



# Pengantar Jaringan Komputer

S-102

**JURUSAN**  
PENGELOLAAN SISTEM DAN JARINGAN



## **Pengantar Jaringan Komputer**

Kode Buku: PJK-S102

Revisi ke- 1

Tanggal: 01 Agustus 2020

Penulis: Wahyu Januar Alfian

Editor: Drs. Rusmanto, M.M.

Layout: Nanang Kuswana, S.Kom.

## **© Hak Cipta Pesantren PeTIK**

Materi/diktat/modul ini dilisensikan sebagai **CC BY versi 4.0** sesuai dengan ketentuan lisensi dari **Creative Commons**

(<https://creativecommons.org/licenses/by/4.0/deed.id>). Anda diperbolehkan **berbagi** (menyalin dan menyebarluaskan kembali materi ini dalam bentuk dan format apapun) dan **mengadaptasi** (mengubah, mengubah, dan membuat turunan dari materi ini) untuk kepentingan apapun, termasuk kepentingan komersial, dengan ketentuan sebagai berikut:

- Anda harus mencantumkan (tidak menghapus) pernyataan hak cipta ini;
- Anda harus menyatakan ada perubahan materi jika Anda telah melakukan perubahan; dan
- Ketentuan lain yang terdapat dalam dokumen lisensi CC BY 4.0.

Jika ada sebagian konten materi/diktat/modul ini mengandung karya cipta atau merek dagang pihak lain maka hak cipta atau merek dagang sebagian konten itu tetap menjadi milik masing-masing pihak.

## KATA PENGANTAR

Puji syukur kami panjatkan kehadirat Allah SWT, karena dengan rahmat dan karunia-Nya kami dapat menyelesaikan modul Jaringan Komputer ini. Sholawat dan salam senantisa tercurah pada junjungan kita Nabi Muhammad SAW. Modul Pengantar Jaringan Komputer ini ditujukan untuk pembelajaran para santri di lingkungan Pesantren PeTIK.

Modul ini disusun berdasarkan pengalaman penulis dalam memberikan pengajaran kepada para santri di lingkungan Pesantren PeTIK. Dalam proses pengajaran di kelas, pengajar atau asistennya dapat memberikan tugas tambahan atau latihan/workshop agar kompetensi santri dapat meningkat secara cepat.

Penulis sangat memahami bahwa apa yang telah di dapatkan selama pembuatan modul belumlah seberapa. Penulis menyadari sepenuhnya bahwa modul ini masih jauh dari sempurna. Oleh karena itu, saran dan kritik yang bersifat membangun sangat penyusun harapkan demi kesempurnaan modul ini. Dan tidak lupa penulis mengucapkan terimakasih kepada semua pihak yang telah membantu penulisan modul ini. Semoga modul ini dapat bermanfaat bagi pembacanya.

Semoga semua usaha yang telah kita lakukan menjadi amal baik yang terus membawa manfaat hingga akhir zaman.

Depok, Agustus 2020

Penulis

## DAFTAR ISI

<b>BAB 1 PENGANTAR JARINGAN KOMPUTER .....</b>	<b>5</b>
1.1 PENDAHULUAN.....	5
1.2 KEUNTUNGAN MENGGUNAKAN JARINGAN KOMPUTER.....	5
1.3 KOMPONEN JARINGAN.....	6
• Komputer Server .....	6
• Komputer Klien (Workstation) .....	7
1.4 PEER-TO-PEER DAN CLIENT-SERVER .....	8
• Jaringan Peer-to-peer .....	8
• Jaringan Client-Server.....	8
1.5 TOPOLOGI JARINGAN.....	8
1.6 PROTOKOL JARINGAN.....	9
<b>BAB 2 MODEL REFERENSI OSI .....</b>	<b>11</b>
2.1 STRUKTUR PROTOKOL JARINGAN MODEL OSI.....	11
<b>BAB 3 MODEL TCP/IP .....</b>	<b>14</b>
3.1 APPLICATION LAYER.....	14
3.2 TRANSPORT LAYER .....	14
<b>BAB 4 IP ADDRESS VERSI 4 .....</b>	<b>16</b>
4.1 FORMAT IP ADDRESS .....	16
• Kelas IP Address .....	16
• IP Private.....	18
• Network ID dan Host ID .....	18
• Subnetting .....	19
<b>BAB 5 IP ADDRESS VERSI 6 .....</b>	<b>20</b>
5.1 PENGANTAR IP ADDRESS VERSI 6 .....	20
5.2 FORMAT IP ADDRESS VERSI 6.....	20
5.3 PENYEDERHANAAN BENTUK ALAMAT .....	21

5.4	FORMAT PREFIX .....	22
<b>BAB 6 PERANGKAT KERAS JARINGAN .....</b>		<b>23</b>
6.1	KARTU JARINGAN (NETWORK INTERFACE CARD – NIC).....	23
6.2	KONSENTRATOR .....	24
<b>BAB 7 MEDIA TRANSMISI.....</b>		<b>27</b>
7.1	MEDIA KABEL (WIRED) .....	27
•	Kabel Coaxial.....	27
•	Kabel Twisted Pair.....	28
•	Kabel Fiber Optik.....	28
7.2	MEDIA NIRKABEL (WIRELESS).....	29
•	Infra Red .....	29
•	Bluetooth .....	29
•	WiFi .....	30
•	Wimax .....	30
<b>BAB 8 MEMBANGUN JARINGAN KOMPUTER LOKAL (LAN) .....</b>		<b>31</b>
8.1	DESAIN JARINGAN .....	31
8.2	INSTALASI JARINGAN .....	31
•	Instalasi Kartu Jaringan (NIC) .....	32
•	Instalasi Kabel Jaringan (UTP) .....	33
•	Memasang RJ-45 ke kabel UTP.....	33
<b>BAB 9 JARINGAN NIRKABEL .....</b>		<b>36</b>
9.1	TAHAPAN MEMBANGUN JARINGAN NIRKABEL .....	36
9.2	TAHAP 1 – MEMASANG PERANGKAT KERAS JARINGAN .....	37
9.3	TAHAP 2 – MENGKONFIGURASI <i>ACCESS POINT</i> .....	37
9.4	TAHAP 3 – MENGHUBUNGKAN ACCESS POINT KE JARINGAN KABEL .....	40
9.5	TAHAP 4 – MENGHUBUNGKAN CLIENT KE JARINGAN NIRKABEL.....	40
9.6	TAHAP 5 – MENGUJI KONEKSI JARINGAN .....	40
<b>BAB 10 KONFIGURASI JARINGAN DI WINDOWS 10 .....</b>		<b>43</b>

10.1 SETTING IP ADDRESS DAN JARINGAN LAN PADA WINDOW 10 .....	43
10.2 PENGUJIAN JARINGAN PADA WINDOWS 10 .....	47
10.3 MEMBERI IDENTITAS KOMPUTER SEBAGAI ANGGOTA SUATU GROUP DALAM WINDOWS 10	49
10.4 SHARE FOLDER DI WINDOWS 10 .....	51
10.4.1 Pengaturan Hak Akses pada Sharing di Windows 10 .....	53
10.4.2. Mengakses file yang dishare dari komputer lain .....	54
10.5 MENGGUNAKAN WIFI ATAU WIRELESS .....	55
<b>BAB 11 KEAMANAN JARINGAN NIRKABEL.....</b>	<b>58</b>
11.1 PENGANTAR KEAMANAN JARINGAN WIRELESS .....	58
11.2 MENYEMBUNYIKAN SSID.....	58
<b>BAB 12 CARA MENGAMANKAN JARINGAN WIRELESS.....</b>	<b>63</b>
12.3 CARA MENGAKTIFKAN WEP .....	67
• Uji coba dengan Windows atau Linux untuk menyambungkan komputer dengan AP telah diberi pengamanan dengan WPA .....	69
12.5 CARA MENYARING ALAMAT MAC .....	69
<b>BAB 13 PENGENALAN MIKROTIK .....</b>	<b>72</b>
13.1 APA ITU MIKROTIK? .....	72
13.2 <i>HARDWARE ROUTER - ROUTERBOARD</i> .....	73
13.3 LISENSI ROUTEROS .....	73
13.4 PRODUK MIKROTIK .....	74
• RB411 .....	74
• RB433 .....	75
• RB750 .....	76
• RB751U-2HnD .....	76
• RB800 .....	77
• RB1100 .....	78
• R52 .....	79
• Mikrobit .....	79

<b>BAB 14 INSTALASI DAN KONEKSI KE MIKROTIK.....</b>	<b>80</b>
14.1 PENDAHULUAN.....	80
14.2 KEBUTUHAN <i>HARDWARE</i> .....	80
14.3 LANGKAH-LANGKAH INSTALASI.....	81
14.4 MENGELOLA PERANGKAT MIKROTIK .....	84
14.5 BEKERJA DENGAN WINBOX .....	84
<b>BAB 15 KONFIGURASI DASAR MIKROTIK .....</b>	<b>86</b>
15.1 KONFIGURASI HOSTNAME.....	86
15.2 KONFIGURASI JARINGAN .....	86
• Konfigurasi IP address .....	87
• Konfigurasi Default Route .....	88
• Konfigurasi DNS.....	89
• Konfigurasi DHCP Client .....	89
15.3 SHARING INTERNET .....	90
15.4 DHCP SERVER.....	91
• Menambah IP Pool.....	93
• Membuat Static Lease .....	94
15.5 BACKUP DAN RESTORE KONFIGURASI.....	96
• Backup Penuh .....	97
• Backup Parsial.....	98
15.6 KONFIGURASI NTP.....	99
<b>DAFTAR PUSTAKA.....</b>	<b>100</b>

## Bab 1

# Pengantar Jaringan Komputer

### Tujuan:

- Mengenal jaringan komputer
- Mengetahui komponen-komponen yang dibutuhkan dalam membuat jaringan
- Mampu membuat jaringan komputer sederhana

### 1.1 Pendahuluan



Gambar 1 Jaringan komputer

Jaringan komputer adalah sekelompok komputer yang saling berhubungan di dalam area tertentu. Dengan jaringan, antar komputer yang satu dengan yang lainnya bisa saling berbagi pakai sumber daya (sharing), sehingga secara tidak langsung meningkatkan efisiensi dalam pemanfaatan sarana yang ada. Sebagai contoh, bila komputer Anda dihubungkan dengan jaringan, maka untuk mencetak Anda cukup menyediakan satu unit printer saja. Printer tersebut dapat

digunakan bersama-sama di dalam jaringan. Selain itu, sharing data memungkinkan Anda untuk mengakses komputer dari lokasi atau komputer yang berbeda.

Bahkan dengan banyaknya tersedia aplikasi multi user saat ini, maka memungkinkan satu aplikasi untuk digunakan secara bersama-sama oleh komputer-komputer di jaringan tersebut.

### 1.2 Keuntungan Menggunakan Jaringan Komputer

Mengingat banyaknya perlengkapan yang harus disediakan untuk membangun suatu jaringan komputer, maka timbul pertanyaan. Apakah sesuai tenaga, biaya dan pikiran yang dikeluarkan dengan manfaat yang dapat diambil dari suatu jaringan? Apakah bukannya hanya suatu pemborosan saja? Untuk lembaga, perusahaan atau suatu institusi yang tidak memerlukan begitu banyak lalu lintas informasi, atau tidak menginginkan efisiensi, barangkali memang

suatu pemborosan. Tetapi tentu saja di era globalisasi informasi telah menjadi kunci utama dan efisiensi sudah merupakan suatu keharusan. Untuk itulah maka jaringan komputer hadir sebagai solusi untuk sarana pertukaran informasi baik di dalam perusahaan maupun ke luar perusahaan secara lebih cepat dan efektif.

Dengan jaringan komputer, banyak yang dapat kita bagi-pakai dan kita tingkatkan efisiensinya, antara lain:

- Pertukaran email antar personil
- Diskusi/Chat
- Berbagi-pakai File
- Berbagi-pakai Program
- Berbagi-pakai Hardware (FDD, CDROM, Fax, Printer dsb.)
- Berbagi akses internet

Dan satu hal yang lebih penting dari semua itu, saat ini jaringan komputer tidak hanya digunakan untuk berkirim email ataupun berbagi-pakai piranti seperti tersebut di atas, melainkan juga berkembang lebih luas sebagai komputasi *workgroup* yang memiliki kemampuan sebagai alat komunikasi modern, kolaborasi dan koordinasi dalam suatu perusahaan, lembaga atau suatu institusi.

### 1.3 Komponen Jaringan

Untuk membuat suatu jaringan komputer Anda membutuhkan komputer atau end device lebih dari satu. Contoh End device termasuk komputer server, PC, notebook, PDA, printer, telepon VoIP, dll. Adapun secara garis besar komputer dibagi menjadi dua, yaitu komputer server dan komputer klien.

- **Komputer Server**

Komputer server adalah komputer yang difungsikan sebagai "pelayan" komunikasi data, serta tempat mengatur lalu lintas data antara komputer-komputer di jaringan. Fungsi pelayanan ini dimungkinkan oleh adanya perangkat lunak/service yang menggunakan sistem protokol sebagai bahasa dalam mengkomunikasikan data. Contoh-contoh server adalah webserver, DNS server, mail server, file server, domain controller server, internet sever, print server dan lain-lain. Internet server memberikan akses internet ke komputer server.

Dalam memilih komputer server pada dasarnya Anda dapat menggunakan komputer biasa. Terutama apabila Anda tidak memiliki dana yang mencukupi untuk membeli suatu komputer khusus server. Komputer server mahal karena disebabkan komputer tersebut memiliki spesifikasi yang berbeda dengan komputer biasa. Misalnya: memungkinkan penggunaan prosesor lebih dari satu di satu motherboard, jumlah slot memory yang banyak, dukungan terhadap device SCSI, memungkinkan pemasangan media penyimpanan yang sangat banyak, dan masih banyak fitur yang lain. Selain daripada itu komputer server memiliki beberapa hardware yang berbeda dengan komputer pada umumnya. Hasilnya komputer khusus server memiliki performa kerja yang lebih tinggi dari komputer biasa.



Gambar 2 Komputer server IBM

Tetapi dalam memilih komputer server tidak serta merta Anda mencari komputer spesifikasi setinggi-tingginya, Anda harus melihat fungsi dari server Anda. Sebagai contoh apabila Anda membuat web server atau mail server Anda harus menggunakan server yang memiliki prosesor dan RAM yang tinggi. Di lain pihak apabila Anda menggunakan server untuk share data dan print server maka Anda bisa menggunakan komputer biasa bahkan Anda bisa menggunakan komputer tersebut sebagai workstation juga.

- **Komputer Klien (Workstation)**

Komputer klien adalah komputer yang digunakan oleh user atau klien secara langsung di suatu jaringan. Melalui workstation inilah para pemakai bekerja menyelesaikan segala pekerjaannya yang berhubungan dengan komputer. Baik itu untuk chatting, browsing, sharing dan sebagainya.

Adapun kriteria komputer yang dapat dijadikan workstation adalah semua komputer yang kita pergunakan sehari-hari. Jadi, tidak ada kriteria khusus. Yang pasti dalam komputer tersebut harus sudah ada Network Interface Card (NIC)-nya. Semakin tinggi spesifikasi komputer yang dipergunakan sebagai wokstation, tentu saja akan semakin baik.

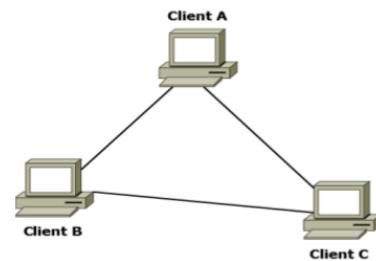
## 1.4 Peer-to-peer dan Client-Server

Jaringan komputer adalah sistem atau rangkaian yang terdiri dari dua komputer atau lebih, dimana diantara satu komputer dengan komputer yang lain saling terhubung oleh sebuah sistem komunikasi, sehingga memungkinkan setiap komputer yang terhubung dalam jaringan tersebut dapat saling tukar menukar data, program, dan sumber daya komputer lainnya.

Sub bab di atas sudah menjelaskan tentang jenis jaringan berdasarkan jangkauan atau LAN (Local Area Network). Dari peranan komputer juga penting dalam menentukan atau membuat suatu jaringan. Berikut contoh jaringan berdasarkan cara mengakses data:

- **Jaringan Peer-to-peer**

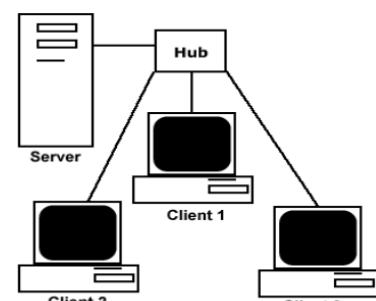
Pada jaringan ini tidak ada istilah komputer klien manapun komputer server karena semua komputer dapat melakukan pengiriman maupun penerimaan informasi sehingga semua komputer berfungsi sebagai klien sekaligus sebagai server. Jaringan peer-to-peer juga memperbolehkan pemakai membagi *resources* dan file pada komputer mereka serta mengakses *resource* yang di-share oleh komputer lain.



Gambar 3 Jaringan peer-to-peer

- **Jaringan Client-Server**

Pada tipe jaringan ini terdapat satu atau beberapa komputer server dan komputer klien. Komputer yang akan menjadi server maupun menjadi komputer klien dapat diubah-ubah melalui software jaringan pada protokolnya. Komputer klien sebagai perantara untuk dapat mengakses data pada komputer server sedangkan komputer server menyediakan informasi yang diperlukan oleh komputer klien.



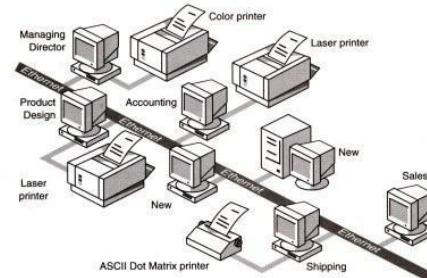
Gambar 4 Jaringan client server

## 1.5 Topologi Jaringan

Topologi jaringan adalah bentuk atau konfigurasi yang digunakan untuk menghubungkan antar komputer pada sebuah jaringan. Pada dasarnya ada beberapa tipe topologi, yaitu:

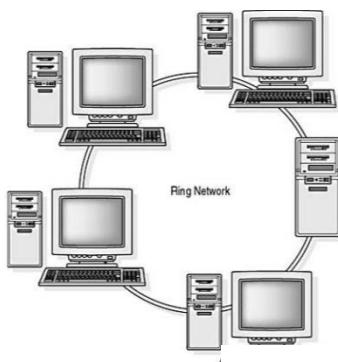
- **Topologi Bus**

Pada topologi ini sebuah saluran/kabel dipakai beramai-ramai oleh semua komputer yang berada dalam jaringan. Karena menggunakan satu jalur maka sering terjadi peristiwa tumbukan paket (*collision*) yang menyebabkan paket harus dikirim lagi. Peristiwa ini menyebabkan penurunan kecepatan transfer data.



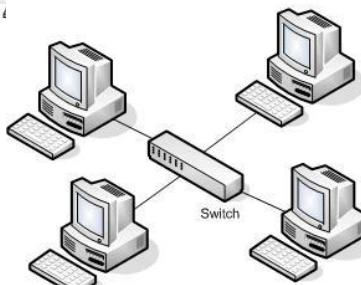
Gambar 5 Topologi bus

- **Topologi Ring**



Pada topologi ini jaringan membentuk suatu jaringan tertutup (*loop*). Komputer yang terhubung hanya bisa mengirimkan data pada saat menerima tiket / token untuk mengirimkan data. Hal ini dilakukan secara *sequential* (berurutan) dari satu komputer ke komputer yang lain. Dengan sistem kerja seperti ini maka *collision* akan terhindari.

• **Topologi Ring**  
Pada topologi ini yang biasanya dapat berupa hub, switch, router



jaringan terpusat pada satu node, berupa konsentrator. Konsentrator

Gambar 7 Topologi star

ataupun PC. Topologi yang paling banyak digunakan saat ini adalah star. Bahkan topologi lainnya dapat berupa seperti layaknya topologi star, seperti topologi bus pada konsentrator.

## 1.6 Protokol Jaringan

Protokol adalah suatu bahasa atau aturan yang digunakan oleh suatu komputer atau node ketika berhubungan dengan node lain di jaringan. Protokol digunakan agar setiap node di jaringan mengerti bagaimana berinteraksi satu sama lain. Seperti Anda berbicara dengan orang Amerika maka jika Anda menggunakan bahasa Indonesia tentu orang tersebut tidak akan mengerti. Anda harus menggunakan bahasa yang dimengerti oleh orang tersebut, yaitu bahasa

Inggris. Begitu juga di jaringan, bahasa yang dimengerti oleh setiap perangkat jaringan adalah protokol.

Salah satu protokol yang paling banyak digunakan bahkan menjadi protokol untuk internet adalah TCP/IP. Walaupun bisa saja suatu perusahaan menggunakan protokol NetBEUI, IPX/SPX, AppleTalk atau yang lain tapi pada umumnya menggunakan TCP/IP. Berikut penjelasannya tentang beberapa protokol tersebut.

NetBEUI atau NetBIOS Extended User Interface adalah protokol jaringan yang dikembangkan oleh International Business Machine Corporation atau yang lebih dikenal dengan IBM dan Microsoft Corporation pada tahun 1985 yang digunakan untuk jaringan lokal (LAN). NetBEUI sendiri adalah ekstensi dari protokol NetBIOS. NetBEUI juga merupakan protokol utama yang digunakan dalam LAN Manager dan Windows for Workgroup.

IPX/SPX atau Internetwork Packet Exchange/Sequenced Packet Exchange, masing-masing berasal dari Xerox Network System, IDP dan SPP protokol. IPX adalah protokol lapisan jaringan (lapisan 3 dari OSI Model), sedangkan SPX adalah lapisan protokol transport (lapisan 4 dari OSI Model). Lapisan SPX terletak di atas IPX dan menyediakan orientasi layanan antara dua node pada jaringan. Fungsi utama IPX/SPX sebagai media transmisi data dan menjamin validitas data yang ditransmisikan oleh IPX sehingga data yang dikirim tidak akan mengalami gangguan atau kerusakan pada data.

Appletalk adalah protokol jaringan yang dikembangkan khusus untuk jaringan yang terdiri atas komputer-komputer Apple Macintosh, yang mengizinkan para pengguna untuk saling berbagi berkas dan printer agar dapat diakses oleh pengguna lainnya. Appletalk merupakan teknologi yang sudah dianggap usang yang kini sudah digantikan oleh Apple Open Transport, yang juga didukung Appletalk itu sendiri, protokol TCP/IP dan beberapa protokol jaringan lainnya.

Istilah TCP/IP terdiri dari dua buah akronim. TCP singkatan dari Transmission Control Protocol dan IP singkatan dari Internet Protocol. TCP adalah protokol yang menangani aliran paket data antar sistem dan IP bertanggungjawab menangani routing paket data. Ciri dari TCP/IP adalah pengalaman komputer di jaringan menggunakan IP address.

## Bab 2

### Model Referensi OSI

#### Tujuan:

- Mengenal Protokol Jaringan Model OSI
- Mengetahui tugas tugas 7 Lapisan OSI

#### 2.1 Struktur Protokol Jaringan Model OSI

OSI adalah singkatan dari Open System Interconnection. OSI dikembangkan oleh ISO (International Organization for Standardization). Dalam model struktur OSI, protokol dibagi dalam 7 lapisan layanan. Dalam struktur model yang berlapis ini, setiap lapisan protokol akan melaksanakan bagian-bagian dari keseluruhan fungsi yang diperlukan dalam komunikasi data. Setiap lapisan protokol akan diikuti lapisan protokol yang lebih rendah berikutnya untuk melaksanakan fungsi-fungsi yang lebih rendah memberikan layanan bagi lapisan di atasnya. Dan perubahan yang terjadi dalam suatu lapisan tidak mempengaruhi lapisan lainnya.

Lapisan (layer) layanan dalam protokol model OSI adalah sebagai berikut:

##### 1. Application layer

Lapisan aplikasi (application layer) bertanggung jawab memberikan layanan-layanan aplikasi bagi para user, misal aplikasi FTP atau SMTP (email)

##### 2. Presentation layer

Lapisan presentasi (presentation layer) bertanggung jawab memberikan dua macam layanan yaitu:

- Translasi

Translasi diperlukan karena sistem pengkodean pada setiap komputer user berbeda-beda sehingga perlu translasi menjadi kode dalam standar Internasional

- Proses enkripsi dan kompresi data

Lapisan presentasi juga bertanggung jawab terhadap enkripsi dan kompresi data, meskipun juga akan ditangani oleh lapisan lainnya.

##### 3. Session layer

Lapisan sesi (session layer) bertanggung jawab memberikan dua macam layanan, yaitu:

- Mengelola proses komunikasi dua arah, misal “session” komunikasi

Sebagai contoh: ketika seseorang mengambil uang dari mesin ATM, berarti orang tersebut telah berpartisipasi dalam sebuah “session”

- Memberikan layanan sinkronisasi

#### 4. Transport Layer

Setiap data atau informasi yang dikirim melalui media komunikasi dalam jaringan akan diubah ke dalam bentuk unit-unit yang dapat dikelola yang disebut sebagai paket. Lapisan transport bertanggung jawab untuk membuat paket-paket tersebut yang memuat data, alamat, urutan, serta mekanisme kontrol kesalahan terhadap data atau informasi yang dikomunikasikan.

#### 5. Network layer

Lapisan network bertanggung jawab terhadap pengiriman paket-paket (pada lapisan yang lebih rendah) dalam dua hal, yaitu:

- Menambahkan alamat jaringan dan informasi lainnya ke dalam paket yang dikirimkan
- Membuat keputusan yang harus dilalui oleh paket yang ditransmisikan melewati banyak jaringan

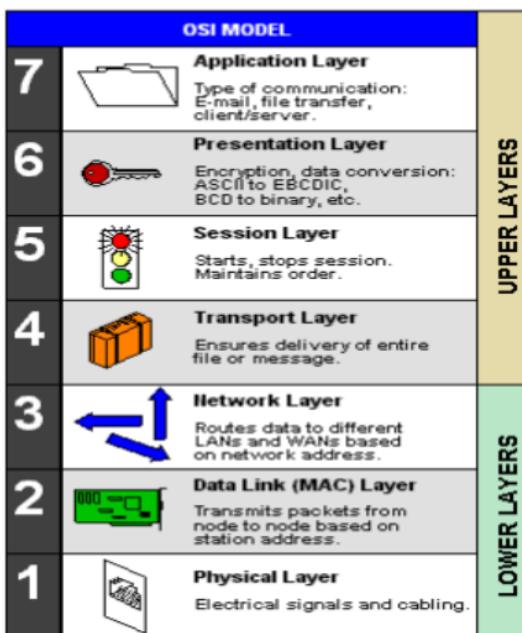
#### 6. Data link layer

Lapisan data link bertanggung jawab dalam dua hal yaitu:

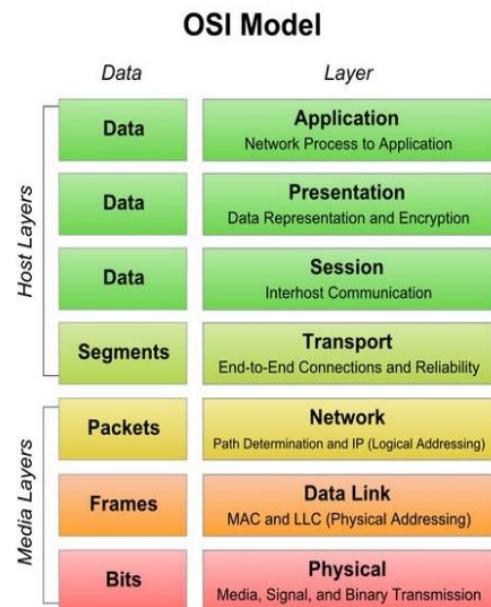
- Memberikan petunjuk kepada paket dalam melewati link dalam jaringan.
- Memberikan “frame” pada paket yang dikirimkan, yaitu dengan menambahkan alamat fisik tujuan ke dalam paket.

#### 7. Physical layer

Lapisan fisik bertanggung jawab melakukan translasi secara fisik dari informasi yang terkandung di dalam paket menjadi jalur sinyal secara aktual, sebagai contoh, bit 0 dan 1 dapat berarti tegangan positif atau negatif atau tegangan rendah atau tinggi. Lapisan ini tidak menambahkan informasi apapun ke dalam paket yang diperoleh dari lapisan di atasnya.



Gambar 8 Lapisan model OSI



Gambar 9 Format data pada model OSI

## Bab 3

### Model TCP/IP

#### Tujuan

- Mengenal Protokol TCP/IP
- Mengetahui Perbedaan Model TCP/IP dan Model OSI Layer

Struktur protokol model TCP/IP dikembangkan oleh DARPA (US Defense Advanced Research Project Agency) yang diperuntukkan untuk paket-paket yang dikirimkan melalui jaringan ARPANET. Saat ini, TCP/IP secara de facto merupakan protokol standar yang digunakan di jaringan Internet.

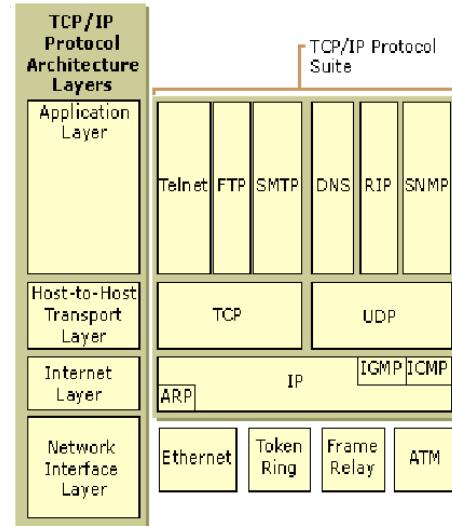
Struktur protokol model TCP/IP terdiri atas empat lapisan protokol, yaitu:

#### 3.1 Application Layer

Pada lapisan ini terletak semua aplikasi yang menggunakan TCP/IP ini. Lapisan ini melayani permintaan pemakai untuk mengirim dan menerima data. Data tersebut kemudian disampaikan ke lapisan transport untuk diproses lebih lanjut. Contohnya adalah HTTP, FTP dan SMTP.

#### 3.2 Transport Layer

Berisi protokol yang bertanggung jawab untuk mengadakan komunikasi antara dua host komputer. Kedua protokol tersebut ialah TCP (Transmission Control Protocol) dan UDP (User Datagram Protocol). Protokol ini bertugas mengatur komunikasi antara host dan pengecekan kesalahan. Data dibagi ke dalam beberapa paket yang dikirim ke lapisan Internet dengan sebuah header yang mengandung alamat tujuan atau sumber dan checksum. Pada penerima, checksum akan diperiksa apakah paket tersebut ada yang hilang diperjalanan.



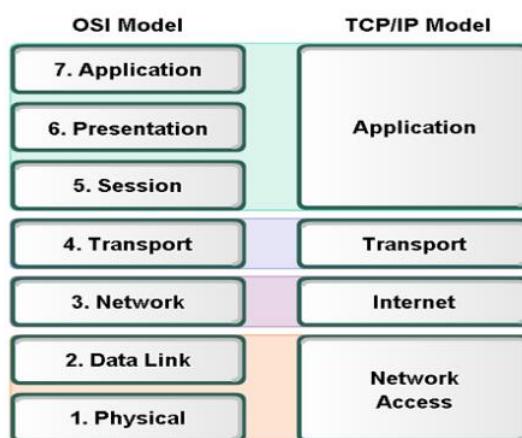
Gambar 10 Protokol TCP/IP

## 1. Network Layer (Internet Layer)

Protokol yang berada pada layer ini bertanggung jawab dalam proses pengiriman paket paket ke alamat yang tepat. Pada layer ini terdapat tiga macam protokol, yaitu: IP, ARP dan ICMP.

## 2. Physical Layer (Network Interface Layer)

Bertanggung jawab mengirim dan menerima data ke dan dari media fisik. Media fisik dapat berupa ethernet, token ring, kabel, serat optik, frame relay atau gelombang radio. Protokol pada layer ini harus mampu menerjemahkan sinyal listrik menjadi data digital yang dimengerti oleh komputer yang berasal dari peralatan.



Gambar 11 Perbandingan protokol OSI dan TCP/IP

## Bab 4

### IP Address Versi 4

#### Tujuan

- Mengetahui format IP versi 4
- Mengkorversi Bilangan Biner ke Desimal
- Memahami Kelas IP Address, Network dan Host ID, Subnetting

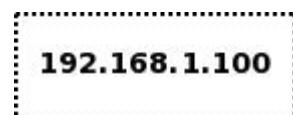
#### 4.1 Format IP Address

IP Address terdiri atas bilangan 32 bit (binary digit atau bilangan duaan) yang dibagi dalam 4 oktet (byte), setiap oktet terdiri dari 8 bit. Diantara oktet-oktet tersebut dibatasi oleh tanda titik (.). Sebagai contoh Anda bisa melihat gambar di bawah:



Gambar 12 IP Address dalam biner

Tetapi IP address agar terlihat lebih sederhana selalu menggunakan bilangan desimal dalam penulisannya. Sebagai contoh Anda bisa melihat gambar di bawah:



Gambar 13 IP Address dalam desimal

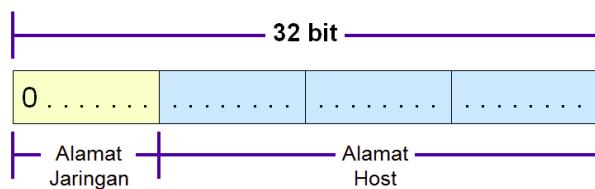
Dikarenakan IP address berasal dari bilangan biner maka setiap oktet pada IP address apabila direpresentasikan dalam bentuk desimal nilai paling kecil adalah 0 (00000000) dan nilai paling besar adalah 255 (11111111).

#### • Kelas IP Address

Untuk mempermudah proses pembagiannya, IP address dikelompokkan dalam kelas-kelas. Alasan yang mendasari pembagiannya atau pengelompokkan IP address ini adalah untuk mempermudah pendistribusian pendaftaran IP address. Secara umum IP address ini dikelompokkan dalam tiga bagian besar kelas IP address.

## Kelas A

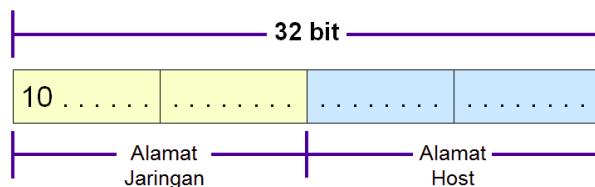
Pada kelas A, hanya delapan bit paling depan untuk mengenali alamat jaringan. Sehingga jumlah komputer yang bisa dipasang dalam jaringan di kelas A adalah  $2^{24}$  atau  $(256 \times 256 \times 256)$ . Ciri dari jaringan yang disusun dalam konfigurasi kelas A adalah bit paling kiri dari alamat IP adalah "0" dan nomor IP mulai alamat 0 sampai 127 pada oktet pertama. Network ID dari kelas A berjumlah 126 jaringan (0 dan 127 dicadangkan). Nomor IP 127.0.0.1 dipakai untuk koneksi localhost, meskipun bit pertama dari nomor IP adalah 0. Netmask / subnetmask default yang digunakan adalah 255.0.0.0.



Gambar 14 IP Address Kelas A

## Kelas B

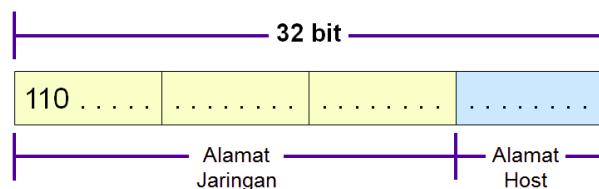
Mempunyai jangkauan alamat IP dari 128 sampai 191 pada oktet pertama nomor IP. Dua bit pertama di sebelah kiri adalah "10". Selain itu yang perlu diperhatikan adalah jumlah bit yang dipakai sebagai alamat jaringan sebanyak 16 bit. Masing-masing jaringan pada kelas ini mempunyai host maksimum  $2^{16}$  (dikurangi 2, untuk alamat jaringan dan alamat broadcast) atau  $((256 \times 256)-2)$ . Netmask / subnetmask default yang digunakan adalah 255.255.0.0.



Gambar 15 IP Address Kelas B

## Kelas C

Tiga bit awal adalah "110". Jangkauan alamat kelas ini adalah 192 sampai 223 untuk oktet pertama alamat IP. Kelas C memakai 24 bit awal sebagai identifikasi jaringan dan hanya menyediakan 8 bit untuk identifikasi host (tentu saja masih harus dikurangi 2, untuk alamat jaringan dan alamat broadcast) atau 254 komputer. Netmask / subnetmask default yang digunakan adalah 255.255.255.0.



Gambar 16 IP Address Kelas C

- **IP Private**

Jenis IP address ada dua macam, yaitu IP Private dan IP Public. IP Private adalah IP address yang berlaku untuk suatu area tertentu saja, misalnya pada sebuah jaringan LAN. Untuk IP Private tidak akan diakui sebagai pengalamatan yang sah di jaringan global atau internet. Sedangkan IP Public adalah pengalamatan yang dapat diakses dari mana saja di internet dan merupakan pengalamatan yang sah di jaringan global. Untuk IP Public tidak bisa Anda gunakan secara bebas tapi Anda dapatkan dari penyedia jasa internet (ISP). Sedangkan IP Private boleh digunakan secara bebas dengan mengikuti aturan sebagai berikut :

1. Kelas A: 10.0.0.0 - 10.255.255.255
2. Kelas B: 172.16.0.0 - 172.31.255.255
3. Kelas C: 192.168.0.0 - 192.168.255.255

- **Network ID dan Host ID**

Untuk menentukan atau mengetahui network id dari suatu IP address dapat dilakukan dengan melakukan operasi logika "AND bitwise" antara ip address dengan netmask. Netmask adalah suatu bilangan biner 32 bit yang digunakan untuk membedakan network id dan host id, dan menunjukkan apakah suatu host berada pada jaringan yang sama. Apabila suatu host pada jaringan yang sama memiliki network id yang sama maka kedua host tersebut dapat saling berkomunikasi secara langsung.

Sebagaimana dijelaskan sebelumnya bahwa setiap kelas IP memiliki pasangan netmask yang sudah ditentukan. Misalnya sebuah IP address kelas A memiliki default netmask 255.0.0.0, default netmask kelas B 255.255.0.0 dan netmask kelas C adalah 255.255.255.0.

Untuk menetukan network ID coba perhatikan contoh berikut:

IP Address	:	192.168.0.1	dalam bit	11000000.10101000.00000000.00000001
Netmask	:	255.255.255.0	dalam bit	11111111.11111111.11111111.00000000
Network ID	:	192.168.0.0	dalam bit	11000000.10101000.00000000.00000000

Host id digunakan untuk mengidentifikasi nomor suatu host dalam suatu jaringan. Setiap interface harus memiliki host id yang unik. Untuk menentukan host id caranya dengan melakukan operasi logika "AND bitwise" antara ip address dengan inverse dari netmask.

Untuk menetukan host id coba perhatikan contoh berikut:

IP Address	:	192.168.0.1	dalam bit	11000000.10101000.00000000.00000001
Netmask	:	0.0.0.255	dalam bit	00000000.00000000.00000000.11111111
Network ID	:	0.0.0.1	dalam bit	00000000.00000000.00000000.00000001

- **Subnetting**

Contoh penerapan lain dari penggunaan netmask adalah penggunaan IP address yang berbentuk classless IP address. Classless IP address adalah IP address yang menggunakan netmask diluar dari netmask default dari tiap kelas. Hal ini digunakan untuk membuat jaringan dengan besar sesuai yang Anda inginkan. Sebagai contoh Anda memiliki IP address 202.180.47.17 Anda menggunakan netmask 255.255.255.248, maka perhitungan network id dan host id-nya:

IP Address	:	202.180.47.17	dalam bit	11001010.10110100.00101111.00010001
Netmask	:	255.255.255.248	dalam bit	11111111.11111111.11111111.11111000
Network ID	:	202.180.47.16	dalam bit	11001010.10110100.00101111.00010000

Untuk mencari host pertama Anda tambahkan satu dari network id. Kemudian untuk mendapatkan IP broadcast Anda satukan bit pada host dan host terakhir Anda kurangkan 1 bit dari broadcast.

Host 1	:	202.180.47.17	dalam bit	11001010.10110100.00101111.00010001
Host End	:	255.180.47.22	dalam bit	11001010.10110100.00101111.00010110
Broadcast	:	202.180.47.23	dalam bit	11001010.10110100.00101111.00010111

Sehingga Network ID = 202.180.47.16/29

Range IP = 202.180.47.17-202.180.47.22 (jumlah host 6)

Dari perhitungan di atas Anda mengetahui bahwa IP address yang bisa Anda gunakan untuk komputer di jaringan sebanyak 6 ip address.

## Bab 5

### IP Address Versi 6

#### Tujuan

- Mengenal IP Address Versi 6
- Mengetahui Format IP Adress versi 6
- Mengkoversi IPv6

#### 5.1 Pengantar IP Address Versi 6

Alamat IP versi 6 (sering disebut sebagai alamat 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 teoretis dapat mengalami hingga  $2^{128}=3,4 \times 10^{38}$  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*.

Seperti halnya IPv4 yang menggunakan bit-bit pada tingkat tinggi (*high-order bit*) sebagai alamat jaringan sementara bit-bit pada tingkat rendah (*low-order bit*) sebagai alamat *host*, dalam IPv6 juga terjadi hal serupa. Dalam IPv6, bit-bit pada tingkat tinggi akan digunakan sebagai tanda pengenal jenis alamat IPv6, yang disebut dengan *Format Prefix (FP)*. Dalam IPv6, tidak ada subnet mask, yang ada hanyalah *Format Prefix*

#### 5.2 Format IP Address Versi 6

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:

```
00100001110110100000000011010011000000000000000000001011110011101100000010101  
010100000000111111111111000101001001110001011010
```

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
```

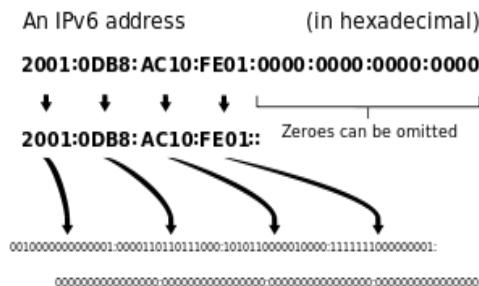
Lalu, setiap blok berukuran 16-bit tersebut dikonversikan ke dalam bilangan heksadesimal dan setiap bilangan heksadesimal tersebut dipisahkan dengan menggunakan tanda titik dua. Hasil konversinya adalah sebagai berikut:

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

### **5.3 Penyederhanaan Bentuk Alamat**

Alamat di atas juga dapat disederhanakan lagi dengan membuang angka 0 pada awal setiap blok yang berukuran 16-bit di atas, dengan menyisakan satu digit terakhir. Dengan membuang angka 0, alamat di atas disederhanakan menjadi:

21da:d3:0:2f3b:2aa:ff:fe28:9c5a



Gambar 17. Penyederhanaan IPv6 dengan bilangan Hexadesimal

Konvensi pengalamatan IPv6 juga mengizinkan penyederhanaan alamat lebih jauh lagi, yakni dengan membuang banyak karakter 0, pada sebuah alamat yang banyak angka 0-nya. Jika sebuah alamat IPv6 yang direpresentasikan dalam notasi *colon-hexadecimal* format

mengandung beberapa blok 16-bit dengan angka 0, maka alamat tersebut dapat disederhanakan dengan menggunakan tanda dua buah titik dua (:). Untuk menghindari kebingungan, penyederhanaan alamat IPv6 dengan cara ini hanya bisa digunakan sekali saja di dalam satu alamat, karena kemungkinan nantinya pengguna tidak dapat menentukan berapa banyak bit 0 yang direpresentasikan oleh setiap tanda dua titik dua (:) yang terdapat dalam alamat tersebut. Tabel di bawah ini dapat mengilustrasikan cara penggunaan hal diatas.

Alamat asli	Alamat asli yang disederhanakan	Alamat yang telah dikompres
fe80:0000:0000:0000:02aa:00ff:fe9a:4ca2	fe80:0:0:0:2aa:ff:fe9a:4ca2	fe80::2aa:ff:fe9a:4ca2
ff02:0000:0000:0000:0000:0000:0002	ff02:0:0:0:0:0:0:2	ff02::2

#### 5.4 Format Prefix

Dalam IPv4, sebuah alamat dalam notasi dotted-decimal format dapat direpresentasikan dengan menggunakan angka prefiks yang merujuk kepada subnet mask. IPv6 juga memiliki angka prefiks, tetapi tidak digunakan untuk merujuk kepada subnet mask, karena memang IPv6 tidak mendukung subnet mask. Prefiks adalah sebuah bagian dari alamat IP, di mana bit-bit memiliki nilai-nilai yang tetap atau bit-bit tersebut merupakan bagian dari sebuah rute atau *subnet identifier*. Prefiks dalam IPv6 direpresentasikan dengan cara yang sama seperti halnya prefiks alamat IPv4, yaitu **[alamat]/[angka panjang prefiks]**. Panjang prefiks menentukan jumlah bit terbesar paling kiri yang membuat prefiks subnet. Sebagai contoh, prefiks sebuah alamat IPv6 dapat direpresentasikan sebagai berikut:

3ffe:2900:d005:f28b::/64

## Bab 6

### Perangkat Keras Jaringan

#### Tujuan

- Mengetahui macam-macam Komponen Jaringan
- Mengetahui Fungsi Perangkat Keras Jaringan

#### 6.1 Kartu Jaringan (Network Interface Card – NIC)

Kartu jaringan merupakan kartu antarmuka (Interface) yang memungkinkan komputer dapat berkomunikasi dalam suatu jaringan. Kartu jaringan inilah yang bertugas untuk mengatur dan menterjemahkan data yang akan dikirim maupun yang akan diterima dalam suatu jaringan.

Sesuai dengan perkembangan teknologi jaringan, saat ini kartu jaringan sudah banyak beredar di pasaran, baik jenis maupun mereknya. Bahkan ethernet card sudah merupakan komponen wajib dari motherboard. Lain halnya pada notebook, modem dialup, ethernet card dan wireless sudah ada di dalamnya menunjang kebutuhan informasi para pengguna mobile. Hal tersebut menjadi bukti bahwa kebutuhan jaringan sudah merupakan hal yang tidak dapat dipisahkan dari dunia teknologi informasi. Namun demikian apabila Anda hendak menggunakan atau menambah kartu jaringan Anda, ada tiga hal pokok yang perlu diperhatikan, yaitu tipe kartu, kecepatan, dan jenis protokol.

- Tipe Kartu

Apakah sesuai atau tidak dengan slot ekspansi yang ada pada mainboard yang akan dipasang.

Ada kartu jaringan yang dapat dipasangkan ke dalam slot ISA, PCI atau PCI Express x1. Saat ini slot tipe ISA sudah mulai tidak banyak lagi beredar. Saat ini slot PCI masih digunakan sebagai slot standard yang ada di PC.

Untuk notebook Anda bisa gunakan kartu jaringan PCMCIA. Dimana PCMCIA merupakan slot ekspansi yang digunakan pada notebook. Kartu jaringan ini, pemasangannya tidak sulit, cukup dimasukkan ke dalam



Gambar 18 Kartu jaringan 3COM

port PCMCIA yang ada pada setiap Notebook dan tidak perlu dibongkar atau covernya dibuka. Cukup ditancapkan dari bagian pinggir atau di depan Notebook tersebut.

- **Jenis Protokol**

Adalah dukungan terhadap kabel atau kecepatan dalam mentransfer data. Saat ini dikenal beberapa protokol untuk sebuah kartu jaringan, diantaranya Ethernet dan Fast Ethernet, Token Ring dsb. Dan yang paling populer saat ini adalah protokol jenis Fast Ethernet. Karena merupakan teknologi yang memberikan kecepatan yang tinggi dengan biaya yang terjangkau.

## 6.2 Konsentrator



Gambar 19 Switch 16 port

Sebuah Konsentrator adalah sebuah perangkat yang menyatukan kabel-kabel network dari tiap-tiap workstation, server atau perangkat lain. Dalam topologi bintang (star), kabel twisted pair datang dari sebuah workstation masuk ke dalam hub. Dalam sebuah konsentrator pada umumnya memiliki lebih dari satu port: 4, 8, 16 atau 24 port. Oleh karena itu dalam merancang suatu jaringan Anda harus sesuaikan jumlah node di jaringan dengan jumlah port yang ada di konsentrator. Apabila kurang maka terpaksa Anda harus menambah konsentrator.

Ada berbagai jenis konsentrator yang ada di pasaran. Oleh karena itu Anda harus cermat dalam memilih sesuai dengan kebutuhan Anda.

### 1. Repeater

Adalah suatu perangkat jaringan yang digunakan untuk memperkuat sinyal yang melemah. Sebagai contoh pada jaringan twisted pair bila panjang kabel 100 meter maka sinyal menjadi melemah sehingga repeater digunakan. Pada repeater device tidak melakukan pengaturan apapun sehingga akan meneruskan sinyal apapun yang diterimanya.

### 2. Hub

Sering disebut multiport repeater, karena sama seperti repeater maka hub akan memperkuat dan meneruskan sinyal yang diterimanya ke semua portnya. Sehingga apabila suatu jaringan yang menggunakan hub dapat dikatakan jaringan tersebut

memiliki topologi star sekaligus bus. Dalam jaringan bus dikenal suatu istilah yang disebut *collision* yaitu peristiwa berbenturannya sinyal-sinyal dalam jaringan. Hal ini disebabkan semua sinyal jaringan melewati satu jalur yang sama. Pada jaringan skala kecil hub akan menjadi pilihan yang tepat karena memberikan akses jaringan yang cukup cepat. Tetapi apabila jumlah komputer pada jaringan bertambah maka *collision* akan semakin sering terjadi, akibatnya kecepatan akan berkurang.

Untuk saat ini hub sudah jarang dipakai dan sudah tidak ada di pasaran. Tetapi hub sering dianalogikan sebagai konsentrator. Sehingga tidak jarang konsentrator jenis lain disebut sebagai hub juga.

### 3. Bridge

Adalah suatu perangkat yang memiliki kegunaan yang sama dengan repeater. Perbedaanya bridge membagi jaringan menjadi segmen-segmen. Pembagian segmen ini berdasarkan MAC address yang dimiliki oleh kartu jaringan yang terhubung dengan port-port bridge. Sehingga tidak semua sinyal yang diterima oleh bridge akan diteruskan, tergantung letak node asal dan tujuan terhubung dengan port yang mana.

### 4. Switch

Sering disebut sebagai multiport bridge. Berbeda dengan hub, pada switch tidak terjadi *collision*. Pada saat komputer mengirim sinyal ke komputer lain di jaringan, switch akan membuat jalur virtual yang menghubungkan port yang terhubung dengan kedua komputer tersebut. Oleh karena itu switch pada jaringan dengan komputer banyak tidak mengalami penurunan kecepatan.

Terdapat jenis switch yang disebut manageable switch yaitu switch yang dapat diatur. Switch jenis ini memiliki fitur yang lebih, seperti: spanning tree protocol, VLAN, trunking, dll. Karena switch jenis ini tergolong jauh lebih mahal, maka lebih banyak digunakan pada perusahaan-perusahaan besar. Switch merupakan jenis konsentrator yang paling banyak dipasaran, karena lebih murah dan performa lebih baik daripada hub.

### 5. Router

Berbeda dengan konsentrator yang lain, router tidak hanya menghubungkan komputer-komputer di jaringan, tetapi juga menghubungkan LAN dengan jaringan yang lain. Misalnya menghubungkan LAN dengan internet. Pada umumnya router dapat Anda

atur dengan menggunakan web atau di-remote dengan terminal. Adapun jenis router yang sering dijumpai di pasaran ADSL router, wireless router, dll.

## 6. Access Point

Adalah konsentrator yang digunakan pada jaringan *wireless*. Semua node di jaringan *wireless* dihubungkan dengan alat ini. Access point pada umumnya memiliki port untuk terhubung dengan jaringan kabel sehingga dapat menghubungkan jaringan kabel dan *wireless*. Access point hanya memberikan koneksi jaringan pada area jangkauannya, yang sering disebut sebagai *hotspot*.

## 7. Wireless Router

Adalah sejenis access point yang dapat menghubungkan jaringan *wireless* dengan jaringan yang lain. Pada wireless router terdapat port yang terhubung dengan jaringan kabel dengan tulisan “internet” dan “LAN”. Dimana “internet” dimaksudkan untuk ke jaringan yang terhubung ke internet dan kabel yang terhubung pada port “LAN” berada pada jaringan yang sama dengan jaringan *wireless*. Wireless Router merupakan pilihan yang tepat untuk membagi akses internet ke jaringan *wireless* dengan mudah.



Gambar 20 Wireless router LinkSys

## 8. Wireless Bridge

Adalah sejenis access point yang dapat meneruskan sinyal *wireless* dari access point lain. Fungsi dari wireless bridge hampir sama seperti wireless repeater.

Tidak semua jaringan membutuhkan konsentrator. Pada jaringan peer to peer sebuah kabel utp dapat digunakan untuk menghubungkan dua buah komputer. Sedangkan pada jaringan wireless disebut dengan jaringan ad-hoc, dimana antara dua komputer terhubung langsung melalui kartu wireless.

## Bab 7

# Media Transmisi

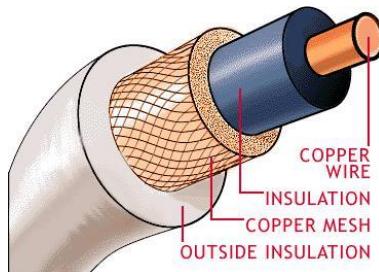
### Tujuan

- Mengetahui Media Penghubung Jaringan
- Mengetahui Media Penghubung Tanpa Kabel
- Dapat Memcramping Kabel UTP

Salah satu yang mempengaruhi kecepatan dari jaringan Anda adalah media transmisi yang Anda gunakan. Pemilihan media transmisi yang sesuai maka akan mengefektifkan jaringan Anda. Media transmisi ada dua macam, yaitu menggunakan kabel (*wired*) dan tanpa kabel/nirkabel (*wireless*)

### 7.1 Media Kabel (Wired)

- **Kabel Coaxial**



Gambar 21 Bagian dalam kabel coaxial

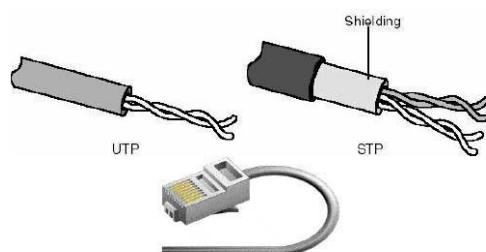
Adalah tipe kabel yang bentuknya sama dengan kabel antena TV. Jenis kabel ini memiliki pelindung (*shielding*) dan insulator untuk pemisah kedua konduktor menyebabkan reliabilitas yang tinggi pada transfer data kecepatan tinggi dengan jarak yang jauh. Oleh karena itu sering dipakai pada *outdoor*. Pada bagian ujung-ujungnya dibutuhkan terminator untuk

menutup jaringan. Kecepatan maksimal yang diberikan 10 Mbps dan 100 Mbps. Kabel coaxial dibagi ke dalam dua tipe:

- Thinnet (10 Base 2): Menggunakan kabel thin coaxial (RG-58) dengan panjang 0,5-185m, interkoneksi antar device dihubungkan dengan konektor “T”, jumlah komputer maksimal yang terhubung dalam satu jalur 30 PC.
- Thicknet: Menggunakan kabel thick coaxial (RG-8) dengan panjang 2,5-500m. Jumlah komputer terhubung maksimal 100 PC dalam satu jalur, dimana pada kabel ini dibutuhkan transceiver antara komputer dengan kabel jaringan. Panjang kabel transceiver maksimal 50m.

- **Kabel Twisted Pair**

Adalah tipe kabel yang terdiri atas 8 kabel kecil yang saling berpilin berpasangan. Jenisnya dibagi atas UTP (*Unshielded Twisted Pair*) dan STP (*Shielded Twisted Pair*). Untuk STP diberikan pelindung tambahan di setiap pasangan kabel untuk memberi proteksi tambahan terhadap induksi. Konektor yang dipakai RJ-45, panjang maksimal 100m, kecepatan transfer data 10Mbps (10 Base TX), 100Mbps (100 Base TX), dan 1000Mbps (1000 Base TX dengan kabel CAT 5e).



Gambar 22 Kabel twisted pair

Kabel ini menjadi kabel yang umum dipakai pada pemasangan jaringan dalam ruangan disebabkan dengan kecepatan transfer data yang tinggi dengan biaya yang relatif murah.

- **Kabel Fiber Optik**

Adalah jenis kabel yang berbeda dengan yang lain dimana core (inti) dari kabel ini berupa serat optic, dan yang dikirimkan bukan listrik melainkan cahaya. Cahaya dihantarkan dengan 2 cara yaitu dengan sistem pemantulan didalam kabel pada kabel multimode dan dihantarkan lurus di dalam kabel pada kabel singlemode. Kabel dapat mengkoneksikan data hingga 2000m pada multimode dan 3000m pada singlemode. Karena yang dihantarkan adalah cahaya maka kecepatannya jauh lebih cepat dibanding dengan yang lain, yaitu mencapai hingga 10 Gbps. Kabel fiber optik pada umumnya digunakan untuk mengkoneksikan jaringan yang memiliki jarak yang sangat jauh yang membutuhkan kecepatan tinggi.



Gambar 23 Kabel fiber optik

## 7.2 Media Nirkabel (Wireless)

Adalah jenis sambungan tanpa kabel, untuk mengirimkan sinyal jaringan digunakan gelombang radio.

- **Infra Red**

Infra merah (infra red) adalah radiasi elektromagnetik dari panjang gelombang lebih panjang dari cahaya tampak, tetapi lebih pendek dari radiasi gelombang radio. Namanya berarti "bawah merah" (dari bahasa Latin *infra*, "bawah"), merah merupakan warna dari cahaya tampak dengan gelombang terpanjang. Radiasi inframerah memiliki jangkauan tiga "order" dan memiliki panjang gelombang antara 700 nm dan 1 mm. Inframerah ditemukan secara tidak sengaja oleh Sir William Herschell, astronom kerajaan Inggris ketika ia sedang mengadakan penelitian mencari bahan penyaring optis yang akan digunakan untuk mengurangi kecerahan gambar matahari pada teleskop tata surya

- **Bluetooth**

Nama "bluetooth" berasal dari nama raja di akhir abad sepuluh, Harald Blatand (Abad 10) yang di Inggris juga dijuluki Harald Bluetooth kemungkinan karena memang giginya berwarna gelap. Ia adalah raja Denmark yang telah berhasil menyatukan suku-suku yang sebelumnya berperang, termasuk suku dari wilayah yang sekarang bernama Norwegia dan Swedia. *Bluetooth* adalah spesifikasi industri untuk jaringan kawasan pribadi (*personal area networks* atau PAN) tanpa kabel.

Bluetooth menghubungkan dan dapat dipakai untuk melakukan tukar-menukar informasi di antara peralatan-peralatan. Spesifikasi dari peralatan Bluetooth ini dikembangkan dan didistribusikan oleh kelompok Bluetooth Special Interest Group. *Bluetooth* beroperasi dalam pita frekuensi 2,4 GHz dengan menggunakan sebuah *frequency hopping receiver* yang mampu menyediakan layanan komunikasi data dan suara secara real time antara host-host bluetooth dengan jarak terbatas. Kelemahan teknologi ini adalah jangkauannya yang pendek dan kemampuan transfer data yang rendah.

- **WiFi**

Adapun standar elektronika yang digunakan adalah IEEE 802.11 dimana jenisnya sebagai berikut:

Spesifikasi	Frekwensi	Kecepatan	Kekuatan Sinyal Outdoor
802.11 a	5 GHz	54 Mbps	50 m
802.11 b	2,4 GHz	11 Mbps	100 m
802.11 g	2,4 GHz	54 Mbps	100 m
802.11 n	2,4 / 5 GHz	600 Mbps	250 m

IEEE802.11n memiliki kecepatan hingga 600Mbps tetapi untuk saat ini hanya bisa digunakan bila menggunakan wifi card dan access point yang bermerk sama. Pada wireless realibilitas dan kecepatan jaringan dipengaruhi oleh jumlah penghalang dan jarak antara satu node dengan node yang lain. Untuk security digunakan sistem pengamanan SSID yang bisa dikatakan sebagai nama jaringan wireless dan pada umumnya dilengkapi key seperti WEP atau WPA.

- **Wimax**

WiMAX adalah singkatan dari Worldwide Interoperability for Microwave Access, merupakan teknologi akses nirkabel pita lebar (broadband wireless access atau disingkat BWA) yang memiliki kecepatan akses yang tinggi dengan jangkauan yang luas. Yang membedakan WiMAX dengan Wi-Fi adalah standar teknis yang bergabung di dalamnya. Jika WiFi menggabungkan standar IEEE 802.11 dengan ETSI (European Telecommunications Standards Intitute) HiperLAN sebagai standar teknis yang cocok untuk keperluan WLAN, sedangkan WiMAX merupakan penggabungan antara standar IEEE 802.16 dengan standar ETSI HiperMAN. Standar keluaran IEEE banyak digunakan secara luas di daerah asalnya, Amerika, sedangkan standar keluaran ETSI meluas penggunaannya di daerah Eropa dan sekitarnya. Untuk membuat teknologi ini dapat digunakan secara global, maka diciptakanlah WiMAX. Kedua standar yang disatukan ini merupakan standar teknis yang memiliki spesifikasi yang sangat cocok untuk menyediakan koneksi berjenis broadband lewat media wireless atau dikenal dengan BWA.

## Bab 8

### Membangun Jaringan Komputer Lokal (LAN)

#### Tujuan:

- Mengetahui Desain Jaringan LAN
- Instalasi Jaringan LAN
- Praktek Crimping Kabel UTP dengan RJ-45

#### 8.1 Desain Jaringan

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

Jenis LAN	Topologi	Bus				
		Star				
		Ring	Token Ring			
			Token Bus			
		Mesh				
	Kecepatan	Menengah ( beberapa s/d 20 Mbps)				
		Tinggi (100 s/d ratusan Mbps)				
		Ultra (lebih dari 1 Gbps)				
	Media Transmisi	Kabel (Wireline)				
		Gelombang Radio (Wireless)				
	Tingkatan LAN	Utama (Backbone LAN)				
		Biasa (floor LAN)				

Gambar 24 Persiapan merancang jaringan

#### 8.2 Instalasi Jaringan

Instalasi jaringan komputer terbagi dalam dua bagian, yaitu instalasi perangkat keras (*Hardware*) dan instalasi perangkat lunak (*Software*). Untuk instalasi hardware maka di

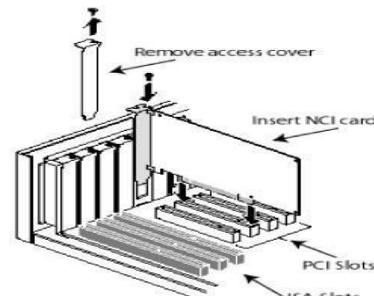
samping komponen LAN yang perlu dipersiapkan seperti yang telah diuraikan di atas, perlu juga dipersiapkan *setting* ruangan, gambar jaringan yang akan dipasang dan *toolset*-nya. Yaitu peralatan bantu yang akan digunakan untuk pekerjaan instalasi yang meliputi: tang penjepit, crimping, pemotong kabel, obeng, cable duck (penutup kabel).

Lebih jelasnya dapat disebutkan sebagai berikut :

- Obeng kembang (sebaiknya yang bermagnet)
  - Obeng minus
  - Test pen
  - Tang penjepit/pemotong kabel
  - Pinset atau tang buaya
  - Crimping (tang untuk memasang konektor RJ-45)
  - LAN tester (jika ada)
- 
- **Instalasi Kartu Jaringan (NIC)**

Yaitu pemasangan kartu jaringan pada slot ekspansi yang tersedia dalam mainboard.

    1. Sebelum memasang kartu jaringan ke slot yang ada di PC, siapkan terlebih dahulu kartu jaringan tersebut. Contoh kartu jaringan yang akan dipasang ke salah satu slot PCI.
    2. Matikan power atau cabut kabel power CPU dari stop kontak. Buka casing box CPU Anda menggunakan obeng kembang.
    3. Setelah casing terbuka, pasang atau tancapkan kartu jaringan / ethernet card ke salah satu socket atau slot ekspansi PCI yang ada. Jangan lupa pasang mur pada plat bagian atasnya sehingga akan kokoh dan tidak mudah goyang.
    4. Setelah kartu jaringan terpasang, maka sebelum casing box-nya ditutup, pasang kembali kabel powernya dan aktifkan komputer tersebut. Untuk saat ini, kartu jaringan pada umumnya mudah dikenali oleh sistem operasi yang digunakan (*Plug and Play*) sehingga memungkinkan *setup* atau *setting* NIC dalam penentuan memory address, DMA dan IRQ-nya langsung dari *software*. Bila tidak dikenali, maka kita memerlukan



Gambar 25 Pemasangan NIC di slot PCI

*software driver* bawaan dari NIC tsb. Untuk NIC yang sudah populer, umumnya dengan sangat mudah dikenali oleh sistem operasi yang kita pergunakan. Bila tidak, maka kita dapat juga memilih *software driver* yang kompatibel dengan NIC yang kita pasang tersebut.

5. Setelah kartu jaringannya dikenali oleh CPU, maka langkah selanjutnya adalah melakukan *setting* jaringannya melalui sistem operasi yang dipergunakan.

- **Instalasi Kabel Jaringan (UTP)**

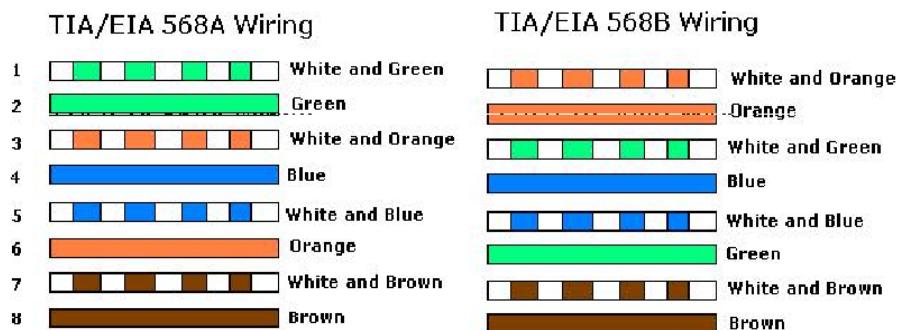
Kita asumsikan bahwa kabel jaringan yang akan kita pergunakan adalah jenis UTP, maka sebelum melakukan pemotongan kabel dari box-nya, lakukan pengukuran sesuai dengan jarak antara Server dengan switch dan jarak antara switch dengan Workstation. Lakukan semua itu satu persatu, dengan rincian sebagai berikut:

1. Ukur panjang kabel UTP dari switch ke komputer sesuai keperluan, lalu potong menggunakan tang pemotong. Sebaiknya jangan terlalu ngepas/kencang (akan menyulitkan ketika ada pergeseran atau pemindahan posisi/lokasi. Untuk pemasangan dari komputer server ke switch jangan melebihi dari 8 meter. Untuk pemasangan dari workstation ke switch di ruangan server jangan melebihi 12 meter. Untuk pemangan ke device lainnya jangan melebihi dari 100 meter.
2. Gunakanlah penutup kabel dan gunakanlah jalur yang tidak dapat dilihat atau dilewati orang agar kabel tertata rapi dan tidak merusak pemandangan ruangan. Penggunaan wall socket akan lebih baik. Setelah dilakukan pemotongan, lakukan pemasangan konektor RJ-45 di kedua ujung kabel UTP tersebut dengan memperhatikan ketentuan urutan warna kabel dalam pemasangan konektor.

- **Memasang RJ-45 ke kabel UTP**

Pemasangan kabel UTP ke konektornya memang tidak terlalu sulit. Yang diperlukan hanyalah Crimping untuk mengupas bagian luar ujung kabel dan sekaligus sebagai penjepitnya, kemudian mengatur susunan warna kabelnya sesuai dengan ketentuan. Namun demikian perlu kehati-hatian, karena jika sudah terlanjur dipasang dan ternyata salah, maka tidak bisa dilakukan perbaikan. Yang bisa dilakukan hanyalah memotong ujung kabel yang sudah terpasang konektor tersebut. lalu membuangnya dan memasang konektor baru. Langkah-langkahnya sebagai berikut :

1. Kupas penutup bagian luar dari kabel Anda dengan hati-hati. Untuk melakukan pengupasan Anda bisa gunakan pisau yang ada di-*crimping*. Untuk panjang dari bagian yang dikupas sedikit lebih panjang dari panjang konektor sekitar 3 cm.
2. Kemudian Anda urai kabel UTP tersebut dan luruskan sehingga rata di tangan Anda. Kemudian Anda susun sesuai standar penyusunan dari kabel twisted pair yaitu:

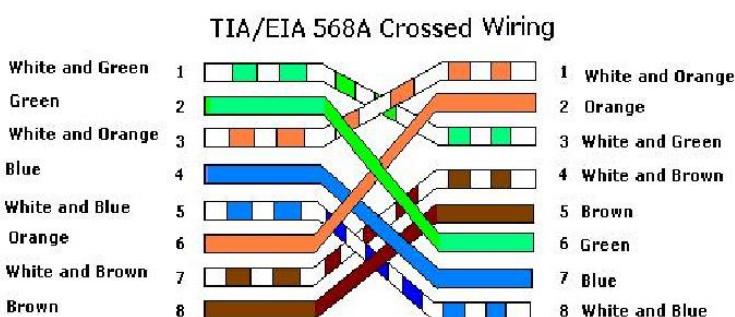


Gambar 26 Susunan kabel 568A dan 568B

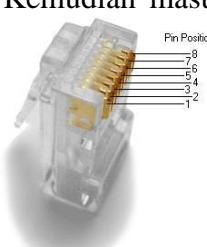
Dua susunan tersebut dapat dikonfigurasikan menjadi dua tipe konfigurasi, yaitu :

- Straight-through, kabel UTP disusun sama di kedua ujungnya. Misalnya di ujung pertama tipe 568A dan di ujung kedua tipe 568A juga. Konfigurasi kabel UTP ini digunakan untuk menghubungkan hub / switch dengan PC atau sebaliknya.
- Crossover, kabel UTO disusun berbeda di kedua ujungnya. Misalnya di ujung pertama tipe 568A dan di ujung kedua tipe 568B. Konfigurasi kabel UTP ini digunakan untuk menghubungkan hub / switch dengan hub / switch atau PC dengan PC. Tipe kabel ini tepat untuk pembuatan jaringan tanpa adanya konsentrator atau peer-to-peer.

Adapun untuk crossover pada jaringan 1000Mbps konfigurasi crossover di atas tidak bisa memberikan kecepatan yang maksimal, hal ini disebabkan pada gigabit ethernet digunakan keseluruhan kabel untuk mengirim dan menerima data. Adapun konfigurasi crossover untuk jaringan gigabit ethernet seperti gambar di bawah.



Gambar 27 Crossover cable pada gigabit ethernet

3. Setelah lurus dan disusun, rapatkan kabel-kabel tersebut kemudian Anda ratakan sekaligus memendekkan tersebut agar bisa masuk ke dalam konektor RJ-45. Untuk melakukan ini Anda bisa ukur panjang kabel yang disisakan dengan panjang konektor. Usahakan jangan terlalu pendek (akan susah dimasukkan) atau terlalu panjang (akan sering terjadi cross talk yang menyebabkan koneksi kabel kurang baik).
4. Kemudian masukkan kabel yang sudah rata dan pendek ke dalam konektor RJ-45.  


Perhatikan susunan kabel ketika dimasukkan ke dalam konektor. Pastikan juga ujung kabel UTP sudah menyentuh ujung dinding dari konektor RJ-45 sehingga apabila tampak dari depan Anda bisa melihat kabel tembaga di dalamnya. Setelah itu usahakan pelindung bagian luar juga masuk ke dalam konektor, agar kabel menjadi lebih kuat dan tidak mudah rusak.
5. Setelah Anda yakin kabel sudah terpasang dengan rapi Anda bisa melakukan crimping pada kabel Anda. Untuk lebih yakin Anda bisa lakukan dua kali.
6. Lakukan pemasangan konektor diujung kedua dan lakukan pengetesan dengan menggunakan LAN Tester



Gambar 28 Susunan kabel



Gambar 30 Crimping

## Bab 9

### Jaringan Nirkabel

#### Tujuan:

- Mengetahui tahapan dalam membangun jaringan nirkabel
- Mampu melakukan konfigurasi *access point*

#### 9.1 Tahapan Membangun Jaringan Nirkabel

Langkah pertama yang harus dilakukan adalah men-setup access point. Umumnya jaringan Wi-Fi memiliki jangkauan hingga 150 kaki (+ 45 m) sementara access point memiliki jangkauan yang dapat diperluas menggunakan repeater yang dapat memperkuat gelombang radio dari jaringan.

Tahapan membangun jaringan wireless adalah sebagai berikut:

- Memasang perangkat keras jaringan
- Mengkonfigurasi access point
- Menghubungkan access point ke jaringan kabel
- Menghubungkan client ke jaringan wireless
- Menguji jaringan



Gambar 31 Jaringan nirkabel

Masing-masing tahapan di atas akan dijelaskan lebih lanjut sebagai berikut:

### 9.2 Tahap 1 – Memasang perangkat keras jaringan

1. Memasang *wireless adapter* ke komputer dan perangkat dalam jaringan. Untuk laptop biasanya sudah tersedia secara *default*.
2. Letakkan *mounting point* pada posisi yang tepat pada *access point*.
  - Untuk penerimaan yang lebih baik, posisi *mounting point* sebaiknya agak lebih tinggi tapi jangan diletakkan tepat di atas perangkat *wireless*.
  - Arahkan kedua antenanya agar berada dalam posisi tegak lurus dengan tanah.
  - Ingat bahwa rintangan seperti dinding batu dapat mengganggu penerimaan sinyal. Oleh karena itu, sebaiknya tempatkan *access point* di tengah-tengah agar dapat melayani semua area yang diinginkan.

### 9.3 Tahap 2 – Mengkonfigurasi *access point*

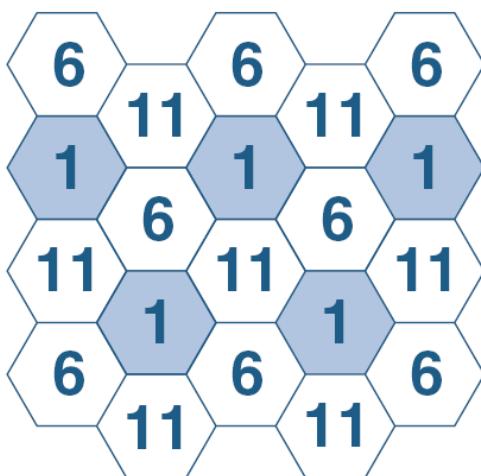
1. Masukkan stop kontak *access point* dan nyalakan.
2. Hubungkan komputer ke *access point* menggunakan kabel UTP.
3. Umumnya *access point* dapat dikonfigurasi melalui aplikasi berbasis web. Jalankan browser pada komputer Anda kemudian tuliskan IP address *access point* pada kolom URL browser. Selanjutnya akan menampilkan halaman login. Masukkan username dan password dari aplikasi konfigurasi *access point*. Ip address, username dan password *default* dari *access point* biasanya tercantum di bagian bawah *access point*.
4. Ubah username dan password *default*. Hal ini penting karena banyak perangkat yang dikirim dengan username dan password yang sama.
5. Konfigurasi *access point* sesuai dengan perintah instalasi.

Jika Anda berencana menghubungkan *access point* ke sebuah *router*, pastikan untuk menonaktifkan layanan DHCP pada *access point*. Kemudian masukkan alamat IP yang unik dan statik ke dalam *access point* yang berada dalam jangkauan alamat yang diizinkan *router*.

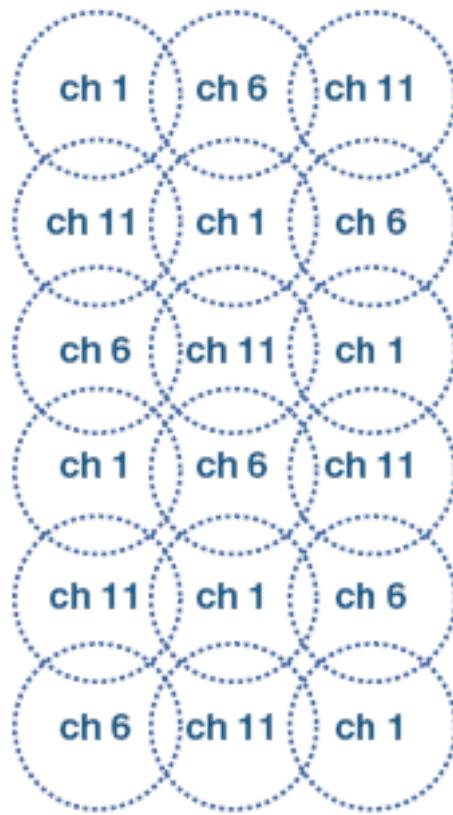
Pastikan Anda memeriksa konfigurasi berikut ini:

- Select AP mode. Banyak *access point* dapat dikonfigurasi untuk beroperasi dalam aturan yang spesifik, seperti sebagai *access point*, *client/slave access point*, *repeater*, dll. Anda dapat memilih mode *access point* pada opsi Access Point (AP).

- Enable or disable DCHP. Kebanyakan *access point* yang digunakan di rumah menggunakan *dynamic host configuration protocol* (DHCP) yang diatur secara *default*, yang secara otomatis mengkonfigurasi komputer klien dengan alamat IP, gateway, dan informasi DNS yang benar. Jika *access point* yang Anda gunakan menyediakan opsi ini, maka opsi ini adalah yang paling mudah untuk diimplementasikan. Opsi yang lain adalah membuat sebuah subnet dan secara manual mengkonfigurasi semua alamat IP, gateway dan informasi DNS untuk setiap perangkat dalam jaringan.
- Set Service Set ID (SSID). Masukkan nama yang unik dan mudah dikenali untuk jaringan nirkabel Anda. Nama ini adalah nama *broadcast* yang dapat dilihat oleh klien *wireless* ketika mencari jaringan.
  - Anda harus selalu mengubah SSID untuk mencegah orang lain menggunakan jaringan Anda.
  - Pastikan Anda menggunakan nama yang sama untuk semua perangkat *wireless* yang menggunakan *access point* ini.
  - Pastikan semua komputer yang terhubung ke *access point* ini memiliki konfigurasi SSID yang sama seperti konfigurasi SSID pada *access point*.
  - Anda dapat mematikan SSID *broadcasting* untuk menyembunyikan identitas jaringan Anda. Dengan demikian klien Anda tidak akan dapat mendeteksi jaringan Anda secara otomatis.
- Set the Channel. Pilih *channel* yang akan digunakan oleh semua perangkat *wireless* untuk berkomunikasi melalui *access point* ini. Konfigurasi ini akan mengubah frekuensi radio dari jaringan *wireless* Anda. Disarankan Anda menggunakan *channel* 1, 6 atau 11.
  - Pastikan semua komputer yang terhubung ke *access point* Anda memiliki konfigurasi *channel* yang sama dengan konfigurasi *access point* Anda.
  - Jika Anda menggunakan dua *access point* pada satu jaringan, berikan *channel* yang berbeda untuk setiap *access point*.
  - Pada *access point* yang saling bersinggungan areanya gunakan *channel* yang berbeda.



Gambar 32 Perencanaan channel access point pada satu lantai



Gambar 33 Perencanaan channel access point pada gedung bertingkat

- (Optional) Enable WEP and define keys. Jika *access point* Anda tidak mengaktifkan enkripsi Wired Equivalent Privacy (WEP) secara default, