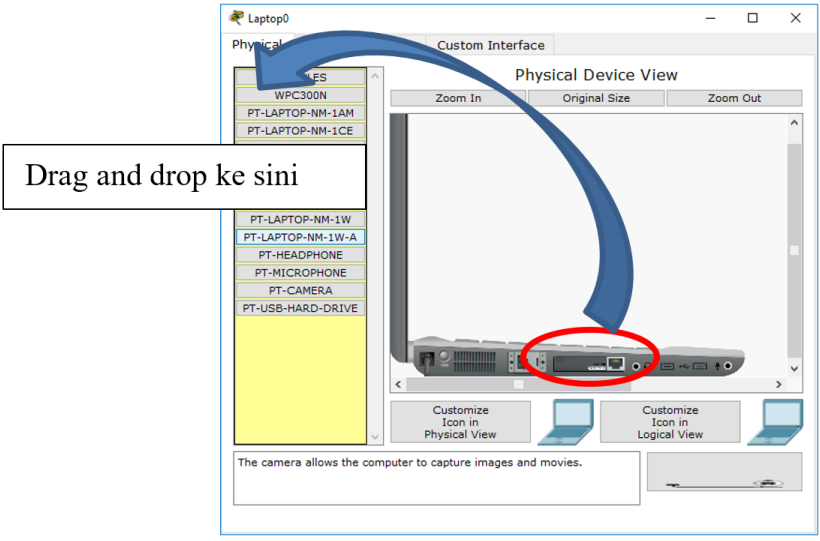
- Lakukan konfigurasi sebagai berikut:

  Nama SSID: jarkom
  Key : jarkom123321
  Channel: 6
  Login password: jarkom123
- Jangan lupa untuk selalu menekan tombol Save ketika selesai melakukan konfigurasi pada setiap halamannya.
- Secara default, Laptop yang digunakan belum terdapat Wireless Interface Card. Klik 2x pada icon laptop, matikan laptop dengan menekan tombol power pada gambar laptop.



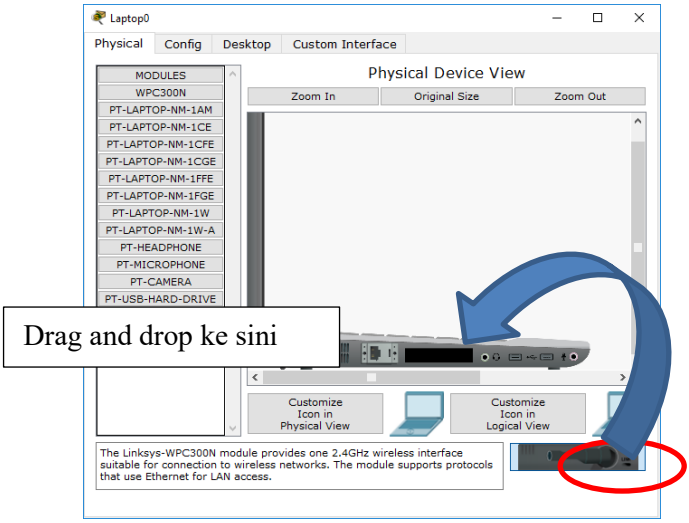
Gambar 4.15 Tombol Power

- Buang interface kabel yang sudah terpasang pada laptop dengan cara drag and drop ke sisi kiri.



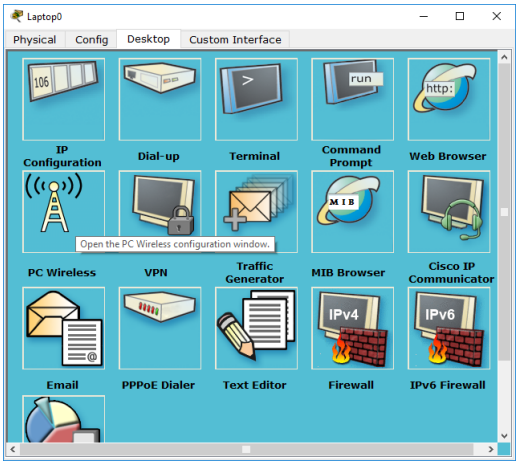
Gambar 4.16 Melepas Interface Kabel

- Setelah slot nya kosong, drag and drop modules WPC300N.



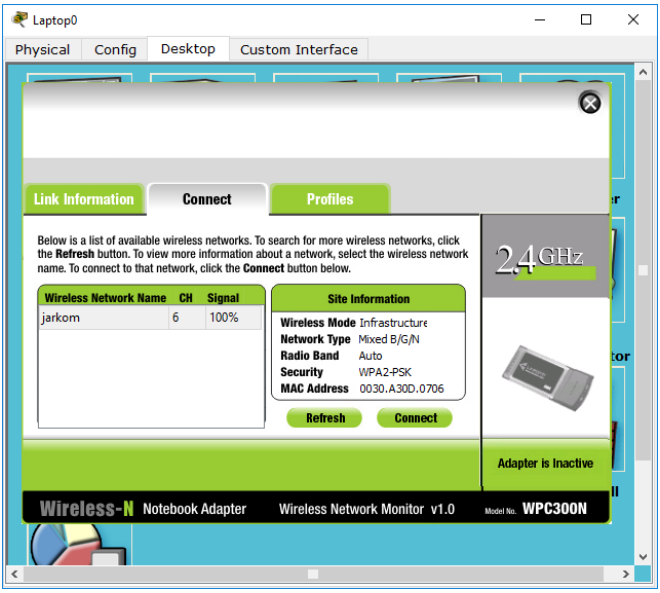
Gambar 4.17 Memasang Interface Wireless

- Hidupkan kembali laptop dengan menekan tombol power. Kemudian tutup windows dengan menekan tanda x pada kanan atas.
- Untuk menghubungkan laptop ke jaringan wireless yang dibuat, masuk kembali ke konfigurasi laptop dengan menekan 2x gambar laptop. Masuk ke tab Desktop, pilih PC Wireless.



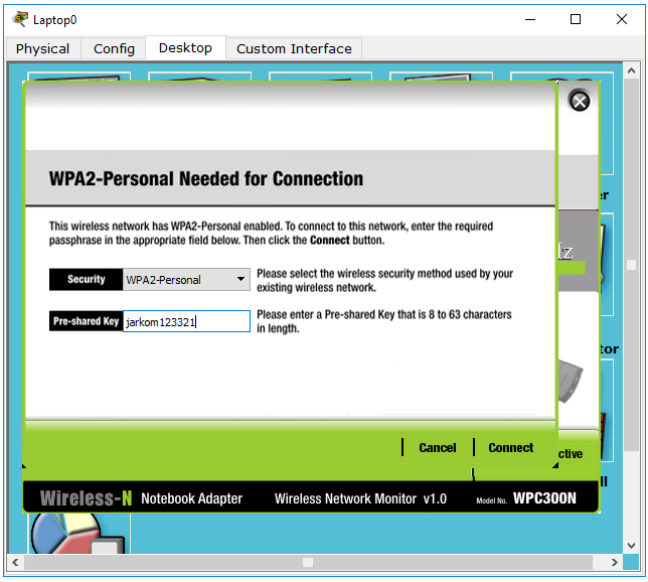
Gambar 4.18 Tab Desktop

- Klik tab Connect, maka akan terlihat SSID yang dipancarkan oleh Access Point. Pilih SSID nya, kemudian klik Connect.



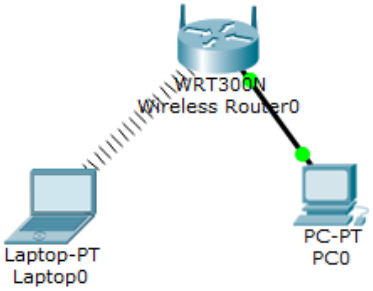
Gambar 4.19 Tampilan PC Wireless

- Masukkan key dari SSID yang dibuat sebelumnya (jarkom123321).



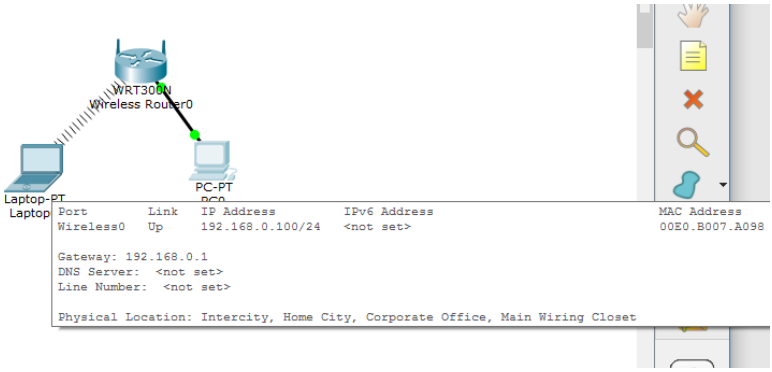
Gambar 4.20 Memasukkan Key

- Tutup semua windows konfigurasi yang ada. Jika laptop sudah terhubung maka akan terlihat tampilan seperti Gambar 4.21.



Gambar 4.21 Laptop0 Terhubung Secara Wireless

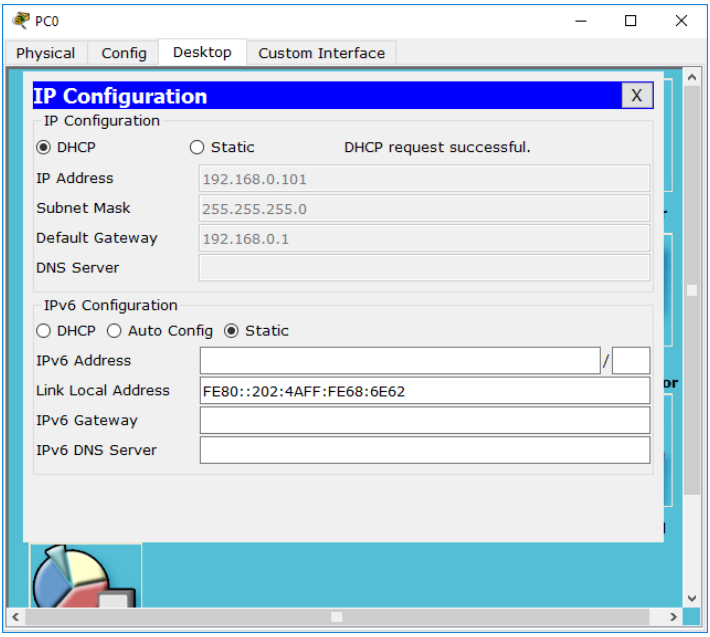
- Pada Wireless Router sudah terdapat DHCP server, sehingga IP setiap client yang terhubung dapat dikasih secara otomatis oleh wireless router. Untuk melihat IP yang didapat bisa dilakukan dengan menaruh pointer mouse ke gambar laptop atau PC yang mau dilihat.



Gambar 4.22 Melihat IP Address

- Untuk PC yang terhubung menggunakan kabel, perlu dilakukan konfigurasi agar mendapat IP Address dari wireless access point. Caranya yaitu dengan masuk ke windows konfigurasi PC dengan mengklik 2x gambar PC. Pilih Tab Desktop masuk ke IP

Configuration. Pilih DHCP pada IP Configuration, sehingga komputer akan meminta IP Address dari Wireless Access Point.



Gambar 4.23 Konfigurasi IP PC0

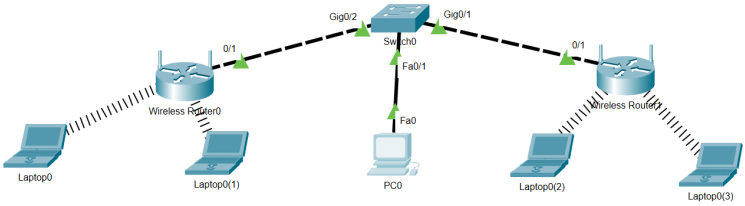
- Untuk mengecek apakah Laptop sudah terhubung ke komputer dapat dilakukan dengan perintah ping. Masuk ke bagian Desktop, pilih Command Prompt, ketik perintah “ping <ip tujuan>”. Jika tertampil seperti gambar dibawah, berarti komputer sudah tersambung ke laptop melalui wireless access point.

```
PC>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=15ms TTL=128
Reply from 192.168.0.100: bytes=32 time=21ms TTL=128
Reply from 192.168.0.100: bytes=32 time=0ms TTL=128
Reply from 192.168.0.100: bytes=32 time=12ms TTL=128

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 21ms, Average = 12ms

PC>
```

Gambar 4.24 Test Ping

4.5 Tugas

Buat jaringan seperti pada Gambar 4.25. Lakukan konfigurasi agar masing-masing Access Point memancarkan sinyal yang berbeda. Lakukan tes konfigurasi agar masing-masing laptop/komputer dapat saling terhubung ke semua laptop/komputer lain.



Gambar 4.25 Tugas Wireless

BAB 5
Pemanfaatan Jaringan Lokal

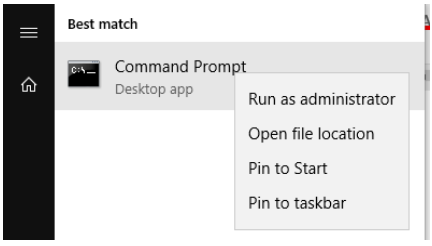
Capaian Pembelajaran:

1. Mampu membuat Infrastruktur pada PC tanpa perangkat tambahan.
2. Mampu melakukan sharing folder untuk berbagi data.
3. Mampu menggunakan printer secara bersama dalam satu jaringan.
4. Mampu berbagi satu akses internet ke komputer-komputer lain tanpa perangkat tambahan.

5.1 Membuat Jaringan Infrastruktur pada PC/Laptop

Selain menggunakan perangkat tambahan (Wireless Access Point), jaringan infrastruktur juga dapat dibuat tanpa perangkat tambahan. Jika tanpa perangkat tambahan, laptop atau PC selain berfungsi sebagai client, juga dapat dibuat menjadi Wireless Access Point pada mode infrastruktur. Untuk membuat jaringan infrastruktur pada windows dapat dilakukan dengan menggunakan software tambahan seperti Baidu Wifi Hotspot, Connectify, Virtual Router dan lainnya. Beberapa software berbayar, tetapi ada juga yang gratis. Selain dengan menggunakan software, jaringan insfrastruktur dapat dibuat dengan menggunakan command prompt. Berikut langkah yang dilakukan untuk membuat jaringan infrastruktur menggunakan Command Prompt:

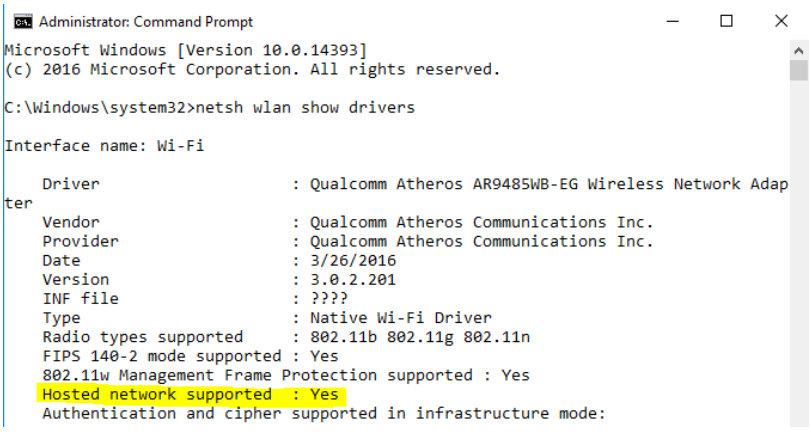
- Jalankan Command Prompt dengan mode Adminstrator. Caranya yaitu dengan mengklik kanan pada icon Command Prompt kemudian pilih Run as administrator.



