MODUL JARINGAN KOMPUTER

Penyusun : Dany Pratmanto M.Kom

STMIK Nusa Mandiri Jakarta

DAFTAR ISI

MODUL 1
KONSEP DASAR JARINGAN KOMPUTER
(Pertemuan 1)

Tujuan

1. Mahasiswa mampu menjelaskan tentang konsep dasar jaringan komputer

Tugas Pendahuluan

1. Apa yang di maksud dengan jaringan komputer ?
2. Apakah manfaat dan tujuan dari jaringan komputer ?

DASAR TEORI

Jaringan Komputer adalah sekelompok komputer otonom yang saling berhubungan antara satu dengan lainnya menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, penggunaan bersama perangkat keras seperti *printer*, *harddisk*, dan sebagainya.

Gambar 1.1 : Ilustrasi Sebuah Jaringan Komputer

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

1. *Sharing resources*

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

2. Media Komunikasi

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

3. Integrasi Data

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

4. Pengembangan dan Pemeliharaan

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

5. Keamanan Data

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

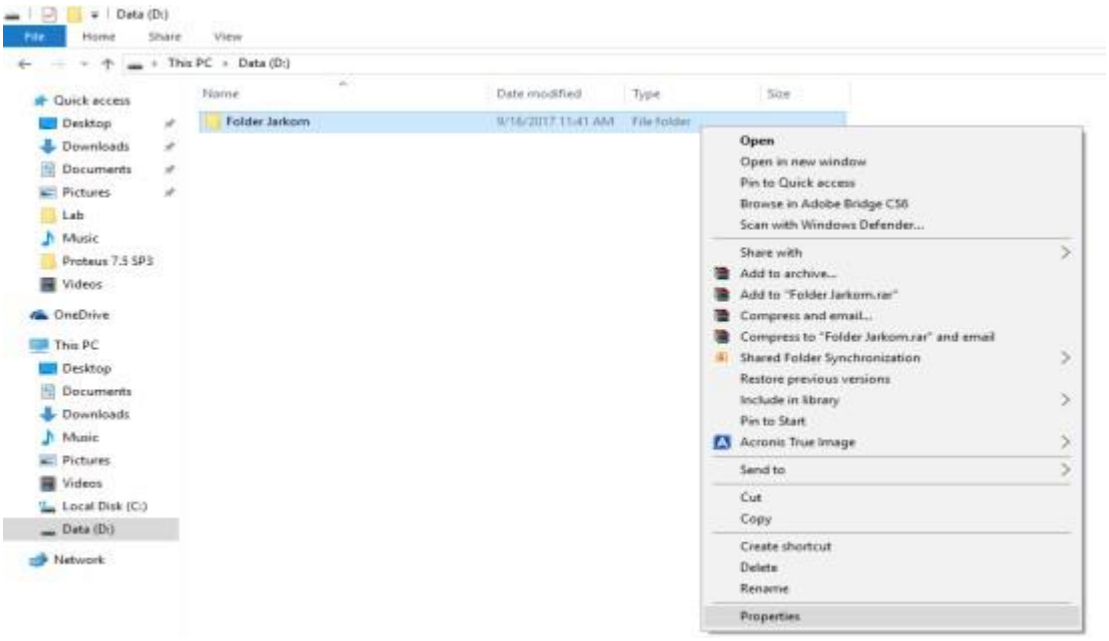
KEGIATAN PRAKTIKUM

Sharing resource/ file.

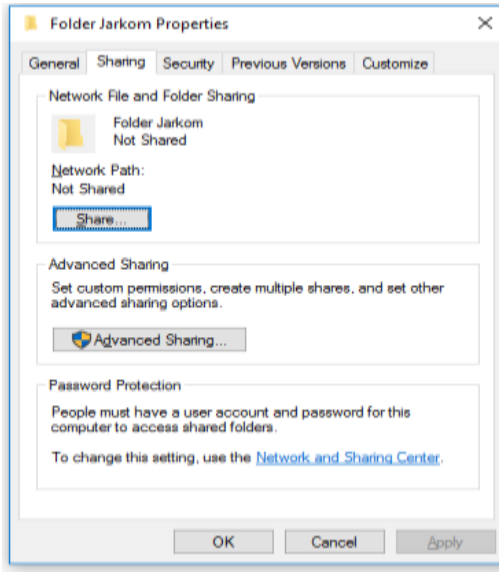
Syarat yang harus dipenuhi dalam sharing resource atau file adalah IP Address. IP Address disini berfungsi sebagai penghubung antara PC yang memberikan resource/file dan PC yang menerima resource/file tersebut.

Langkah langkah Sharing resource/file pada PC yang menggunakan Sistem Operasi windows sebagai berikut :

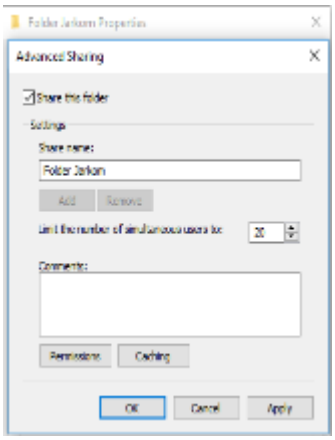
Pilih folder / file yang ingin dishare, Klik kanan dan masuk ke properties



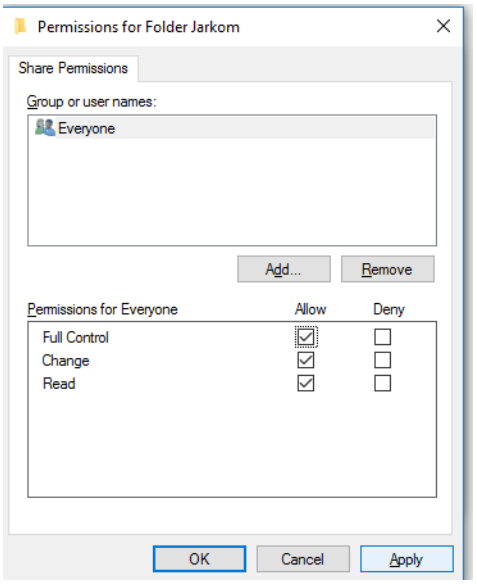
Masuk ke Menu Sharing



Masuk ke Advance Sharing dan centang pada kolom Share This Folder

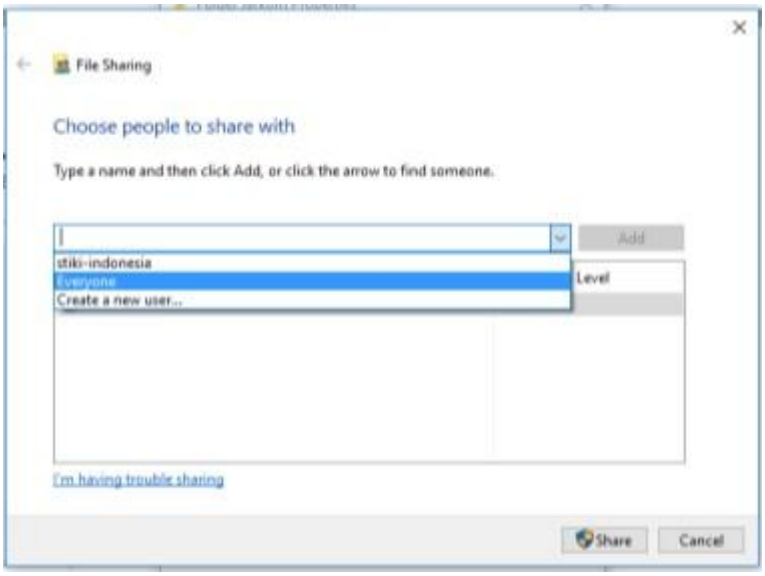


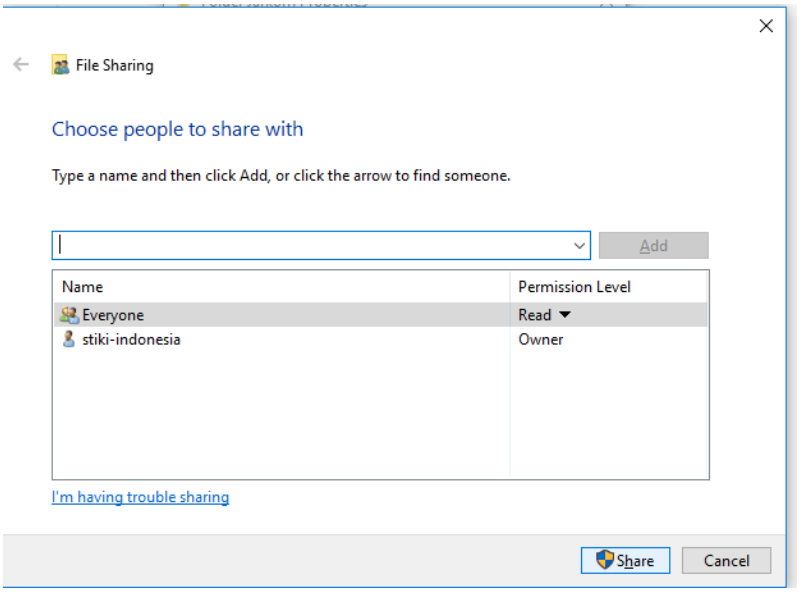
Untuk Mengatur apa saja yang client boleh lakukan terhadap file yang disharing, masuk ke Permission, dan centang pada ALLOW untuk semua perintah yang ada, lalu APPLY.



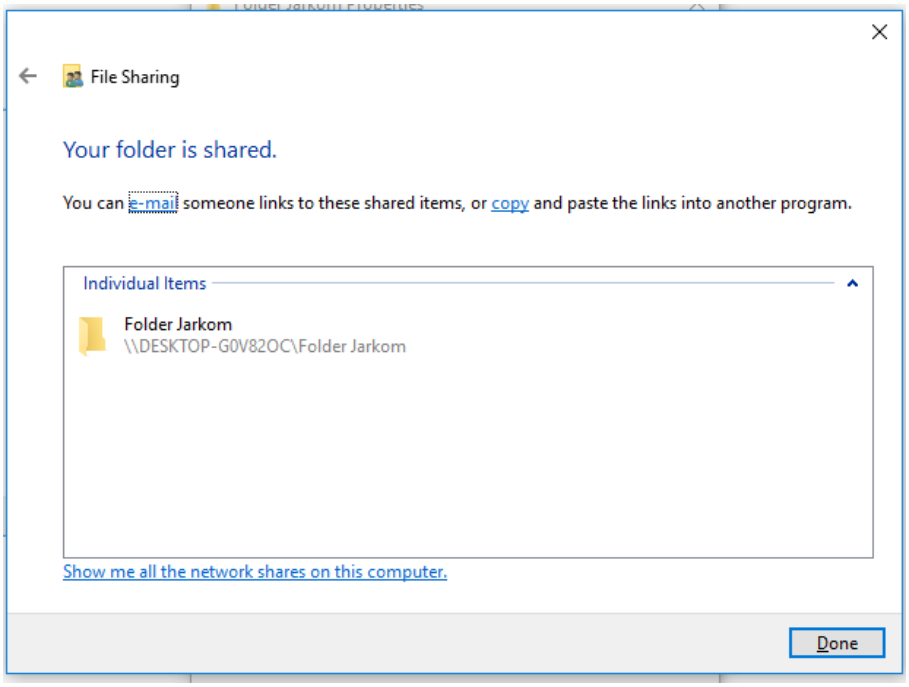
Kita juga bisa memilih kepada siapa saja kita bisa membagikan file kita dengan cara klik SHARE -> Everyone lalu klik add -> SHARE.


Folder Jarkom Properties
General
Sharing
Security
Previous Versions
Customize
Network File and Folder Sharing
Folder Jarkom
Shared
Network Path:
\\DESKTOP-G0VB2OC\Folder Jarkom
Share...
Advanced Sharing
Set custom permissions, create multiple shares, and set other advanced sharing options.
Advanced Sharing...
Password Protection
People must have a user account and password for this computer to access shared folders.
To change this setting, use the Network and Sharing Center.
Close
Cancel
Apply


File Sharing
Choose people to share with
Type a name and then click Add, or click the arrow to find someone.
Add
stiki-indonesia
Everyone
Create a new user...
Level
I'm having trouble sharing
Share
Cancel


File Sharing
Choose people to share with
Type a name and then click Add, or click the arrow to find someone.
Add
Name
Permission Level
Everyone
Read
stiki-indonesia
Owner
I'm having trouble sharing
Share
Cancel

Setelah selesai, akan muncul pemberitahuan bahwa file kita sudah bisa dishare lalu Klik DONE.



Tugas

1. Sebutkan dan jelaskan jenis jenis dari jaringan komputer

MODUL 2

MODEL REFERENSI OSI

(Pertemuan 2, 3)

Tujuan

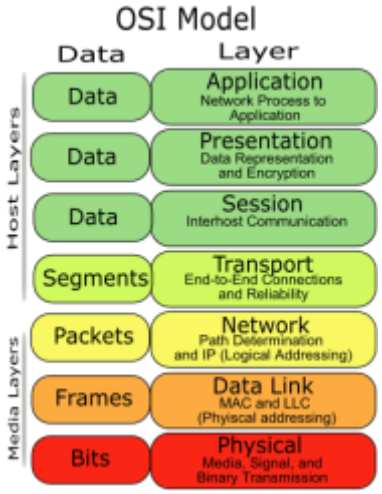
1. Mahasiswa mampu menjelaskan dan memahami konsep Model Refrensi OSI, Model Refrensi TCP/IP dan *Ecapsulation*

Tugas Pendahuluan

1. Apakah yang anda ketahui tentang Model OSI ?
2. Sebutkan dan jelaskan bagian bagian dari Model OSI

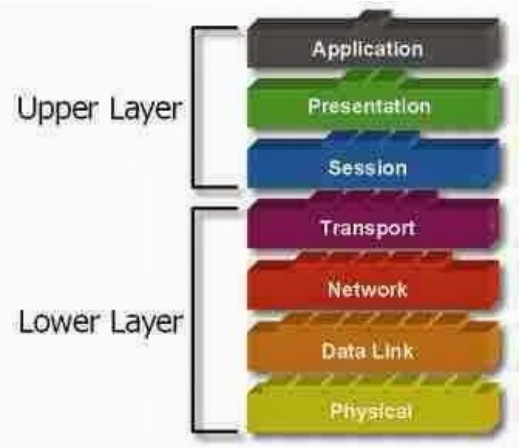
DASAR TEORI

Open System Interconnection (OSI) adalah standar komunikasi yang diterapkan di dalam jaringan komputer. Standar itulah yang menyebabkan seluruh alat komunikasi dapat saling berkomunikasi melalui jaringan. Model referensi OSI menggambarkan bagaimana informasi dari suatu *software* aplikasi di sebuah komputer berpindah melewati sebuah media jaringan ke suatu *software* aplikasi di komputer lain. Model referensi OSI secara konseptual terbagi ke dalam 7 lapisan dimana masing-masing lapisan memiliki fungsi jaringan yang spesifik. Model *Open Systems Interconnection* (OSI) diciptakan oleh International *Organization for Standardization* (ISO) yang menyediakan kerangka logika terstruktur bagaimana proses komunikasi data berinteraksi melalui jaringan.



Gambar 2.1 : Model OSI *Layer*

Model *Layer* OSI dibagi dalam dua group yaitu *upper layer* dan *lower layer*. *Upper layer* adalah *layer* yang fokus pada aplikasi pengguna dan bagaimana *file* direpresentasikan di komputer. *Lower layer* adalah intisari komunikasi data melalui jaringan aktual.



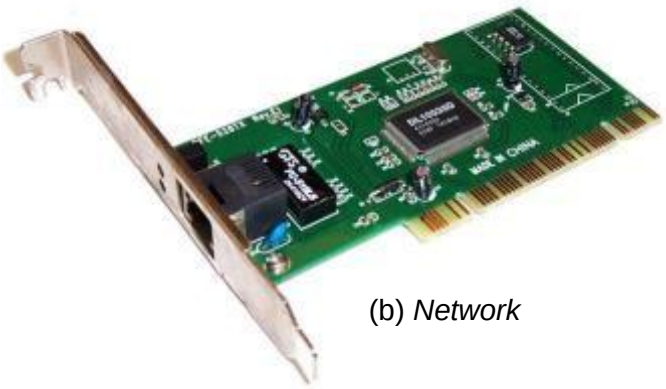
Gambar 2.2 : *Group* OSI *Layer*

Berikut ini merupakan ke-tujuh lapisan OSI *Layer* :

1. *Physical Layer*

   Layer pertama pada OSI adalah *Physical Layer*, dimana posisinya terletak pada urutan paling bawah. *Physical layer* merupakan lapisan yang berhubungan dengan fisik. *Physical layer* ini berhubungan erat dengan fungsi pensinyalan, dan merupakan *layer* yang paling dekat dengan *hardware* atau perangkat keras jaringan secara fisik. Pada *physical layer* terdapat perangkat keras dasar jaringan yang terdiri dari *Network Adapter, Repeater,* Modem dan *Network Cable*.

(a) *Network Cable*



(b) *Network*

(c)

(d) Modem

Gambar 2.3 : Contoh Perangkat *Physical Layer*

2. *Data-link layer*

   Data-link layer berfungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai *frame*. Selain itu, pada level ini terjadi koreksi kesalahan, *flow control*, pengalamatan perangkat keras (MAC *Address*), dan menentukan bagaimana perangkat-perangkat beroperasi. Komponen yang termasuk dalam *Data-Link layer* adalah *Switch* dan *Bridge*.

(a) Switch

(b)

Gambar 2.4 : Contoh Perangkat *Data-Link Layer*

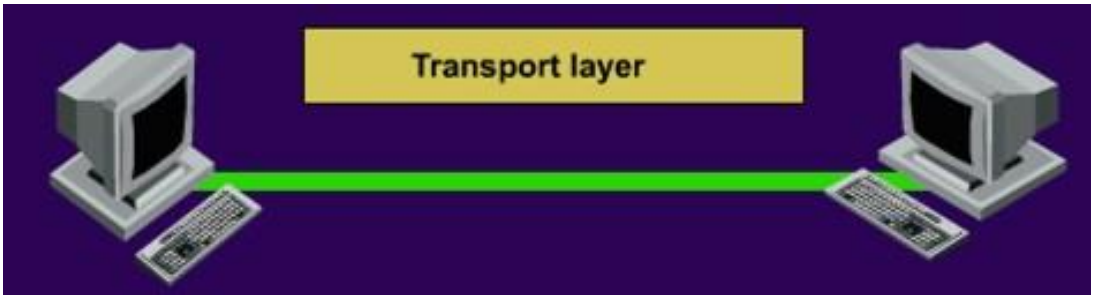
3. *Network Layer*

   Network Layer berfungsi untuk menyediakan fungsi *routing* sehingga paket dapat dikirim keluar dari segmen *network* lokal ke suatu tujuan yang berada pada suatu *network* lain. Selain itu, fungsi lain dari *network layer* adalah mendefinisikan alamat-alamat IP, membuat *header* untuk paket-paket, dan kemudian melakukan *routing* melalui *internetworking* . Komponen yang digunakan pada *layer* ini adalah *Router*.

Gambar 2.5 : *Router*

4. *Transport Layer*

Transport layer merupakan pusat dari model OSI. *Transport layer* berfungsi untuk menyediakan *multiplexing*, kendali aliran dan pemeriksaan *error* serta memperbaikinya. Selain itu, *transport layer* berfungsi juga untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima.



Gambar 2.6 : Proses *Transport Layer*

5. *Session layer*

   Session layer berfungsi untuk mendefinisikan bagaimana koneksi dapat dibangun, dipelihara, atau dihancurkan. Lapisan *session layer* ini bekerja pada perangkat lunak yang memiliki fungsi pengelolaan data, salah satunya adalah SQL. Dengan menggunakan perangkat lunak SQL ini, maka *session layer* dapat bekerja dalam membangun komunikasi dengan jaringan, sehingga terbangunlah sebuah koneksi jaringan tertentu.

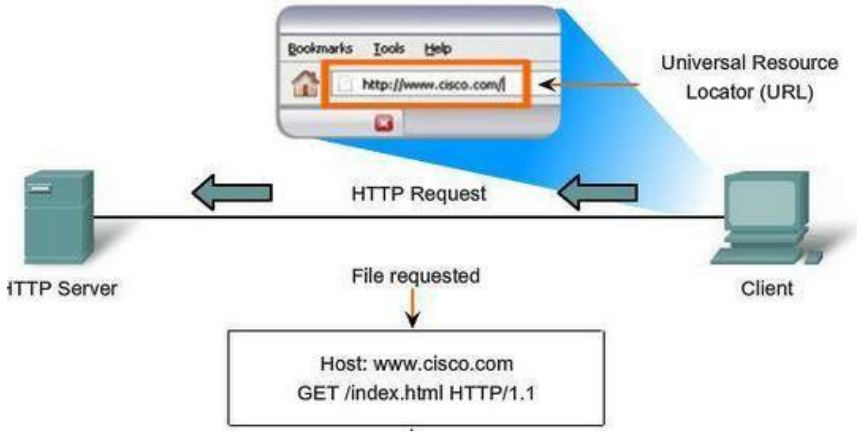
Gambar 2.7 : Contoh Perangkat *Session Layer*

6. *Presentation layer*

   Presentation layer berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Tugas- tugas seperti kompresi, dekompresi, enkripsi dan dekripsi data dilakukan pada *Presentation Layer*.

7. *Application Layer*

Application layer berfungsi sebagai antarmuka dengan aplikasi fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan.



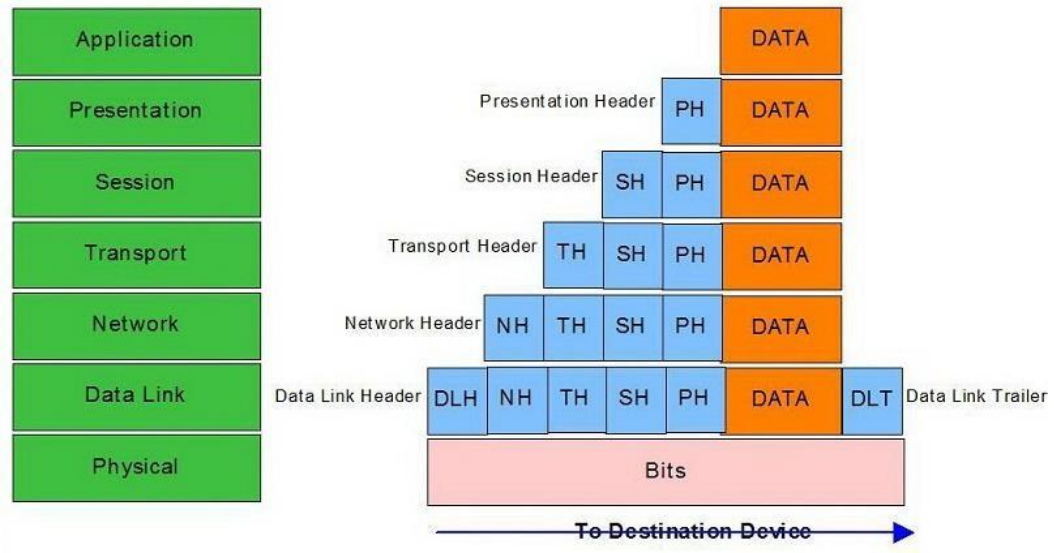
Gambar 2.8 : Contoh Proses dalam *Application Layer*

TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) adalah gabungan dari protokol TCP (*Transmission Control Protocol*) dan IP (*Internet Protocol*) sebagai sekelompok protokol yang mengatur komunikasi data dalam proses pertukaran data dari satu komputer ke komputer lain di dalam jaringan internet yang akan memastikan pengiriman data sampai ke alamat yang dituju. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (protocol *suite*). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini, karena protokol ini mampu bekerja dan diimplementasikan pada perangkat lunak (*software*) di berbagai sistem operasi. Istilah yang diberikan kepada perangkat lunak ini adalah TCP/IP *stack.*

Encapsulation

Encapsulation **(**Enkapsulasi) merupakan suatu proses yang membuat satu jenis paket data jaringan menjadi jenis data lainnya. Enkapsulasi terjadi ketika sebuah protokol yang berada pada lapisan yang lebih rendah menerima data dari protokol yang berada pada lapisan yang lebih tinggi dan meletakkan data ke format data yang dipahami oleh protokol tersebut. Dalam Model OSI, proses enkapsulasi yang terjadi pada lapisan terendah umumnya disebut sebagai "*framing*". Lapisan *data-link* dalam model OSI merupakan lapisan yang bertanggung jawab dalam melakukan enkapsulasi atau *framing* data sebelum dapat ditransmisikan di atas media jaringan.



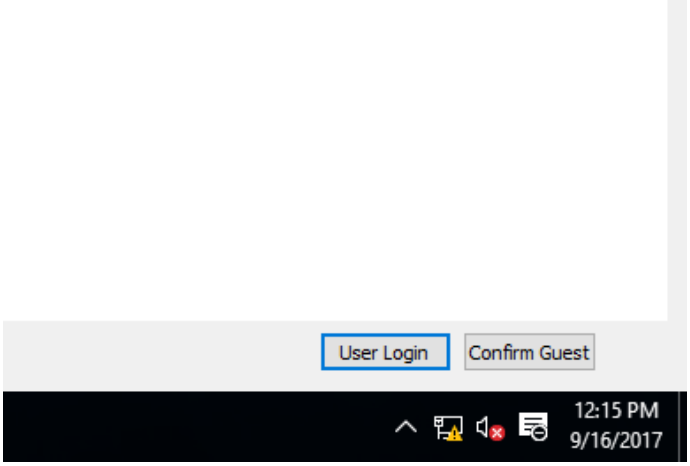
Gambar 2.9 : Proses Enkapsulasi

Beberapa jenis enkapsulasi antara lain:

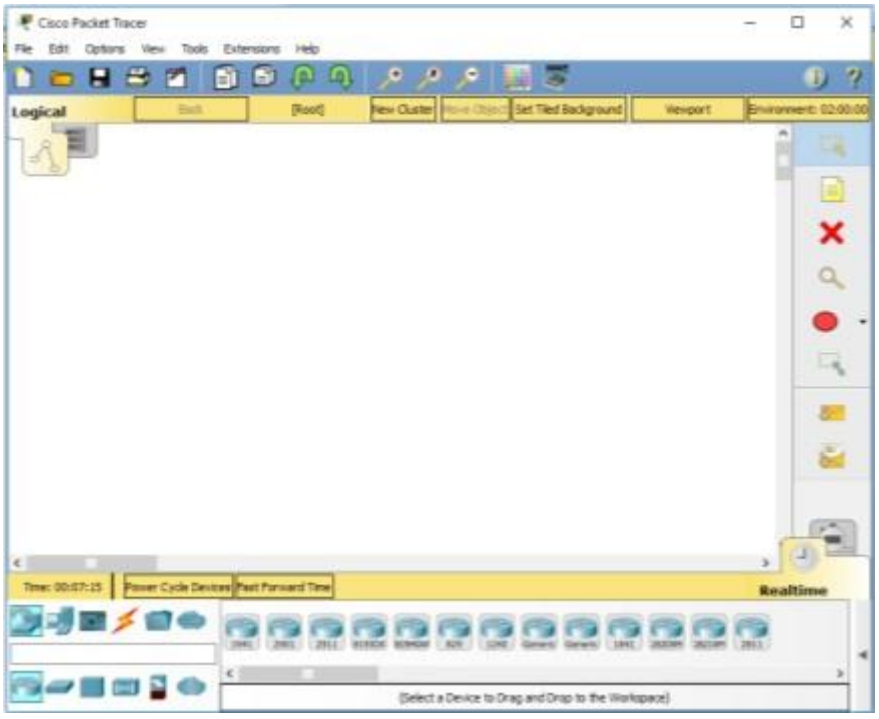
a. *Frame Ethernet* yang melakukan enkapsulasi terhadap datagram yang dibentuk oleh *Internet Protocol* (IP), yang dalam datagram tersebut juga melakukan enkapsulasi terhadap paket data yang dibuat oleh protokol TCP atau UDP. Data yang dienkapsulasi oleh protokol TCP atau UDP tersebut merupakan data aktual yang ditransmisikan melalui jaringan.
b. *Frame Ethernet* yang dienkapsulasi ke dalam bentuk frame *Asynchronous Transfer Mode* (ATM) agar dapat ditransmisikan melalui *backbone* ATM.

KEGIATAN PRAKTIKUM

Buka Cisco Packet Tracer pada PC anda, lalu klik Guest Login, tunggu beberapa detik, lalu klik Confirm Guest, maka akan muncul tampilan seperti berikut :



Gambar Confirm Guest

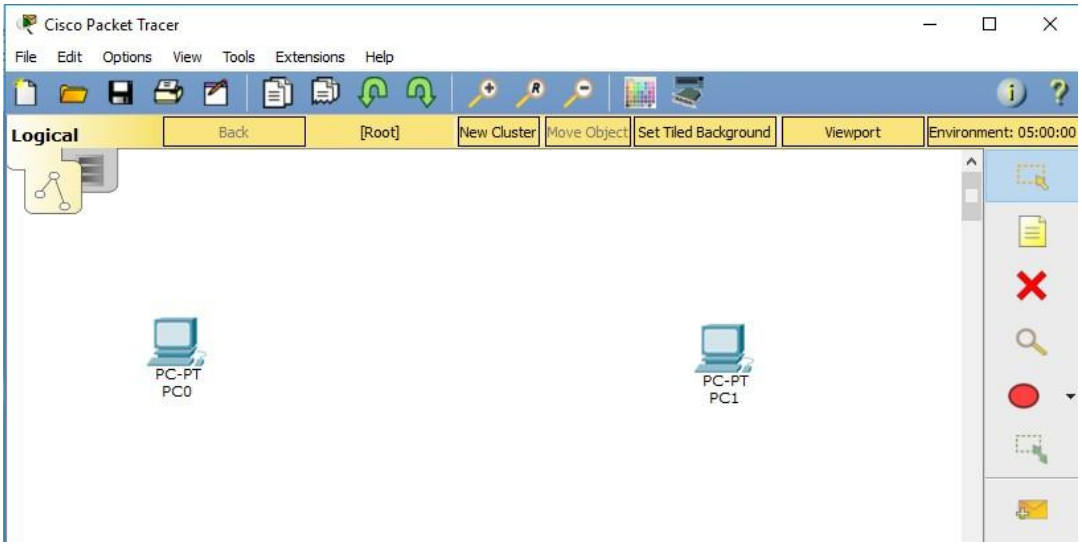


Gambar menu utama Packet Tracer

Lalu klik pada End Device atau dengan menekan Ctrl + Alt + V, lalu pilih Generic PC

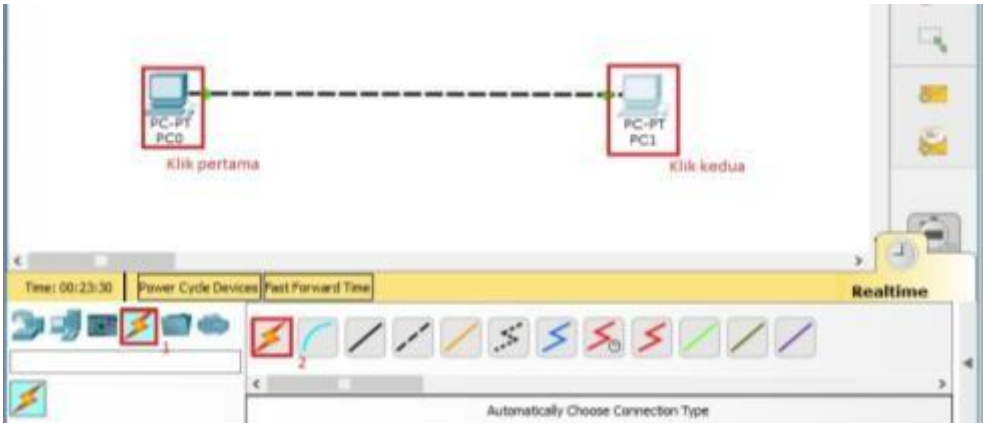
Gambar End Device

Lalu drag 2 PC pada menu utama dengan cara mengklik pada tempat yang diinginkan.



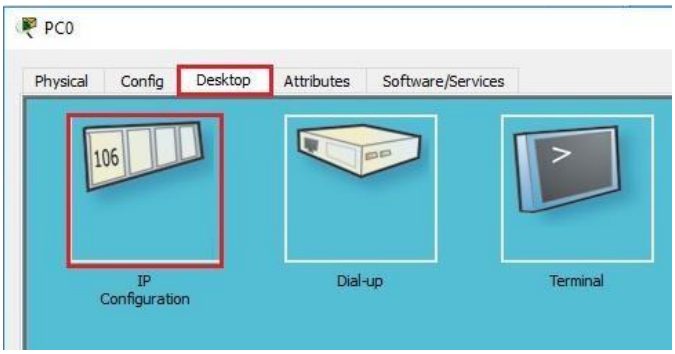
Gambar 2 PC

Lalu hubungkan kedua PC menggunakan kabel automatical.



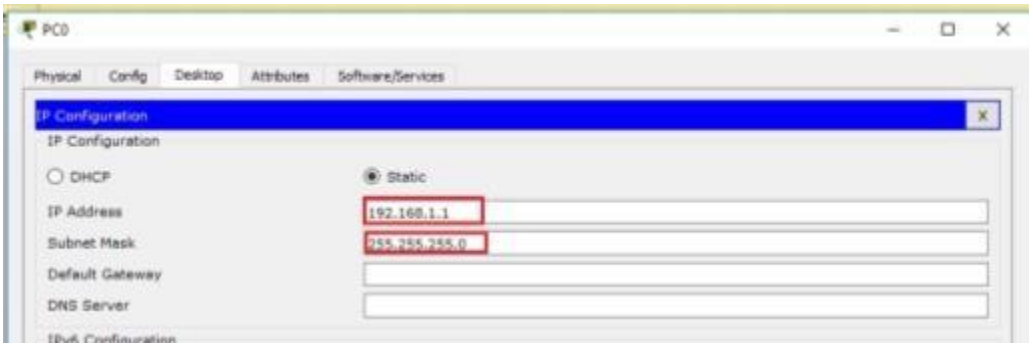
Gambar kedua PC telah terhubung dengan kabel

Klik pada PC untuk memberi IP address pada masing-masing PC yang ada, klik tab Desktop maka akan muncul tampilan sebagai berikut, dan untuk mengkonfigurasi IPnya klik IP Configuration :



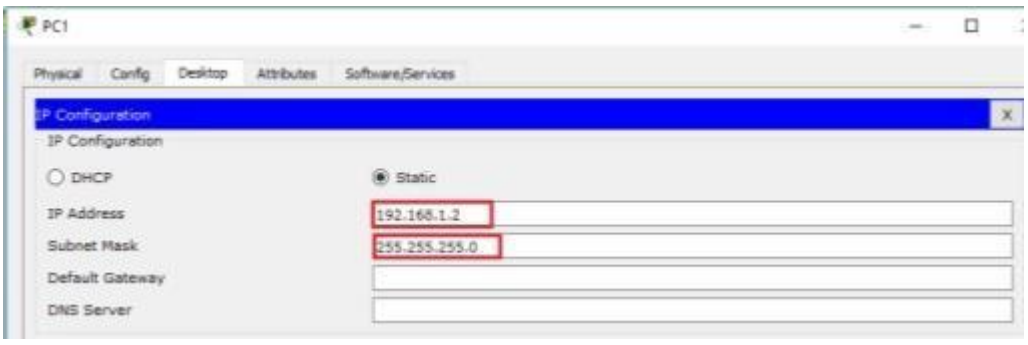
Gambar menu PC0

Pada jendela konfigurasi, isikan IP dengan 192.168.1.1 dan Subnetmasknya 255.255.255.0 seperti gambar berikut ini :



Gambar Konfigurasi IP pada PC0

Lakukan hal yang sama pada PC1 hanya saja IP yang digunakan berbeda yaitu 192.168.1.2 seperti gambar berikut ini :

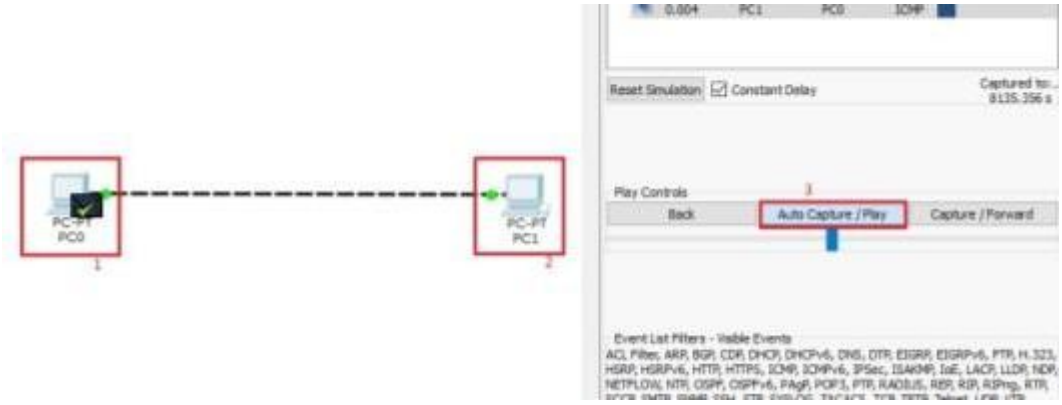


Gambar Konfigurasi IP pada PC1

Lakukan pengujian dengan cara mengirim pesan/data dari salah satu PC ke PC yang terhubung, Klik Simulation, lalu klik Add Simple PDU :

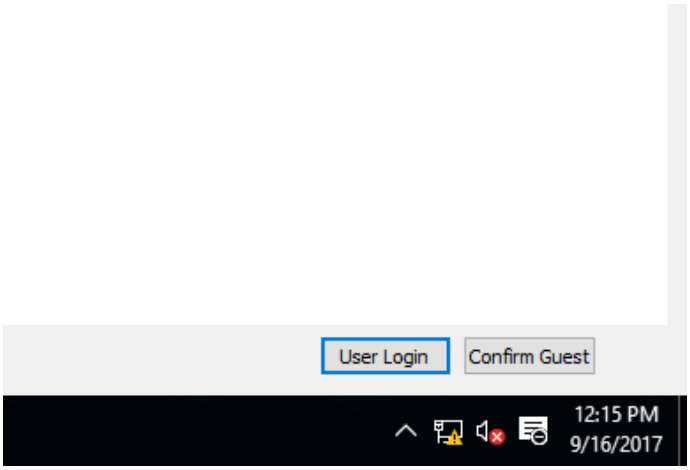
Gambar Simulation

Lalu klik pada PC0 dan kedua klik pada PC1, dan untuk memulai pengiriman file klik Auto Capture/Play, jika sudah terdapat tanda centang (√) maka PC anda berhasil terhubung :

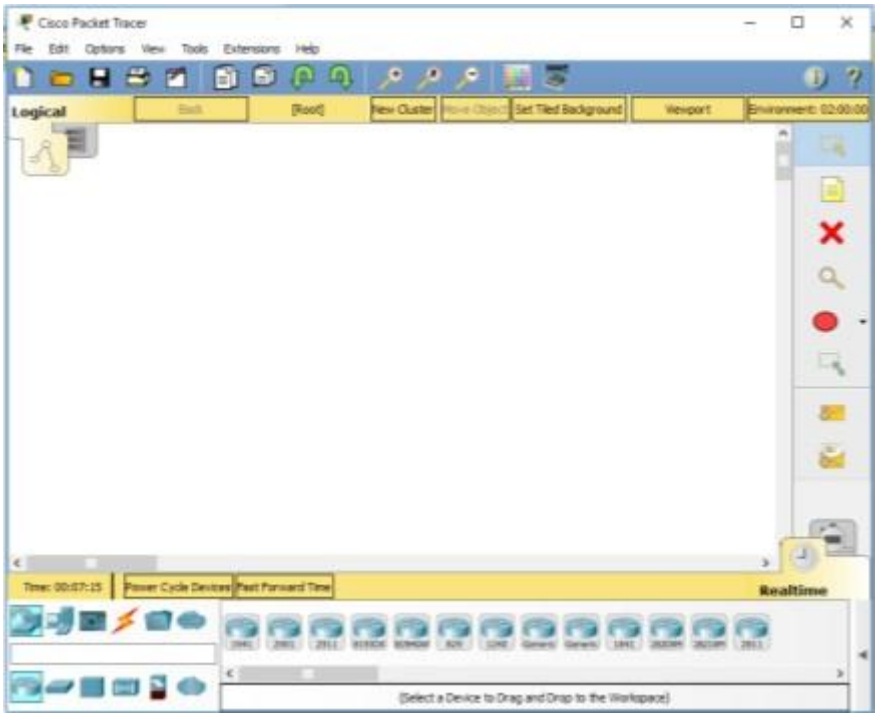


Langkah penghubungan 2 komputer dengan switch :

Buka Cisco Packet Tracer pada PC anda, lalu klik Guest Login, tunggu beberapa detik, lalu klik Confirm Guest, maka akan muncul tampilan seperti berikut :



Gambar Confirm Guest

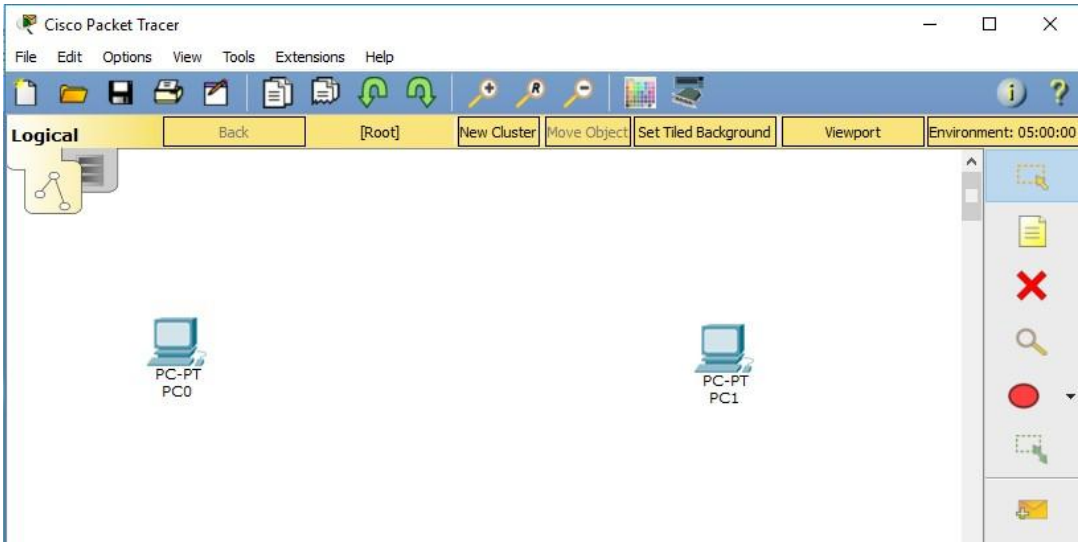


Gambar menu utama Packet Tracer

Lalu klik pada End Device atau dengan menekan Ctrl + Alt + V, lalu pilih Generic PC

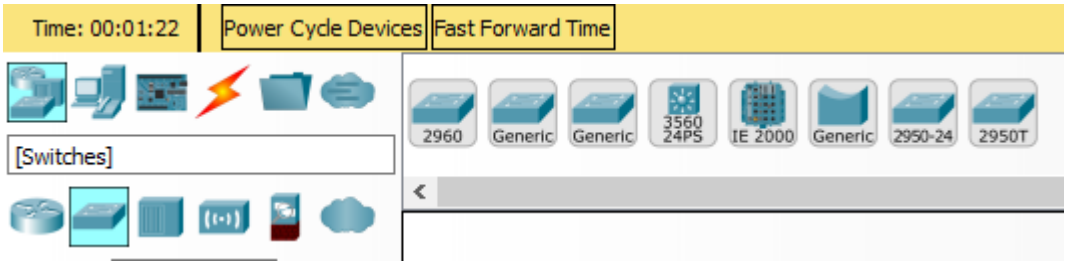
Gambar End Device

Lalu drag 2 PC pada menu utama dengan cara mengklik pada tempat yang diinginkan.

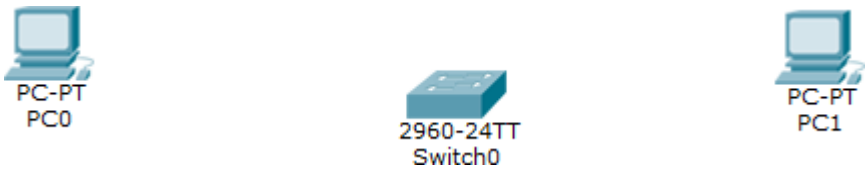


Gambar 2 PC

Tambahkan switch pada gambar

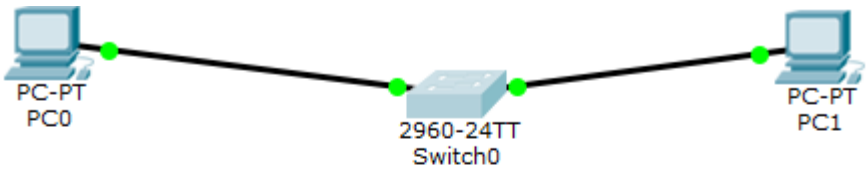


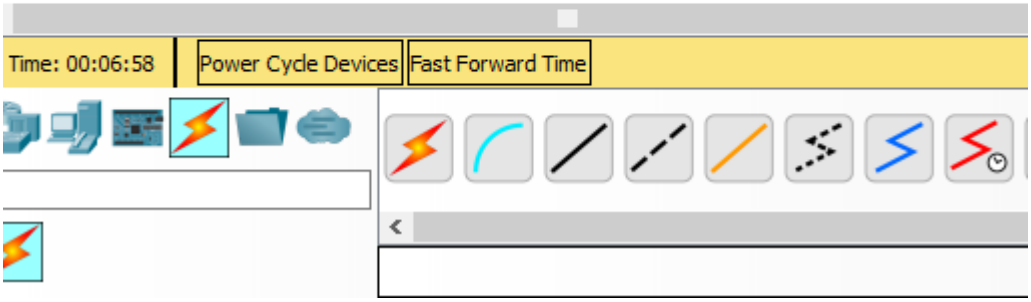
Gambar pilihan switch



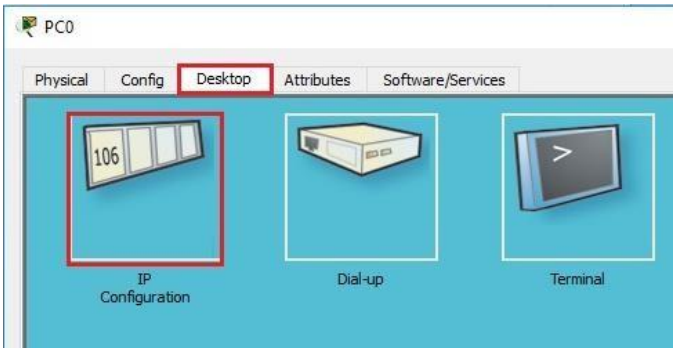
Setelah ditambahkan switch

Sambungkan kabel penghubung antara 2 komputer dengan switch



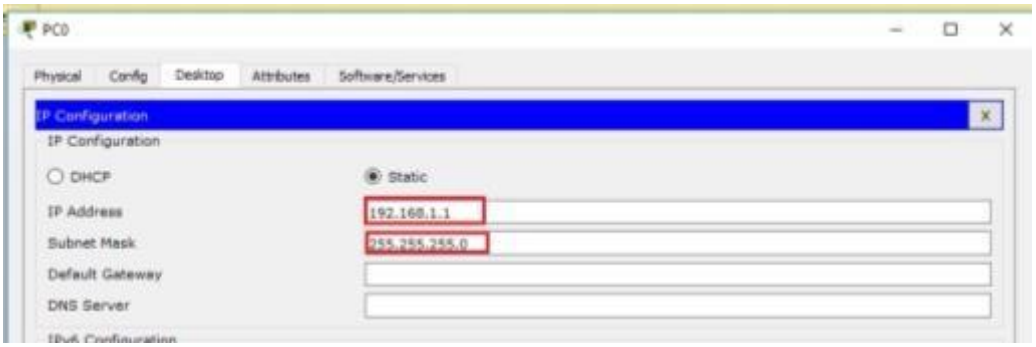


Klik pada PC untuk memberi IP address pada masing-masing PC yang ada, klik tab Desktop maka akan muncul tampilan sebagai berikut, dan untuk mengkonfigurasi IPnya klik IP Configuration :



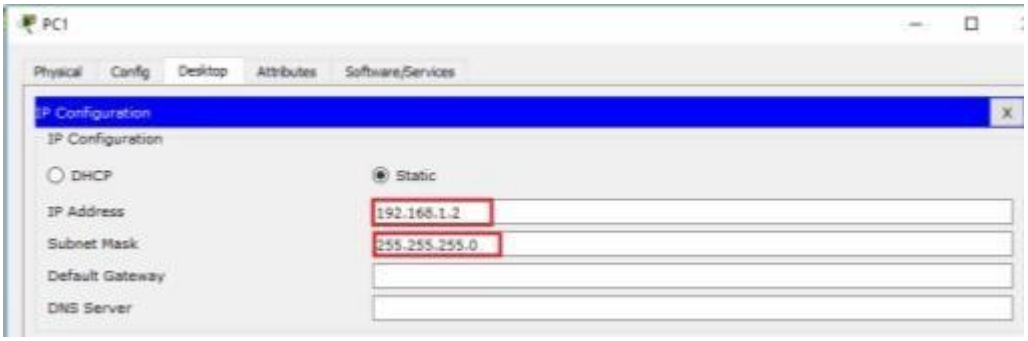
Gambar menu PC0

Pada jendela konfigurasi, isikan IP dengan 192.168.1.1 dan Subnetmasknya 255.255.255.0 seperti gambar berikut ini :



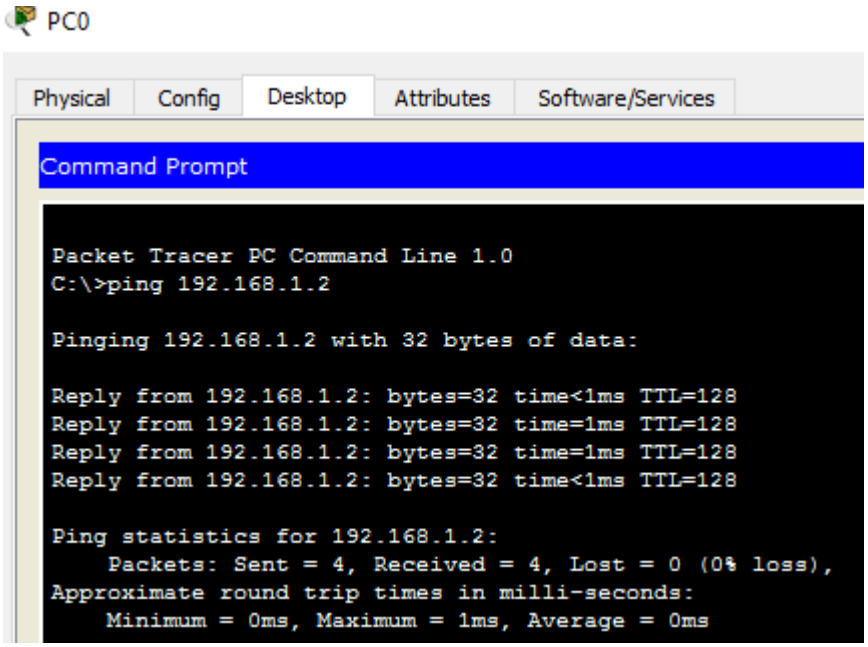
Gambar Konfigurasi IP pada PC0

Lakukan hal yang sama pada PC1 hanya saja IP yang digunakan berbeda yaitu 192.168.1.2 seperti gambar berikut ini :



Gambar Konfigurasi IP pada PC1

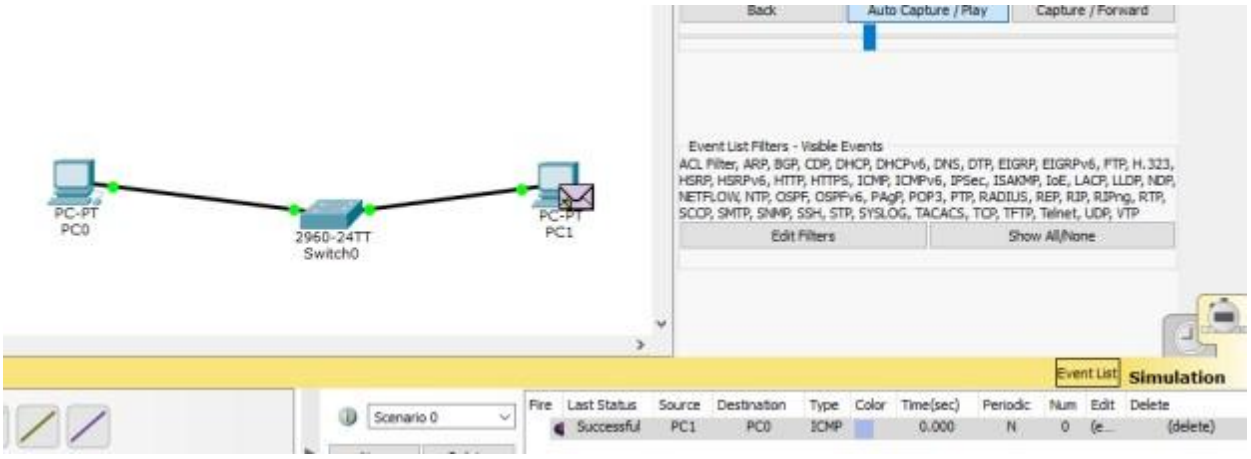
Untuk Menguji jaringan, kita bisa PING PC 01 melalui PC 02. Dengan cara Klik PC0 -> Dekstop -> Comand Promt, lalu masukan “PING 192.168.1.2 (alamat IP PC 1)” seperti gambar dibawah



Lakukan pengujian dengan cara mengirim pesan dari salah satu PC ke PC yang terhubung, Klik Simulation, lalu klik Add Simple PDU :

Gambar Simulation

Lalu klik pada PC0 dan kedua klik pada PC1, dan untuk memulai pengiriman file klik Auto Capture/Play, jika sudah terdapat tanda centang (√) atau last status pada event list sudah menunjukan “successful” maka PC anda berhasil terhubung.



Tugas

1. Sebutkan komponen komponen yang terdapat pada masing masing lapisan Model OSI!
2. Jelaskan komponen yang ada pada masing masing *layer* pada Model OSI!

MODUL 3

TOPOLOGI JARINGAN KOMPUTER

(Pertemuan 5, 6)

Tujuan

1. Mahasiswa mampu menjelaskan dan memahami konseptopologi jaringan komputer serta dapat memahami penggunaan media transmisi yang sesuai

Tugas Pendahuluan

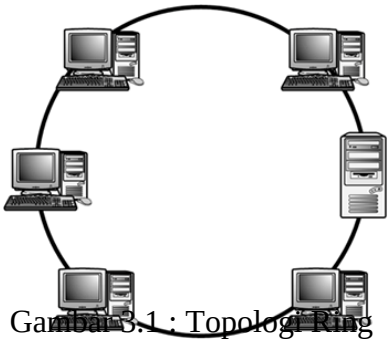
1. Apakah yang anda ketahui tentang topologi jaringan komputer?
2. Sebutkan dan jelaskan macam-macam topologi pada jaringan komputer
3. Sebutkan dan jelaskan jenis-jenis media transmisi.

DASAR TEORI

Topologi merupakan suatu pola hubungan antara terminal dalam jaringan komputer. Pola ini sangat erat kaitannya dengan metode *access* dan media pengiriman yang digunakan. Topologi yang ada sangatlah tergantung dengan letak geografis dari masing-masing terminal, kualitas kontrol yang dibutuhkan dalam komunikasi ataupun penyampaian pesan, serta kecepatan dari pengiriman data. Ada beberapa topologi jaringan komputer, yaitu topologi *ring, bus, star, mesh,* dan *tree*.

1. Topologi *Ring*

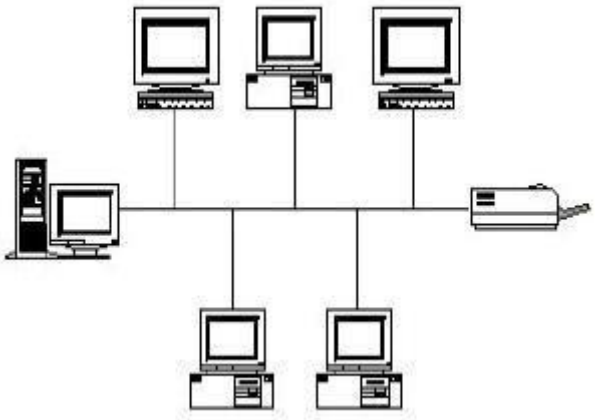
Pada topologi *ring* setiap komputer di hubungkan dengan komputer lain dan seterusnya sampai kembali lagi ke komputer pertama, dan membentuk lingkaran sehingga disebut *ring*, topologi ini berkomunikasi menggunakan data token untuk mengontrol hak akses komputer untuk menerima data, misalnya komputer 1 akan mengirim *file* ke komputer 4, maka data akan melewati komputer 2 dan 3 sampai di terima oleh komputer 4.



Gambar 3.1 : Topologi Ring

2. Topologi *Bus*

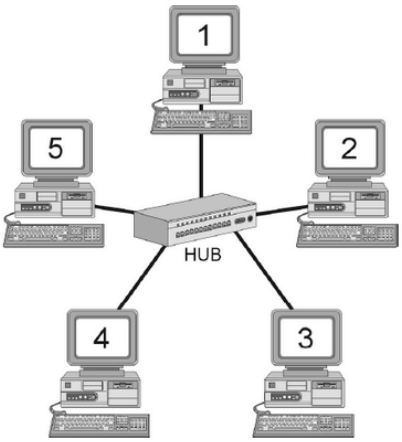
Pada topologi *bus* digunakan sebuah kabel tunggal atau kabel pusat di mana seluruh *workstation* dan *server* dihubungkan. Keunggulan topologi *bus* adalah pengembangan jaringan atau penambahan *workstation* baru dapat dilakukan dengan mudah tanpa mengganggu *workstation* lain. Kelemahan dari topologi ini adalah bila terdapat gangguan di sepanjang kabel pusat maka keseluruhan jaringan akan mengalami gangguan



Gambar 3.2 : Topologi *Bus*

3. Topologi *Star*

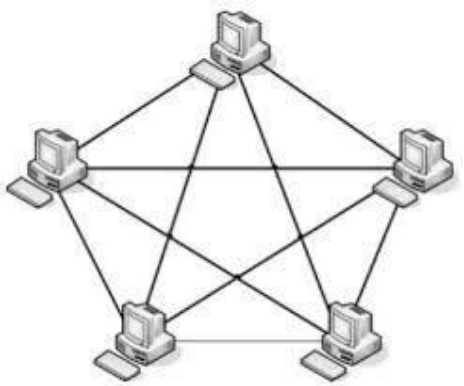
Topologi *Star* merupakan topologi jaringan yang bentuknya berupa konvergensi dari *node* tengah ke setiap *node* atau pengguna. Masing- masing *workstation* dihubungkan langsung ke *Hub* atau *Switch*. *Hub* atau *Switch* berfungsi untuk menerima sinyal dari komputer dan meneruskannya ke semua komputer yang terhubung dengan *Hub* atau *Switch* tersebut.



Gambar 3.3 : Topologi Star

4. Topologi *Mesh*

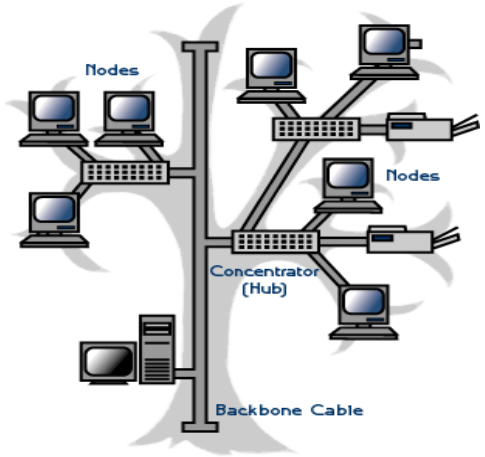
Topologi *mesh* adalah suatu bentuk hubungan antar perangkat dimana setiap perangkat saling terhubung secara langsung ke perangkat lainnya yang berada dalam satu jaringan. Pada topologi *mesh* setiap perangkat dapat berkomunikasi secara langsung dengan perangkat lain karena perangkat saling terhubung secara langsung atau bisa disebut dengan istilah *dedicated links*.



Gambar 3.4 : Topologi *Mesh*

5. Topologi *Tree*.

Topologi *tree* adalah salah satu dari topologi jaringan komputer yang paling banyak diterapkan didalam pembuatan sebuah jaringan komputer. Dengan bentuk menyerupai pohon dengan ranting-ranting, topologi ini akan mencakup lebih banyak komputer yang dapat terhubung dengan jaringan komputer. Didalam topologi *tree* terdapat sebuah perangkat (*switch* atau *hub*) pada level teratas yang menjadi pusat utama komunikasi bagi semua komputer yang terhubung.



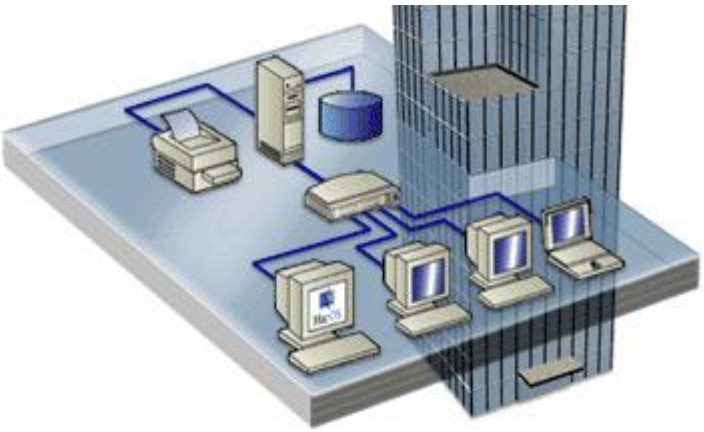
Gambar 3.5 : Topologi *Tree*

Jenis – jenis Jaringan Komputer

Berdasarkan jarak dan area kerjanya, jaringan komputer dibedakan menjadi tiga kelompok, yaitu LAN, MAN, dan WAN.

1. *Local Area Network* (LAN)

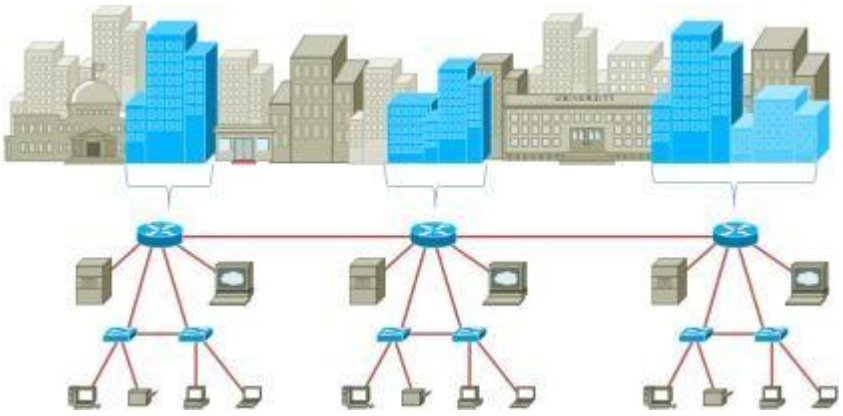
   Local Area Network (LAN), merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan *workstation* dalam kantor suatu perusahaan atau pabrik-pabrik untuk pemakaian bersama sumber daya (misalnya *printer*) dan saling bertukar informasi.



Gambar 3.6 : LAN (*Local Area Network*)

2. *Metropolitan Area Network* (MAN)

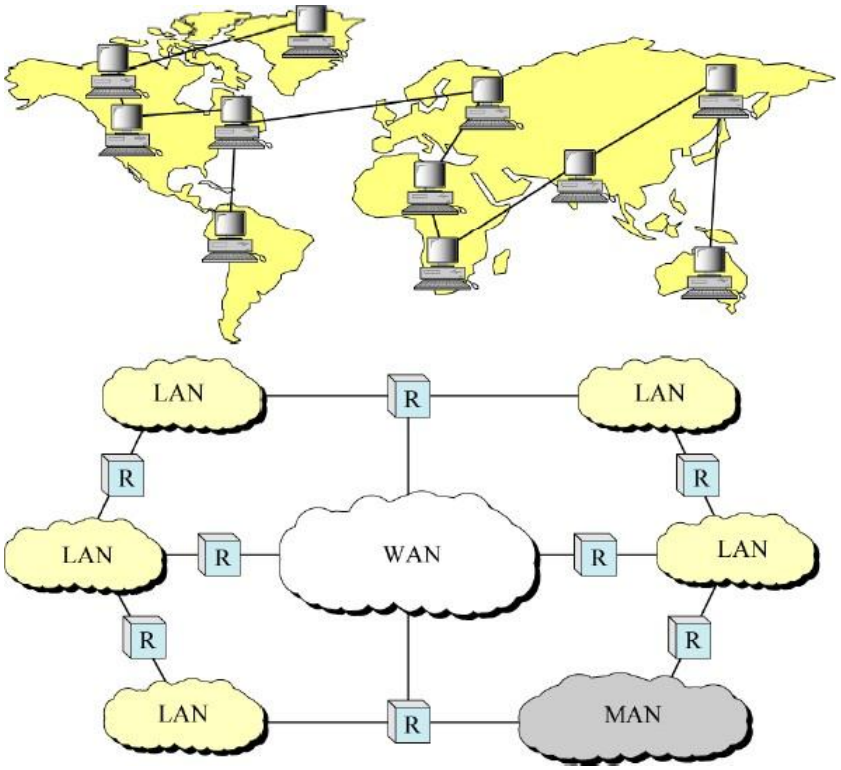
   Metropolitan Area Network (MAN), pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel.



Gambar 3.7 : MAN (*Metropolitan Area Network*)

3. *Wide Area Network* (WAN)

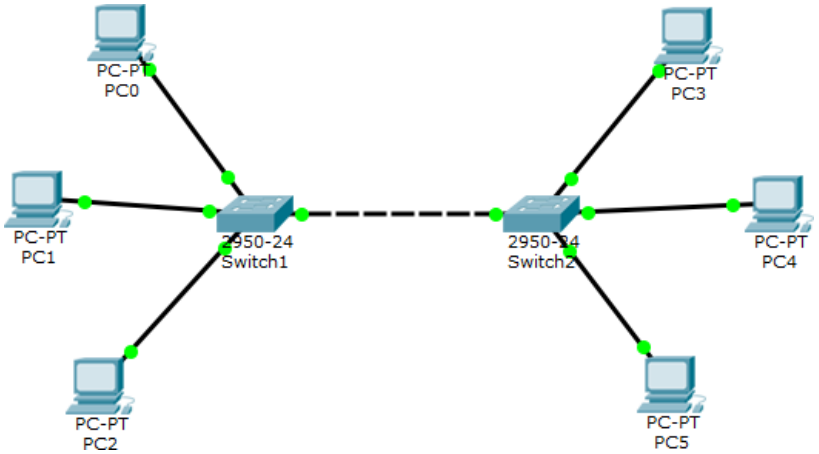
   Wide Area Network (WAN), jangkauannya mencakup daerah geografis yang luas, seringkali mencakup sebuah negara bahkan benua. WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan program-program (aplikasi) pemakai.



Gambar 3.8 : WAN (*Wide Area Network*)

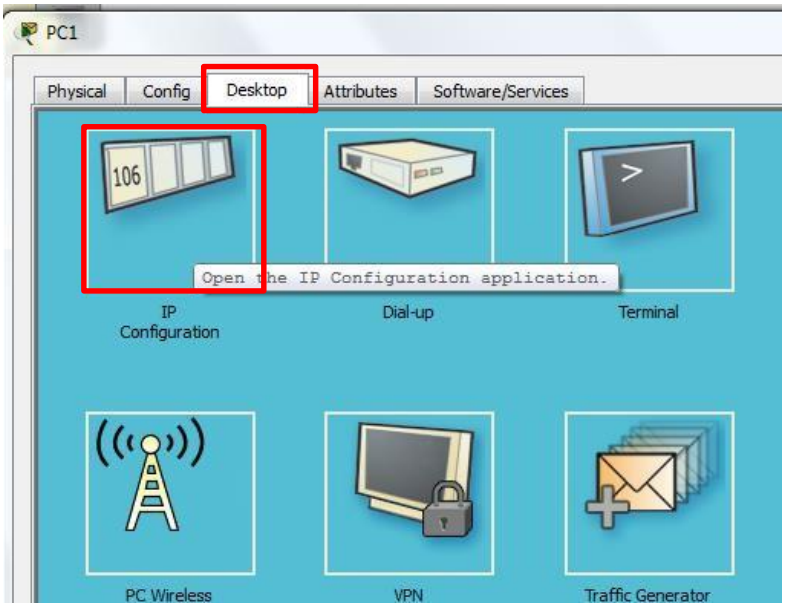
KEGIATAN PRAKTIKUM

Buatlah topologi jaringan pada *Packet Tracer* menggunakan 2 *switch* dan 6 PC.



Gambar 3.9 : Praktik Membangun Topologi Jaringan

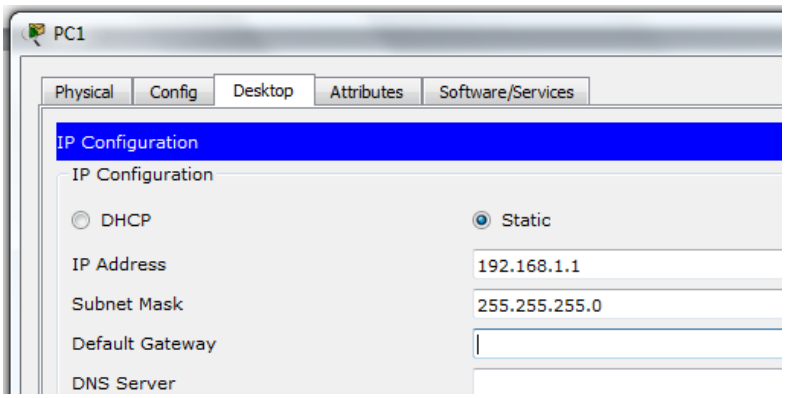
Selanjutnya berikanlah IP *Address* pada masing masing PC agar semua PC bisa terhubung. Klik pada PC lalu pilih ***Desktop*** dan pilih **IP *Configuration***.



Gambar 3.10 : Sub-Menu IP *Configuration*

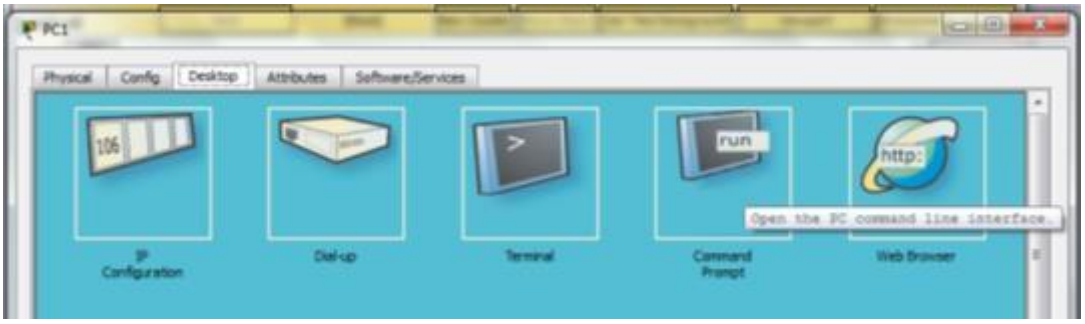
Berikan IP *Address* 192.168.1.1 dan *subnet mask* /24 yaitu 255.255.255.0

Pada PC lain berikan juga IP *Address* yang berada dalam 1 jaringan dengan PC1



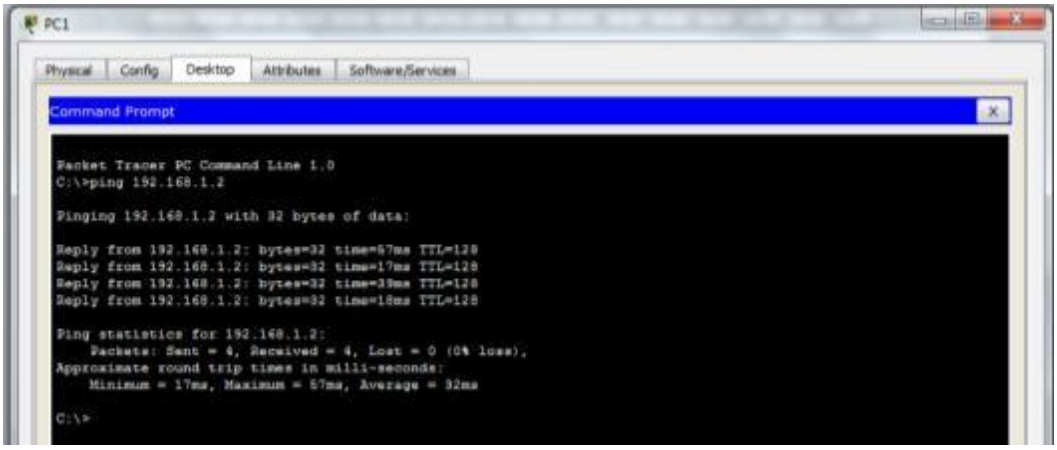
Gambar 3.11 : Memasukkan IP *Address*

Jika semua PC sudah diberikan IP *Address*, sekarang lakukan tes PING untuk mengetahui apakah masing-masing PC sudah terhubung. Klik pada PC lalu pilih ***desktop*** dan **pilih *Command Prompt***



Gambar 3.12 : Sub-Menu *Command Prompt*

Selanjutnya lakukan ping ke PC yang lain.



Gambar 3.13 : Tes PING

Media Transmisi

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

1. ***Guided Media* (Media dengan Kabel)**

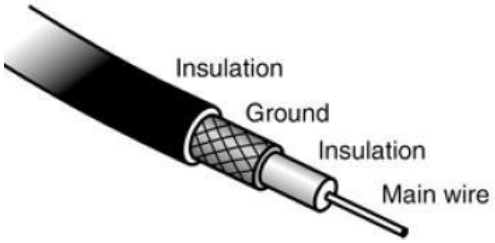
   Guided media menyediakan jalur transmisi sinyal yang terbatas secara fisik, meliputi *twisted-pair cable*, *coaxial cable* (kabel koaksial) dan *fiber-optic cable*. Sinyal yang melewati media-media tersebut diarahkan dan dibatasi oleh batas fisik media.

   a. Coaxial Cable

   Kabel *coaxial* biasa disebut kabel TV (televisi) karena mirip dengan kabel yang digunakan pada antena TV. Kabel ini biasa digunakan untuk membuat instalasi

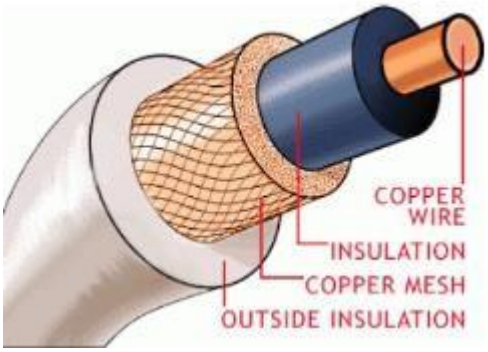
jaringan bertopologi *bus* atau cincin. Namun, kabel ini tidak dapat mendukung jaringan dengan topologi *star* karena *hub*-nya tidak memiliki *port* BNC-*Male*. Apabila dibuka, di dalam kabel *coaxial* akan terdapat dua kawat penghantar, yaitu pengahantar luar (berupa serabut) dan penghantar dalam. Kedua pengahantar tersebut akan menjadi media pengirim (*transmitter*) dan media penerima (*receiver*). Ada 2 tipe kabel *coaxial*, yaitu *thin coaxial cable* dan *thick coaxial cable*

- *Thin coaxial cable* (Kabel *coaxial* "kurus")



Gambar 3.14 : *Thin coaxial cable*

- *Thick coaxial cable* (kabel *coaxial* "gemuk")



Gambar 3.15 : *Thick coaxial cable*

b. Twisted-Pair Cable

Twisted-pair cable adalah sebuah kabel yang terdiri dari beberapa dawai kawat tembaga yang digabungkan menjadi satu dengan cara dipilin atau dibelit enam kali per-inchi membentuk spiral. Jenisnya ada kabel UTP, STP dan FTP.

- *Unshielded Twisted Pair* (UTP)

  Kabel UTP (*Unshielded Twisted Pair*) merupakan media transmisi yang digunakan untuk menghubungkan antara komputer satu dengan komputer yang lain dengan menggunakan *port* RJ45-*Male*. Kabel UTP dapat digunakan untuk membangun jaringan LAN yang besar dengan terminal berupa *switch*.

Gambar 3.16 : Kabel UTP

- *Foiled Twisted Pair* (FTP)

  Tak berbeda jauh dengan *Unshielded Twisted Pair* (UTP), jenis kabel jaringan *Twisted Pair* yang satu ini juga terdiri dari 4 pasang (*pair*) kabel tembaga, yang mana tiap *pair*-nya dipilin (*twisted*) saling berlilitan sehingga membentuk sebuah pola berbentuk spiral. Hanya kabel yang juga dikenal dengan nama S/UTP ini menggunakan aluminium foil yang dipasang tepat di bawah karet luar untuk melindungi isolator sehingga kabel jaringan FTP lebih tahan terhadap interferensi elektromagnetik yang berasal dari sekitar kabel.

Gambar 3.17 : Kabel FTP

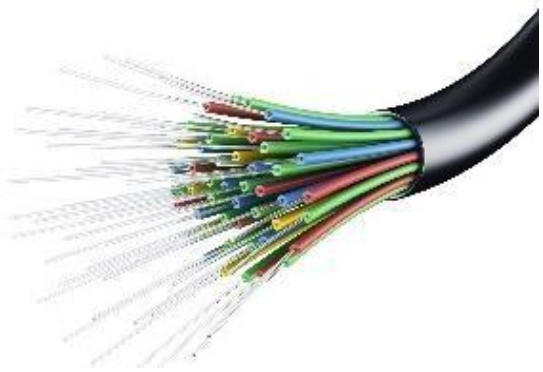
- *Shielded Twisted Pair*

  Keuntungan menggunakan kabel STP adalah lebih tahan terhadap interferensi gelombang elektromagnetik baik dari dari dalam maupun dari luar. Kekurangannya adalah mahal, susah pada saat instalasi (terutama masalah *grounding*), dan jarak jangkauannya hanya 100m . kabel jaringan *Twisted Pair* yang populer dengan nama STP ini harus disambungkan dengan konektor RJ-11

Gambar 3.18 : Kabel STP

c. Fiber Optic Cable

Kabel *Fiber Optik* adalah teknologi kabel terbaru. Terbuat dari serat optik. Di tengah-tengah kabel terdapat filamen glas, yang disebut "*core*", dan di kelilingi lapisan "*cladding*", "*buffer coating*", material penguat, dan pelindung luar. Informasi ditransmisikan menggunakan gelombang cahaya dengan cara mengkonversi sinyal listrik menjadi gelombang cahaya.



Gambar 3.19 : Kabel *Fiber Optic*

2. *Unguided Media* (Tanpa Kabel)

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

KEGIATAN PRAKTIKUM

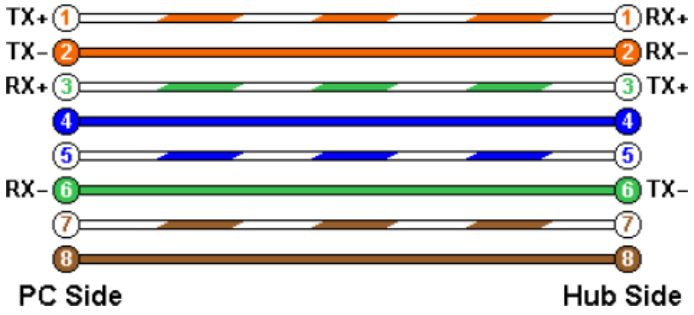
Koneksi Kabel UTP.

Siapkan 2 meter kabel UTP dan 5 buah *connector* RJ-45

Untuk pemasangan kabel UTP pada *port* RJ45, harus menggunakan urutan warna yang sudah menjadi aturan. Cara pemasangan jaringan dibagi menjadi dua, terutama untuk jaringan dengan media transmisi kabel UTP, yaitu model *straight* (sejajar) dan *cross over* (silang). Penjelasannya sebagai berikut :

Model *Straight* (Sejajar)

Model sejajar atau straight merupakan model pemasangan kabel yang sangat sederhana dan mudah untuk dilakuka. Model pemasangan kabel ini akan berguna apabila menggunakan terminal berupa *switch* atau *hub*.



Gambar 3.20 : Susunan Kabel UTP *Stright*

Pada gambar di atas, *port* kiri dan kanan memiliki susunan warna yang sama. Susunannya adalah:

Nomor 1 : Putih Orange

Nomor 2 : Orange

Nomor 3 : Putih Hijau

Nomor 4 : Biru

Nomor 5 : Putih Biru

Nomor 6 : Hijau

Nomor 7 : Putih Coklat

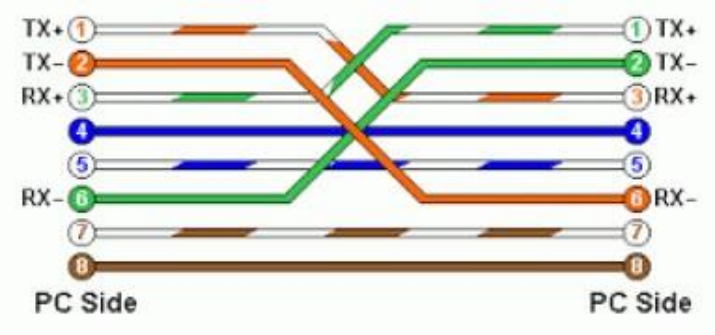
Nomor 8 : Coklat

Model *Cross Over* (Silang)

Pemasangan kabel dengan cara silang atau *cross over* digunakan untuk menghubungkan 2 komputer dengan media transmisi kabel UTP dan *port* RJ45. Pada pemasangan silang, urutan

kabel yang disilang hanya pada nomor 1,2,3, dan 6. Penyilangan tersebut disebabkan karena total kabel yang digunakan dalam *port* RJ45 hanya 6 pin kabel, yaitu nomor 1,2,3,4,5, dan 6. Apabila hendak memasang dua unit komputer dalam satu jaringan dengan terminal tidak berupa *hub* atau *switch*, maka harus memasang kabel dengan sistem silang.

Secara garis besar, urutan pemasangan yang disusun secara silang adalah:



Gambar 3.21 : Susunan Kabel UTP *Cross Over*

Urutan warna yang dapat digunakan pada port A, analoginya adalah urutan pada ujung kabel pertama.

Nomor 1 : Putih Orange

Nomor 2 : Orange

Nomor 3 : Putih Hijau

Nomor 4 : Biru

Nomor 5 : Putih Biru

Nomor 6 : Hijau

Nomor 7 : Putih Coklat

Nomor 8 : Coklat

Urutan warna yang dapat digunakan pada port B, analoginya adalah urutan pada ujung kabel kedua.

Nomor 1 : Putih Hijau

Nomor 2 : Hijau

Nomor 3 : Putih Orange

Nomor 4 : Biru

Nomor 5 : Putih Biru

Nomor 6 : Orange

Nomor 7 : Putih Coklat

Nomor 8 : Coklat

MODUL 4

IP *ADDRESS*

(Pertemuan 6, 7)

Tujuan

1. Mahasiswa mampu menjelaskan dan menerapkan teori tentang IP *Address* versi 4 dan IP *Address* Versi 6.

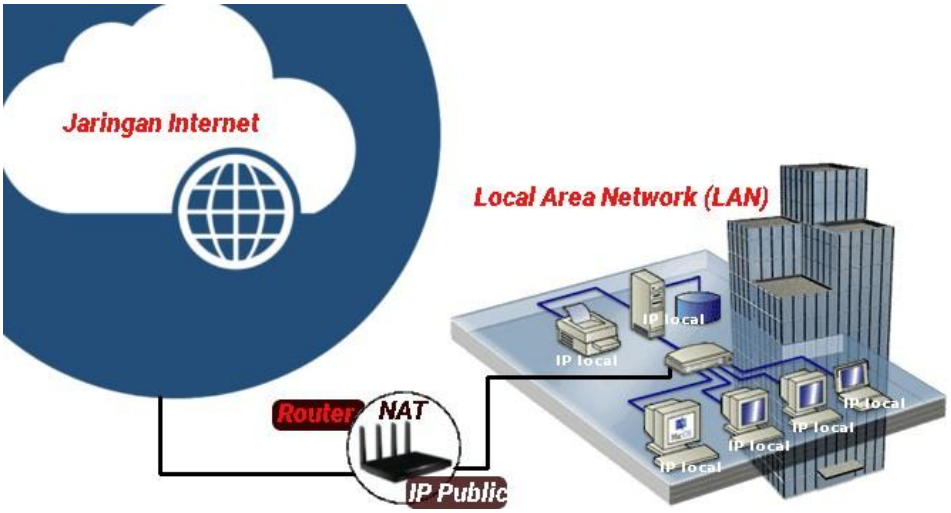
Tugas Pendahuluan

1. Apakah yang dimaksud dengan IP Versi 4
2. Apakah yang dimaksud dengan IP Versi 6
3. Jelaskan perbedaan antara IPV 4 dan IPV6

DASAR TEORI

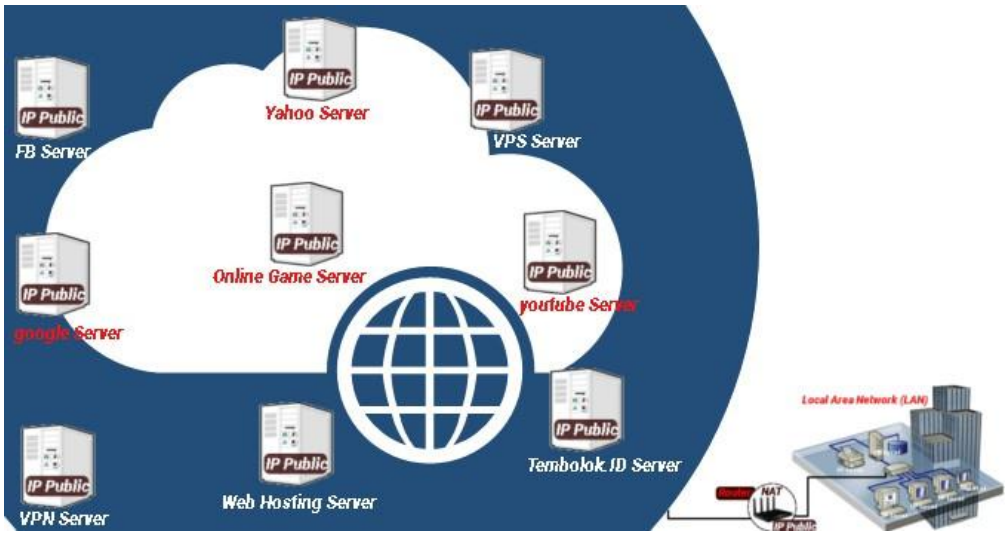
IP *Address* adalah adalah protokol yang memberikan alamat atau identitas untuk peralatan di dalam jaringan . IP *Address* ada yang di sebut sebagai IP *Private* dan IP Publik.

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



Gambar 4.1 : IP *Private*

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



Gambar 4.2 : IP Publik

IPv4 (Internet *Protocol* versi 4)

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

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

Alamat IPv4 terbagi menjadi tiga jenis, yaitu alamat *unicast*, *broadcast*, dan *multicast*.

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

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

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

Pembagian kelas IP *Address* versi 4 :

a. **IP *Address* Kelas A**, merupakan IP *address* dengan jumlah yang sangat besar, sehingga biasanya digunakan untuk jaringan yang sangat besar dengan jumlah *host* yang sangat banyak. Sebagai contoh pada penggunaan IP *address* : 113.46.5.6 , 113 berfungsi sebagai *network* ID sedangkan 46.5.6 berfungsi sebagai *host* ID nya.

b. **IP *Address* Kelas B,** merupakan IP *address* dengan jumlah *host* yang sedang, jumlah maksimal *host* berkisar 65.534 *host*, sehingga IP ini cocok untuk jaringan dengan jumlah *host* yang tidak terlalu besar dan tidak terlalu kecil. Sebagai contoh penggunaan IP *address* Kelas B adalah : 132.92.121.1 , 132.92 berfungsi sebagai *network* ID sedangkan 121.1 berfungsi sebagai *host* ID.

c. **IP *Address* Kelas C**, merupakan IP *address* dengan jumlah *host* yang sangat kecil sehingga IP *address* ini digunakan untuk jaringan kecil seperti disekolah-sekolah, dikantor-kantor maupun instansi rumahan, jumlah maksimal *host* pada IP address ini hanya 254 *host*. Seabagai contoh penggunaan IP Address Kelas C adalah : 192.168.1.2 , 192.168.1 merupakan *network* ID dan 2 merupakan *host* ID-nya

d. **IP *Address* Kelas D**

Alamat IP kelas D disediakan hanya untuk alamat-alamat IP *multicast*, namun berbeda dengan tiga kelas di atas. Empat bit pertama di dalam IP kelas D selalu diset ke bilangan biner 1110. 28 bit sisanya digunakan sebagai alamat yang dapat digunakan untuk mengenali *host*.

e. **IP *Address* Kelas E**

Alamat IP kelas E disediakan sebagai alamat yang bersifat eksperimental atau percobaan dan dicadangkan. Empat bit pertama selalu diset kepada bilangan biner

1111. 28 bit sisanya digunakan sebagai alamat yang dapat digunakan untuk mengenali *host*.

Struktur Paket IPv4

Gambar 4.3 : Struktur Paket IPv4

- ***Version*** mengindentifikasi versi IP, yang dimana untuk IPV4 nilai diset menjadi 4
- ***Header* (IHL)** berfungsi mengidentifikasi ukuran header IP .
- **TOS (*Type of service*)** digunakan untuk menentukan kualitas transmisi dari sebuah datagram IP.
- ***Total Length*** dapat didefinisikan panjang keseluruhan dari datagram IP, dimana mencakup *header* IP dan muatan yang didalamnya dalam bentuk *byte*. Minimum-panjang datagram adalah 20 *byte* (*header* 20-*byte* + 0 *byte* data) dan maksimal adalah 65.535 *byte*
- ***Indetification*** merupakan bagian yang digunakan mengindentifikasi sebuah paket IP yang tertentu yang akan difregmentasikan.
- ***Flag*** digunakan untuk mengontrol apakah *router* diperbolehkan untuk fragmen dan untuk menunjukkan bagian-bagian dari sebuah paket ke *receiver*.
- ***Fragment Offset*** merupakan jumlah byte dari awal paket yang dikirim. Selain itu *Fragment Offset* digunakan untuk mengidentifikasikan *offset* di mana fragmen yang dimulai.
- ***Time to Live*** digunakan untuk mengidentifikasikan berapa banyak saluran jaringan di mana sebuah datagram IP dapat berjalan .
- ***Protocol*** mendefinisikan protokol yang digunakan dalam bagian data dari datagram IP.
- ***Header Checksum*** berguna untuk melakukan pengecekan integritas terhadap header IP. *Header Checksum* berisi nilai *checksum* yang dihitung dari seluruh *field* dari *header* paket IP.
- ***Source address*** adalah sebuah alamat IPv4 yang menunjukkan pengirim paket.
- ***Destination address*** adalah sebuah alamat IPv4 yang menunjukkan penerima paket

IPV 6 (*Internet Protocol* Versi 6)

Alamat IP versi 6 (IPv6) adalah sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol Internet versi 6. Panjang totalnya adalah 128-bit, dan secara teoritis dapat mengalamati hingga 2128=3,4 x 1038 *host* komputer di seluruh dunia.

Contoh alamat IPv6 adalah 21da:00d3:0000:2f3b:02aa:00ff:fe28:9c5a

Sama seperti halnya IPv4, IPv6 juga mengizinkan adanya DHCPv6 Server sebagai pengelola alamat. Jika dalam IPv4 terdapat *dynamic address* dan *static address*, maka dalam IPv6, konfigurasi alamat dengan menggunakan DHCP Server dinamakan dengan ***stateful address configuration***, sementara jika konfigurasi alamat IPv6 tanpa DHCP Server dinamakan dengan ***stateless address configuration***. Pada IPv6 terdapat 3 jenis tipe alamat IP yaitu :

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

Pengalamatan pada IPv6

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

Berikut ini adalah contoh alamat IPv6 dalam bentuk bilangan biner:

```
00100001110110100000000011010011000000000000000000010111100111011000000010101
0101000000000
11111111111111000101000100111000101101O
```

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

```
0010000111011010    0000000011010011    0000000000000000    0010111100111011
0000001010101010    0000000011111111    1111111000101000    1001110001011010
```

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

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

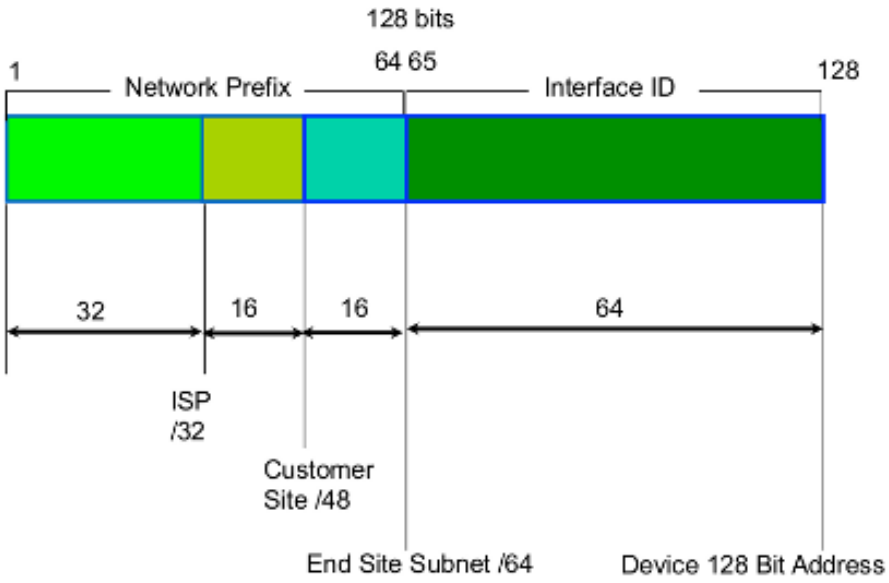
Struktur Paket IPv6 :

Gambar 4.4 : Format Paket IPv6

- ***Version*** : field yang menunjukkan versi Internet Protokol, yaitu 6.
- ***Prior*** : field yang menunjukkan nilai prioritas. *Field* ini memungkinkan pengirim paket mengidentifikasi prioritas yang diinginkan untuk paket yang dikirimkan

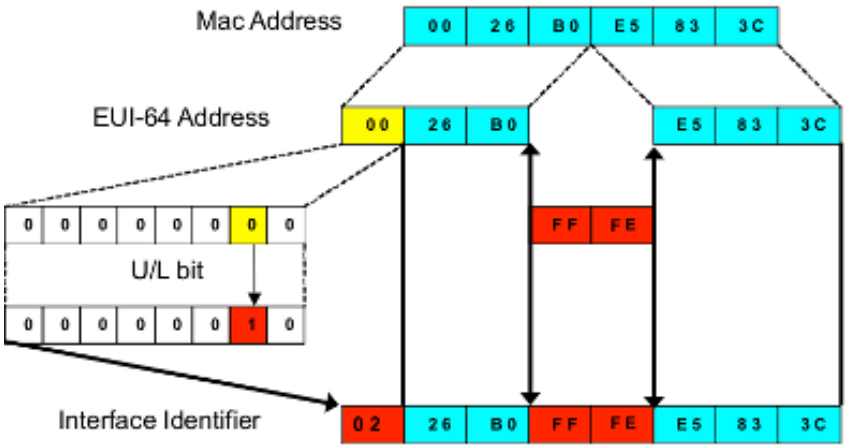
- ***Flow Label*** : digunakan oleh pengirim untuk memberi label pada paket-paket yang membutuhkan penanganan khusus dari *router* IPv6, seperti *quality of service* yang bukan *default*, misalnya *service-service* yang bersifat *real-time*.
- ***Payload Length*** : *field* berisi 16 bit yang menunjukkan panjang *payload*, yaitu sisa paket yang mengikuti *header* IP, dalam oktet.
- ***Next Header*** : field 8 bit yang berfungsi mengidentifikasi *header* yang mengikuti *header* IPv6 utama.
- ***Hop Limit*** : field berisi 8 bit *unsigned integer*. Menunjukkan jumlah *link* maksimum yang akan dilewati paket sebelum dibuang. Paket akan dibuang bila *Hop Limit* bernilai nol.
- ***Source Address*** : field 128 bit, menunjukkan alamat pengirim paket.
- ***Destination Address*** : field 128 bit, menunjukkan alamat penerima paket.

Secara struktur penulisan alamat IPv6 dibagi menjadi 2 yaitu ***Network Prefix*** dan ***Interface ID***. *Network Prefix* adalah alokasi alamat yang diberikan dari RIR (*Regional Internet Registry*) dan juga alokasi dari ISP. Untuk *Interface* ID merupakan pengalamatan pada sisi *host*/perangkat di jaringan.



Gambar 4.5 : Struktur Penulisan Alamat IPv6

Khusus pengalamatan pada ***Interface* ID** bisa menuliskan nya dengan *hexadecimal* secara manual menggunakan *subnetting*, secara otomatis dapat didefiniskan secara otomatis berdasarkan MAC *Address* dari perangkat yang ada. Metode ini disebut sebagai **EUI-64** yang mana bisa digunakan untuk menjaga keunikan di setiap alamat IPv6.



Gambar 4.6 : Pengalamatan Interface ID pada IPv6

Perbedaan IPv4 dan IPv6

1. Kelas Pengalamatan

   Di dalam IPv4 dikenal dengan kelas pengalamatan, yang terdiri dari 5 kelas yaitu Kelas A, Kelas B, Kelas C, Kelas D dan kelas E. Biasanya yang dipakai oleh umum ada di kelas A, B, dan C, sedangkan Kelas D untuk multicast dan Kelas E untuk penelitian. Namun kadang ada yang menyebut Kelas D dan E itu di satukan. Sedangkan di dalam IPv6, tidak dikenal penamaan kelas-kelas tersebut. Tetapi di dalam IPv6 dikenal jenis pengalamatan, yaitu Pengalamatan *Unicast*, Pengalamatan *Multicast*, dan pengalamatan *Anycast*. Alamat Unicast dibagi lagi menjadi 3 bagian, yaitu Alamat *Link Local*, Alamat *Site Local*, dan Alamat Global.
2. *Routing*

   Di IPv4, memiliki jalur yang lebih lambat dalam melakukan *routing*, hal ini dikarenakan adanya pemeriksaan *header* MTU di setiap *routing* dan *switching*. Sedangkan di IPv6, proses *routing* menjadi lebih sederhana. Dengan begini proses *routing* di IPv6 menjadi lebih cepat.

3. *Mobile* IP

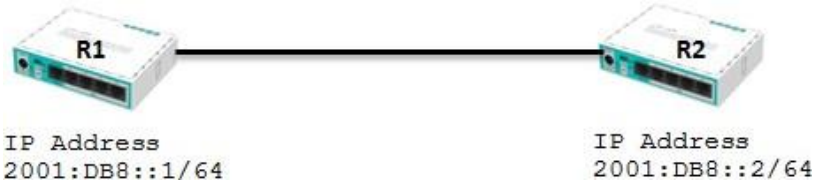
   Dukungan IPv4 terhadap perangkat *mobile* sangat kurang. Karena IPv4 tidak diperuntukkan untuk sebuah perangkat *mobile*. Karena itu sering terjadi *roaming*. Sedangkan pada IPv6 mendukung perangkat *mobile* di dalam desain IP.

4. Keamanan

   Untuk menjaga keamanan IPv4 mengggunakan IPsec, sebagai fitur keamanannya. Tetapi fitur ini hanya sebagai fitur tambahan. Sedangkan di IPv6, IPsec secara *default* telah digunakan. Jadi setiap proses akan melewati IPsec terlebih dahulu.

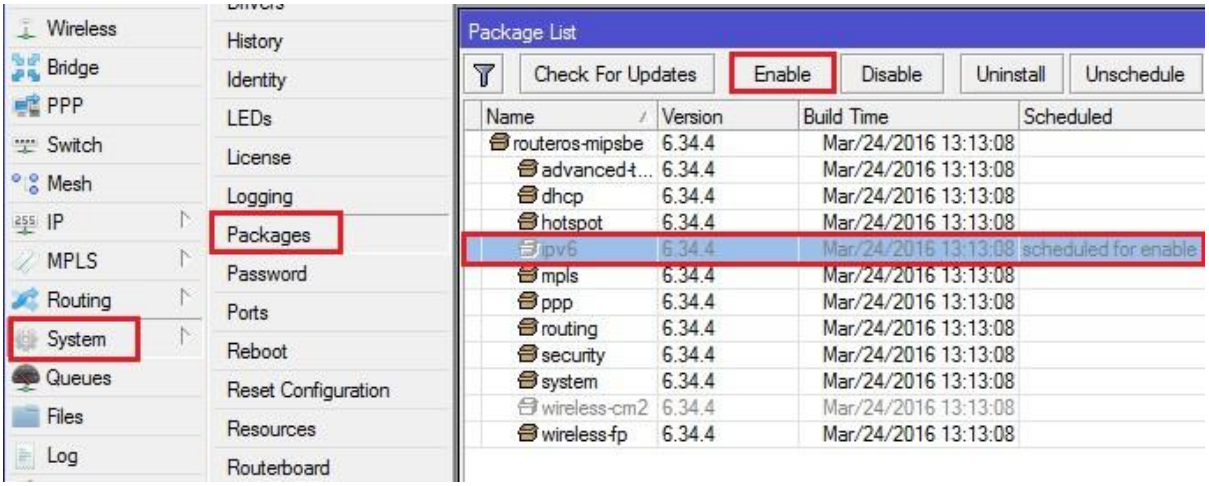
KEGIATAN PRAKTIKUM

Konfigurasi IP Address versi 6 pada *Router* Mikrotik



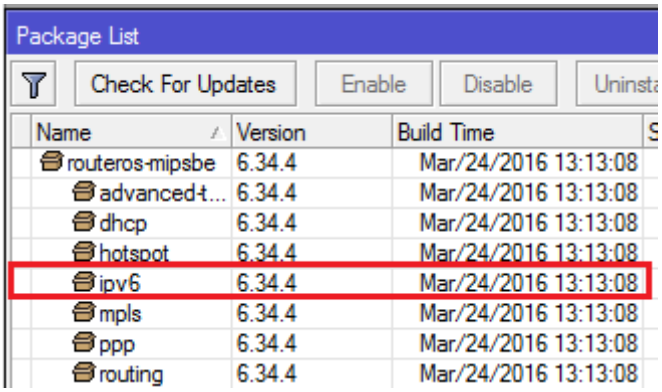
Gambar 4.7 : Konfigurasi IPv6 pada *Router* Mikrotik

Untuk alokasi IPv6, MikroTik sudah menambahkan fitur IPv6 pada sistem RouterOS. Secara *default* walaupun sudah ditambahkan pada sistem, untuk saat ini fitur tersebut tidak diaktifkan (*disable*). Untuk menggunakannya fitur IPv6 harus diaktifkan terlebih dahulu. Masuk pada menu ***System***>***Packages***> pilih **IPv6**> klik tombol ***Enable***. Kemudian reboot router supaya fitur IPv6 aktif.



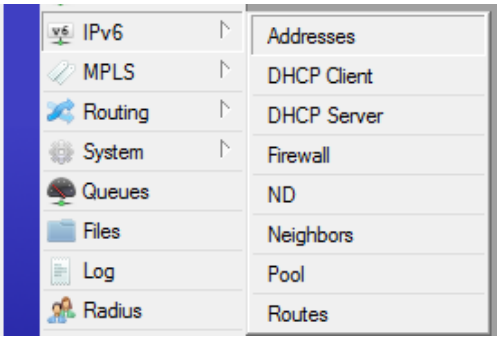
Gambar 4.8 : Mengaktifkan Fitur IPv6

Ketika *router* sudah di *reboot* maka fitur IPv6 akan aktif



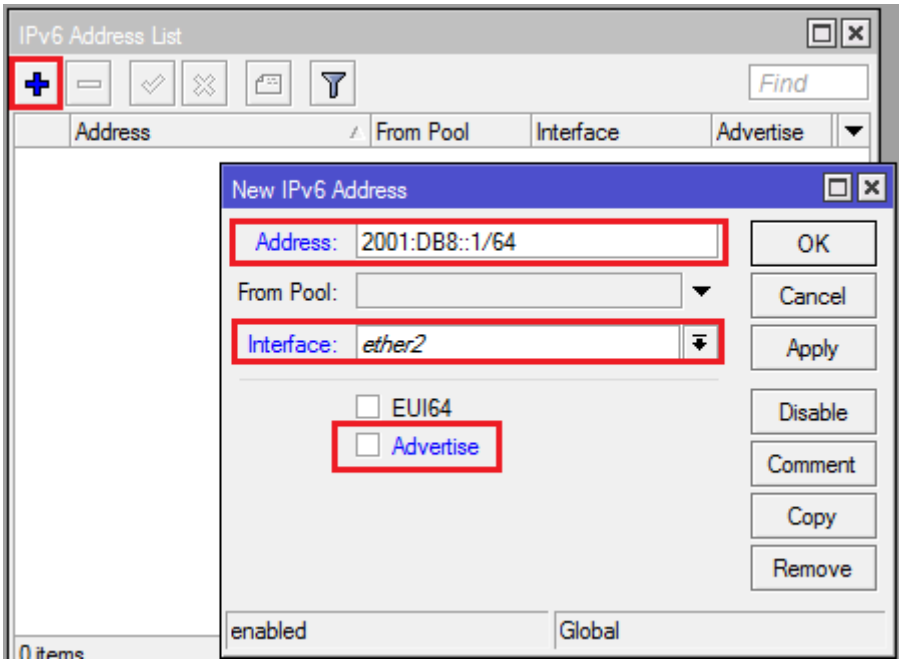
Gambar 4.9 : IPv6 Berhasil Diaktifkan

Untuk konfigurasi Ipv6 klik menu IPv6 dan pilih *Addresses*



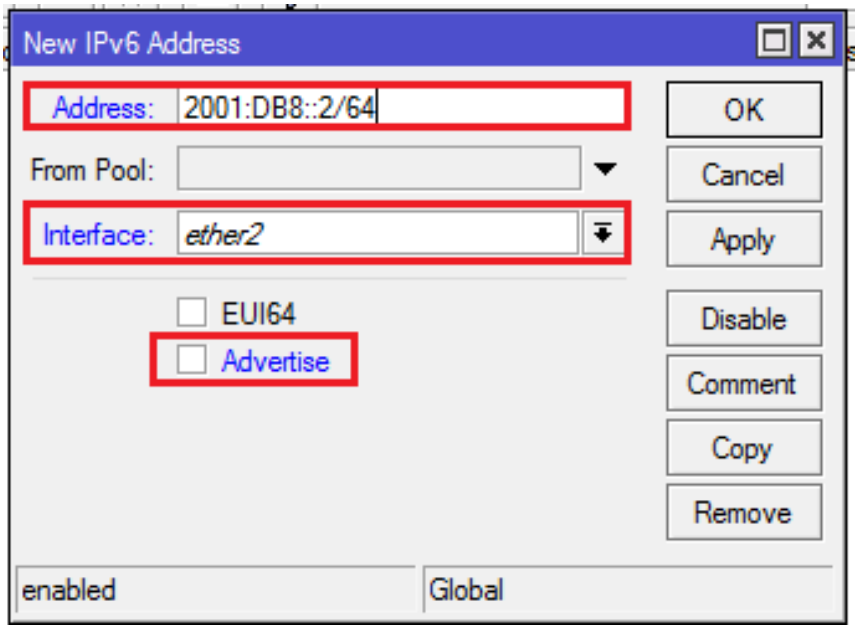
Gambar 4.10 : Tampilan Menu IPv6 *Address*

Pada *router* 1 gunakan IP *Address* `2001:DB8::1/64`, pada *interface* gunakan *interface* yang terhubung ke *router* 2 dan hilangkan tanda centang di *Advertise*



Gambar 4.11 : Mengatur IP *Address* pada *Router* 1

Pada *router* 2 gunakan IP *Address* `2001:DB8::2/64` , *interface*nya gunakan *interface* yang terhubung ke *router* 1 dan hilangkan juga tanda centang di *Advertise* .



Gambar 4.12 : Mengatur IP *Address* pada *Router* 2

Selanjutnya lakukanlah pengujian melalui CLI , klik ***New Terminal***

Pada CLI masuk terlebih dahulu ke ipv6 *address* lalu lakukan ping ke IP yang ada di *router* 1

```
Ipv6 address
/ping 2001:DB8::1
```

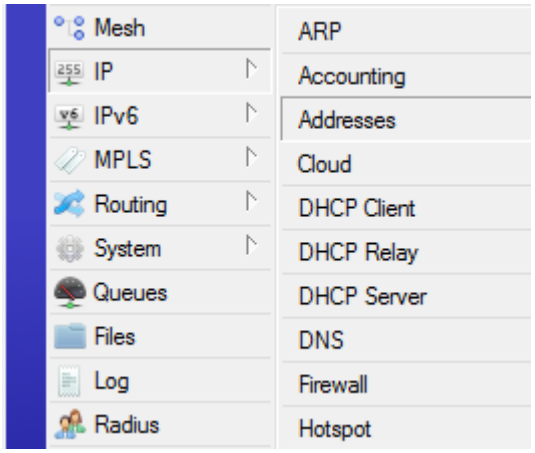
Dan jika berhasil terhubung maka tampilannya akan seperti gambar dibawah ini.

```
[admin@MikroTik] > ipv6 address
[admin@MikroTik] /ipv6 address> /ping 2001:DB8::1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 2001:db8::1                                56  64 0ms   echo reply
    1 2001:db8::1                                56  64 0ms   echo reply
    2 2001:db8::1                                56  64 0ms   echo reply
    3 2001:db8::1                                56  64 0ms   echo reply
    4 2001:db8::1                                56  64 0ms   echo reply
    sent=5 received=5 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

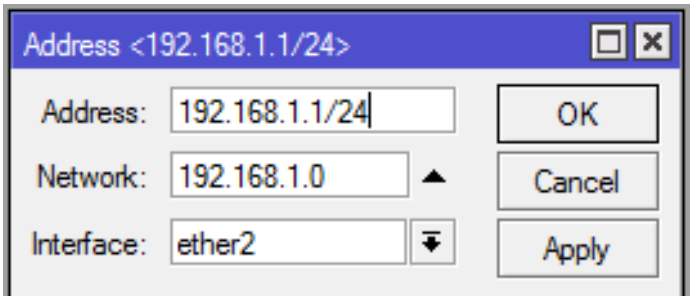
Gambar 4.13 : Tampilan Hasil Pengujian Berhasil

Konfigurasi IP Address versi 4 pada *Router* Mikrotik

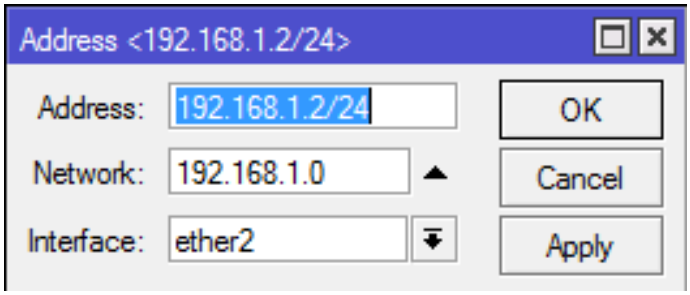
Buka aplikasi winbox pada PC lalu login ke router MikroTik, Untuk memberikan IP Address klik menu IP lalu pilih Addresses.



Pada menu Addresses klik tanda + untuk menambahkan IP Address . Pada router 1 berikan IP Address 192.168.1.1/24 dan interfacenya gunakan interface yang terhubung ke router 2



Kemudian pada Router 2 berikan IP Address 192.168.1.2/24 dan interface nya gunakan interface yang terhubung ke router 1.



Selanjutnya lakukanlah pengujian. Klik New Terminal dan ketikkan perintah berikut.

Ping 192.168.1.2

```
[admin@MikroTik] > ping 192.168.1.2
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.1.2                                56  64 0ms
    1 192.168.1.2                                56  64 0ms
    2 192.168.1.2                                56  64 0ms
    3 192.168.1.2                                56  64 0ms
    sent=4 received=4 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms

[admin@MikroTik] >
```

Tugas

1. Buat sebuah topologi jaringan pada GNS3 dengan 3 *Switch* . Masing masing *switch* terhubung dengan 5 PC.
2. Berikan IP *Address* pada masing-masing PC agar semua PC terhubung.
3. Konfigurasi IP versi 6 pada 3 *router* agar router tersebut bisa saling terhubung.

MODUL 5

SUBNETTING

(Pertemuan 9, 10, 11)

Tujuan

1. Mahasiswa mampu menjelaskan serta menerapkan tentang pembagian IP *Address* menggunakan konsep *subnetting*

Tugas Pendahuluan

1. Apakah yang dimaksud dengan *subnetting* ?
2. Sebutkan dan jelaskan cara cara *subnetting!*

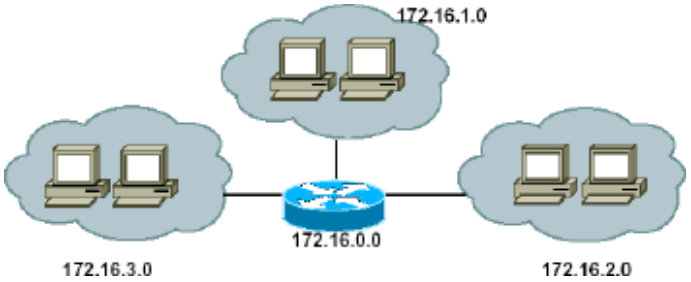
DASAR TEORI

Subnetting adalah cara membagi satu jaringan menjadi beberapa sub jaringan. Beberapa bit dari bagian *Host* ID dialokasikan menjadi bit tambahan pada bagian NetID. Cara ini menciptakan sejumlah NetID tambahan dan mengurangi jumlah maksimum *host* yang ada dalam tiap jaringan tersebut. Gambar 5.1 adalah contoh sebuah jaringan dengan IP Address 172.16.0.0.

Gambar 5.1 : Sebuah Jaringan dengan 1 subnet

Gambar 5.1 di atas menunjukkan bahwa jaringan tersebut hanya memiliki satu IP jaringan yaitu 172.16.0.0 (Kelas B). Jadi untuk HostID akan menggunakan NetID sebagai acuan pembagian IP Address dalam jaringan tersebut. Dengan *Subnetting*, sebuah alamat jaringan tunggal ini dapat dipecah menjadi banyak sub jaringan (*sub network*, atau *subnet*).

Gambar 5.2 adalah contoh sebuah jaringan yang dipecah menjadi beberapa sub jaringan.



Gambar 5.2 : Sebuah Jaringan di bagi menjadi 3

Tujuan *Subnetting* :

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

Fungsi Subnetting :

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

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

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

   Classless Inter-Domain Routing (CIDR) adalah sebuah cara alternatif untuk mengklasifikasikan alamat-alamat IP berbeda dengan sistem klasifikasi ke dalam kelas A, kelas B, kelas C, kelas D, dan kelas E. Disebut juga sebagai *supernetting*. CIDR merupakan mekanisme *routing* dengan membagi alamat IP jaringan ke dalam kelas-kelas A, B, dan C. CIDR digunakan untuk mempermudah penulisan notasi *subnet mask* agar lebih ringkas dibandingkan penulisan notasi *subnet mask* yang

sesungguhnya. Untuk penggunaan notasi alamat CIDR pada *classfull address* pada kelas A adalah /8 sampai dengan /15, kelas B adalah /16 sampai dengan /23, dan kelas C adalah /24 sampai dengan /28. *Subnet mask* CIDR /31 dan /32 tidak pernah ada dalam jaringan yang nyata.

Tabel 5.1 *Subnetting* dengan Metode CIDR

# bits	# hosts	Usable hosts	netmask		Cisco mask
/4	268435456	268435454	240.0.0.0		15.255.255.255
/5	134217728	134217726	248.0.0.0		7.255.255.255
/6	67108864	67108862	252.0.0.0		3.255.255.255
/7	33554432	33554430	254.0.0.0		1.255.255.255
/8	16777216	16777214	255.0.0.0	*class A network*	0.255.255.255
/9	8388608	8388606	255.128.0.0		0.127.255.255
/10	4194304	4194302	255.192.0.0		0.63.255.255
/11	2097152	2097150	255.224.0.0		0.31.255.255
/12	1048576	1048574	255.240.0.0		0.15.255.255
/13	524288	524286	255.248.0.0		0.7.255.255
/14	262144	262142	255.252.0.0		0.3.255.255
/15	131072	131070	255.254.0.0		0.1.255.255
/16	65536	65534	255.255.0.0	*class B network*	0.0.255.255
/17	32768	32766	255.255.128.0		0.0.127.255
/18	16384	16382	255.255.192.0		0.0.63.255
/19	8192	8190	255.255.224.0		0.0.31.255
/20	4096	4094	255.255.240.0		0.0.15.255
/21	2048	2046	255.255.248.0		0.0.7.255
/22	1024	1022	255.255.252.0		0.0.3.255
/23	512	510	255.255.254.0		0.0.1.255
/24	256	254	255.255.255.0	*class C network*	0.0.0.255
/25	128	126	255.255.255.128		0.0.0.127
/26	64	62	255.255.255.192		0.0.0.63
/27	32	30	255.255.255.224		0.0.0.31
/28	16	14	255.255.255.240		0.0.0.15
/29	8	6	255.255.255.248		0.0.0.7
/30	4	2	255.255.255.252		0.0.0.3
/31	*point to point links only*				
/32	1	1	255.255.255.255	*single IP address*	use host notation

Contoh Subnetting dengan metode CIDR

a. Menghitung Subnet Kelas C

Pada kelas C penghitungan yang digunakan adalah pada octet ke 4.

Diketahui suatu IP 192.168.1.0/26. Berarti *subnetmask*nya /26 yaitu 255.255.255.192, jika diubah ke dalam bilangan biner menjadi 11111111.11111111.11111111.11000000.

1. Jumlah *Subnet* = 2^x (dimana x adalah banyaknya bineri 1 pada octet terakhir (yang bergaris bawah) untuk kelas C. Jadi Jumlah *Subnet*nya adalah $2^2 = 4$ subnet.

2. Jumlah *Host per Subnet* = $2^y - 2$ (dimana y adalah banyaknya bineri 0 pada octet terakhir untuk kelas C). Jadi Jumlah *Host per Subnet*nya adalah $2^6 - 2 = 62$ *host*
3. Blok *Subnet* = 256 – nilai octet terakhir *subnetmask*. Jadi Blok *Subnet*nya adalah 256 – 192 = 64. Untuk *subnet* berikutnya ditambahkan hasil dari blok *subnet* tersebut. Jadi Blok *Subnet* seluruhnya adalah 0, 64, 128, 192.
4. Buat tabelnya seperti berikut dengan catatan :

   – *Subnet* : sesuai pada blok *subnet*.

   – *Host* Pertama : 1 angka setelah *subnet*.

   – *Broadcast* : 1 angka sebelum *subnet* berikutnya.

   – *Host* terakhir : 1 angka sebelum *broadcast*.

Tabel 5.2 Rekapitulasi Perhitungan *Subnet* Kelas C

Subnet	192.168.1.**0**	192.168.1.**64**	192.168.1.**128**	192.168.1.**192**
***Host* Pertama**	192.168.1.**1**	192.168.1.**65**	192.168.1.**129**	192.168.1.**193**
***Host* Terakhir**	192.168.1.**62**	192.168.1.**126**	192.168.1.**190**	192.168.1.**254**
Broadcast	192.168.1.**63**	192.168.1.**127**	192.168.1.**191**	192.168.1.**255**

b. Menghitung Subnet Kelas B

Untuk kelas B ada 2 teknik yang digunakan dalam perhitungan. Untuk *subnetmask* /17 sampai /24, perhitungannya sama persis dengan kelas C, tetapi pada kelas B terletak pada octet ke 3 saja yang digunakan. Sedangkan untuk *subnetmask* /25 sampai /30 perhitungannya yaitu pada octet ke 3 dan 4.

Diketahui suatu IP 172.16.0.0/25. Berarti *subnetmask*nya /25 yaitu 255.255.255.128, jika diubah ke dalam bilangan biner menjadi 11111111.11111111.11111111.10000000.

1. Jumlah *Subnet* = $2^9 = 512$ *subnet*
2. Jumlah *Host per Subnet* = $2^7 - 2 = 126$ *host*
3. Blok *Subnet* = 256 – 128 = 128. Jadi Blok *Subnet* seluruhnya adalah (0, 128)
4. Tabelnya menjadi :

Tabel 5.3 Rekapitulasi Perhitungan *Subnet* Kelas B

Subnet	172.16.**0.0**	172.16.**0.128**	172.16.**1.0**	…	172.16.**255.128**
***Host* Pertama**	172.16.**0.1**	172.16.**0.129**	172.16.**1.1**	…	172.16.**255.129**
***Host* Terakhir**	172.16.**0.126**	172.16.**0.254**	172.16.**1.126**	…	172.16.**255.254**
Broadcast	172.16.**0.127**	172.16.**0.255**	172.16.**1.127**	…	172.16.**255.255**

c. Menghitung *Subnet* Kelas A

Pada kelas A perhitungan dilakukan pada octet ke 2, 3 dan 4.

Diketahui suatu IP 10.0.0.0/16. Berarti *subnetmask*nya /16 yaitu 255.255.0.0, jika diubah ke dalam bilangan biner menjadi 11111111.11111111.00000000.00000000.

1. Jumlah *Subnet* = 2^8 = 256 subnet
2. Jumlah *Host per Subnet* = 2^{16} – 2 = 65534 *host*
3. Blok *Subnet* = 256 – 255 = 1. Jadi Blok *Subnet* seluruhnya : 0,1,2,3,4, dst.
4. Tabelnya menjadi :

Tabel 5.4 Rekapitulasi Perhitungan *Subnet* Kelas A

Subnet	10.**0.0.0**	10.**1.0.0**	…	10.**254.0.0**	10.**255.0.0**
***Host* Pertama**	10.**0.0.1**	10.**1.0.1**	…	10.**254.0.1**	10.**255.0.1**
***Host* Terakhir**	10.**0.255.254**	10.**1.255.254**	…	10.**254.255.254**	10.**255.255.254**
Broadcast	10.**0.255.255**	10.**1.255.255**	…	10.**254.255.255**	10.**255.255.255**

2. VLSM (*Variable Length Subnet Mask*)

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

Manfaat VLSM:

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

Subnetting dengan metode VLSM :

Di sebuah sekolah terpasang sebuah IP 202.40.10.0/24 dan IP tersebut akan dibagi ke dalam 5 bagian yaitu :
Pimpinan dengan 3 *host*
Guru dengan 55 *host*
Siswa dengan 108 *host*
Teknisi 26 *host* dan Administrasi 11 *host*
Tentukanlah *network address*, *Range* IP, dan *Broadcast Address* pada setiap bagian yang telah ditentukan !

Pembahasan :
Urutkan terlebih dahulu jaringan dari yang paling banyak *host*nya:

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

Tabel 5.5 Urutan Jaringan

NetMask Desimal	*NetMask* Biner	Format CIDR	Jumlah *Host*
255.255.255.0	11111111.11111111.11111111.00000000	/24	254
255.255.255.128	11111111.11111111.11111111.10000000	/25	126
255.255.255.192	11111111.11111111.11111111.11000000	/26	62
255.255.255.224	11111111.11111111.11111111.11100000	/27	30
255.255.255.240	11111111.11111111.11111111.11110000	/28	14
255.255.255.248	11111111.11111111.11111111.11111000	/29	6
255.255.255.252	11111111.11111111.11111111.11111100	/30	2

1. Siswa : 108 *host*

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

   $108 \leq 2^7 - 2$

   $108 \leq 128 - 2$

   $108 \leq 126$

   Network Address : 202.40.10.0/25

   Range IP *Address* : 202.40.10.1 – 202.40.10.126

   Broadcast Address : 202.40.10.127

2. Guru : 55 *host*

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

   $55 \leq 2^6 - 2$

   $55 \leq 64 - 2$

   $55 \leq 62$

   Network Address : 202.40.10.128/26

   Range IP *Address* : 202.40.10.129 – 202.40.10.190

   Broadcast Address : 202.40.10.191

3. Teknisi : 26 *host*

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

$26 \leq 2^5 - 2$

$26 \leq 32 - 2$

$26 \leq 30$

Network Address : 202.40.10.192/27

Range IP *Address* : 202.40.10.193 – 202.40.10.222

Broadcast Address : 202.40.10.223

4. Administrasi : 11 *host*

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

$11 \leq 2^4 - 2$

$11 \leq 16 - 2$

$11 \leq 14$

Network Address : 202.40.10.224/28

Range IP *Address* : 202.40.10.225 – 202.40.10.238

Broadcast Address : 202.40.10.239

5. Pimpinan : 3 *host*

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

$3 \leq 2^4 - 2$

$3 \leq 8 - 2$

$3 \leq 6$

Network Address : 202.40.10.240/27

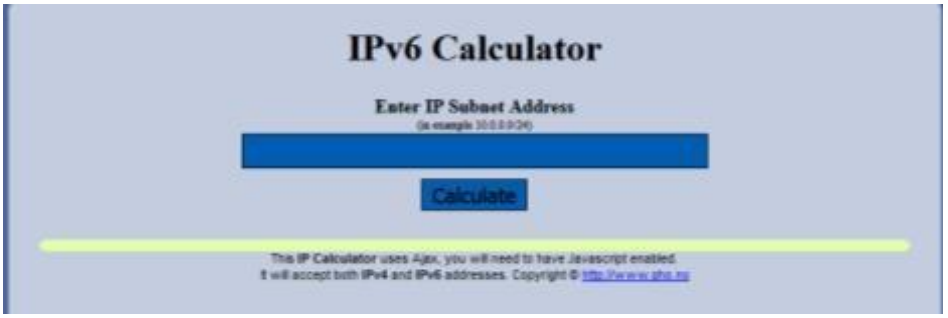
Range IP *Address* : 202.40.10.241 – 202.40.10.246

Broadcast Address : 202.40.10.247

Subnetting IPv6 dapat menggunakan IP *calculator* seperti :

http://www.ipv6calculator.net/

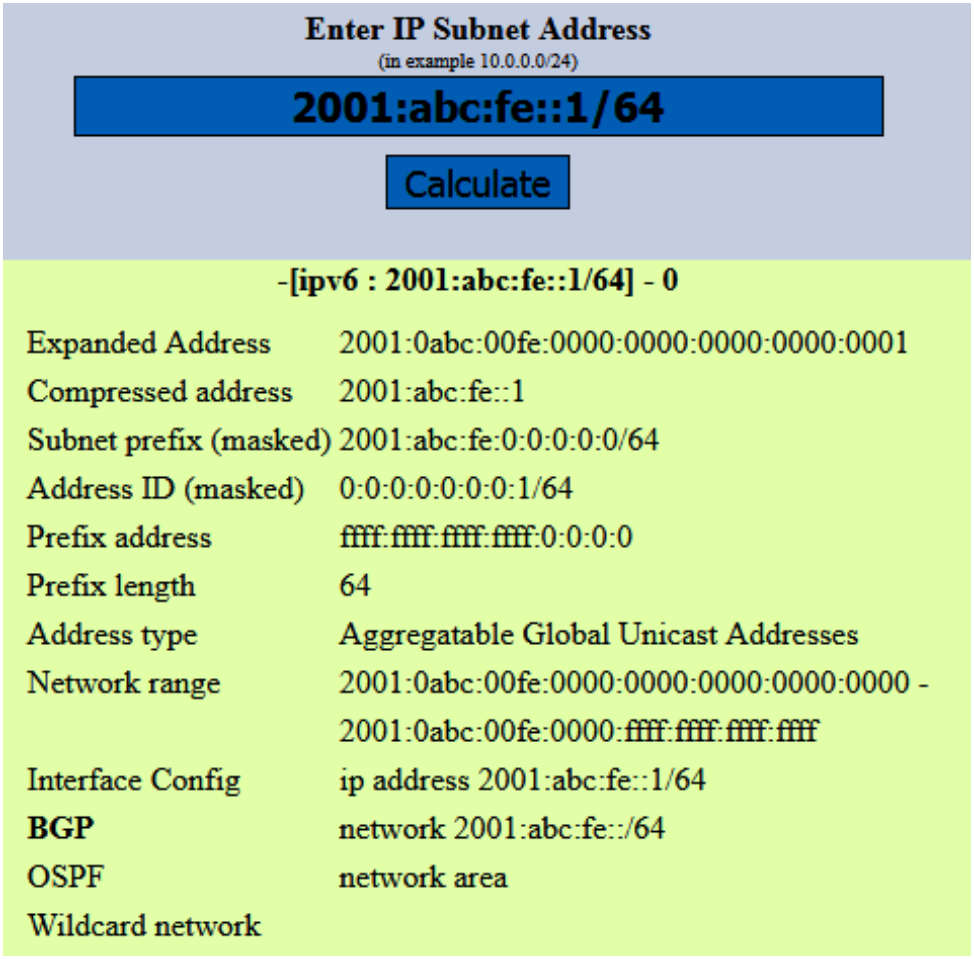
http://www.subnetonline.com/pages/subnet-calculators/ipv6-subnet-calculator.php



Gambar 5.3 IPv6 *Calculator*

Sebagai contoh untuk IPv6 Address **2001:abc:fe::1/64**

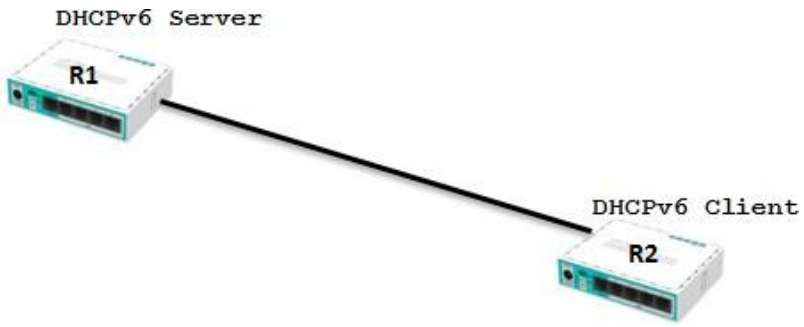
Maka akan diperoleh informasi yang cukup detail dari IPv6 Address tersebut.



Gambar 5.4 Detail Informasi IPv6 *Calculator*

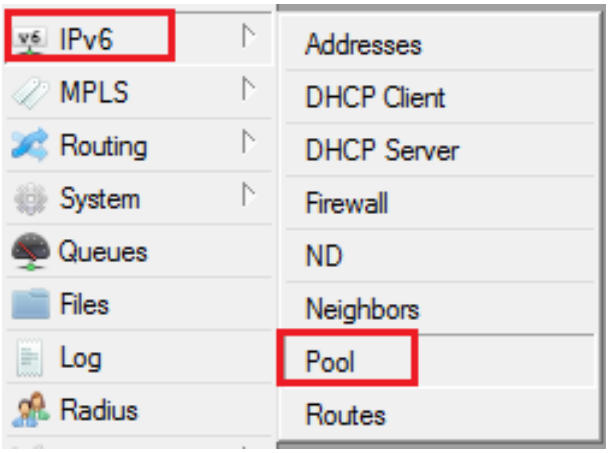
KEGIATAN PRAKTIKUM

Konfigurasi IP DHCPv6 *Server* dan IP DHCPv6 Client pada MikroTik



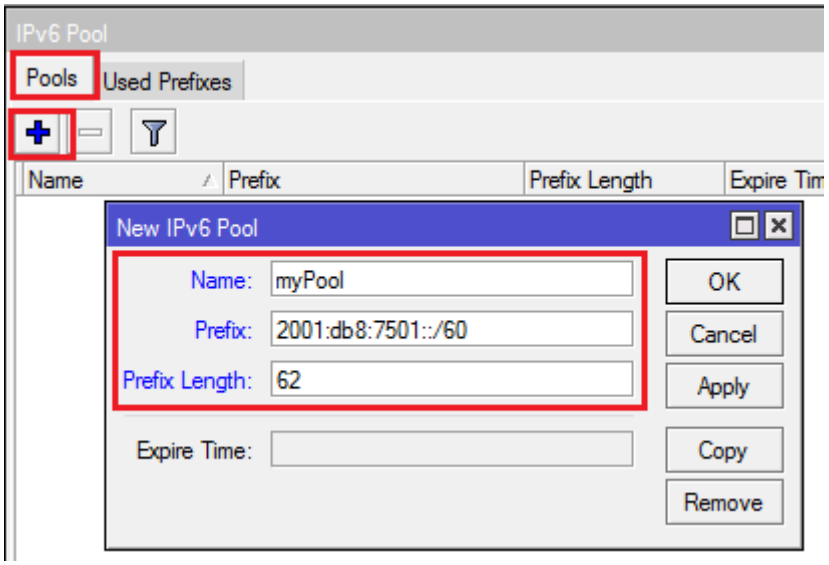
Gambar 5.5 Konfigurasi IP *Address Server* dan *Client*

Pertama buat *pool* untuk DHCP *Server* terlebih dahulu. Klik IPv6 dan pilih *Pool*.



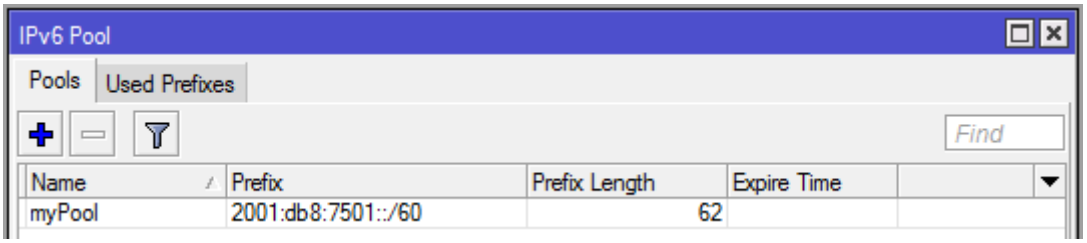
Gambar 5.6 Membuat *Pool* pada DHCP *Server*

Selanjutnya buatlah *Pool Name* nya , *prefix* dan *prefix Length*. Setelah itu klik OK



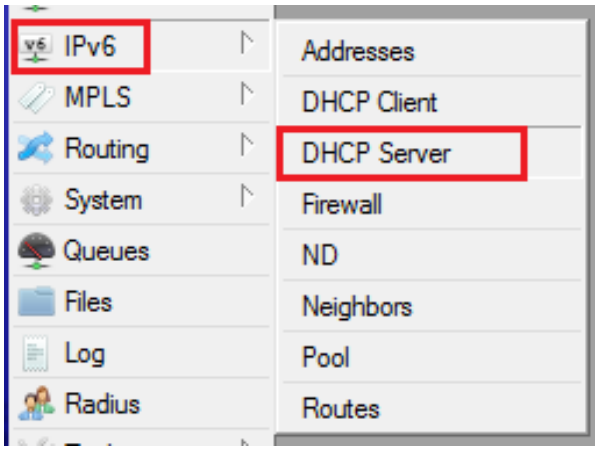
Gambar 5.7 Menambahkan Nama *Pool*, *Prefix*, dan *Prefix Length*

Akan muncul *Pool* yang telah dibuat.



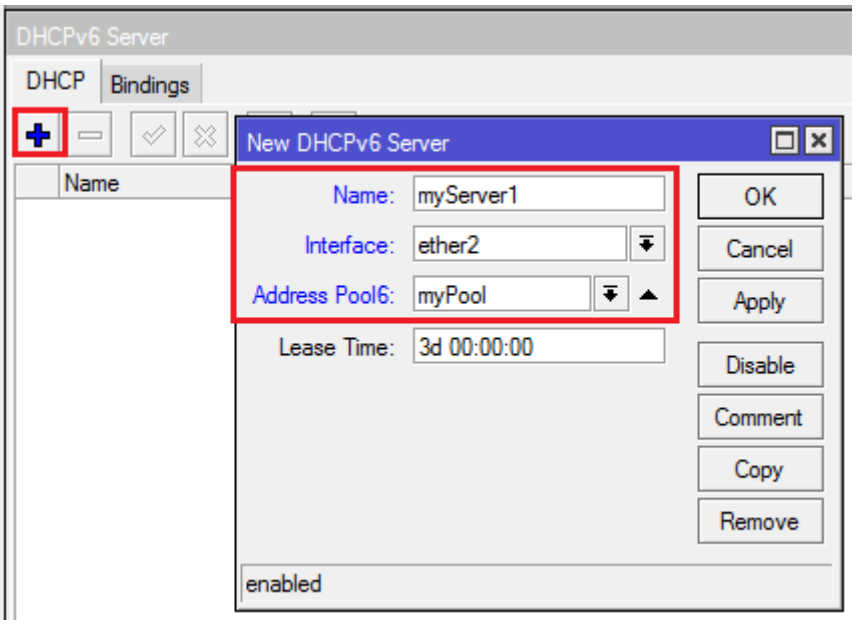
Gambar 5.8 *Pool* yang Dibuat

Selanjutnya konfigurasi IPv6 DHCP *Server*. Klik IPv6 dan pilih DHCP-*Server*.



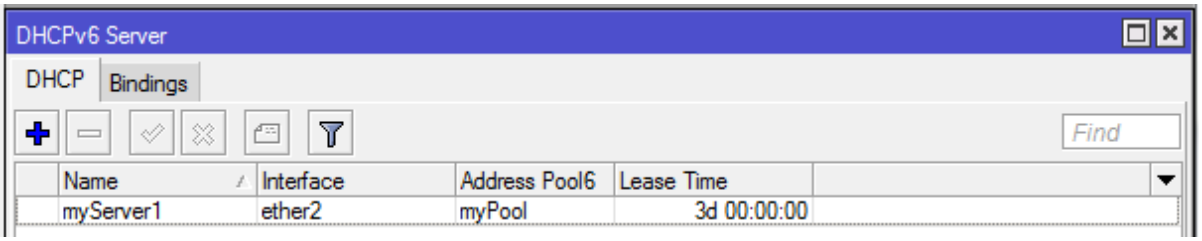
Gambar 5.9 Mengkonfigurasi IPv6 DHCP *Server*

Klik tanda + untuk membuat DHCP *Server* , ***Name*** gunakan nama untuk DHCP *Server* bisa disesuaikan sesuai keinginan, ***Interface*** nya gunakan *interface* yang akan di jadikan sebagai DHCP Server, dan ***Address Pool6*** gunakan IP *Pool* yang telah dibuat . lalu klik OK.



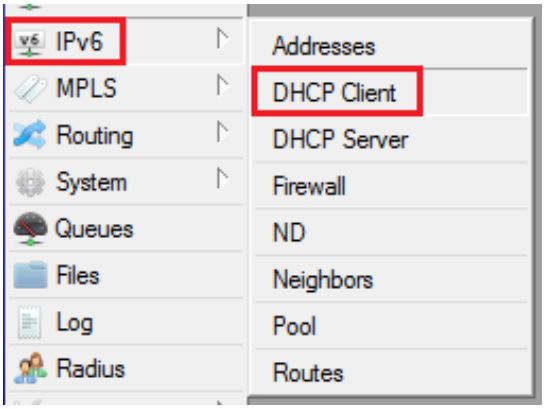
Gambar 5.10 Menambahkan Nama, *Interface* dan *Address Pool6* untuk DHCP *Server*

DHCP *Server* telah selesai dibuat dan hasilnya akan seperti gambar dibawah ini.



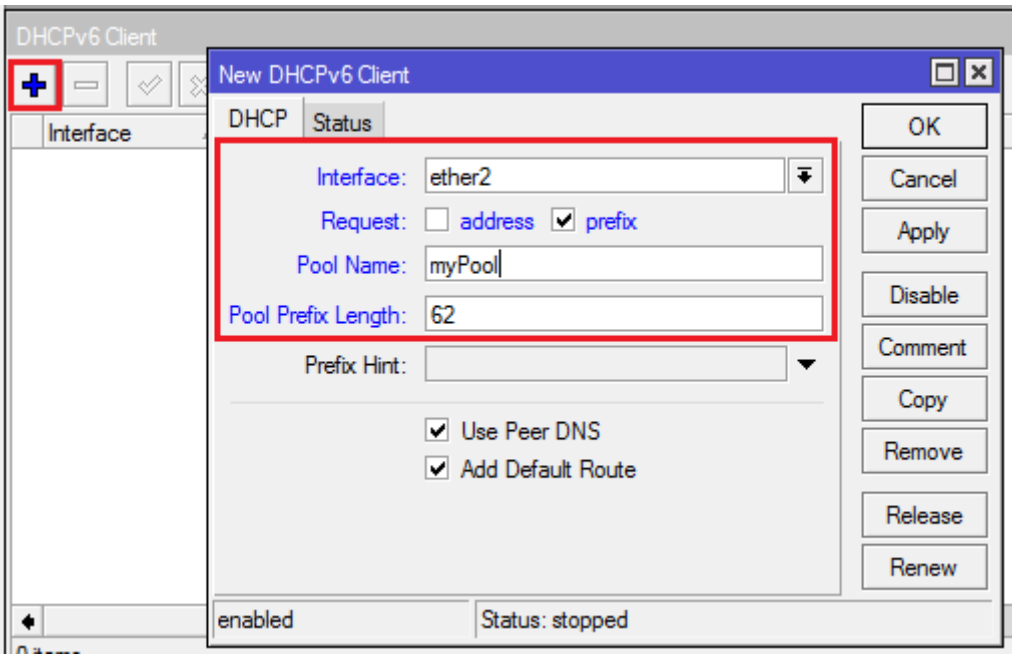
Gambar 5.11 Hasil DHCP *Server*

Selanjutnya membuat DHCP-*Client* agar *client* mendapatkan IP *Address* dari DHCP *Server*. Klik **IPv6** dan pilih **DHCP-*Client*.**



Gambar 5.12 Mengkonfigurasi IPv6 DHCP *Client*

Selanjutnya tambahkan **DHCP *Client***. ***Interface*** gunakan *interface* yang akan dipakai sebagai DHCP-*Client* nya, ***Request*** gunakan ***Prefix***, ***Pool Name*** nya isikan sesuai *Pool* DHCP *Server*, ***Pool Prefix Length*** gunakan **62**. Jika sudah, klik OK.



Gambar 5.13 Mengatur *Interface, Request, Pool Name,* dan *Pool Prefix Length* DHCP *Client*

Untuk mengecek nya bisa melalui CLI sebagai berikut. Masuk terlebih dahulu ke **ipv6 dhcp-*client*** lalu ketik ***print detail*.**

```
[admin@MikroTik] > ipv6 dhcp-client
[admin@MikroTik] /ipv6 dhcp-client> print
Flags: D - dynamic, X - disabled, I - invalid
 #    INTERFACE                          STATUS        REQUEST
 0    ether2                             bound         prefix
[admin@MikroTik] /ipv6 dhcp-client> print detail
Flags: D - dynamic, X - disabled, I - invalid
 0    interface=ether2 status=bound duid="0x000300016c3b6bc202cb"
      dhcp-server-v6=fe80::6e3b:6bff:fed3:fb8b request=prefix
      add-default-route=yes use-peer-dns=yes pool-name="myPool"
      pool-prefix-length=62 prefix-hint=::/0
      prefix=2001:db8:7501::/62, 2d23h28m29s
[admin@MikroTik] /ipv6 dhcp-client>
```

Gambar 5.14 Tampilan Hasil Pengecekan IPv6 DHCP *Client*

Praktikum subnetting versi 4, membuat topologi dengan beda subnet,

Terdapat sebuah Jaringan dengan IP Address 192.168.1.2/29 , bagi lah IP Address tersebut menjadi 2 segmen jaringan untuk Jaringan di 2 ruangan yaitu Ruangan A dan ruangan B . Karena menggunakan /29 jadi di masing masing ruangan akan terdapat 6 host.

Berikut ini adalah IP Address di setiap ruangan :

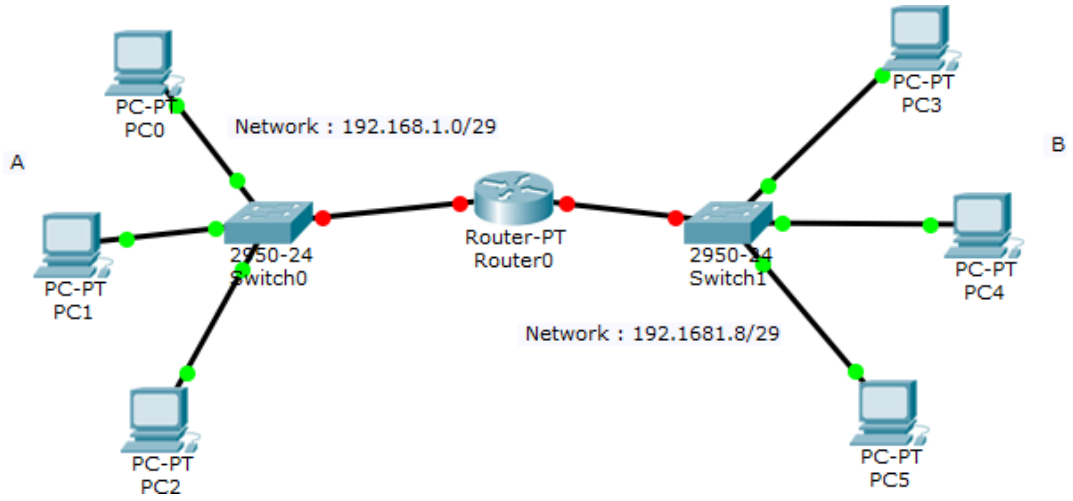
Ruangan A

Network : 192.168.1.0
Host : 192.168.1.1 - 192.168.1.6
Broadcast : 192.168.1.7

Ruangan B

Network : 192.168.1.8
Host : 192.168.1.9 – 192.168.1.14
Broadcast : 192.168.1.15

Topologi pada Packet Tracer



Tugas

1. Pada sebuah perusahaan terdapat 5 gedung, Gedung A, B, C, D, dan gedung E.
2. Perusahaan tersebut mempunyai IP 192.168.2.0/24 yang akan di bagi ke setiap gedung. Gedung A mempunyai 45 *host*, gedung B 80 *host*, gedung C 12 *host*, gedung D 60 *host*, dan gedung E 7 *host*. Tentukanlah *Network Address*, *Range* IP dan IP *Broadcast* di masing masing gedung.
3. Buatlah sebuah DHCP-*Server* pada mikrotik dan 2 DHCP *Client* dan masing masing *Client* mendapatkan IP DHCP dari DHCP *Server*.

MODUL 6

PROTOCOL, BRIDGING* DAN *SWITCHING

(Pertemuan 12, 13)

Tujuan

1. Mahasiswa mampu menjelaskan tentang ptotokol *bridging* dan *switching*.

Tugas Pendahuluan

1. Apakah yang anda ketahui tentang *protocol* ?
2. Jelaskan pengertian dan fungsi dari *protocol* TCP, UDP, RTP, SIP.
3. Apakah yang dimaksud dengan *Bridging* dan *Switching* ?

DASAR TEORI

Protokol adalah aturan yang mengatur komunikasi diantara beberapa komputer di dalam sebuah jaringan sehingga komputer-komputer anggota jaringan dan komputer yang berbeda *platform* dapat saling berkomunikasi . Ada beberapa jenis *protocol* yaitu TCP, UDP, RTP, dan SIP.

1. TCP (*Transmission Control Protocol*)

   Transmission Control Protocol (TCP) adalah salah satu jenis protokol yang memungkinkan kumpulan komputer untuk berkomunikasi dan bertukar data didalam suatu *network* (jaringan). TCP merupakan suatu protokol yang berada di lapisan transpor (baik itu dalam tujuh lapis model referensi OSI atau model DARPA) yang berorientasi sambungan (*connection-oriented*) dan dapat diandalkan (*reliable*).

   Karakteristik *Protocol* TCP :

   a. *Reliable* berarti data ditransfer ke tujuannya dalam suatu urutan seperti ketika dikirim.
   b. Berorientasi sambungan (*connection-oriented*): Sebelum data dapat ditransmisikan antara dua host, dua proses yang berjalan pada lapisan aplikasi harus melakukan negosiasi untuk membuat sesi koneksi terlebih dahulu. Koneksi TCP ditutup dengan menggunakan proses terminasi koneksi TCP (TCP *connection termination*).

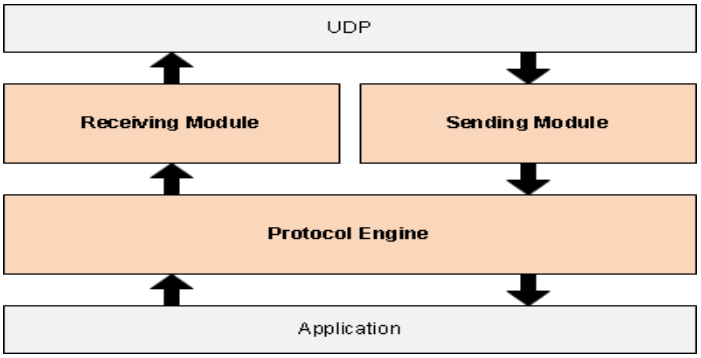
c. Mengirimkan paket secara "*one-to-one*": hal ini karena memang TCP harus membuat sebuah sirkuit logis antara dua buah protokol lapisan aplikasi agar saling dapat berkomunikasi. TCP tidak menyediakan layanan pengiriman data secara *one-to-many*.
d. Melakukan segmentasi terhadap data yang datang dari lapisan aplikasi (dalam DARPA *Reference Model*)

Kegunaan *Protocol* TCP :

a. Menyediakan komunikasi logika antar proses aplikasi yang berjalan pada *host* yang berbeda
b. Protokol transport berjalan pada *end systems*.
c. Pengiriman *file* (*file transfer*). *File Transfer* Protokol (FTP) memungkinkan pengguna komputer yg satu untuk dapat mengirim ataupun menerima *file* ke komputer jaringan. Karena masalah keamanan data, maka FTP seringkali memerlukan nama pengguna (*username*) dan *password*.
d. *Remote login*. *Network terminal* Protokol (telnet) memungkinkan pengguna komputer dapat melakukan *log in* ke dalam suatu komputer didalam suatu jaringan.

2. UDP (*User Datagram Protocol*)

User Datagram Protocol (UDP) merupakan bagian dari *internet protocol*. Dengan UDP, aplikasi komputer dapat mengirimkan pesan kepada komputer lain dalam jaringan lain tanpa melakukan komunikasi awal.UDP melakukan komunikasi secara sederhana dengan mekanisme yang sangat minimal. Ada proses *checksum* untuk menjaga integritas data. UDP digunakan untuk komunikasi yang sederhana seperti *query* DNS (*Domain Name System*), NTP (*Network Time Protocol*) DHCP (*Dinamic Host Configuration Protocol*), dan RIP (*Routing Information Protocol*).



Gambar 6.1 Protokol UDP

Karakteristik *protocol* UDP :

a. *Connectionless* , Pesan-pesan UDP akan dikirimkan tanpa harus dilakukan proses negosiasi koneksi antara dua *host* yang hendak berukar informasi.
b. *Unreliable* , Pesan-pesan UDP akan dikirimkan sebagai datagram tanpa adanya nomor urut atau pesan *acknowledgment*. Protokol lapisan aplikasi yang berjalan di atas UDP harus melakukan pemulihan terhadap pesan-pesan yang hilang selama transmisi.
c. UDP menyediakan mekanisme untuk mengirim pesan-pesan ke sebuah protokol lapisan aplikasi atau proses tertentu di dalam sebuah *host* dalam jaringan yang menggunakan TCP/IP. HeaderUDP berisi *field Source Process Identification* dan *Destination Process Identification*.
d. UDP menyediakan penghitungan *checksum* berukuran 16-bit terhadap keseluruhan pesan UDP.

Kegunaan *protocol* UDP:

a. Protokol yang “ringan” (*lightweight*): Untuk menghemat sumber daya memori dan prosesor, beberapa protokol lapisan aplikasi membutuhkan penggunaan protokol yang ringan yang dapat melakukan fungsi-fungsi spesifik dengan saling bertukar pesan.
b. Protokol lapisan aplikasi yang mengimplementasikan layanan keandalan: Jika protokol lapisan aplikasi menyediakan layanan transfer data yang andal, maka kebutuhan terhadap keandalan yang ditawarkan oleh TCP pun menjadi tidak ada.
c. Protokol yang tidak membutuhkan keandalan.
d. Transmisi *broadcast*: Karena UDP merupakan protokol yang tidak perlu membuat koneksi terlebih dahulu dengan sebuah *host* tertentu, maka transmisi *broadcast*

pun dimungkinkan. Sebuah protokol lapisan aplikasi dapat mengirimkan paket data ke beberapa tujuan dengan menggunakan alamat *multicast* atau *broadcast*. Hal ini kontras dengan protokol TCP yang hanya dapat mengirimkan transmisi *one-to-one*.

3. RTP (*Real Time Transport Protocol*)

   Real Time Transport Protocol (RTP) umumnya digunakan dalam jaringan IP. RTP dirancang untuk menyediakan fungsi transport jaringan ujung ke ujung untuk aplikasi yang mengirimkan data *real time,* misalnya audio atau video, melalui layanan jaringan *multicast* atau *unicast*.

4. SIP (*Session Initiation Protocol*)

   Session Initiation Protocol (SIP) merupakan standar *protocol* yang dipublikasikan oleh *Internet Engineering Task Force* (IETF) sebagai RFC3261. SIP didesain untuk konektifitas antara user dan perangkat dimanapun dan kapanpun dalam melakukan pertukaran informasi. Saat ini HTTP dan SMTP merupakan dua protokol yang paling banyak digunakan dalam proses pertukaran informasi, tetapi kedua protokol ini tidak dibuat untuk memprovide aktifitas manusia secara esensial, hanya sebagai protokol yang men*support* kegiatan tersebut. SIP menggabungkan kedua protokol tersebut ke dalam satu kesatuan yaitu menggunakan pola pertukaran informasi (*message exchange*) dari HTTP, *format message*, dan *encoding* serta penggunaan skema URI (*user@domain*) seperti SMTP.

BRIDGING

Bridge adalah sebuah komponen jaringan yang digunakan untuk memperluas jaringan atau membuat sebuah segmen jaringan. *Bridge* juga dapat digunakan untuk menggabungkan dua buah media jaringan yang berbeda. Konsep *bridge* adalah menggabungkan 2 atau lebih *interface ethernet* atau sejenisnya sehingga seolah olah berada dalam 1 segmen jaringan yang sama layaknya *switch*. Dengan mengaktifkan mode *bridge* pada 2 buah *interface*, maka tidak perlu lagi memasang IP *Address* pada *interface* yang dijadikan sebagai *bridge* dan ini akan menonaktifkan fungsi *routing* diantara kedua *interface* tersebut. *Bridge* tidak dapat dibuat dengan *interface* yang bukan bertipe *ethernet* seperti serial, IPIP, PPPoE, dll.

Fungsi *Bridge* :

1. *Bridge* dapat berfungsi menghubungkan 2 buah jaringan komputer LAN yang sejenis, sehingga dapat memiliki satu jaringan LAN yang lebih besar dari ketentuan konfigurasi LAN tanpa *bridge*.
2. *Bridge* juga dapat menghubungkan beberapa jaringan komputer yang terpisah, baik itu tipe jaringan yang sama maupun yang berbeda.
3. *Bridge* juga dapat berfungsi sebagai *router* pada jaringan komputer yang luas, hal seperti ini sering dinamakan dengan istilah *Bridge-Router*. Lalu *bridge* juga dapat men-*copy frame* data yaitu dari suatu jaringan yang lain, dengan alasan jaringan itu masih terhubung. Dan masih banyak lagi fungsi lainnya dari *bridge*.

Jenis-Jenis *Bridge* :

1. *Transparent Bridging*, jenis *bridge* yang digunakan pada *network Ethernet*.
2. *Source-route Bridging*, jenis bridge yang digunakan pada *network Token Ring*.
3. *Translational Bridging*, digunakan untuk menghubungkan *network* yang berbeda.

SWITCHING

Switching merupakan suatu sistem kontrol penggantian, pengalihan, pengubahan atau pemindahan , digunakanuntuk memaksimalkan penggunaan *bandwith*. Jika tidak dilakukan *switching*, maka data akan terus dikirim walaupun sudah tidak terpakai lagi.

Multi layer switching adalah perangkat jaringan komputer yang melakukan proses *switch* pada OSI *layer* 2seperti jaringan biasa dan memberikan fungsi tambahan pada lapisan OSI yang lebih tinggi. MLS juga memberikan cara menyusun perangkat *network switch* menjadi beberapa tingkatan dikarenakan *end user* yang terkoneksi ke dalam suatu jaringan memiliki jumlah yang banyak, sehingga kita perlu melakukan *trunking* (menyambungkan *switch* satu dengan *switch* lain) antar *network switch* secara bertingkat.

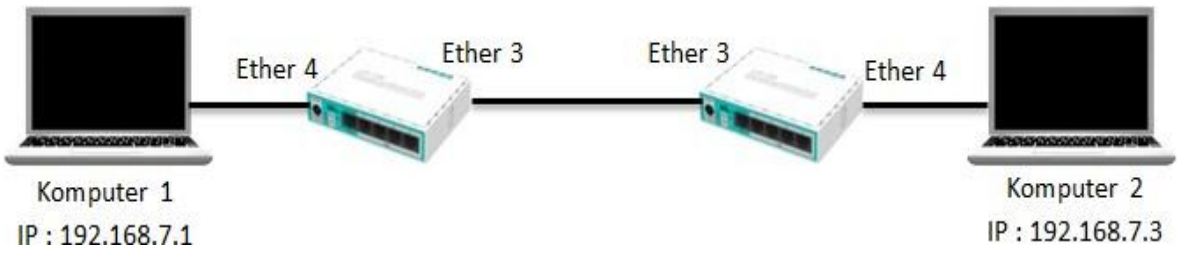
Istilah *multilayer switching* dalam istilah Cisco merujuk pada sebuah teknologi canggih dimana *router* berkomunikasi dengan *switch* untuk memberitahukan kepada *switch* bagaimana cara mem-*forward frame* tanpa bantuan dari *router* tersebut.

Cisco *multi layer switching* ini memiliki tiga komponen :

1. *Router*, Menangani paket pertama dalam setiap aliran data. *Route processor* juga membuat keputusan *forwarding* berdasarkan alamat tujuan pada *layer*
2. *Switching engine*, Memantau paket yang dilewatkan ke *route processor* atau sebaliknya, dan mempelajari bagaimana *route processor* menangani paket tersebut.
3. *Multilayer switching protocol*, Protokol sederhana yang digunakan oleh *route processor* untuk memungkinkan *switching multilayer* dan untuk memberitahukan kepada *switching engine* untuk membersihkan *tabel swithcing*nya jika ada perubahan pada *routing table* atau pada konfigurasi *access control list*.

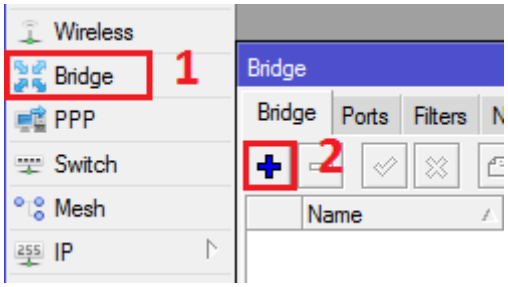
KEGIATAN PRAKTIKUM

Membuat *Bridge*

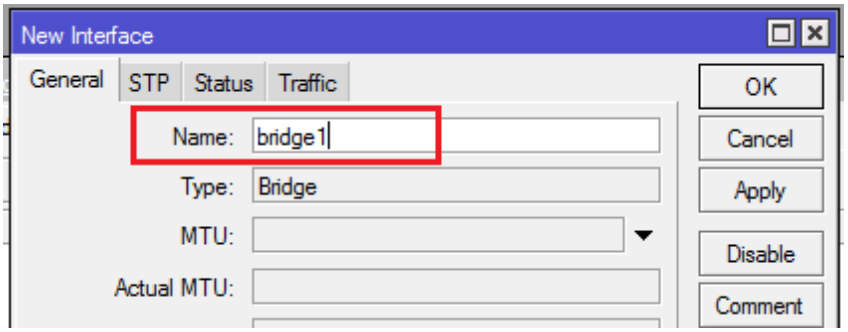


Gambar 6.2 *Bridging* Dua Buah Komputer

Langkah pertama klik ***Bridge*** setelah itu akan muncul jendela ***Bridge*** selanjutnya klik ***Bridge*** lalu klik tanda **Tambah** (+) setelah itu muncul jendela ***New Interface*** pada ***Name*** isikan "***bridge1***" setelah itu klik ***Apply*** dan klik **OK**.



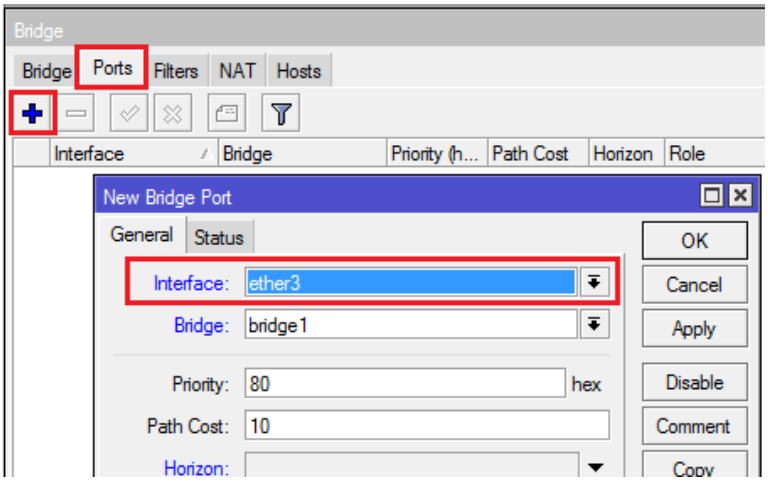
Gambar 6.3 Tampilan Menu *Bridge*



Gambar 6.4 Menambahkan Nama *Bridge*

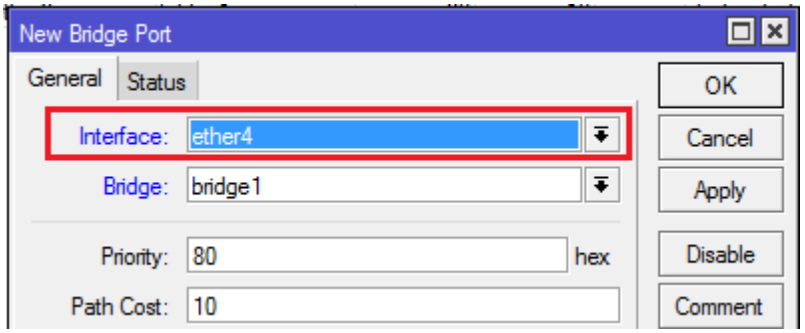
Port Bridge

Pada jendela ***Bridge*** klik ***Ports*** setelah itu klik tanda **Tambah** (+) akan muncul jendela ***New Bridge Port*** pada jendela ***New Bridge Port*** pada ***Interface*** gunakan *ether* berapa saja yang akan dijadikan *bridge* setelah itu klik ***Apply*** dan klik **OK**.



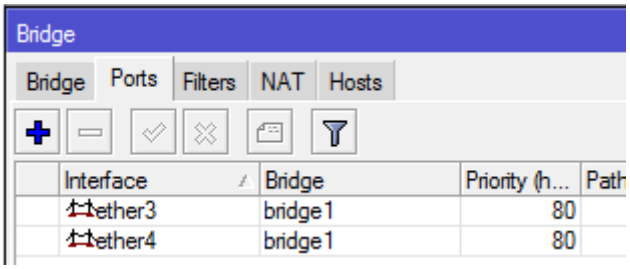
Gambar 6.5 Menambahkan *Port* Baru

Lakukan hal yang sama untuk menambahkan ***Port Bridge*** .



Gambar 6.6 Menambahkan *Bridge Port* Baru

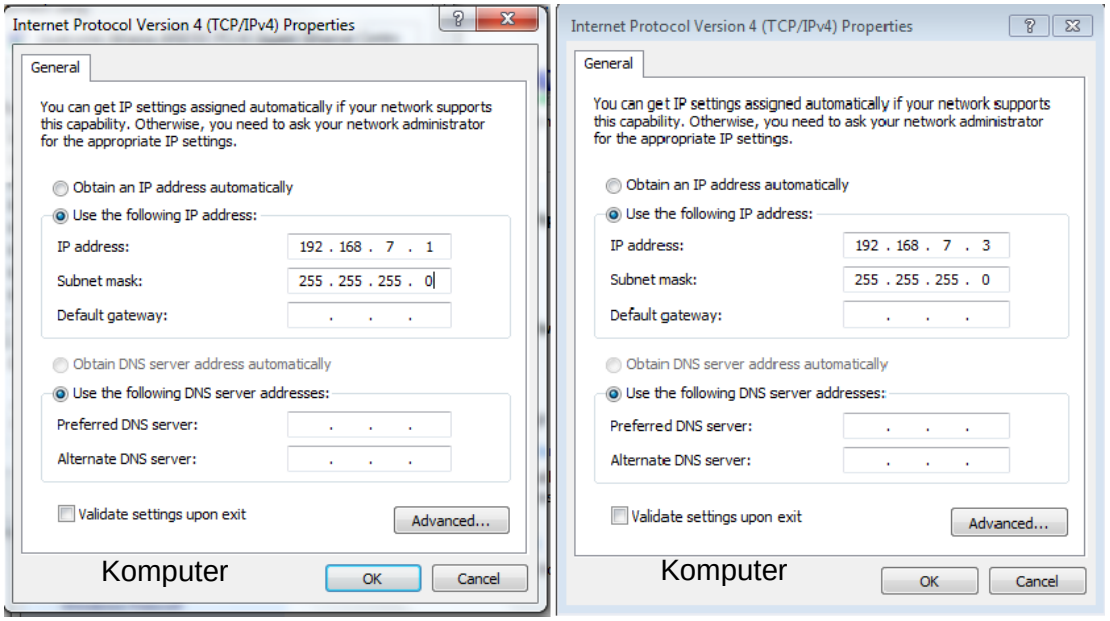
Hasil dari ***Port Bridge*** yang kita buat seperti gambar di bawah ini.



Gambar 6.7 Tampilan *Port Bridge*

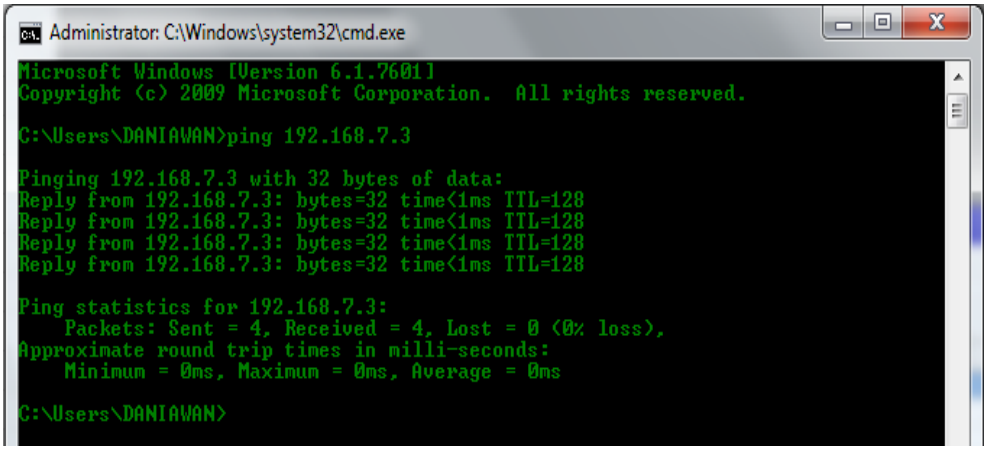
Konfigurasi *Bridge*

Konfigurasi **IP *Address*** pada masing komputer .

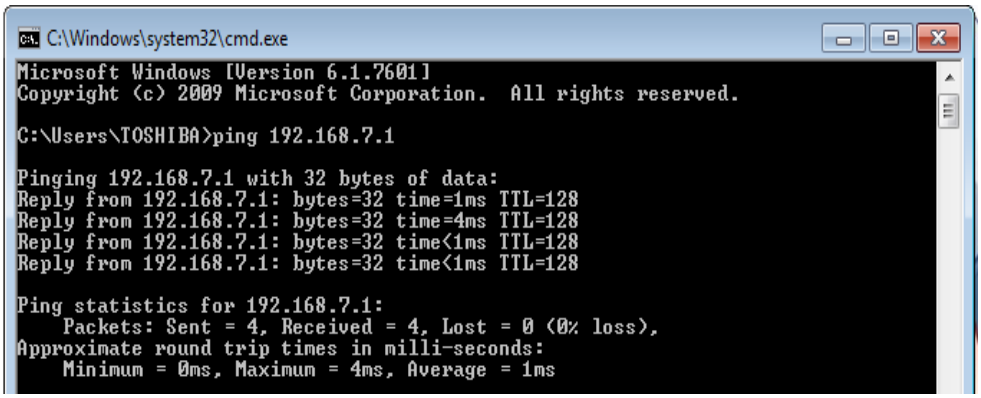


Gambar 6.8 Mengkonfigurasi IP *Address* pada Komputer 1 dan Komputer 2

Selanjutnya melakukan pengujian , ping dari komputer 1 ke komputer 2 dan sebaliknya.



Gambar 6.9 Ping dari komputer 1 ke komputer 2

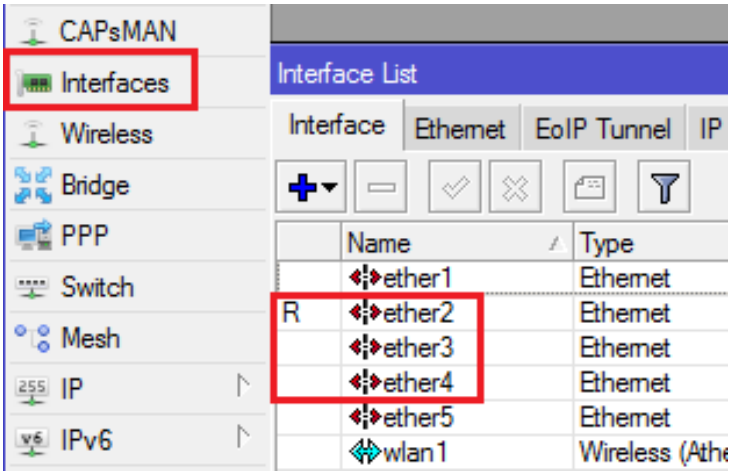


Gambar 6.10 Ping dari komputer 2 ke komputer 1

SWITCHING pada MikroTik

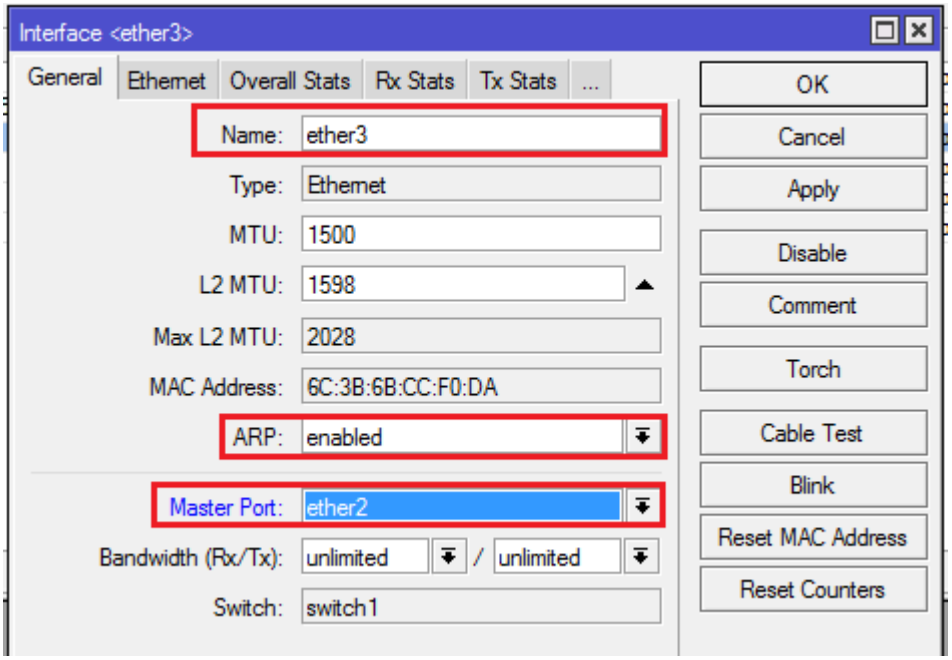
Switching pada MikroTik dimaksudkan agar port-port pada mikrotik berfungsi layaknya sebagai switch yang berada dalam 1 segmen jaringan.

Untuk konfigurasinya, klik interface dan tentukan port router yang akan di ubah menjadi mode switch. Disini untuk sederhananya hanya menggunakan 3 port pada router yaitu ether 2 yang menjadi master port switch (port yang terhubung ke LAN) dan ether3, ether4 yang port nya sebagai port switch.



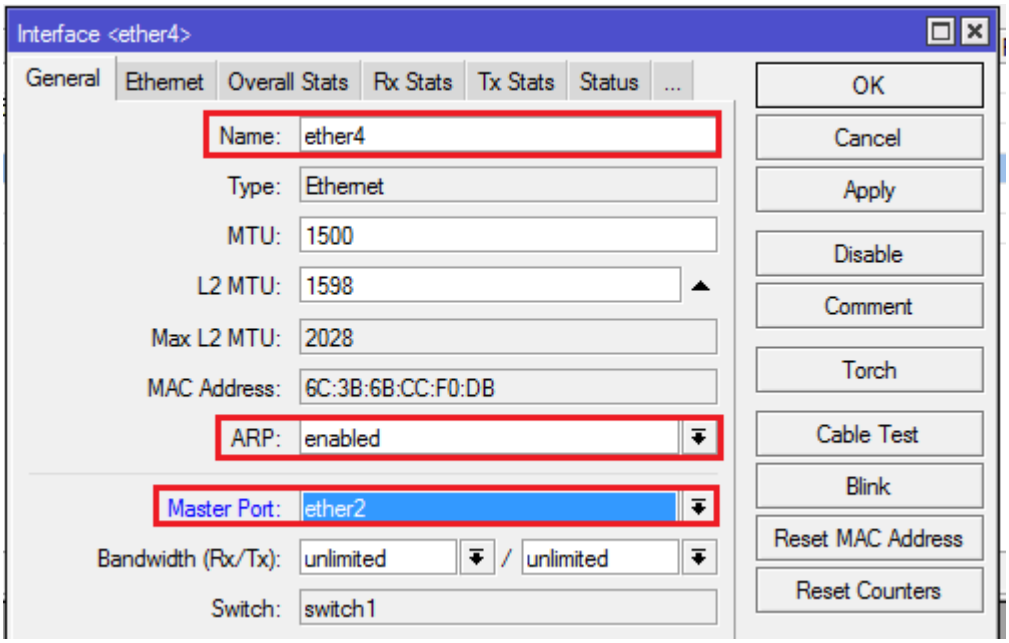
Gambar 6.11 Penentuan port untuk Switch

Kemudian konfigurasi port router ether3, Name nya bisa di sesuaikan sesuai keinginan tetapi untuk lebih mudahnya bisa dibiarkan nama port router nya. ARP biarkan enabled, dan master port pilih port atau interface router yang terhubung ke LAN



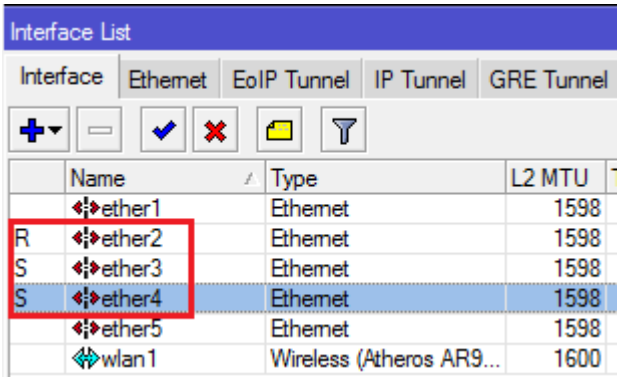
Gambar 6.12 Konfigurasi Switch pada ether3

Konfigurasi juga pada interface ether4



Gambar 6.13 Konfigurasi Switch pada ether4

Dan hasilnya akan seperti gambar dibawah ini. Interface yang diubah modenya menjadi mode Switch akan terdapat tanda S



Gambar 6.14 Hasil Konfigurasi Switch port Router

Tugas

1. Buatlah konfigurasi *bridge* menggunakan 3 buah *router*.
2. Sertakan laporan.

MODUL 7

ROUTING, ROUTING PROTOCOL

(Pertemuan 14, 15)

Tujuan

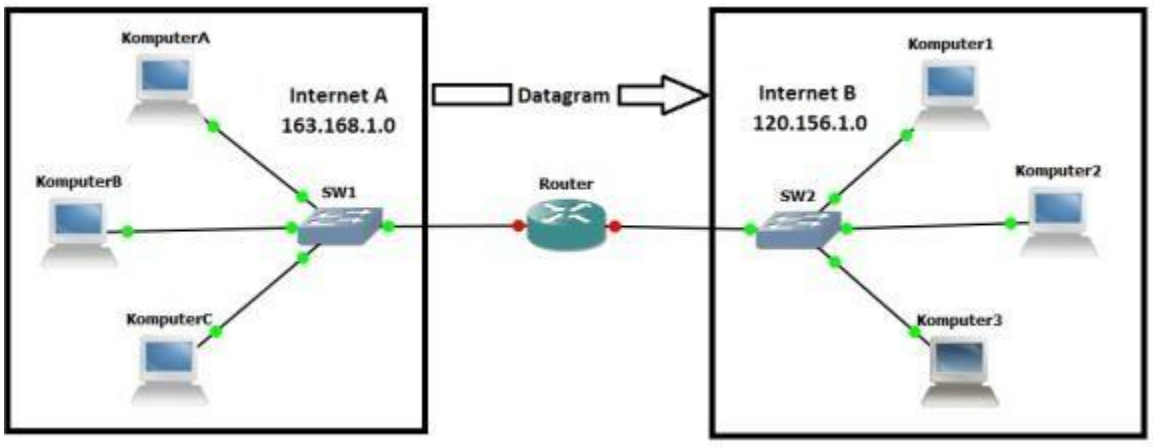
1. Mahasiswa mampu menjelaskan serta menerapkan tentang *routing* pada jaringan komputer serta protokol *routing*

Tugas Pendahuluan

1. Jelaskan apakah yang dimaksud dengan *routing!*
2. Sebutkan dan jelaskan jenis-jenis *routing*!
3. Sebutkan dan jelaskan jenis-jenis *protocol routing*!

DASAR TEORI

Routing adalah proses pengiriman data maupun informasi dengan meneruskan paket data yang dikirim dari jaringan satu ke jaringan lainnya. *Routing* ada 2 jenis yaitu *routing static* dan *routing dynamic*. *Routing Static* adalah suatu mekanisme *routing* yang tergantung dengan *routing table* dengan konfigurasi manual. Disisi lain *Routig Dynamic* adalah suatu mekanisme *routing* dimana pertukaran *routing table* antar *router* yang ada pada jaringan dilakukan secara *dynamic*.



Gambar 7.1 *Routing*

Protokol *Routing* mengatur *router-router* sehingga dapat berkomunikasi satu dengan lain dan saling memberikan informasi antara satu router dengan router lainnya dan juga saling memberikan informasi *routing* yang dapat mengubah isi *forwarding table.* Jenis jenis dari protokol *routing* dinamis itu beragam ,contohnya adalah :

1. RIP (*Routing Information Protocol*).

   Routing Information Protocol (RIP) adalah sebuah protokol *routing* dinamis yang digunakan dalam jaringan LAN (*Local Area Network*) dan WAN (*Wide Area Network*). Protokol ini menggunakan algoritma *Distance-Vector Routing*. Protokol ini telah dikembangkan beberapa kali, sehingga terciptalah RIP Versi 2 . Kedua versi ini masih digunakan sampai sekarang, meskipun begitu secara teknis telah dianggap usang oleh teknik-teknik yang lebih maju, seperti *Open Shortest Path First* (OSPF) dan protokol OSI IS-IS. RIP juga telah diadaptasi untuk digunakan dalam jaringan IPv6, yang dikenal sebagai standar RIPng . Ada tiga versi dari *Routing Information Protocol* yaitu : RIPv1, RIPv2, dan RIPng.
2. IGRP (*Internal Gateway Routing Protocol*).

   IGRP (*Interior Gateway Routing Protocol*) adalah *protocol distance vector* yang diciptakan oleh perusahaan Cisco untuk mengatasi kekurangan RIP. Jumlah *hop* maksimum menjadi 255 dan sebagai *metric*, IGRP menggunakan *Bandwidth*, MTU, *Delay* dan *Load*. IGRP adalah *protocol routing* yang menggunakan *Autonomous System* (AS) yang dapat menentukan routing berdasarkan *system*, interior atau exterior.
3. EIGRP (*Enchanced Internal Gateway Routing Protocol*).

   EIGRP (*Enhanced Interior Gateway Routing Protocol*) adalah *routing protocol* yang hanya di adopsi oleh *router* cisco atau sering disebut sebagai *proprietary protocol* pada CISCO. Dimana EIGRP ini hanya bisa digunakan sesama *router* CISCO saja dan *routing* ini tidak didukung dalam jenis *router* yang lain.
4. OSPF (*Open Shortest Path First*).

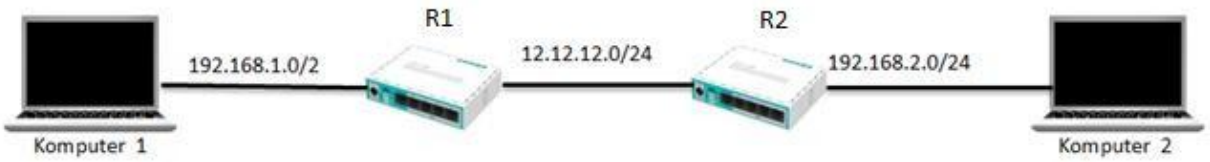
   Open Shortest Path First (OSPF) adalah sebuah protokol *routing* otomatis (*Dynamic Routing*) yang mampu menjaga, mengatur dan mendistribusikan informasi *routing* antar *network* mengikuti setiap perubahan jaringan secara dinamis.
5. BGP (*Border Gateway Protocol*).

   Border Gateway Protocol (BGP) merupakan salah satu jenis *routing* protokol yang digunakan untuk koneksi antar *Autonomous System* (AS), dan salah satu jenis *routing*

protokol yang banyak digunakan di ISP besar. BGP termasuk dalam kategori *routing* protokol jenis *Exterior Gateway Protokol* (EGP).

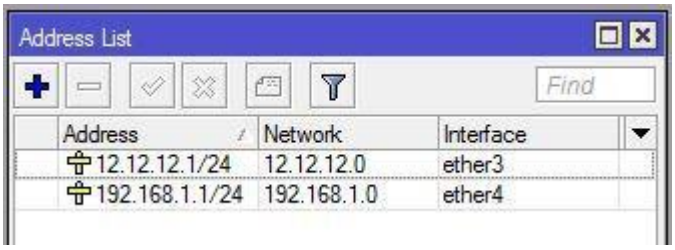
KEGIATAN PRAKTIKUM

Static Routing



Gambar 7.2 *Static Routing*

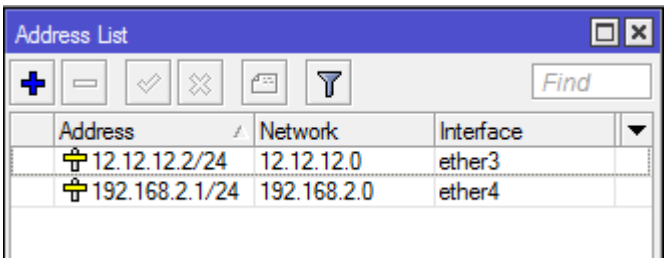
Konfigurasi IP *Address* pada *router* 1. Pada *interface ether3* menggunakan ip *address* *12.12.12.1* dan pada *interface ether4* yang terhubung ke komputer menggunakan ip *address* 192.168.1.1 .



IP Addres pada router 1

Gambar 7.3 IP *Address* pada *Router* 1

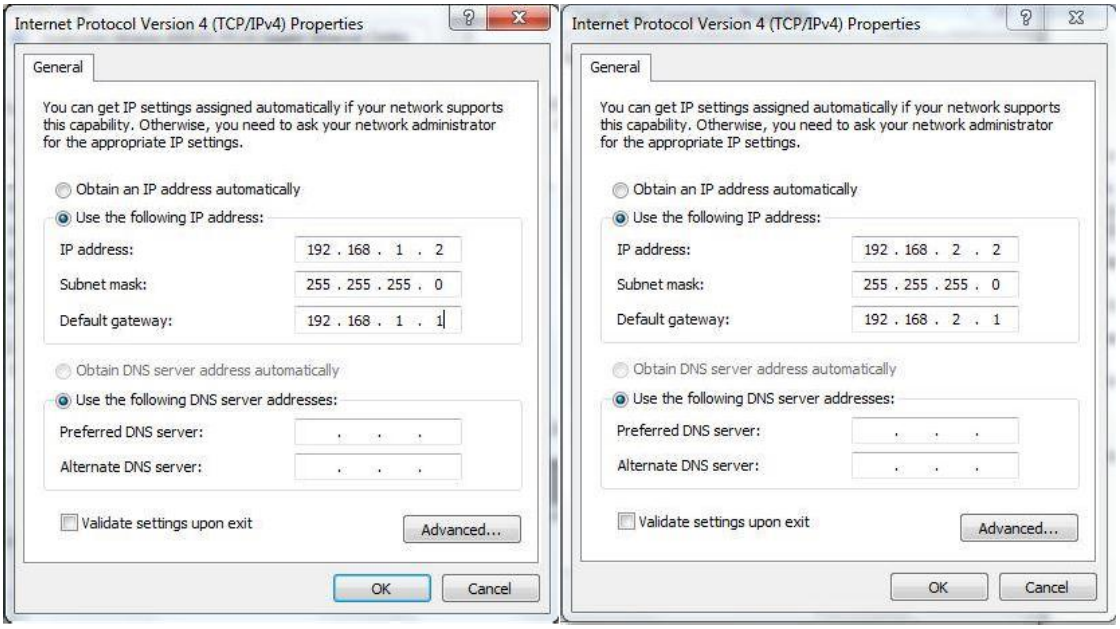
Konfigurasi IP *address* pada *router* 2. Pada *interface ether3* menggunakan ip *address* *12.12.12.2* dan pada *interface ether4* yang terhubung ke komputer 2 menggunakan ip *address* 192.168.2.1.



IP Addres pada router 2

Gambar 7.4 IP *Address* pada *Router* 2

Langkah ketiga melakukan konfigurasi Ip *Address* pada komputer 1 dan komputer 2 .



IP Addres Komputer 1 **IP Addres Komputer 2**

Gambar 7.5 Konfigurasi IP *Address* pada Komputer 1 dan Komputer 2

Selanjutnya melakukan *routing* ,buka CLI/ *New Terminal* dan ketikkan perintah *ip route add dst-address=192.168.2.0/24 gateway=12.12.12.2* pada *router* 1.

```
[admin@MikroTik] > ip route add dst-address=192.168.2.0/24 gateway=12.12.12.2
```

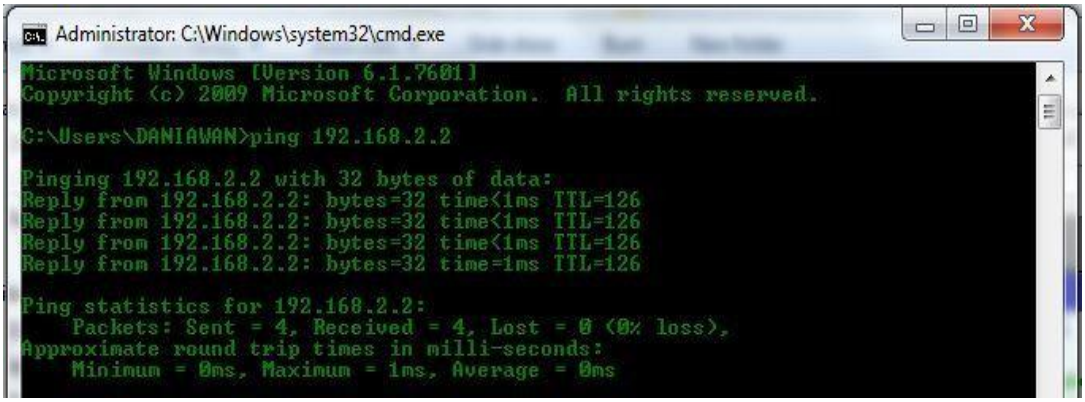
Pada router 2 ketikan perintah *ip route add dst-address=192.168.1.0/24 gateway=12.12.12.1*.

```
[admin@MikroTik] > ip route add dst-address=192.168.1.0/24 gateway=12.12.12.1
```

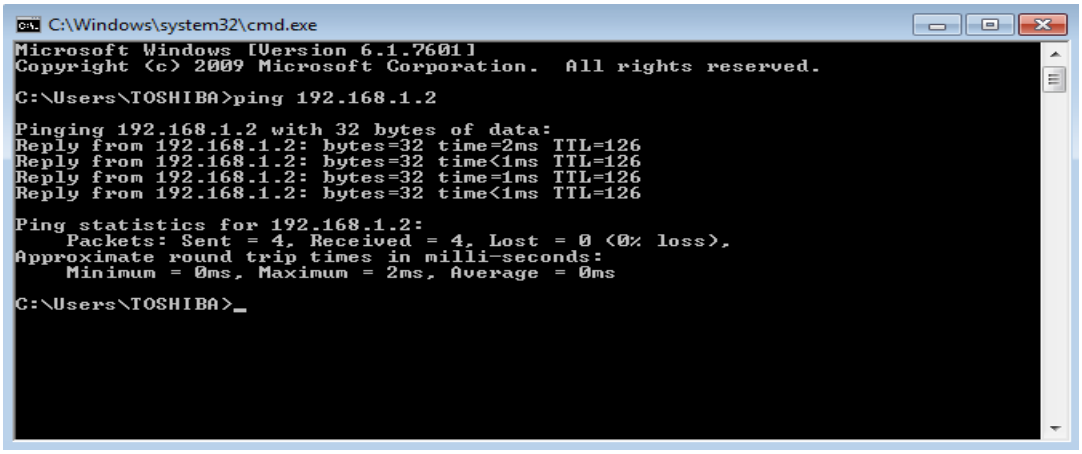
Dst-address adalah network tujuan dari pengiriman data.

Gateway = ip yang terhubung dengan router yang nantinya akan menjadi jalur pengiriman data

Selanjutnya lakukanlah pengujian apakah komputer 1 dan komputer 2 terhubung ,dengan cara melakukan Ping dari komputer 1 dan sebaliknya .

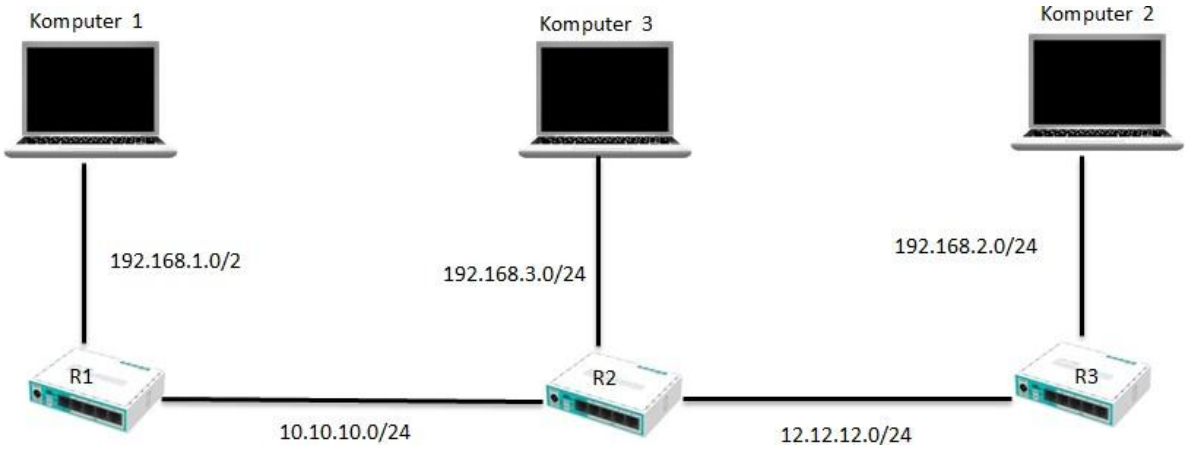


Gambar 7.6 Ping dari komputer 1 ke komputer 2



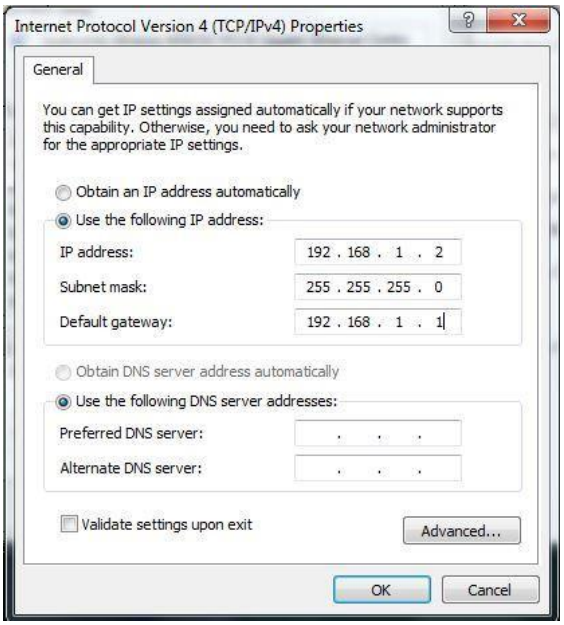
Gambar 7.7 Ping dari komputer 2 ke komputer 1

Static Routing Menggunakan 3 Router

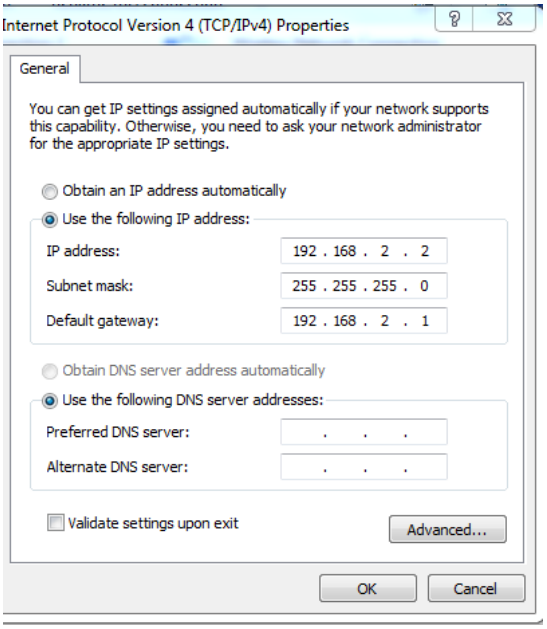


Gambar 7.8 : Topologi Routing Static

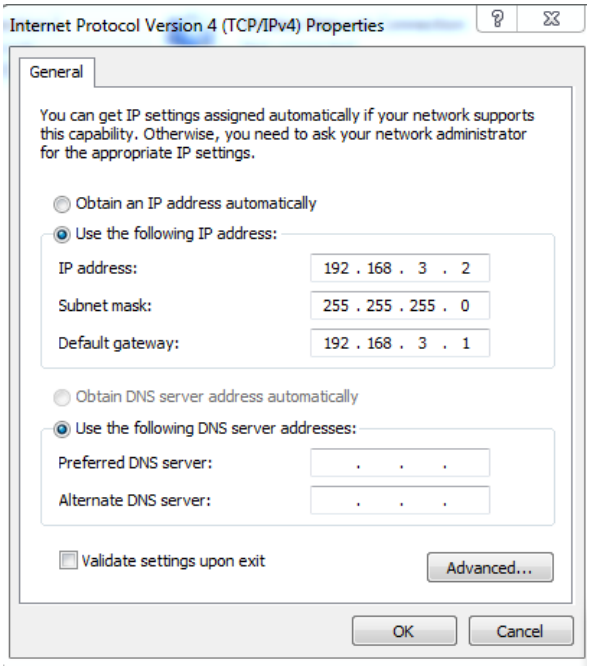
Konfigurasi IP Address pada masing masing komputer .



Komputer 1

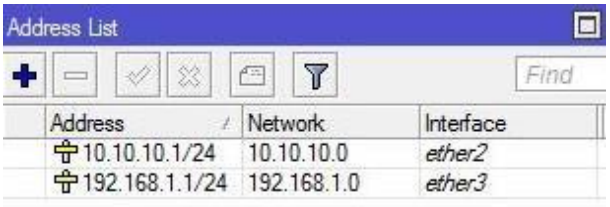


Komputer 2

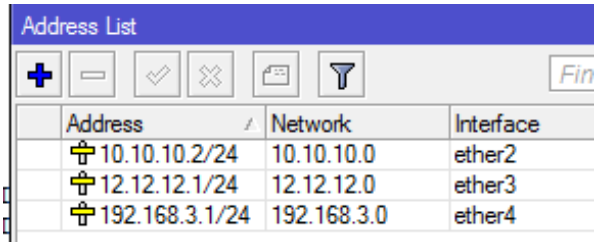


Komputer 3

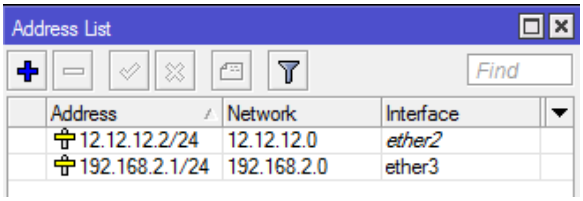
Setelah konfigurasi IP Address pada masing masing komputer, sekarang konfigurasi IP Address pada masing masing Router.



Router 1



Router 2



Router 3

Konfigurasi IP Address sudah selesai, sekarang konfigurasi routing pada masing masing router. Ketikkan perintah berikut ini pada router 1.

ip route add dst-address=192.168.2.0/24 gateway=10.10.10.2
ip route add dst-address=192.168.3.0/24 gateway=10.10.10.2

```
[admin@MikroTik] > ip route add dst-address=192.168.2.0/24 gateway=10.10.10.2
[admin@MikroTik] > ip route add dst-address=192.168.3.0/24 gateway=10.10.10.2
```

Konfigurasi routing pada router 2.

ip route add dst-address=192.168.1.0/24 gateway=10.10.10.1
ip route add dst-address=192.168.2.0/24 gateway=12.12.12.2

```
[admin@MikroTik] > ip route add dst-address=192.168.1.0/24 gateway=10.10.10.1
[admin@MikroTik] > ip route add dst-address=192.168.2.0/24 gateway=12.12.12.2
```

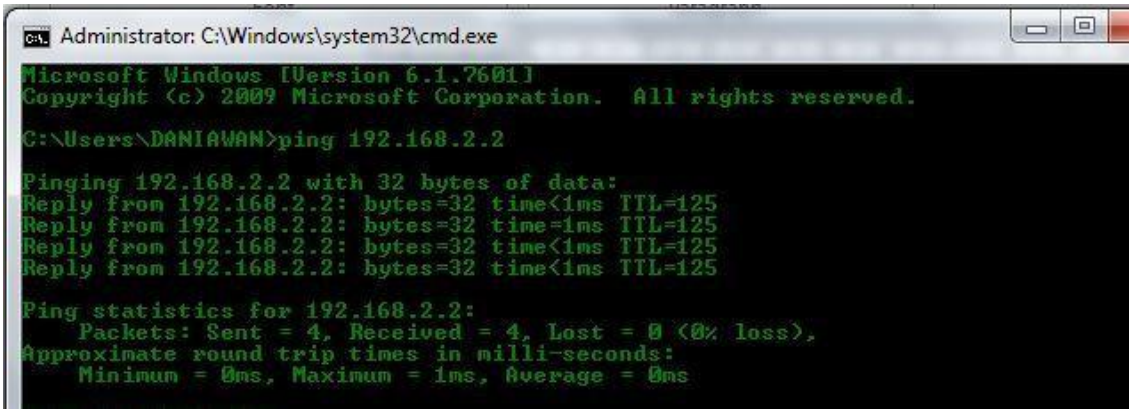
Konfigurasi routing pada router 3.

ip route add dst-address=192.168.3.0/24 gateway=12.12.12.1
ip route add dst-address=192.168.1.0/24 gateway=12.12.12.1

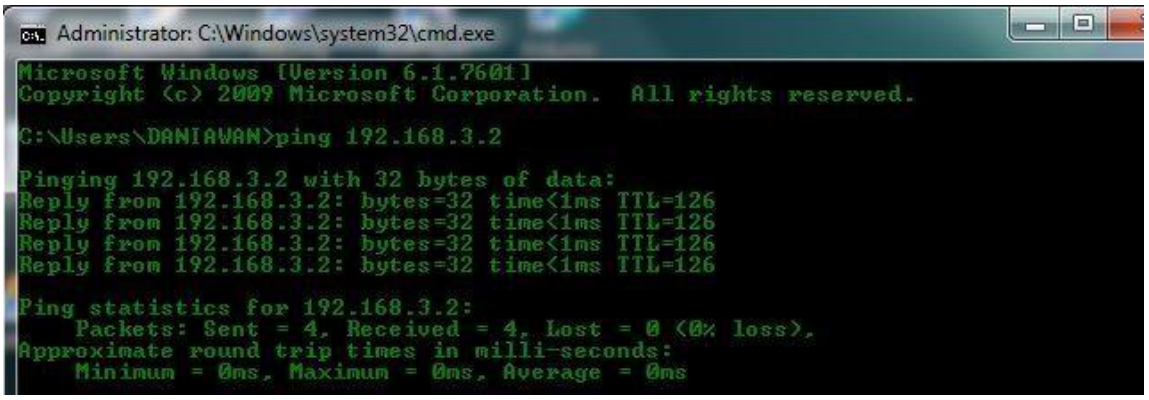
```
[admin@MikroTik] > ip route add dst-address=192.168.3.0/24 gateway=12.12.12.1
[admin@MikroTik] > ip route add dst-address=192.168.1.0/24 gateway=12.12.12.1
```

Selanjutnya lakukanlah pengujian pada masing-masing komputer.

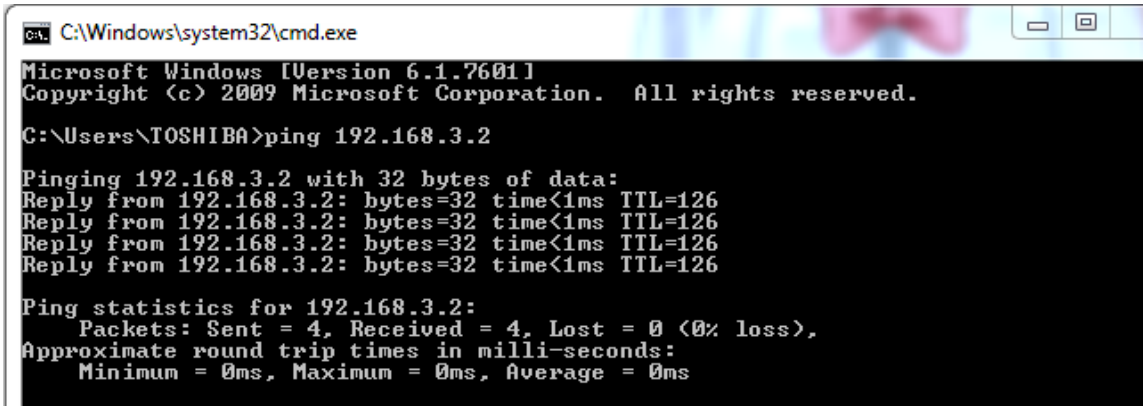
Ping dari komputer 1 ke komputer 2



Ping dari komputer 1 ke komputer 3



Ping dari komputer 2 ke komputer 3



Tugas

1. Buatlah *Static Routing* menggunakan 3 buah *router* MikroTik
2. Sertakan Laporan.

DAFTAR PUSATAKA

Efendi, I. (n.d.). √ *Pengertian dan Macam-macam Topologi Jaringan Komputer*. Retrieved September 3, 2020, from https://www.it-jurnal.com/pengertian-dan-macam-macam-topologi-jaringan-komputer/

Haryanto, E. V. (2012). *Jaringan Komputer* (P. Y. Jati (ed.)). ANDI Yogyakarta.

Kurniawan, A. (n.d.). *Pengertian Jaringan Komputer : Manfaat, Tujuan, Jenis, Topologi*. Retrieved September 3, 2020, from https://www.gurupendidikan.co.id/jaringan-komputer/

Nimda. (n.d.). *Apa itu jaringan Komputer? - Fakultas Teknik*. Retrieved September 3, 2020, from https://www.teknik.unpas.ac.id/blogs/apa-itu-jaringan-komputer/