Gambar 5.1 Running CMD

- Tidak semua driver (Wireless Card) yang dapat dibuat menjadi Access Point. Untuk mengecek apakah driver dari wireless card yang digunakan mendukung fitur tersebut dapat dilakukan dengan perintah:

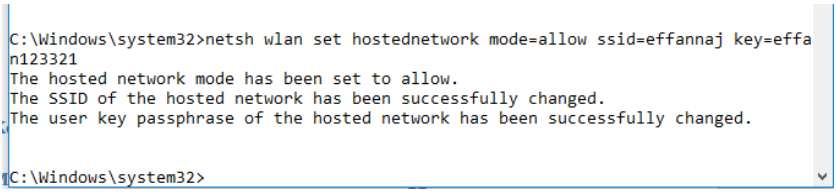
  ```
  netsh wlan show drivers
  ```



Gambar 5.2 Pengecekan Hosted Network

- Jika muncul tulisan Hosted network supported: Yes, berarti driver wireless card yang digunakan dapat difungsikan sebagai Wireless Access Point.
- Untuk memfungsikan wireless interface card sebagai Access Point, dapat dilakukan dengan perintah berikut:

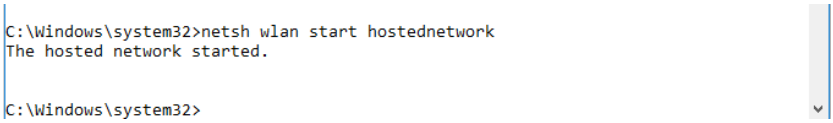
  ```
  netsh wlan set hostednetwork mode=allow ssid=<ssid> key=<key>
  ```



Gambar 5.3 Konfigurasi Hosted Network

- Untuk menjalankan SSID yang telah dibuat dapat dilakukan dengan perintah berikut:

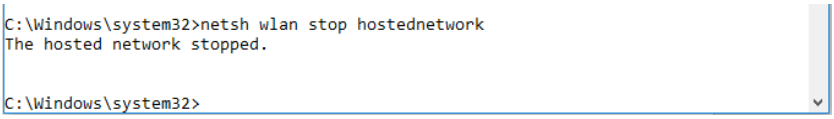
  ```
  netsh wlan start hostednetwork
  ```



Gambar 5.4 Menjalankan Hosted Network

- Untuk mengecek apakah komputer yang digunakan sudah memancarkan sinyal dengan SSID yang telah dikonfigurasi sebelumnya, dapat dilakukan melalui komputer lain, atau smartphone.
- Untuk mematikan Access Point yang dibuat dapat dilakukan dengan perintah:

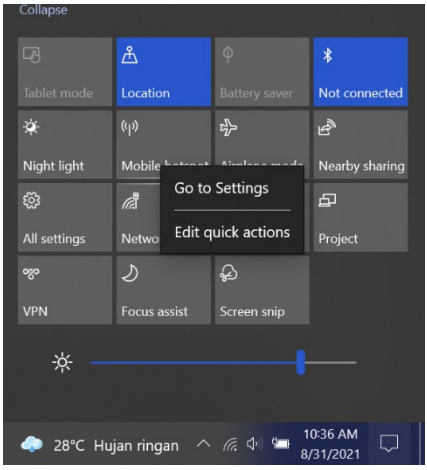
  `netsh wlan stop hostednetwork`



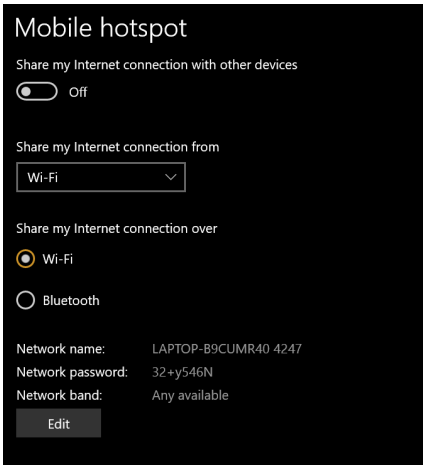
Gambar 5.5 Mematikan Hosted Network

- Cara seperti ini sering dilakukan untuk keperluan sharing akses internet.

Selain menggunakan hostednetwork, pada windows 10 juga terdapat fasilitas mobile hotspot dimana fasilitas ini mirip dengan tethering yang ada di smartphone android. Untuk mengaktifkan fitur ini, minimal terdapat satu koneksi jaringan yang aktif (wifi atau ethernet/Local Area Connection). Cara mengaktifkannya yaitu dengan memilih menu notification disamping jam windows dan memilih mobile hotspot. Untuk mengatur nama sinyal dan password dapat dilakukan dengan mengklik kanan pada mobile hotspot kemudian pilih Go to Settings. Mobile Hotspot akan memancarkan sinyal dan membuat jaringan infrastruktur. Selain itu fitur ini juga dapat melakukan share koneksi internet yang dimiliki suatu komputer ke perangkat lain.



Gambar 5.6 Mobile Hotspot



Gambar 5.7 Konfigurasi Mobile Hotspot

5.2 Sharing Folder dan Printer

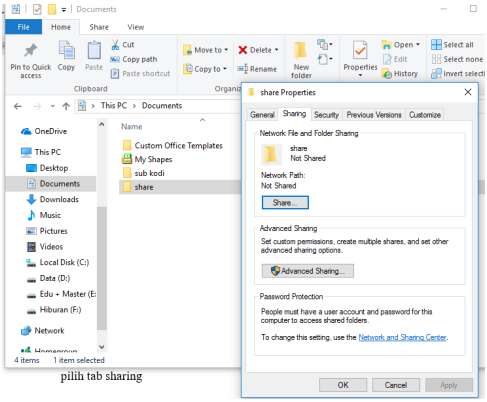
Sharing merupakan fitur yang memungkinkan pengguna untuk berbagi folder, penggunaan perangkat, atau akses internet secara bersama-sama dalam satu jaringan yang sama baik itu peer to peer maupun jaringan client server.

a. Sharing folder

Sharing folder bertujuan untuk berbagi dokumen antar jaringan. Komputer yang terhubung dalam jaringan yang sama, dapat menyalin

atau memasukkan file ke dalam suatu folder yang telah di share. Langkah yang dilakukan untuk share folder yaitu:

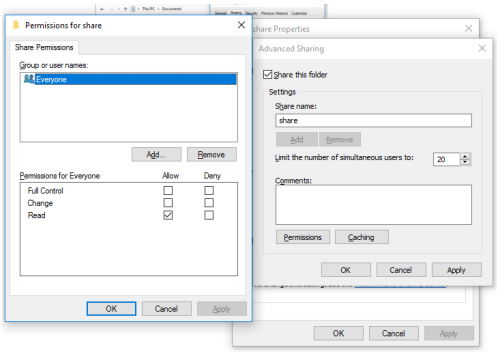
- Buka folder explorer.
- Klik kanan folder yang akan di share, kemudian pilih properties dan pilih tab sharing



pilih tab sharing

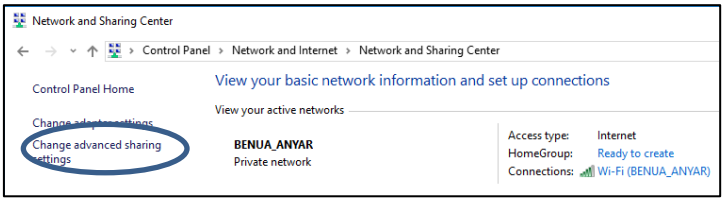
Gambar 5.8 Share Folder

- Klik Advanced Sharing (dapat juga memilih Share..), centang Share this folder, atur jumlah user yang dapat terhubung bersama-sama dalam satu waktu. Klik permissions, jika ingin folder yang di share dapat ditulis atau seseorang dapat memasukkan, menghapus atau memodifikasi isi folder tersebut, centang Full Control pada halaman permission. Kemudian Klik OK



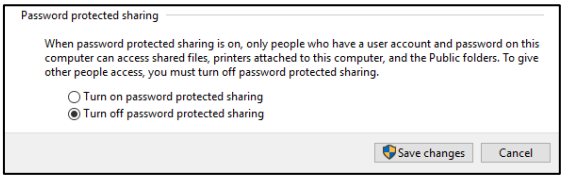
Gambar 5.9 Pengaturan Permissions

- Untuk mengakses file sharing secara default mengharuskan komputer yang hendak terhubung memasukan username dan password. Username dan password ini merupakan username dan password user account yang terdapat pada komputer, sehingga pada komputer yang hendak berbagi (share) harus ada user account dengan password. Jika ingin mematikan autentikasi ketika hendak mengambil file sharing dapat dilakukan dengan masuk ke Change advanced sharing setting pada Network and Sharing Center.



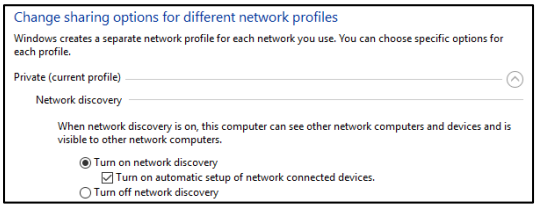
Gambar 5.10 Change advanced sharing settings

- Pada bagian All Networks, pilih Turn Off Password Protected Sharing.

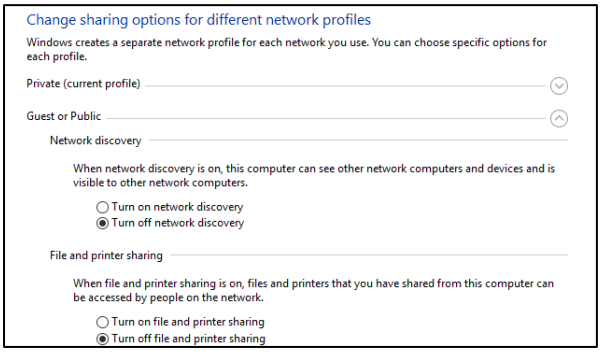


Gambar 5.11 Mematikan Password Protected Sharing

- Selain itu pada menu Advanced sharing settings juga terdapat pilihan untuk menaktifkan atau mematikan Network discovery, dimana fitur ini memiliki fungsi agar komputer terlihat oleh komputer lainnya jika terhubung ke jaringan yang sama. Fitur ini dapat diaktifkan pada jaringan private, jaringan public atau keduanya.

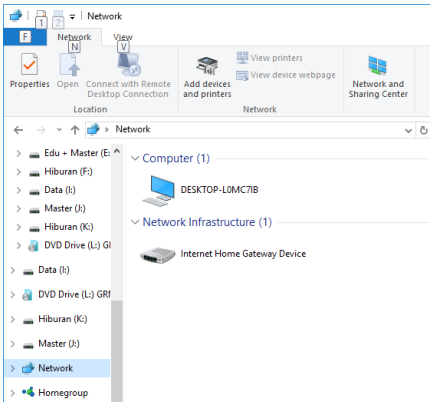


Gambar 5.12 Pengaturan Network Discovery



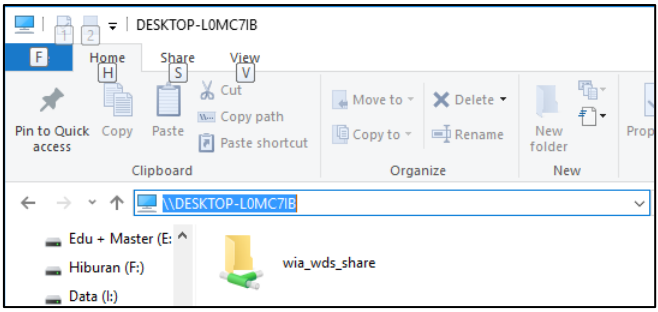
Gambar 5.13 Pengaturan jaringan Public

- Untuk mengakses folder sharing dapat dilakukan dengan beberapa cara, yaitu:
  - Melalui Network discovery, cara ini dapat dilakukan hanya jika diaktifkan fitur network discovery pada komputer yang melakukan sharing folder. Caranya yaitu dengan masuk ke Network pada folder explorer.



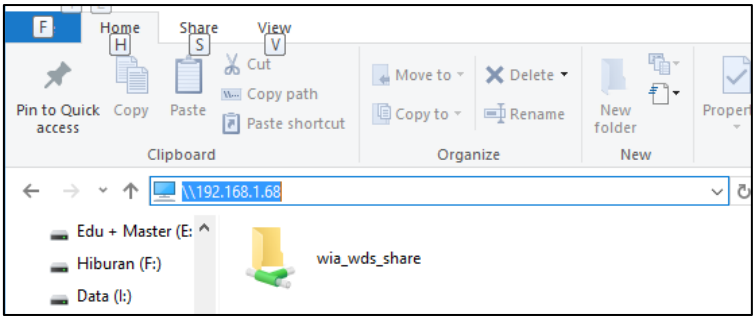
Gambar 5.14 Mengakses Lewat Network Discovery

- Cara berikutnya yaitu dengan memasukkan alamat \\<nama komputer tujuan> pada folder explorer. Misal \\DESKTOP-L0MC7IB



Gambar 5.15 Mengakses menggunakan nama komputer

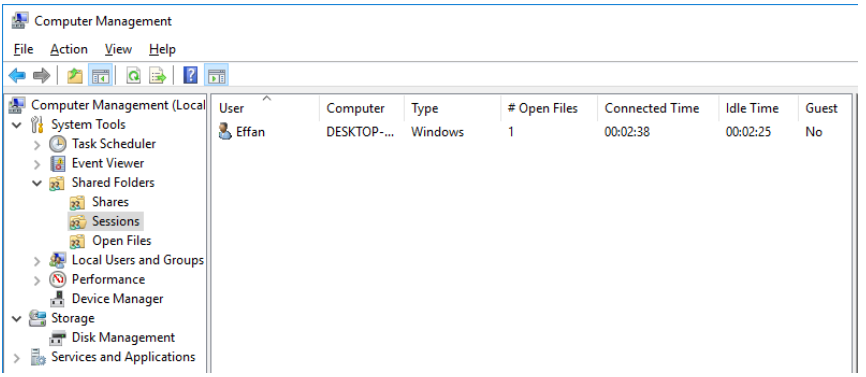
- Cara lainnya yaitu dengan memasukan alamat IP dari komputer tujuan. Misal \\192.168.1.68 pada folder explorer.



Gambar 5.16 Mengakses Menggunakan IP Address

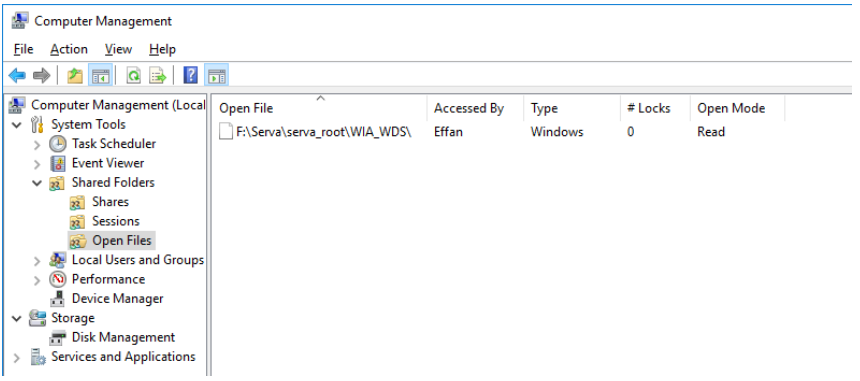
- Jika meminta password (fitur password protected sharing diaktifkan), masukkan username dan password dari account komputer tujuan.
- Jika sudah terhubung, dapat menyalin isi dalam folder yang di sharing. Jika permission di setting read and write, maka selain dapat menyalin juga dapat menghapus, memodifikasi dan menambahkan isi dalam folder sharing tersebut.

- Komputer yang sedang mengakses folder sharing dapat dilihat melalui Computer Management pada bagian Shared Folder, Sessions.



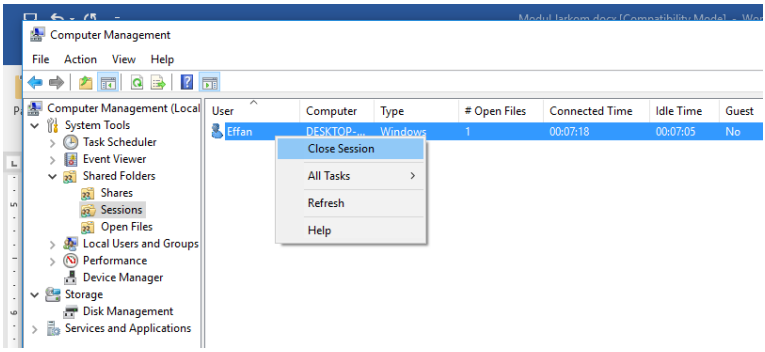
Gambar 5.17 Monitoring Sessions

- Sedangkan file yang sedang dibuka oleh komputer lain dapat dilihat pada bagian Open Files.



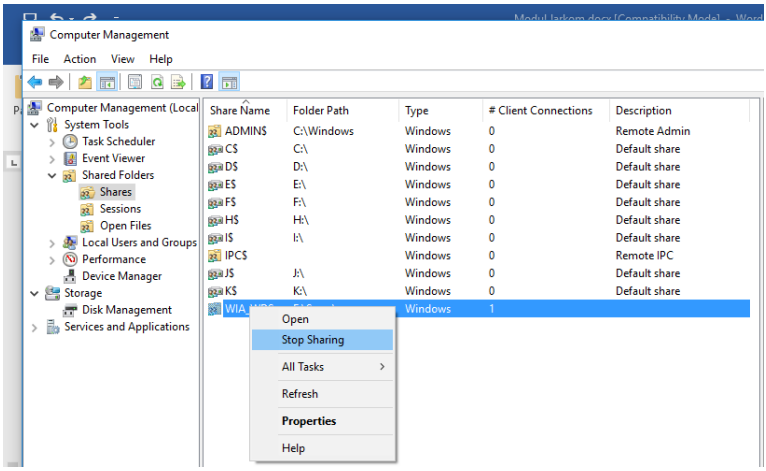
Gambar 5.18 Monitoring Open Files

- Jika ingin memutuskan sesi komputer yang sedang terhubung, klik kanan pada nama komputer yang ingin diputus, kemudian pilih Close Sessions. Cara yang sama juga dapat dilakukan untuk menutup file yang sedang dibuka oleh komputer lain.



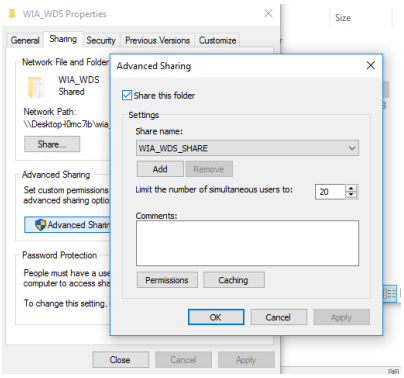
Gambar 5.19 Mematikan Session

- Untuk mematikan folder sharing dapat dilakukan dengan cara berikut:
  - Pada computer management masuk ke Shared Folders, Share. Klik kanan pada folder yang di share, kemudian pilih Stop Sharing.



Gambar 5.20 Mematikan Sharing

  - Cara lainnya yaitu dengan menghilangkan centang pada Advanced sharing

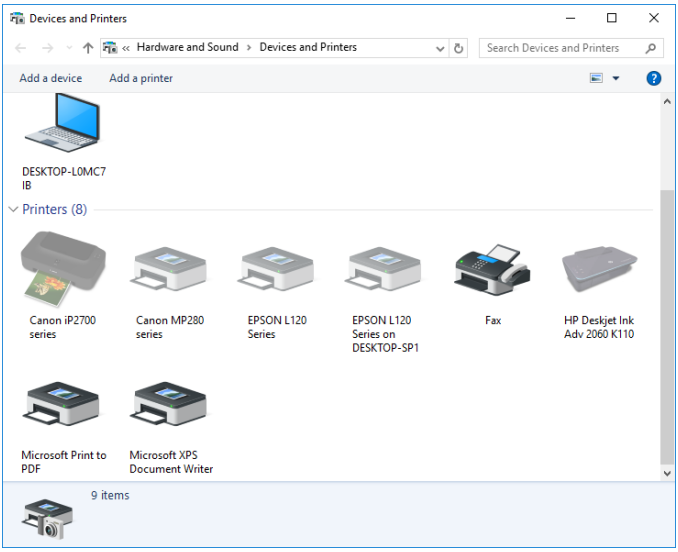


Gambar 5.21 Mematikan Sharing Melalui Explorer

b. Sharing Printer

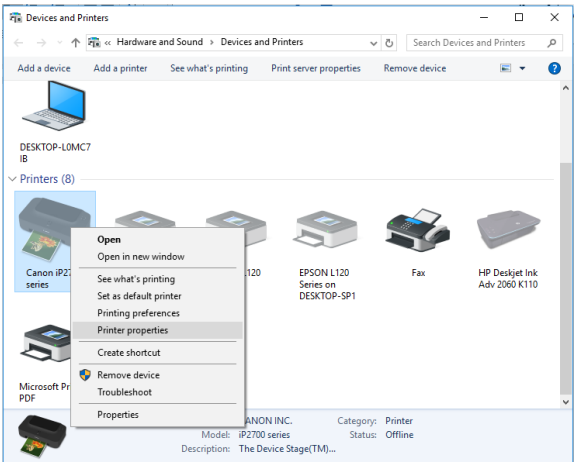
Cara melakukan sharing printer mirip dengan sharing folder, langkahnya yaitu:

- Masuk ke Devices and Printers pada control panel.



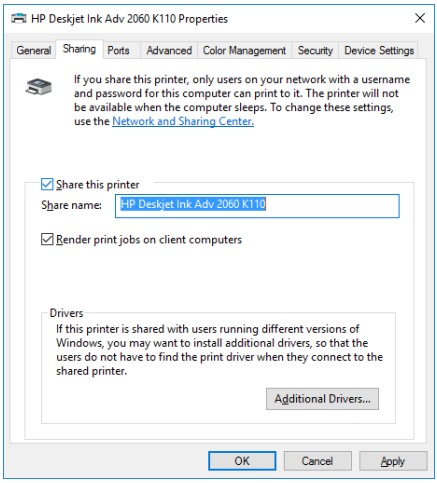
Gambar 5.22 Device and Printer

- Klik kanan pada Printer yang akan di share kemudian pilih printer properties.



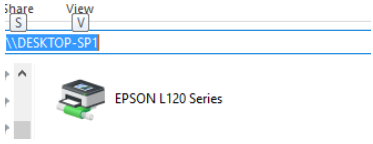
Gambar 5.23 Printer Properties

- Masuk ke tab sharing kemudian centang Share this printer. Klik OK



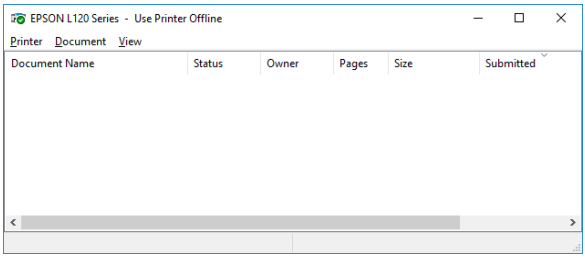
Gambar 5.24 Konfigurasi Sharing Printer

- Untuk mengakses printer, dapat masuk ke folder explorer seperti langkah untuk mengakses folder sharing. Klik 2x printernya, komputer akan otomatis menginstall driver printer.



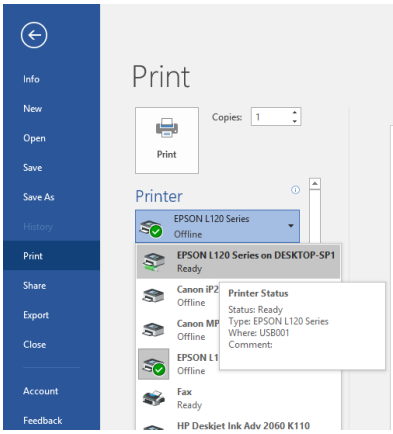
Gambar 5.25 Mengakses Printer

- Jika muncul tampilan seperti dibawah, maka printer siap digunakan.



Gambar 5.26 Tampilan Status Printer

- Untuk menggunakan printer yang sudah terhubung, print dokomen seperti biasa, kemudian pilih printer yang digunakan. Printer yang terhubung lewat jaringan, pada nama printernya terdapat tulisan "on <nama atau IP komputer>", misal EPSON L120 Series on DESKTOP-SP1.



Gambar 5.27 Print melalui Word

5.3 Tugas

Buatlah jaringan Wireless menggunakan komputer/laptop, kemudian lakukan sharing folder full access sehingga komputer yang terhubung ke jaringan tersebut bisa melihat, serta memperbaharui isi di dalam folder tersebut.

BAB 6
IPV4 dan Subnetting

Capaian Pembelajaran:

1. Memahami konsep bilangan biner dan konversi ke desimal.
2. Memahami pengalamatan menggunakan IPv4.
3. Memahami konsep subnetting.
4. Mampu membagi alamat IP address menggunakan subnetting.
5. Mampu membagi alamat IP address menggunakan VLSM.

6.1 Pendahuluan

IP Address merupakan alamat setiap komputer. Seperti dijelaskan pada BAB sebelumnya, dalam jaringan komputer dikenal ada alamat MAC Address dan juga IP Address. IP Address ini ibarat nama seseorang sedangkan MAC Address ibarat tampang atau muka dari seseorang. Nama dan tampilan muka seseorang merupakan identitas yang digunakan sebagai pembeda antara orang yang satu dengan orang yang lain. Ibarat muka seseorang, MAC Address merupakan alamat bawaan dari lahir yang seharusnya tidak berubah-ubah. Sedangkan IP Address merupakan pemberian yang menunjukkan identitas dari perangkat tersebut ketika terhubung ke jaringan. IP Address terdiri dari 32 bit untuk versi 4 (IPv4) dan 128 bit (IPv6). Pada buku ini hanya akan dibahas mengenai IPv4.

Untuk mempermudah penulisan dan manajemen oleh manusia, IPv4 ditulis dengan menggunakan bilangan desimal tetapi pemrosesan oleh router maupun komputer dengan menggunakan bilangan biner. Untuk itu dalam mempelajari IPv4 terlebih dahulu mengerti bagaimana cara konversi dari bilangan desimal ke biner maupun sebaliknya.

Bilangan biner hanya terdiri dari dua bilangan yaitu 1 dan 0, sedangkan bilangan desimal memiliki orde 10 dimana ada 10 bilangan yaitu dari 0 hingga 9. Digit terkecil dari bilangan biner disebut sebagai bit. Setiap digit bilangan desimal memiliki nilai pangkat 10, misal nilai satuan terkecil (paling kanan) dari desimal memiliki nilai 10^0,

sedangkan digit puluhan memiliki nilai 10^1, digit ratusan memiliki nilai 10^2 dan seterusnya. Sehingga jika ada bilangan 9 0 3 4 desimal, maka berarti bernilai seperti berikut:

10^3	10^2	10^1	10^0
9	0	3	4

Nilai tersebut dapat dihitung dengan:
$= 9 \times 10^3 + 0 \times 10^2 + 3 \times 10^1 + 4 \times 10^0$
$= 9000 + 0 + 30 + 4$
$= 9034$

Penilaian bilangan seperti itu juga dilakukan pada bilangan biner dimana bilangan biner merupakan bilangan orde 2 sehingga nilai digit terkecil dari bilangan biner bernilai 2^0, 2^1, 2^2 dan seterusnya, atau jika didesimalkan bernilai 1, 2, 4, 8 dan seterusnya. Sehingga jika ingin mengubah bilangan biner 1 1 0 1 menjadi bilangan desimal bisa dilakukan dengan cara berikut:

Nilai Biner	2^3	2^2	2^1	2^0
Nilai Desimal	8	4	2	1
Bilangan Biner	1	1	0	1

Nilai 1101 jika dikonversi ke desimal dapat dihitung dengan:
$= 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$
$= 1 \times 8 + 1 \times 4 + 0 \times 2 + 1 \times 1$
$= 8 + 4 + 0 + 1$
$= 13$

Sehingga nilai 1101 jika dikonversi ke desimal menjadi 13. Pada IPv4 32 bit dari alamat IP dipisah menjadi 4 segmen per 8 bit dengan tanda pemisah titik seperti berikut:

xxxxxxxxx. xxxxxxxxx. xxxxxxxxx. xxxxxxxxx

Dalam penulisan nilai biner, 1101 sama saja dengan 00001101.

Untuk melakukan konversi dari desimal ke biner dapat dilakukan dengan cara sebaliknya. Misal ingin mengkonversi bilangan 51 ke biner dapat dilakukan sebagai berikut:

1. Langkah pertama yaitu dengan menuliskan nilai desimal setiap digit biner nya seperti berikut:

128	64	32	16	8	4	2	1

2. Pada posisi bit dengan nilai yang lebih besar dari 51 maka nilai bit nya akan bernilai 0. Yaitu pada posisi dengan nilai 128 dan 64.

128	64	32	16	8	4	2	1
0	0						

3. Nilai yang lebih kecil dari 51 dan yang paling mendekati 51 nilai bit nya bernilai 1. Jadi posisi bit dengan nilai 32 akan bernilai 1.

128	64	32	16	8	4	2	1
0	0	1					

4. Karena posisi bit dengan nilai 32 sudah bernilai 1 maka nilai tersisa yang perlu dicari yaitu 51 – 32 = 19. Selanjutnya nilai yang lebih kecil dari 19 dan yang paling akan bernilai 1 yaitu 16.

128	64	32	16	8	4	2	1
0	0	1	1				

5. Karena posisi bit dengan nilai 16 juga bernilai 1 maka nilai tersisa yang perlu dicari yaitu 19 – 16 = 3. Pada nilai posisi bit masih terdapat nilai 8, 4, 2 dan 1. Nilai yang lebih besar dari 3 akan bernilai 0, yaitu nilai 8 dan 4.

128	64	32	16	8	4	2	1
0	0	1	1	0	0		

6. Selanjutnya nilai yang lebih kecil dari 3 dan yang paling mendekati akan bernilai 1, yaitu posisi 2.

128	64	32	16	8	4	2	1
0	0	1	1	0	0	1	

7. Karena ada bit 1 dengan pada nilai 2 maka nilai tersisa yang akan dicari yaitu 3 – 2 = 1. Sehingga untuk mendapatkan nilai 51 maka posisi bit terakhir bernilai 1.

128	64	32	16	8	4	2	1
0	0	1	1	0	0	1	1

8. Bilangan 51 jika dikonversi ke biner bernilai 00110011 atau 110011. Jika dikonversi balik maka akan didapat perhitungan seperti berikut:
   = 32 + 16 + 2 + 1
   = 51

6.2 Subnet Mask

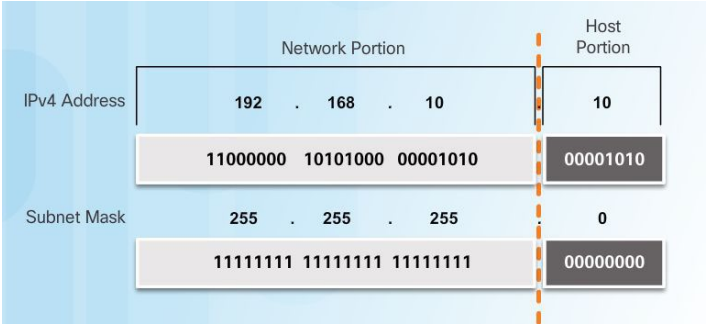
Setiap alamat IPv4 terdiri dari dua bagian yaitu identitas jaringan (Network ID) dan identitas host (Host ID). Dua buah alamat IP dikatakan berada pada alamat jaringan yang sama jika memiliki identitas jaringan yang sama persis. Dalam satu identitas jaringan yang sama tidak boleh ada dua perangkat yang memiliki identitas host yang sama. Untuk mengetahui bagian mana dari IPv4 yang merupakan Network ID dan bagian mana yang merupakan HostID maka perlu adanya suatu penanda, penanda ini yang disebut sebagai subnet mask. Dalam penulisan alamat IPv4 selalu didampingi dengan subnet mask dari IP tersebut yang akan menandakan bagian yang masuk Network ID atau Host ID. Bit 1 pada Subnet Mask menunjukkan porsi untuk Network atau Network ID sedangkan bit 0 pada subnet mask menunjukkan porsi untuk Host (Host ID). Jika terdapat IP address 192.168.10.10 dengan subnetmask 255.255.255.0 maka untuk mendapatkan network portion dan host portion dengan mengubah nilai desimal IP dan subnet mask nya ke dalam bilangan biner sehingga network portion dan host portion terlihat pada Gambar 6.1.

Pada Gambar 6.1 nilai network portion dari IP tersebut adalah 192.168.10, sehingga jika ada dua perangkat komputer yang terhubung langsung atau terhubung menggunakan switch maka kedua PC tersebut harus berada dalam network yang sama yaitu 192.168.10. Untuk host portion kedua PC tersebut wajib berbeda, karena tidak boleh ada dua alamat host yang sama dalam satu jaringan. Sehingga kita bisa melakukan konfigurasi seperti berikut:

IP PC 1: 192.168.10.10

IP PC 2: 192.168.10.11

Dengan Subnetmask yang sama yaitu 255.255.255.0.



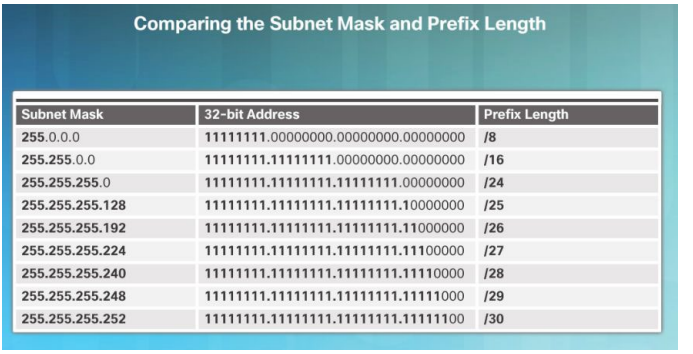
Gambar 6.1 Network Portion dan Host Portion

Subnet Mask akan menentukan batas yang mana yang menjadi network portion yang mana yang menjadi host portion. Network portion selalu merupakan bagian disisi sebelah kiri, sedangkan host portion merupakan bagian sebelah kanan. Berdasarkan hal tersebut, maka tidak mungkin ada nilai 0 dari bit subnetmask yang berada diantara nilai 1. Bit 1 dari subnetmask selalu berada disebelah kiri dan bit 0 disebelah kanan sehingga tidak mungkin ada nilai subnetmask seperti berikut : 255.0.255.0 atau 255.255.255.1. Nilai subnet mask disetiap kelompok 8 bit nya yang mungkin adalah sebagai berikut:

0	00000000	248	11111000
128	10000000	252	11111100
192	11000000	254	11111110
224	11100000	255	11111111
240	11110000		

Sehingga contoh nilai subnetmask yang mungkin adalah 255.255.248.0 atau 255.240.0.0.

Subnet Mask bisa ditulis dengan menggunakan prefix length untuk mempersingkat penulisan. Prefix length didapat dengan menghitung jumlah bit 1 (bit network) dari subnetmask tersebut. Penulisan prefix length didahului dengan tanda notasi slash (/) dan diikuti dengan jumlah bit 1 nya. Gambar 6.2 menunjukkan contoh penulisan Prefix Length.

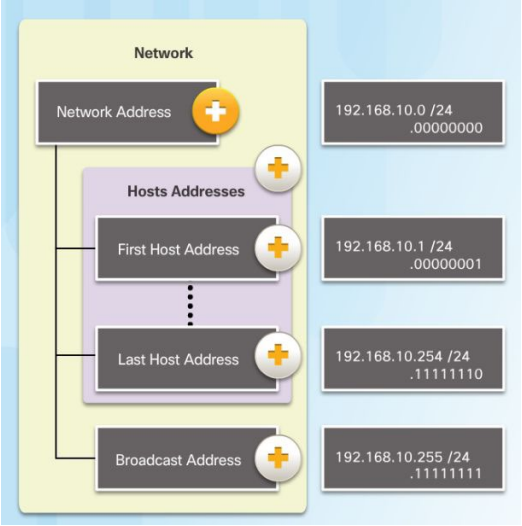


Gambar 6.2 Prefix Length

6.3 Alamat Network, Host dan Broadcast

Dari suatu blok alamat IP Address terdiri dari Alamat Network, Host dan Broadcast. Alamat Network merupakan identitas penanda suatu network. Alamat network ini digunakan oleh router dalam mencari arah network yang dituju. Alamat network ini tidak boleh digunakan sebagai alamat komputer atau perangkat karena merupakan identitas dari network nya. Alamat Host merupakan alamat yang dapat digunakan oleh perangkat atau komputer sebagai alamat IP nya. Sedangkan alamat Broadcast merupakan alamat yang digunakan untuk mengirimkan pesan keseluruh perangkat yang berada di dalam network tersebut. Alamat broadcast juga tidak dapat digunakan sebagai alamat suatu perangkat atau komputer.

Alamat Network merupakan alamat pertama dalam suatu jaringan yang ditandai dengan nilai bit dari host portion nya bernilai 0 semua. Sedangkan alamat Broadcast merupakan alamat akhir dari suatu jaringan yang ditandai dengan nilai bit dari host portion nya bernilai 1 semua. Alamat host merupakan alamat diantara alamat network dan alamat broadcast. Contoh ada suatu alamat network 192.168.10.0/24, maka pembagian alamatnya seperti pada Gambar 6.3.



Gambar 6.3 Pembagian Alamat Network, Host dan Broadcast

6.4 Pengelompokan IP

Ada dua cara pembagian IP address yaitu Classfull dan classless addressing. Classfull addressing merupakan pembagian IP address berdasarkan kelas. Ciri dari setiap kelasnya dibedakan dari nilai 8 bit pertama dari IP Addressnya. Pada Class A, 8 oktet pertama dari IP bernilai 0 – 127. Pada Class B bernilai 128 – 191, dan Class C bernilai 192 – 223 seperti terlihat pada Tabel 6.1.

Tabel 6.1 ClassFull Addressing

Class	HOB	NET ID Bits	Host ID Bits	No of Networks	Host Per Network	Start Address	End Address
Class A	0	8	24	2^7=128	2^{24}=16,777,216	0.0.0.0	127.255.255.255
Class B	10	16	16	2^{14}=16,384	2^{16}=65,536	128.0.0.0	191.255.255.255
Class C	110	24	8	2^{21}=2,097,152	2^8=256	192.0.0.0	223.255.255.255
Class D	1110	-	-	-	-	224.0.0.0	239.255.255.255
Class E	1111	-	-	-	-	240.0.0.0	255.255.255.255

Sumber: https://networkustad.com/

Class A hingga class C merupakan IP address unicast, dimana IP tersebut digunakan untuk mengirimkan data dari satu komputer ke satu komputer lainnya. Class D merupakan IP address multicast, dimana IP address ini digunakan untuk mengirimkan data ke satu kelompok

perangkat. Sedangkat Class E merupakan class experimental yang digunakan untuk keperluan penelitian.

Pada sistem Classless Addresing tidak mengenal pembagian kelas. Penulisan subnet mask pada classless addressing dengan menggunakan prefix length.

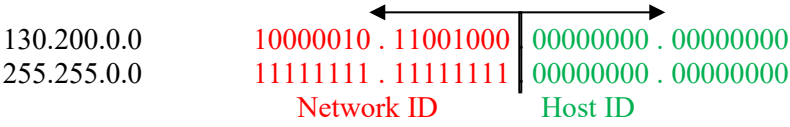
6.5 Subnetting

Merupakan cara untuk membagi suatu blok alamat network menjadi ke dalam sub jaringan yang lebih kecil (subnet). Subnetting akan membuat beberapa network tambahan tetapi akan mengurangi jumlah host tiap network nya. Subnetting dilakukan dengan mengorbankan bit yang seharusnya untuk host (Host Portion) menjadi bit subnet atau bit untuk network (network Portion).

Contoh kasus:

Terdapat suatu blok IP kelas B 130.200.0.0 dengan default mask 255.255.0.0. Dari network IP tersebut, ingin dibuat 4 Alamat subnet yang lebih kecil. Cara agar dapat membagi menjadi 4 alamat yang lebih kecil yaitu:

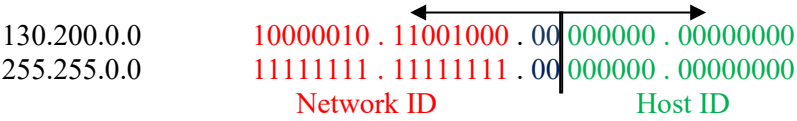
1. Ubah terlebih dahulu alamat IP dan subnetmask kedalam bentuk biner sehingga dapat dilihat batas yang mana Network ID dan yang mana Host ID.



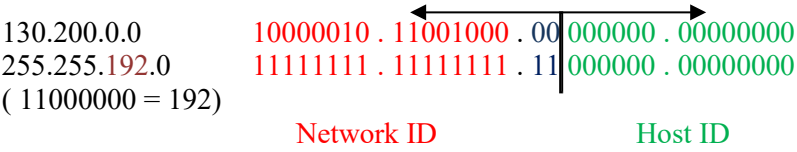
2. Tentukan jumlah bit host yang harus dikorbankan untuk menjadi bit subnet atau bit network yang baru. Jika ingin membuat 4 network baru maka jumlah bit host yang harus diambil sebanyak 2 bit. Hal ini dikarenakan jika ingin membuat jaringan yang berbeda maka alamat network (subnet) nya harus berbeda. Jika hanya diambil 1 bit maka kombinasi alamat network yang mungkin hanya 1 dan 0, sedangkan jika diambil 2 bit maka kombinasi alamat network yang mungkin menjadi 4 yaitu 00, 01, 10 dan 11. Sehingga untuk

membuat 4 subnet baru maka perlu mengorbankan 4 bit host yang akan menjadi bit subnet.

3. Sekarang korbankan 2 bit di host ID untuk menjadi network ID juga, sehingga posisi batas antara network portion dan host portion menjadi bergeser.

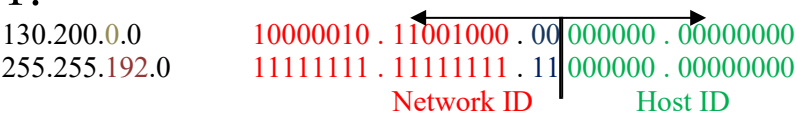


4. Karena 2 bit telah dijadikan bit network juga, maka subnet masknya harus diubah jadi satu (bit 1 menunjukan network, bit 0 menunjukan host). Karena bitnya diubah jadi 1, Jadi nilai desimalnya berubah menjadi 255.255.192.0

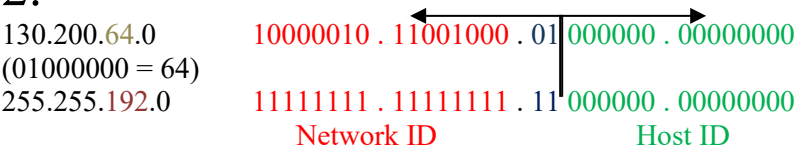


5. Dengan adanya batas baru antara network portion dan host portion maka didapat 4 alamat baru sebagai berikut:

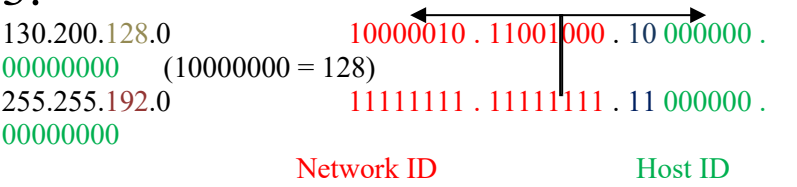
1.



2.



3.



4.

130.200.192.0 10000010 . 11001000 . 11 000000 .
00000000 (11000000 = 192)
255.255.192.0 11111111 . 11111111 . 11 000000 .
00000000

Network ID Host ID

6. Setelah mendapatkan 4 alamat network seperti diatas, selanjutnya perlu dicari alamat broadcast dan alamat host dari tiap-tiap network tersebut.

1) 10000010 . 11001000 . 00 111111 . 11111111 ➔
130.200.63.255
Network ID Host ID

2) 10000010 . 11001000 . 01 111111 . 11111111 ➔
130.200.127.255
Network ID Host ID

3) 10000010 . 11001000 . 10 111111 . 11111111 ➔
130.200.191.255
Network ID Host ID

4) 10000010 . 11001000 . 11 111111 . 11111111 ➔
130.200.255.255
Network ID Host ID

Untuk mengetahui berapa jumlah host yang dapat digunakan dalam tiap networknya dapat digunakan rumus $2^h - 2$ ➔ $2^{14} - 2 = 16382$. (h merupakan jumlah bit host ID atau host portion)

Jadi dapat disimpulkan IP host yang dapat digunakan untuk komputer pada subnetwork kedua yaitu:

130.200.64.1
130.200.64.2
…dst hingga
130.200.127.254

Alamat 130.200.127.255 udah jadi alamat broadcast sehingga tidak dapat digunakan untuk alamat PC atau perangkat.

Contoh Kasus:
Diberikan satu blok IP kelas C (subnet 255.255.255.0). Dari IP tersebut akan dibuat minimal 20 sub network baru. Tentukan subnet mask nya, dan berapa jumlah host dalam tiap network.
Jawab:
Kelas C default mask 255.255.255.0. untuk membuat network baru, perlu dikorbankan bit host nya.

11111111 . 1111111 . 1111111 . 00000000

Cari berapa bit yang harus dikorbanin untuk membentuk minimal 20 network.

- Jika ingin membuat network baru yang berbeda maka bit network atau subnet nya harus berbeda.
- Jika 2 bit yang dikorbankan menjadi bit subnet maka kombinasi networknya adalah : 00, 01, 10, 11 ➔ hanya dapat membuat 4 network.
- Jika 3 bit yang diambil maka didapat kombinasi: 000, 001, 010, 011, 100, 101, 110, 111. ➔ hanya dapet 8 network
- Jika S bit. Maka ada 2^S Sub Network yang terbentuk.
- Jika ingin didapat minimal 20 netrok baru maka : $2^S >= 20$ ➔ S= 5 ➔ menghasilkan 32 sub network. Jika S=4 maka hanya didapat 16 sub network baru

Jadi jumlah bit yang dikorbankan ada 5 bit, sehingga menjadi seperti berikut:

11111111.1111111.11111111.11111 000

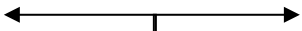
Sehingga Subnet Mask nya menjadi : 255.255.255.248

Jika 5 bit host diambil untuk bit network baru maka jumlah bit host ID nya jadi hanya tersisa 3 bit. Kombinasi dari 3 bit menghasilkan $2^3 = 8$ alamat.

Tetapi jangan lupa dikurangkan dengan 2 untuk Network address dan Broadcast address dalam tiap networknya sehingga tiap network hanya mempunyai 8 – 2 = 6 Host.

Contoh Kasus:
Dikasih satu blok IP kelas C 202.233.44.0 mask 255.255.255.255.0 dari IP ini akan dibuat 8 subnet yang beda. Tentukan kedelapan subnet tersebut, lengkap dengan broadcast addressnya, serta jumlah host dalam satu subnetnya.
Jawab :
8 subnet ➔ 2^3 jadi S = 3
Jumlah bit host ID yang dikorbankan sebanyak 3.

202.233.44.0 : 11001010 . 11101001 . 00101100 . 00000000
255.255.255.0 : 11111111 . 11111111 . 11111111 . 00000000



202.233.44.0 : 11001010 . 11101001 . 00101100 . 000 00000
255.255.255.224: 11111111 . 11111111 . 11111111 . 111 00000

Cara ngitung kedelapan network dengan cepat bisa menggunakan rumus:
256 – (subnet barunya) = 256 – 224 = 32 ➔ jadi networknya kelipatan 32. Yaitu:

1) 202.233.44.0 mask 255.255.255.224 atau /27
2) 202.233.44.32 /27
3) 202.233.44.64 /27
4) 202.233.44.96 /27
5) 202.233.44.128 /27
6) 202.233.44.160 /27
7) 202.233.44.192 /27
8) 202.233.44.224 /27

Alamat broadcast, bisa dicari dengan cepat dengan mengurangi satu dari network diatasnya sehingga alamat broadcast nya adalah:

1) 202.233.44.0 broadcast 202.233.44.31
2) 202.233.44.32 broadcast 202.233.44.63
3) 202.233.44.64 broadcast 202.233.44.95
4) 202.233.44.96 broadcast 202.233.44.127
5) 202.233.44.128 broadcast 202.233.44.159
6) 202.233.44.160 broadcast 202.233.44.191
7) 202.233.44.192 broadcast 202.233.44.223
8) 202.233.44.224 broadcast 202.233.44.255

(network = host 0 semua; broadcast = host 1 semua)

Untuk mencari jumlah host dalam satu subnet dapat dihitung dengan melihat selisih antar sub network tersebut yaitu 32. Sehingga dalam satu blok subnetwork tersebut terdapat 32 alamat dimana 1 alamat digunakan untuk alamat network dan satu alamat digunakan untuk alamat broadcast sehingga jumlah host per subnet nya berjumlah: 32 – 2 = 30 host. Atau bisa dihitung menggunakan rumus sebelumnya yaitu $2^n - 2 = 30$ host (n = jumlah bit host ID).

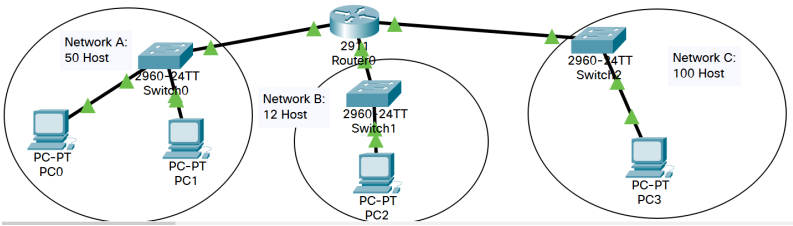
6.6 Variable Length Subnet Mask (VLSM)

Pembagian dengan subnetting yaitu membagi suatu blok IP menjadi network-network yang lebih kecil yang disebut subnetwork. Masing-masing subnetwork ini memiliki besar blok yang sama rata, dimana tiap sub netwok akan memiliki jumlah host yang sama. Pada kondisi tertentu setiap sub network bisa memiliki kebutuhan jumlah host yang berbeda-beda. Untuk melakukan pembagian berdasarkan kebutuhan yang berbeda-beda ini digunakan VLSM. Dengan menggunakan VLSM maka memungkinkan untuk membagi sub network dengan jumlah host sesuai dengan kebutuhan sub network tersebut.

Contoh Kasus:

Admin jaringan diberikan blok alamat IP 192.168.1.0/24. Sesuai dengan kebutuhan jaringan, maka perlu dibuat 3 buah sub network yaitu

Network A, B dan C. masing-masing masing network ini memiliki kebutuhan jumlah host yang berbeda, dimana network A membutuhkan 50 host, network B membutuhkan 12 host dan network C membutuhkan 100 host seperti pada Gambar 6.4.



Gambar 6.4 Contoh Kasus VLSM

Untuk menyelesaikan kasus tersebut, maka tidak bisa dengan menggunakan subnetting biasa yang akan membagi network dengan jumlah host yang sama. Jika menggunakan subnetting biasa maka:

- Untuk membagi menjadi minimal 3 sub network baru maka perlu dikorbankan 2 bit host sehingga didapat 4 kombinasi alamat yaitu 00, 01, 10 dan 11.
- Jika diambil 2 bit maka sub mask nya berubah menjadi /26 atau 255.255.255.192
- Dengan subnetmask tesebut maka akan didapat 4 blok alamat kelipatan 64 (256 – 192) yaitu:
  - 192.168.1.0 / 26 dengan alamat broadcast 192.168.1.63
  - 192.168.1.64 / 26 dengan alamat broadcast 192.168.1.127
  - 192.168.1.128 / 26 dengan alamat broadcast 192.168.1.191
  - 192.168.1.192 / 26 dengan alamat broadcast 192.168.1.255
- Jumlah host per subnet dari kedua alamat tersebut berjumlah 64 alamat atau $2^6 – 2$.
- Network C memerlukan 100 host sedangkan yang tersedia hanya 64 host, maka tidak memenuhi kebutuhan dari network C.

Jika menggunakan VLSM maka langkah yang dilakukan sebagai berikut:

- Buat blok subnet dengan pembagian blok yang memiliki kebutuhan terbesar dibagi terlebih dahulu. Pembagian dimulai dari alamat awal blok subnet asal, yaitu 192.168.1.0/24.
- Kebutuhan host terbesar yaitu sebanyak 100 host pada network C sehingga harus dibagi terlebih dahulu. Buat subnet mask baru untuk kebutuhan 100 host. Jika dibutuhkan minimal 100 host, maka jumlah bit host yang mendekati adalah 7 bit atau $2^7 - 2$ yaitu sebanyak 126 host (lebih besar dari 100).
- Tentukan subnetmask serta alamat broadcast untuk network C. Jumlah bit host yang diperlukan untuk kebutuhan network C adalah 7 bit sehingga subnet mask nya menjadi /25. Total bit pada IP sebesar 32, sehingga jika 7 bit digunakan untuk host maka bit yang tersisa untuk network sejumlah 32 – 7 = 25 bit atau prefix length /25 atau 255.255.255.128.
- Cari alamat broadcast untuk network C dengan cara membuat bit host menjadi 1 semua. Sehingga didapat jumlah alamat broadcast yaitu 192.168.1.127. sehingga untuk network C didapat alamat seperti berikut:
  - Alamat network: 192.168.1.0
  - Subnet mask 255.255.255.128
  - Broadcast : 192.168.1.127
  - Host yang bisa digunakan sebanyak 126 yaitu mulai dari 192.168.1.1 hingga 192.168.1.126.
- Setelah alamat network C didapat selanjutnya dicari lagi network dengan jumlah kebutuhan host terbesar selanjutnya yaitu network A dengan kebutuhan 50 host. Tentukan alamat network dari network A, yaitu merupakan alamat selanjutnya setelah blok alamat network C. alamat terakhir di network C yaitu 192.168.1.127 maka alamat berikutnya yaitu 192.168.1.128 merupakan alamat network dari network A.
- Setelah alamat network didapat kemudian tentukan subnet mask dari network A sesuai kebutuhan. Berdasarkan kebutuhan network A berjumlah minimum 50 host, maka jumlah bit host yang diperlukan

sebanyak 6 bit atau $2^6 – 2$ yaitu 62 host. Untuk memenuhi kebutuhan 50 host dari network A diperlukan sebanyak 6 bit host yang mampu menghasilkan sebanyak 62 host (lebih besar dari 50).

- Jika 6 bit digunakan untuk host maka jumlah bit yang digunakan untuk network yaitu 32 – 6 = 26 atau prefix length /26 atau subnet mask 255.255.255.192.
- Langkah selanjutnya yaitu mencari alamat broadcast. Jika ada alamat network 192.168.1.128 /26 maka didapat alamat broadcast yaitu 192.168.1.191. sehingga untuk network A didapat alamat seperti berikut:
  - Alamat network: 192.168.1.128
  - Subnet mask 255.255.255.192
  - Broadcast : 192.168.1.191
  - Host yang bisa digunakan sebanyak 62 yaitu mulai dari 192.168.1.129 hingga 192.168.1.190.
- Selanjutnya untuk network B terlebih dahulu ditentukan alamat network nya. Alamat network dari network B merupakan alamat selanjutnya dari network A yang telah didapat sebelumnya. Alamat terakhir atau alamat broadcast dari network A yaitu 192.168.1.191 sehingga alamat selanjutnya adalah 192.168.1.192 yang akan menjadi alamat network dari network B.
- Langkah berikutnya yaitu mencari subnet mask dari network B sesuai dengan kebutuhan jumlah host. Network B memerlukan 12 Host sehingga jumlah bit host yang diperlukan untuk network B yaitu 4 bit atau $2^4 – 2 = 14$ host (lebih besar dari yang dibutuhkan yaitu 12). Jika diperlukan jumlah bit host sebanyak 4 bit maka jumlah bit network sebanyak 32 – 4 = 28 bit. Sehingga didapat prefix length /28 atau 255.255.255.240.
- Setelah didapatkan subnet mask selanjutnya dicari broadcast nya. Alamat network 192.168.1.192 dengan sabnet mask 255.255.255.240 maka didapat alamat broadcast yaitu 192.168.1.207. Sehingga untuk network B didapat alamat seperti berikut:

- Alamat network: 192.168.1.192
- Subnet mask 255.255.255.240
- Broadcast : 192.168.1.207
- Host yang bisa digunakan sebanyak 14 yaitu mulai dari 192.168.1.193 hingga 192.168.1.206.

Sehingga dapat disimpulkan untuk membagi alamat berdasarkan Gambar 6.4 maka didapat alamat seperti pada Tabel 6.2.

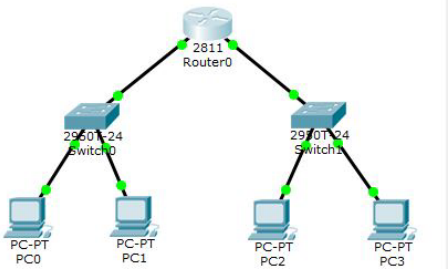
Tabel 6.2 Hasil Pembagian IP dengan VLSM

Subnet	Kebutuhan	Alokasi	Alamat Network	Prefix Length	Subnet Mask	Host	Broadcast
C	100	126	192.168.1.0	/25	255.255.255.128	192.168.1.1 – 192.168.1.126	192.168.1.127
A	50	62	192.168.1.128	/26	255.255.255.192	192.168.1.129 – 192.168.1.190	192.168.1.191
B	12	14	192.168.1.192	/28	255.255.255.240	192.168.1.193 – 192.168.1.206	192.168.1.207

Ketiga network dari A, B dan C mempunyai subnet mask yang berbeda-beda, inilah yang disebut sebagai Variable Length Subnet Mask (VLSM). Jika dilihat IP terakhir yang digunakan yaitu 207 sehingga masih bisa membuat alamat network lainnya setelah ip 207 tersebut. Permasalahan pada VLSM adalah tidak semua protokol routing yang bisa mendukung pembagian IP menggunakan VLSM. Protokol routing yang classfull seperti RIP tidak bisa digunakan jika pembagian IP jaringannya menggunakan VLSM.

6.7 Tugas

Buat jaringan seperti topologi Gambar 6.3 dengan menggunakan paket tracer.



Gambar 6.5 Tugas Subnetting

Gunakan blok alamat IP 192.168.1.xxx. Setiap network hanya memiliki 2 buah komputer yang terhubung. Atur subnet yang diperlukan dengan alamat host seminimal mungkin. Setiap komputer harus terhubung dengan komputer lainnya (dapat dicoba dengan perintah ping).

BAB 7
Dasar Routing (Statis dan Dinamis)

Capaian Pembelajaran:

1. Memahami konsep dasar routing.
2. Memahami konsep routing statis dan routing dinamis.
3. Memahami konsep Distance Vector dan Link State.

7.1 Dasar Routing

Router dalam memforward paket ke tujuan dengan melihat alamat IP tujuan dari paket tersebut. Dalam jaringan komputer setiap Router akan terhubung ke banyak router lain. Ibarat sebuah jalan, di tiap persimpangan terdapat rambu-rambu penunjuk arah yang akan memandu pengendara untuk sampai pada tujuannya. Pada tiap router terdapat persimpangan/koneksi ke arah router lain, sehingga router harus mengetahui ke arah manakah suatu paket tersebut akan diteruskan. Untuk mengetahui ke arah mana paket diteruskan, router harus mempunyai data arah jalan berdasarkan alamat IP. Data arah jalan ini disebut tabel routing. Setiap paket yang datang ke router, router akan membaca alamat IP tujuan dari paket tersebut. Router kemudian membaca tabel routing yang dia punya untuk melihat kearah manakah paket tersebut akan diteruskan. Jika tujuan paket tidak ada di dalam tabel routing sebuah router, maka router akan membuang paket tersebut dan memberikan balasan "Destination Host Unreacheble"

Ada dua cara router dalam membuat tabel routing yaitu secara static yang disebut sebagai routing statik dan secara dinamik yang disebut routing dinamik. Pada routing statik setiap router harus dikonfigurasi oleh admin untuk memberi tahu jalan yang akan dituju oleh paket yang lewat. Setiap tujuan yang mungkin akan di tuju oleh paket didefinisikan oleh admin dan dimasukkan secara manual ke dalam konfigurasi router. Routing static akan efektif jika jaringan yang dimanajemen tidak terlalu besar, atau setiap router nya tidak memiliki banyak jalan alternatif.

Peran admin akan sangat berpengaruh dalam menentukan tujuan paket. Jika admin salah dalam melakukan konfigurasi maka bisa terjadi looping dimana suatu paket beredar memutar di jaringan tanpa sampai ke tujuan. Routing statik mempunyai keunggulan dalam penggunaan resource router serta bandwidth. Dalam membentuk tabel routing, routing statis tidak perlu menggunakan protokol routing yang akan berkomunikasi dengan router-router lainnya sehingga tidak memakan bandwidth atau resource router (CPU dan Memory).

Pada Routing dinamik, admin cukup mengkonfigurasi network-network yang akan terhubung langsung dengan router tersebut, tanpa memikirkan ke arah mana seharusnya paket dilewatkan. Setiap router akan saling berkomunikasi bertukar pesan menggunakan algoritma protokol routing tertentu. Hasil komunikasi antar router ini akan membuat sebuah tabel routing yang akan menentukan ke arah mana paket dikirim. Routing dinamik sangat efektif jika digunakan dalam jaringan yang memiliki banyak jalur alternatif. Admin juga tidak perlu repot untuk memasukkan semua alternatif jalan ke arah tujuan. Kelemahan routing dinamik yaitu ada nya proses komunikasi untuk membentuk tabel routing yang akan memakan bandwidth dan resource router tersebut.

Tabel 7.1 Perbedaan Routing Statik dan Routing 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

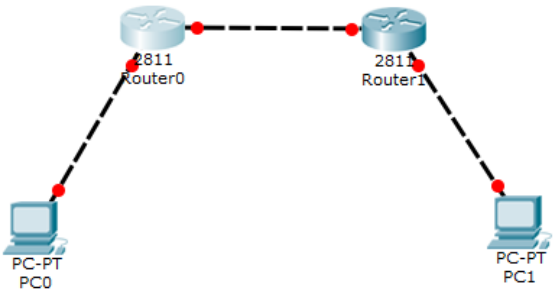
Dalam membentuk tabel routing dengan routing dinamik terdapat berbagai protokol routing diantaranya RIP, RIPv2, EIGRP, OSPF, BGP. Protokol routing ini dikelompokkan berdasarkan lingkup kerjanya yaitu Interior Routing Protocol (IGP) dan Exterior Routing Protocol (EGP). IGP merupakan routing protocol yang bekerja dalam satu Autonomous System (AS). AS merupakan kelompok yang terdiri satu atau lebih IP prefix yang dibawah satu control administrative misal satu ISP (Internet Service Provider). Contoh protokol IGP yaitu RIP, RIPv2, EIGRP, OSPF dan lainnya. EGP merupakan routing protocol untuk menghubungkan antar IGP contoh protokol EGP yaitu BGP.

Protokol Routing juga dapat dikelompokkan berdasarkan cara berkomunikasi dan mendapatkan jalur untuk tabel routing yaitu Distance Vector dan Link-State. Distance Vector yaitu protokol routing yang akan mencari jalur berdasarkan jarak dan arah terdekat (Hop Counts). Jarak terdekat dilihat dengan berapa banyak router yang dilalui untuk mencapai tujuan. Link-state merupakan protokol routing yang mencari jalur berdasarkan biaya (cost) yang dapat memperhitungkan delay, bandwidth serta kondisi link lainnya. Jika dianalogikan sebagai GPS, Distance Vector akan mencari jalur dengan jarak terpendek, sedangkan Link-State akan berusaha untuk mencari jalur dengan waktu tercepat. Perbedaan lainnya dari Distance Vector dan Link-state yaitu cara berkomunikasi dengan router lainnya. Distance Vector akan mengirimkan update informasi mengenai tabel routing yang dipunya ke router tetangganya secara periodic, sedangkan link-state akan mengirimkan update informasi mengenai perubahan status link jika ada perubahan dari status link tersebut, misal dari link yang sebelumnya hidup menjadi mati, atau adanya perubahan bandwidth dari link tersebut.

7.2 Simulasi Routing menggunakan Packet Tracer

1) Routing Statis

Buka Packet Tracer, buat topologi seperti Gambar 7.1.



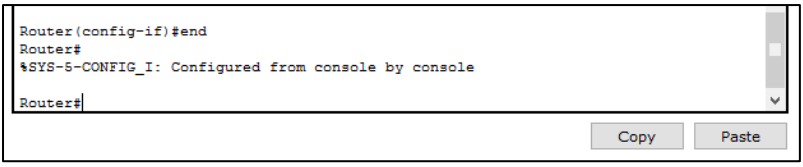
Gambar 7.1 Topologi Routing

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

Jangan lupa untuk mengatur gateway pada setiap PC. IP Gateway adalah IP Router pada interface yang satu network dengan PC0. Jika sudah di konfigurasi sesuai dengan konfigurasi diatas, lakukan test ping dari PC0 ke PC1. Lakukan pada mode simulasi, kemudian amati sampai dimana paketnya terkirim dan amati pula balasan pada perintah ping di command prompt.

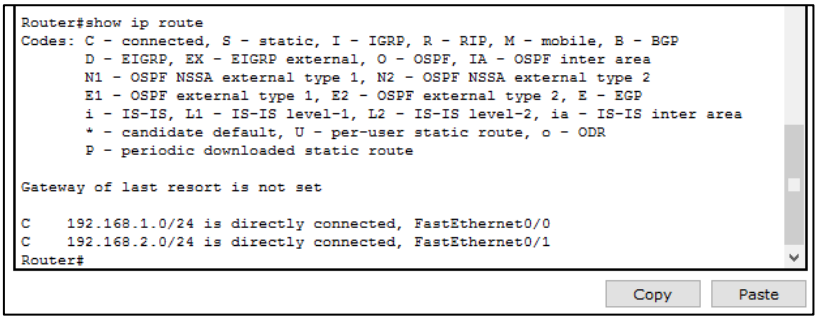
Cek tabel routing pada setiap router, caranya yaitu:

- Klik 2x pada Router0
- Masuk ke bagian CLI
- Masukan perintah end, kemudian tekan enter 2x.



Gambar 7.2 CLI Router

- Masukkan perintah “show ip route”

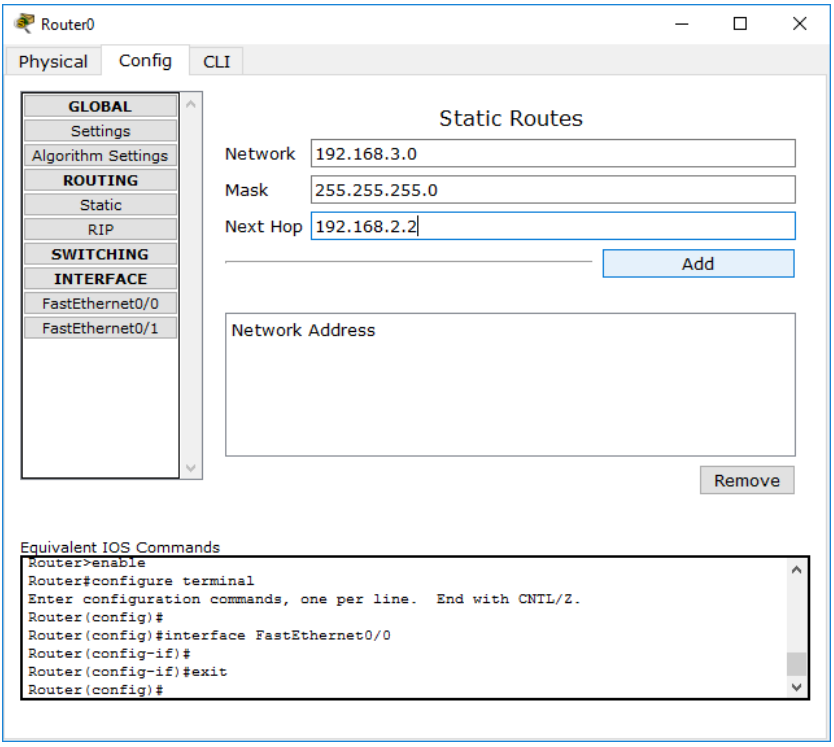


Gambar 7.3 Show Ip Route

- Lakukan perintah yang sama pada Router1 kemudian catat hasilnya.

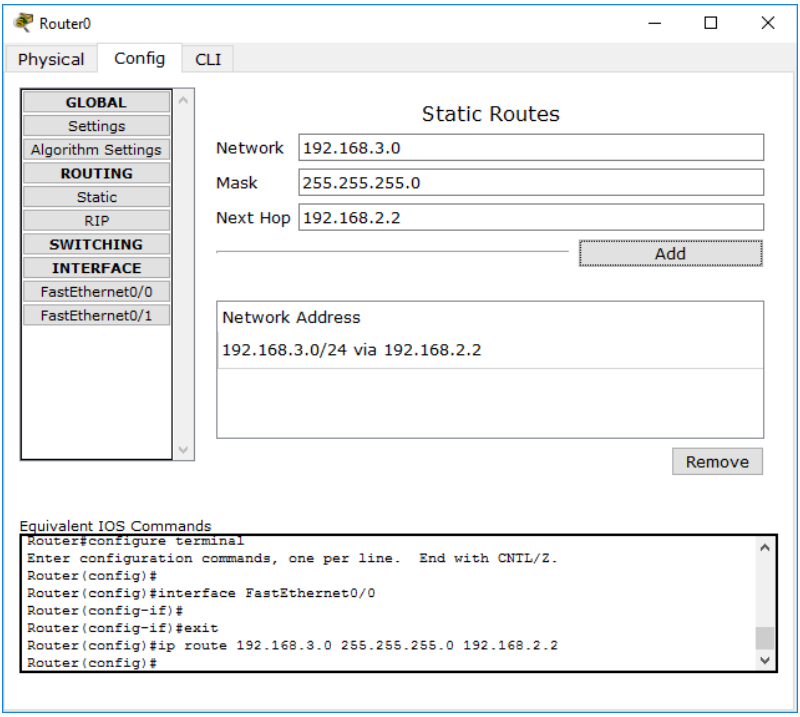
Masukan routing statis dengan cara berikut:

- Klik pada Router0, masuk ke bagian Config.
- Masuk ke menu Routing Static.
- Masukkan alamat IP sebagai berikut



Gambar 7.4 Konfigurasi Routing Static

- Klik Tombol Add sehingga muncul seperti Gambar 7.5

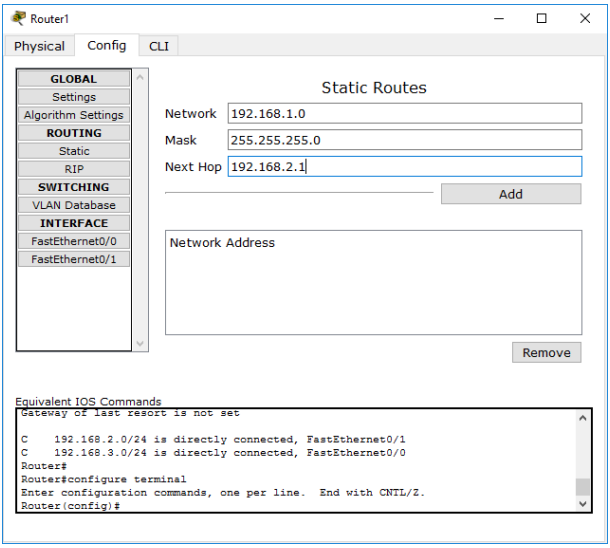


Gambar 7.5 Penambahan Routing Static

Konfigurasi diatas 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).

Lakukan perintah “show ip route” sama seperti langkah sebelumnya pada router0 dan router1. Amati perbedaan dengan sebelumnya. Lakukan Ping kembali dari PC0 ke PC1 pada mode simulasi, amati perjalanan paket yang terjadi.

Tambahkan router statis pada router1 dengan cara yang sama. Masukkan seperti Gambar 7.6.



Gambar 7.6 Routing Statis pada Router 1

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.

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

2) Routing Dinamis menggunakan RIP

Pada routing statis 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 statis.

Buat topologi sama seperti pada praktek routing statis. Konfigurasi IP interface yang sama juga seperti praktek sebelumnya.

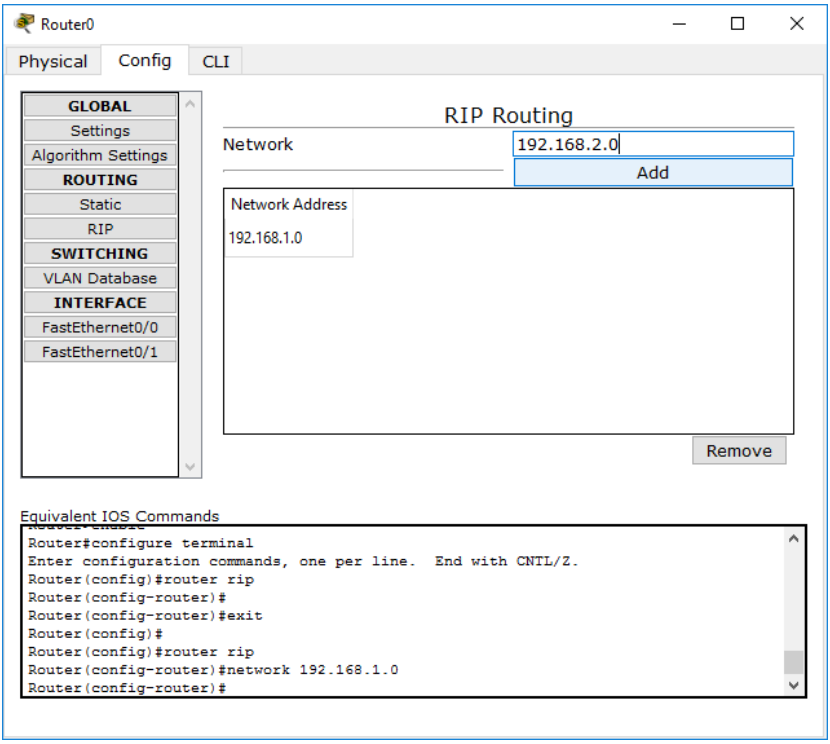
PC0 : 192.168.1.2/24

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

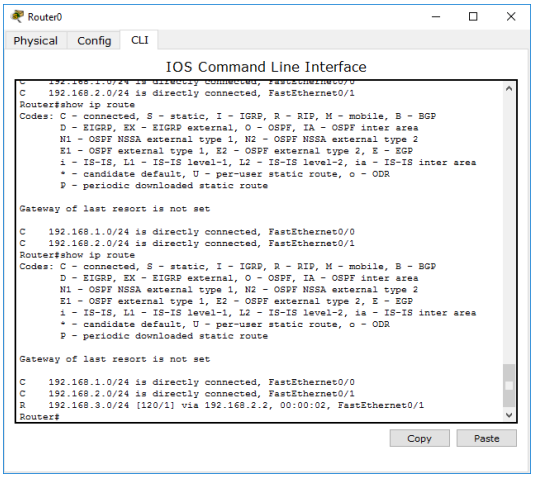
PC1 : 192.168.3.2/24

Lakukan langkah pengamatan yang sama seperti pada praktek routing statis, yang berbeda hanya pada saat konfigurasi routing. Lakukan konfigurasi routing seperti gambar dibawah.



Gambar 7.7 Konfigurasi RIP

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. Pada Router1 dimasukkan network 192.168.2.0 dan 192.168.3.0. 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 RIP nya maka hasil tabel routing seperti Gambar 7.8.



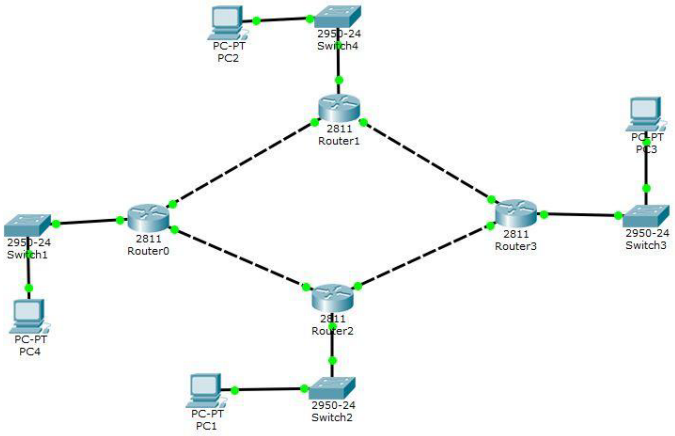
Gambar 7.8 Show IP Route RIP

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.

Lakukan tes ping dari PC0 ke PC1, amati hasilnya.

7.3 Tugas

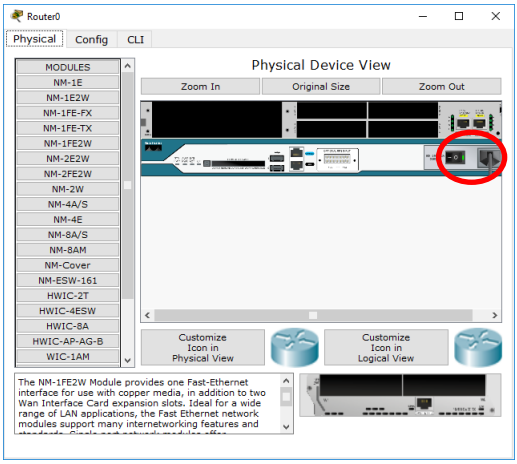
Buat jaringan seperti Gambar 7.9.



Gambar 7.9 Tugas Routing

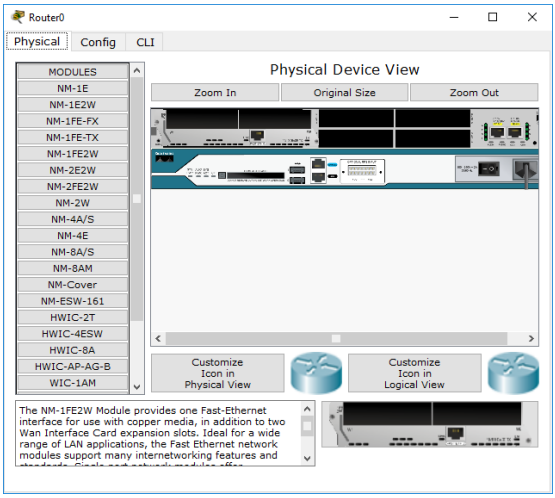
Setiap router harus mempunyai 3 interface Ethernet, secara default Router 2811 hanya memiliki 2 port FastEthernet sehingga perlu ditambah modul Ethernet lagi. Untuk menambah modul bisa dilakukan dengan langkah berikut:

- Matikan Router dengan menekan tombol power



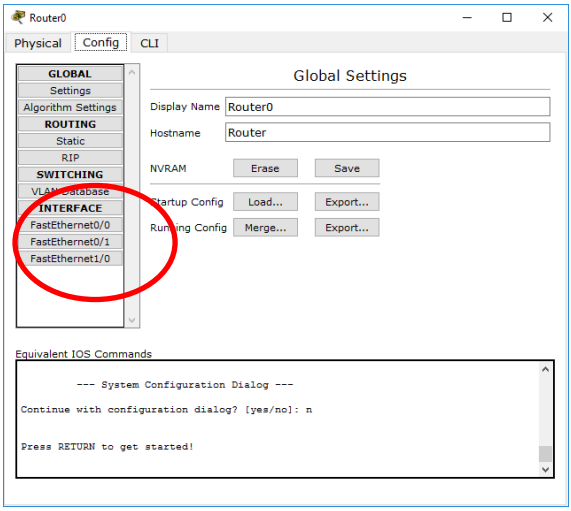
Gambar 7.10 Mematikan Router

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



Gambar 7.11 Menambah Slot Router

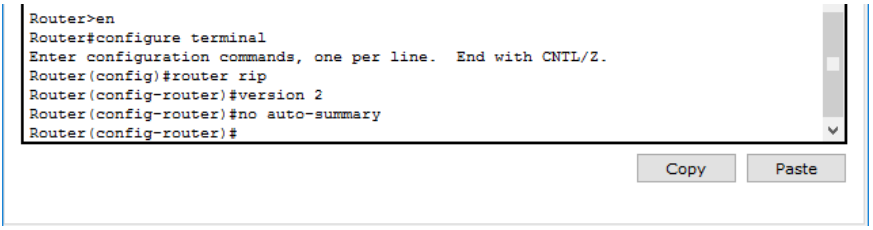
- Hidupkan kembali routernya dengan menekan tombol power.
- Untuk mengecek apakah interface sudah terpasang dengan benar bisa masuk ke bagian interface di tab confing, muncul 3 interface.



Gambar 7.12 Interface Baru

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 7.13 Konfigurasi RIP Version 2

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 8
Pengenalan VMWare dan Mikrotik

Capaian Pembelajaran:

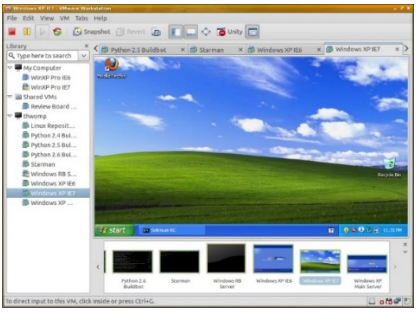
1. Mampu mengimplementasikan router Mikrotik pada jaringan.
2. Mampu menggunakan fitur Hotspot Login pada Mikrotik.
3. Mampu menerapkan manajemen bandwidth pada Mikrotik.

8.1 Dasar VMWare dan Mikrotik

1) VMWare

VMWare merupakan software untuk virtual machine yang berfungsi untuk menjalankan sistem operasi secara virtual dalam satu perangkat keras yang telah memiliki sistem operasi lainnya. Misal pada komputer dengan sistem operasi windows 10 kemudian di install aplikasi VMWare, pada aplikasi VMWare kemudian diinstall sistem operasi linux mint, sehingga seolah-olah (secara virtual) mempunyai 2 komputer dengan windows 10 dan linux mint yang terhubung melalui jaringan.

VMWare mengeluarkan produk Player dimana pengguna dapat menggunakan aplikasi ini secara gratis, tetapi dibatasi hanya dapat menjalankan satu buah mechine secara virtual. Produk lainnya yaitu VMWare Workstation yang berbayar. Pada VMWare Workstation dapat menjalankan lebih dari satu mechine (Sistem Operasi) secara virtual.



Gambar 8.1 Tampilan VMWare

Selain VMWare terdapat produk lain yang sejenis yang dapat menjalankan Sistem Operasi secara virtual, contohnya yaitu VirtualBox, Microsoft Virtual PC dan lainnya.

2) Mikrotik

MikroTik RouterOS™ adalah sistem operasi Router yang handal dengan berbagai fitur jaringan. MikroTik RouterOS dibuat oleh perusahaan Mikrotik di Latvia yang dibentuk oleh Johnson Trully dan Armin Riekstins. Dengan adanya MikroTik RouterOS, kita dapat membuat sebuah komputer menjadi Router dengan berbagai fitur. Fitur tersebut yaitu Routing, Firewall, NAT, Hotspot, Tunneling Protocol, DNS server, DHCP Server, dan lainnya. MikroTik RouterOS layaknya sebuah sistem operasi yang dapat dipasang di komputer. Untuk menginstall RouterOS diperlukan 1 buah harddisk yang akan difungsikan penuh untuk RouterOS tersebut. Untuk menjalankan fungsi Router, komputer yang di install RouterOS harus memiliki lebih dari satu interface jaringan. Konfigurasi RouterOS dapat dilakukan menggunakan CLI layaknya Router Cisco, atau juga dapat menggunakan aplikasi Winbox maupun konfigurasi melalui browser layaknya Router Wireless.

Mikrotik selain membuat RouterOS juga membuat RouterBoard yang layaknya seperti minipc yang terinstall RouterOS didalamnya. RouterBoard ini sangat digemari oleh masyarakat karena harganya yang relative murah dengan fitur yang banyak. Mikrotik memang sering digunakan untuk jaringan menengah ke bawah seperti Warnet, kantor kecil, sekolah, hotel, cafe dan lainnya. Fitur yang banyak digemari dari Mikrotik yaitu Hotspot Login, dimana user akan diminta autentikasi terlebih dahulu ketika ingin mengakses jaringan yang terhubung dengan mikrotik tersebut. Fitur Hotspot Login banyak dimanfaatkan di Hotel, café, warnet.

RouterBoard lebih digemari dibandingkan hanya membeli RouterOS. Dengan menggunakan RouterBoard, maka tidak perlu bergantung pada PC lagi. RouterBoard memiliki ukuran yang lebih

kecil, dan lebih hemat listrik dibandingkan penggunaan PC untuk router.

Gambar 8.2 Tampilan Mikrotik

Gambar 8.3 Board Mikrotik

Mikrotik RouterOS bukan sistem operasi yang gratis, sehingga jika ingin memanfaatkan secara penuh maka diperlukan lisensi dari MikroTikls. Lisensi pada mikrotik menggunakan level yang akan menentukan fitur dan layanan. Level Mikrotik dimulai dari 0 hingga 6, dimana level 0 merupakan level yang diberikan secara gratis oleh Mikrotik, sedangkan level 6 merupakan level dengan fitur terlengkap dari Mikrotik sehingga harganya juga lebih mahal. Berikut level lisensi dari Mikrotik:

- Level 0 (gratis); tidak membutuhkan lisensi untuk menggunakannya dan penggunaan fitur hanya dibatasi selama 24 jam setelah instalasi dilakukan.
- Level 1 (demo); pada level ini kamu dapat menggunakannya sbg fungsi routing standar saja dengan 1 pengaturan serta tidak memiliki limitasi waktu untuk menggunakannya.

- Level 3; sudah mencakup level 1 ditambah dengan kemampuan untuk menajemen segala perangkat keras yang berbasiskan Kartu Jaringan atau Ethernet dan pengelolan perangkat wireless tipe klien.
- Level 4; sudah mencakup level 1 dan 3 ditambah dengan kemampuan untuk mengelola perangkat wireless tipe akses poin.
- Level 5; mencakup level 1, 3 dan 4 ditambah dengan kemampuan mengelola jumlah pengguna hotspot yang lebih banyak.
- Level 6; mencakup semua level dan tidak memiliki limitasi apapun.

Selain lisensi itu juga terdapat lisensi CHR (Cloud Hosted Router) yang merupakan versi RouterOS yang berjalan pada virtual machine. CHR memiliki semua fitur dari RouterOS dengan lisensi yang berbeda. CHR memiliki 4 level lisensi, yaitu:

- Free
- p1 perpetual-1 ($45)
- p10 perpetual-10 ($95)
- p-unlimited perpetual-unlimited ($250)

Tabel 8.1 Lisensi Mikrotik

License	Speed limit	Price
Free	1Mbit	FREE
P1	1Gbit	$45
P10	10Gbit	$95
P-Unlimited	Unlimited	$250

Perbedaan dari keempat lisensi tersebut yaitu dari segi kecepatan pada tiap interfacenya. Untuk lisensi free dibatasi hanya memiliki kecepatan 1 Mbps setiap interfacenya. CHR Free cukup untuk penggunaan sekala kecil atau untuk pembelajaran.

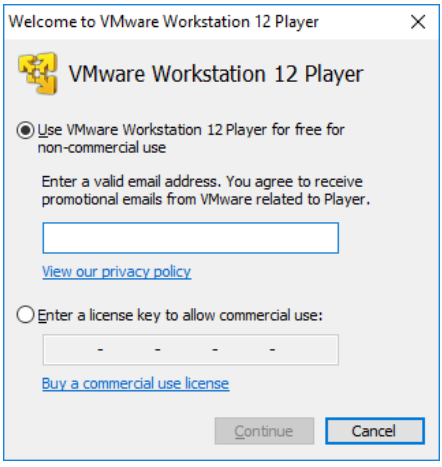
8.2 Praktek Penggunaan VMWare

Pada praktikum ini, akan diinstall OS linux pada VMWare, langkahnya yaitu:

- Install VMWare Player

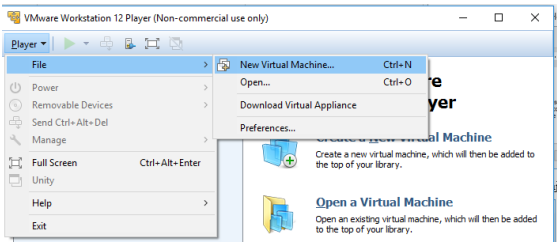
Gambar 8.4 Instalasi VMWare Player

- Jalankan VMWare Player, masukan email untuk menjalankan pertama kali.



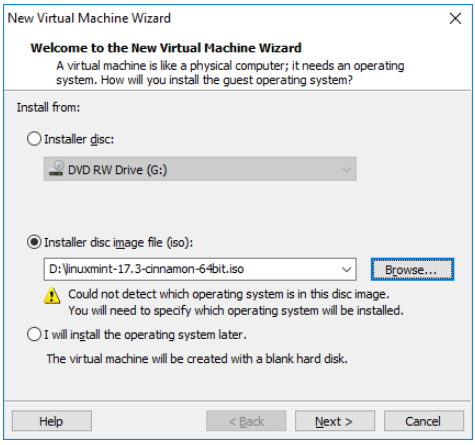
Gambar 8.5 Input email

- Buat mesin virtual baru, Klik Player, File, New Virtual Machine.



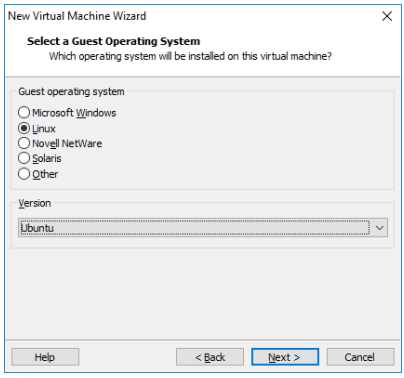
Gambar 8.6 Buat Mesin Virtual Baru

- Pilih Installer disc image file (iso), klik browse, pilih file ISO linux mint.



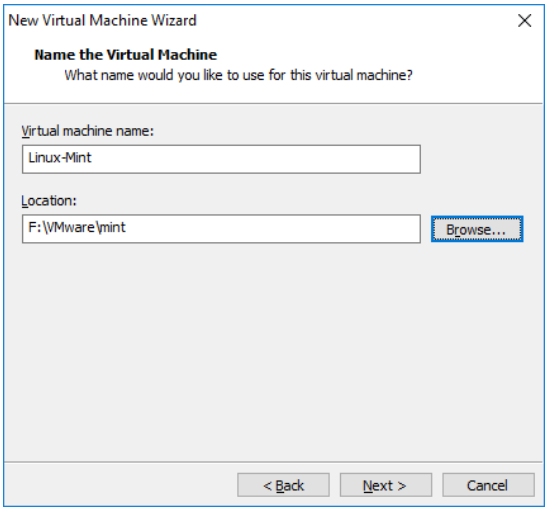
Gambar 8.7 Konfigurasi Image File

- Klik next, pilih linux version Ubuntu.



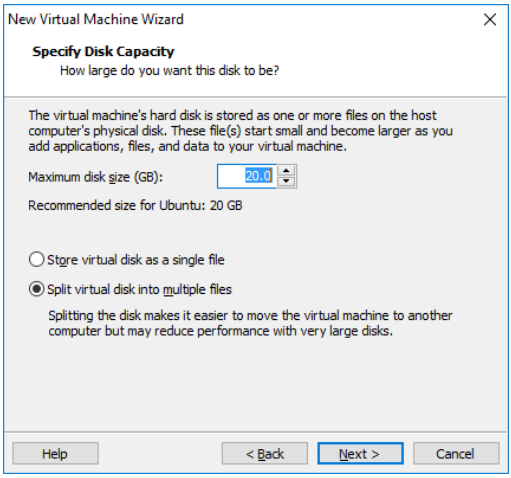
Gambar 8.8 Konfigurasi Versi Linux

- Masukkan nama virtual machine, beserta lokasi penyimpanan file untuk virtual machine.



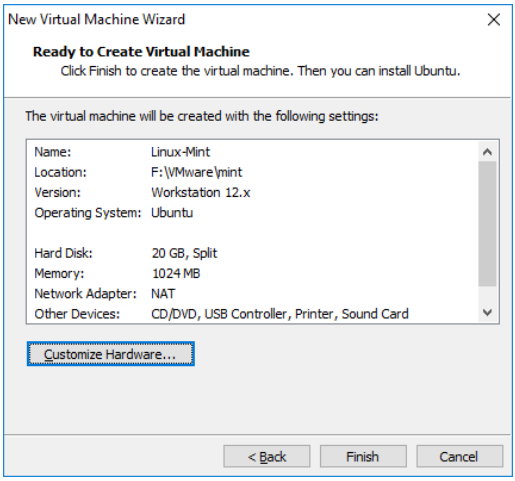
Gambar 8.9 Konfigurasi Lokasi Penyimpanan

- Masukkan jumlah maksimum kapasitas harddisk yang akan digunakan dan metode penyimpanannya



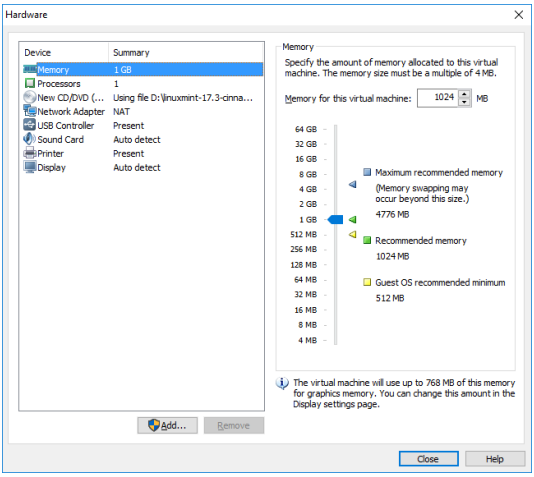
Gambar 8.10 Konfigurasi Harddisk

- Untuk mengatur hardware machine virtual, klik Costumize Hardware.



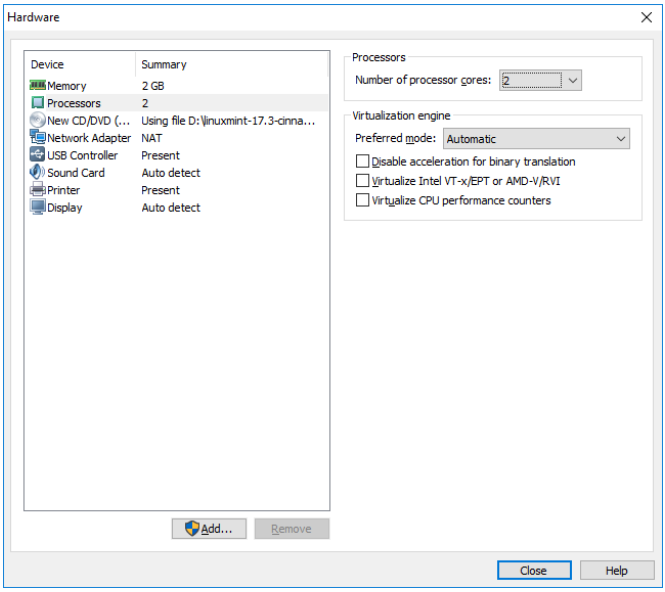
Gambar 8.11 Costumize Hardware

- Atur RAM yang akan digunakan, RAM ini akan mengambil RAM dari komputer yang digunakan. Jika menggunakan komputer yang besar (masih banyak free RAM) memory virtual dapat diperbesar, misal 2 GB.



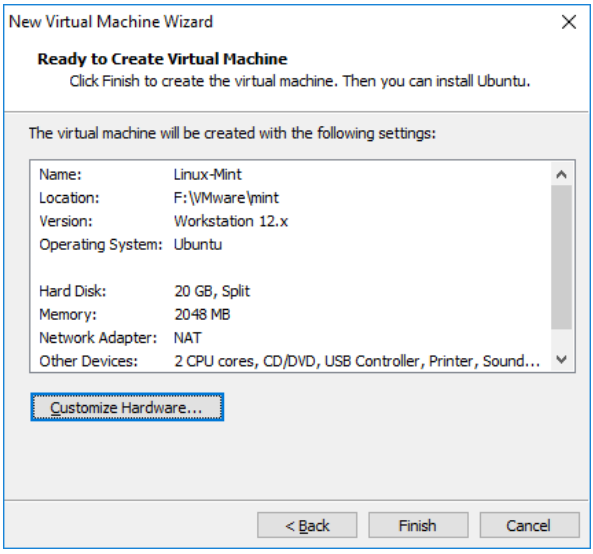
Gambar 8.12 Konfigurasi RAM

- Untuk jumlah core prosesor dapat diatur, misal menggunakan 2 core.



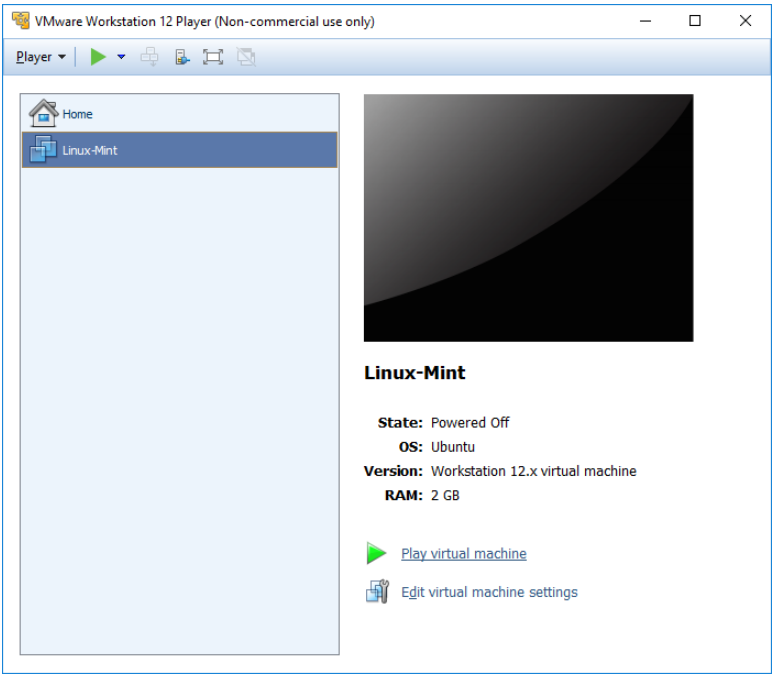
Gambar 8.13 Konfigurasi Prosesor

- Close jika selesai mengatur konfigurasi. Dan klik finish.



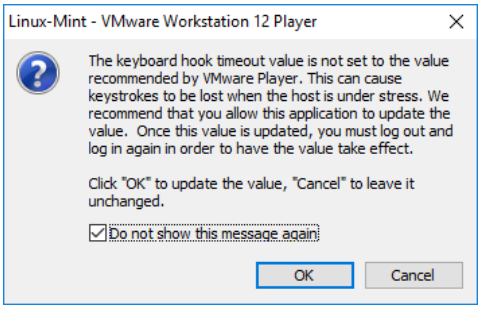
Gambar 8.14 Selesai Konfigurasi

- Untuk menjalankan Virtual Machine, klik play virtual machine.



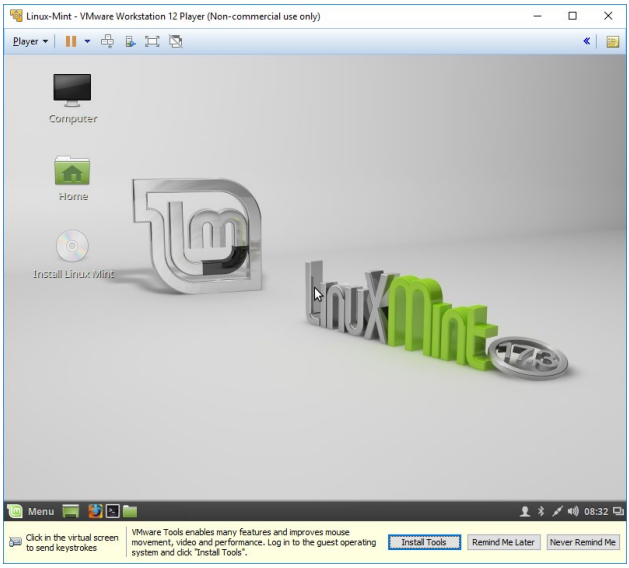
Gambar 8.15 Menjalankan Virtual Machine

- Klik OK jika muncul notifikasi keyboard.



Gambar 8.16 Notifikasi Keyboard

- Machine virtual sudah berhasil menjalankan instalasi linux mint. Selanjutnya dapat melakukan instalasi seperti pada komputer biasa.

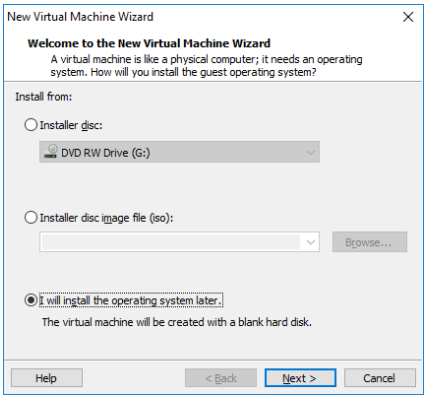


Gambar 8.17 Linux Mint pada WMWare

8.3 Praktek Penggunaan Mikrotik CHR

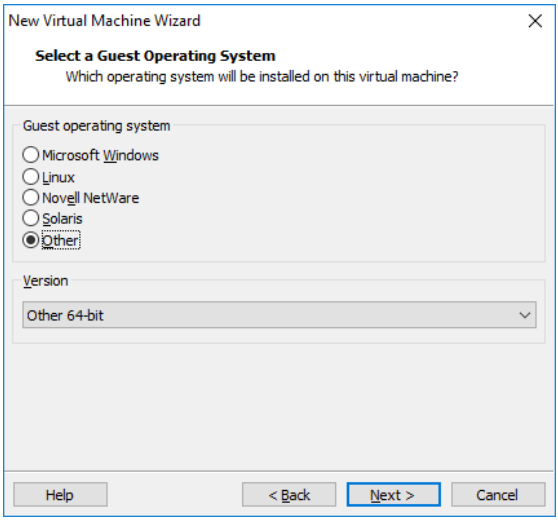
Untuk pembelajaran, dapat menggunakan mikrotik RouterOS CHR free yang berjalan pada Virtual Machine. RoterOS CHR dapat di download di website mikrotik https://mikrotik.com/download. Pilih format yang akan di download, untuk VMWare dapat memilih format VMDK. Langkah menjalankan RouterOS CHR pada mikrotik yaitu:

- Bikin virtual machine baru dengan memilih Create a New Virtual Machine, kemudian pilih I will install the operating system leter.



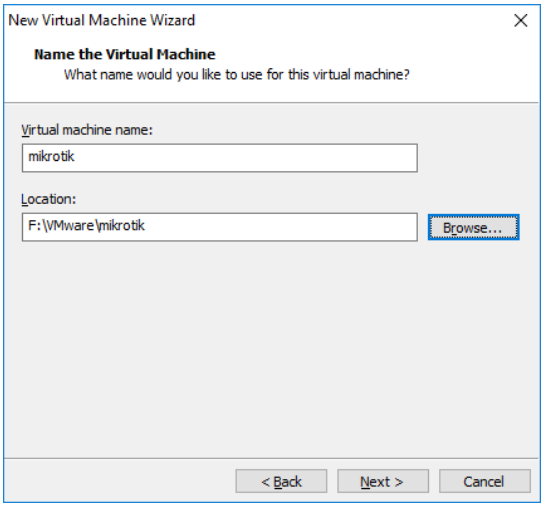
Gambar 8.18 Membuat Virtual Machine Mikrotik

- Pilih Other 64-bit



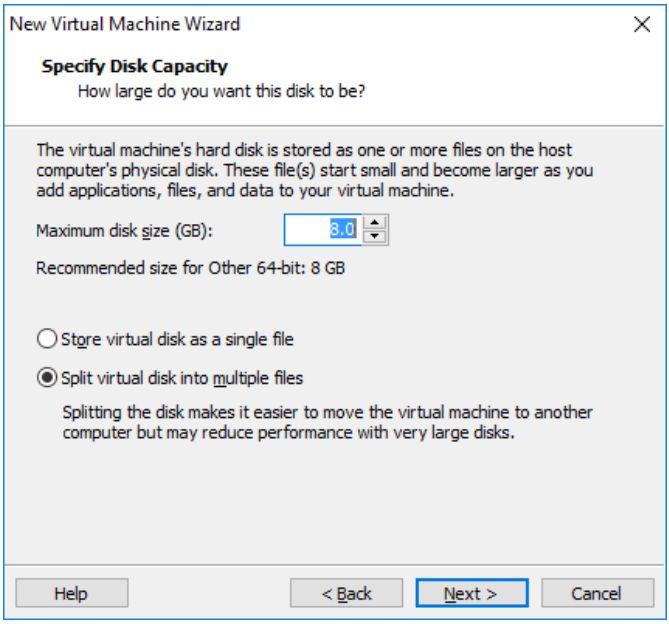
Gambar 8.19 Konfigurasi Sistem Operasi

- Input nama machine dan lokasi penyimpanan datanya. Disarankan untuk membuat folder baru. Misal disimpan pada direktori F:/VMware/mikrotik



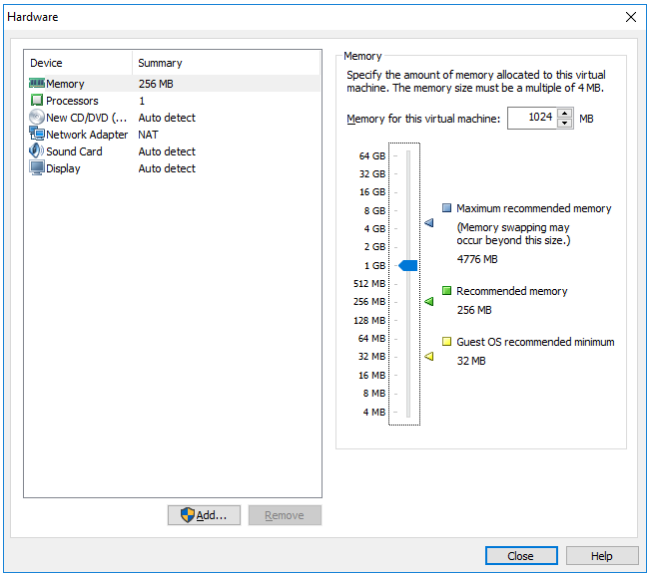
Gambar 8.20 Konfigurasi Lokasi Penyimpanan

- Klik next di split virtual disk



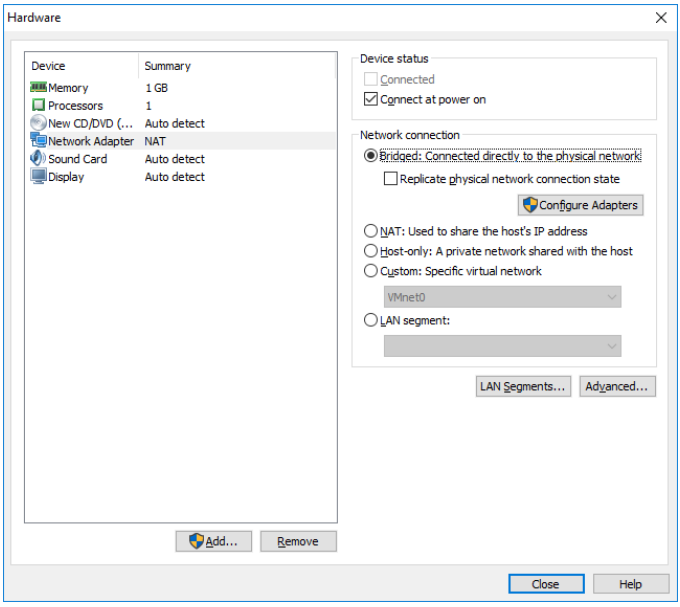
Gambar 8.21 Konfigurasi Harddisk

- Pilih Customize Hardware, kemudian sesuaikan dengan memory yang ingin digunakan.



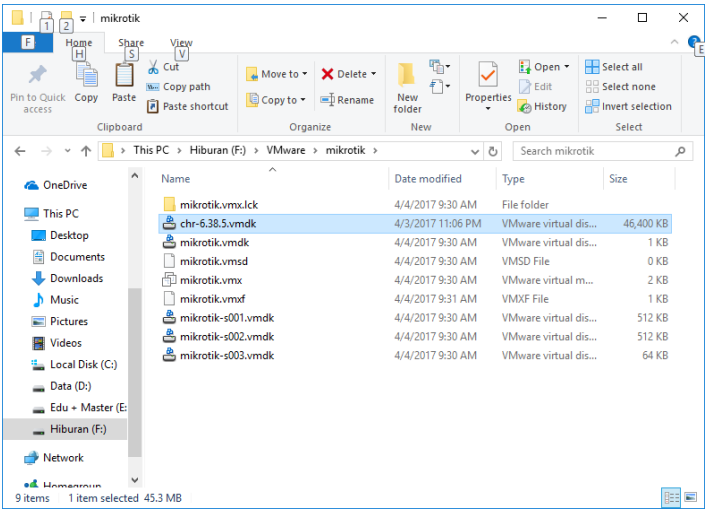
Gambar 8.22 Konfigurasi RAM

- Pada Network Adapter, pilih Bridged



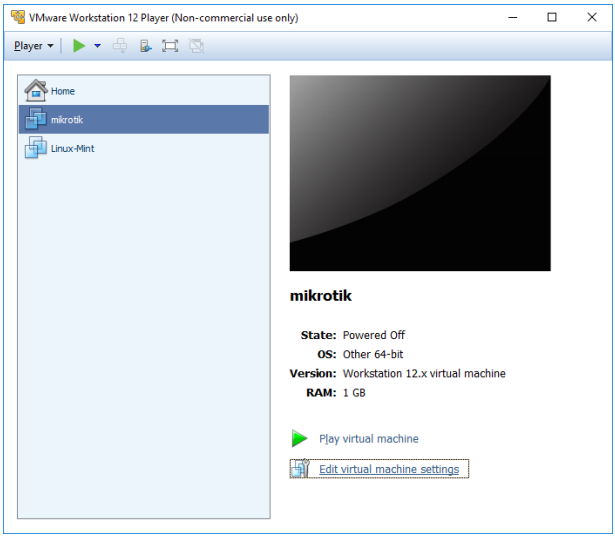
Gambar 8.23 Konfigurasi Jaringan

- Close dan finish, sehingga terbuat virtual machine baru.
- Copy file CHR yang di download ke dalam folder virtual machine yang dibuat (F:/VMware/mikrotik)



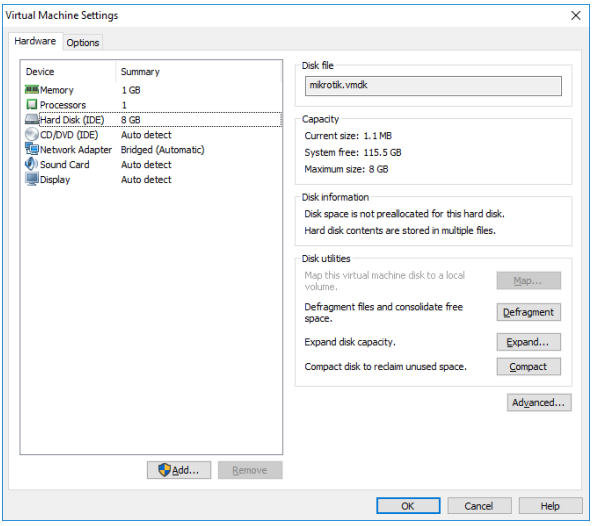
Gambar 8.24 Memasukkan file CHR

- Selanjutnya masukkan image mikrotik ke dalam virtual machine tersebut. Caranya masuk ke Edit virtual machine settings.



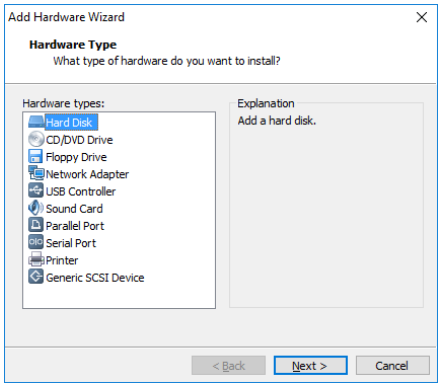
Gambar 8.25 Edit Virtual Machine

- kemudian pilih Add.



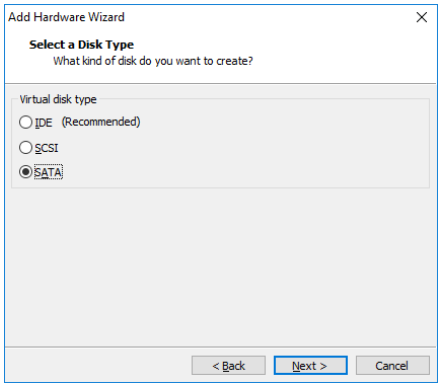
Gambar 8.26 Menambah Harddisk

- Pilih Hard Disk untuk menambah Hard Disk baru pada virtual machine, klik next.



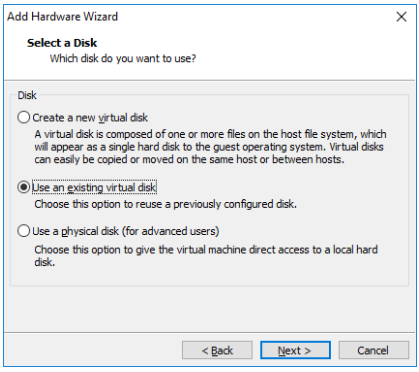
Gambar 8.27 Konfigurasi Menambah Harddisk

- Pilih SATA, tekan next.



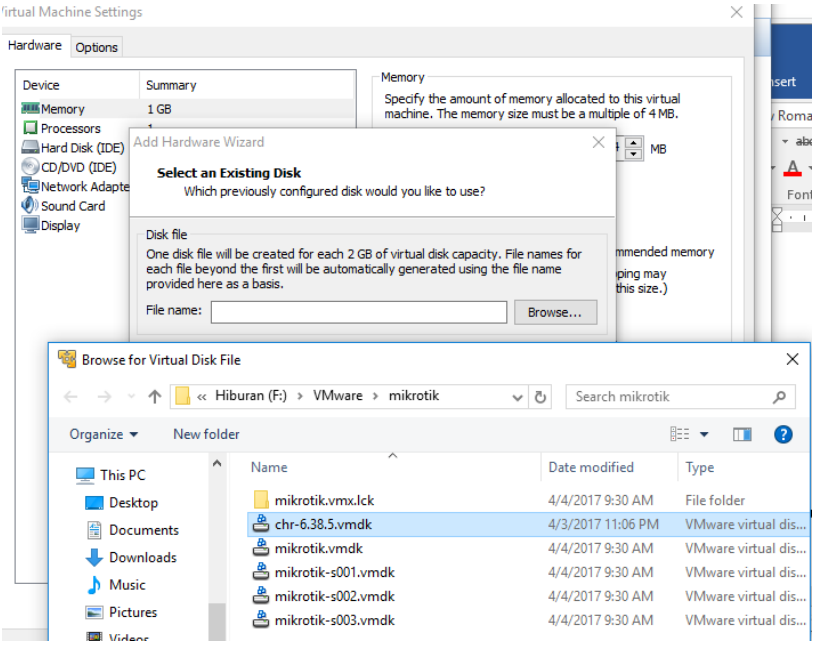
Gambar 8.28 Konfigurasi Tipe Harddisk

- Pilih Use an existing virtual disk



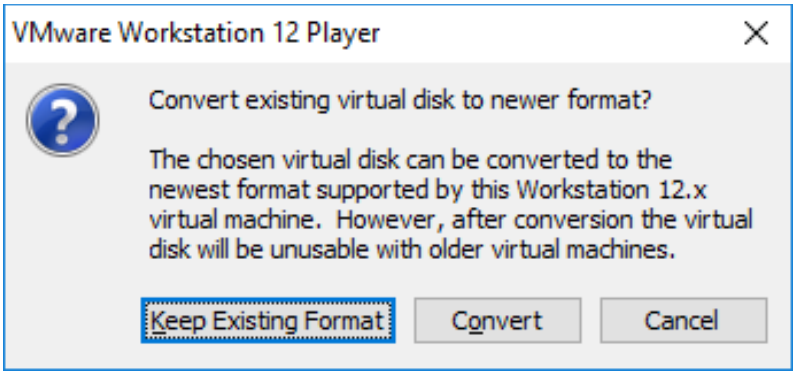
Gambar 8.29 Memasukkan Virtual Disk

- Masukkan file CHR dengan mengklik browse.



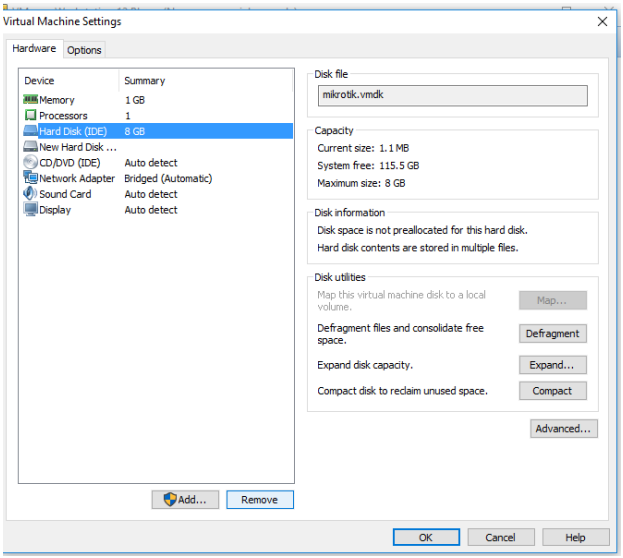
Gambar 8.30 Memasukkan File CHR

- Klik Finish, kemudian klik Convert jika muncul peringatan Convert existing virtual disk to newer format



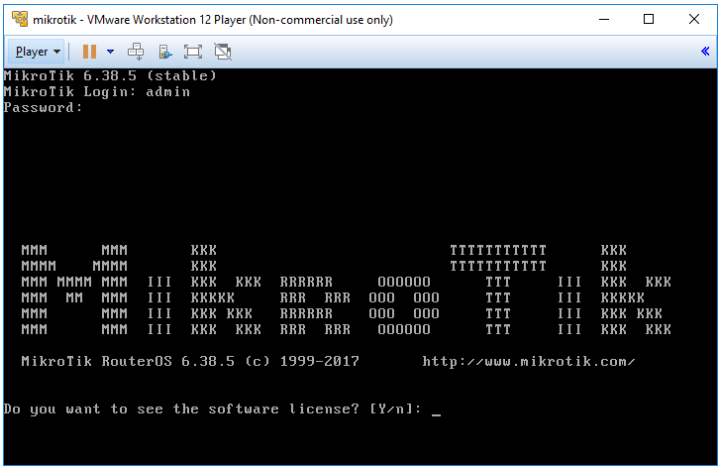
Gambar 8.31 Convert ke format baru

- Hapus Hard Disk yang ada sebelumnya, dengan mengklik Hard Disk nya di Device, kemudian klik Remove.



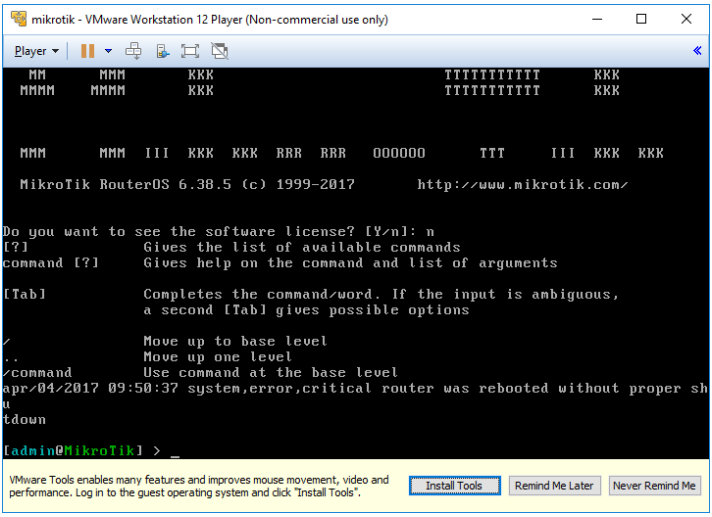
Gambar 8.32 Menghapus Harddisk

- Klik OK. Kemudian jalankan virtual machine dengan memilih Play virtual machine.
- Mikrotik sudah jalan, untuk login pertama kali gunakan login admin tanpa password.



Gambar 8.33 Tampilan Awal Mikrotik

- Tekan n, Mikrotik sudah bisa digunakan



Gambar 8.34 Tampilan Mikrotik

- Tekan ctrl+alt jika ingin berpindah cursor dari VMware ke windows.

8.4 Tugas

Buat sharing internet dengan menggunakan hostednetwork / Mobile Hotspot. Hidupkan mikrotik pada VMWare dan lakukan konfigurasi hotspot login sehingga ketika ada client yang mencoba konek internet menggunakan jaringan hostednetwork yang dibuat, akan diarahkan ke mikrotik VMWare sehingga muncul halaman login terlebih dahulu. Client baru bisa mengakses internet ketika sudah login menggunakan username dan password yang terkonfigurasi pada mikrotik.

DAFTAR PUSTAKA

Athailah. (2013). *Panduan Singkat Menguasai Router.* Jakarta: Mediakita.

Kustanto, & Saputro, D. T. (2015). *Belajar Jaringan Komputer Berbasis Mikrotik OS.* Gava Media.

Lammle, T. (2013). *CCNA Routing and Switching Study Guide: Exams 100-101, 200-101, and 200-120.* Sybex.

MADCOMS MADIUN. (2015). *Panduan Lengkap Membangun Sendiri Sistem Jaringan Komputer.* Yogyakarta: Penerbit Andi.

Sofana, I. (2012). *Cisco CCNA dan Jaringan Komputer.* Penerbit Informatika.

Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks.* Pearson.

Towidjojo, R. (2014). *Mikrotik Kungfu.* Jasakom.

Wendell, O. (2016). *CCENT/CCNA ICND1 100-105 Official Cert Guide.* Cisco Press.

Wendell, O. (2016). *CCNA ROUTING AND SWITCING ICND2 200-105 Official Cert Guide.* Cisco Press.

Jaringan Komputer

EFFAN NAJWAINI

Jaringan komputer merupakan sebuah sistem yang terdiri atas komputer/laptop/smartphone atau yang sering disebut sebagai end device serta perangkat jaringan yang saling bekerja sama untuk melakukan pertukaran data

Pada teknologi digital, data disimpan dalam satuan bit (0/1). Semua data baik itu file, gambar, suara, video dikodekan ke dalam nilai binner yang kemudian data ini dapat disimpan maupun dipindahkan ke media lainnya. Pada proses komunikasi data, data berupa nilai bit ini dikirimkan melalui suatu media transmisi. Jika media transmisi yang digunakan merupakan kabel tembaga, maka data tersebut akan disimbolkan menggunakan tegangan dan arus listrik, sedangkan jika menggunakan kabel optik, maka data tersebut disimbolkan menggunakan cahaya..

ISBN 978-623-7694-65-6 (PDF)
ISBN 978-623-7694-64-9

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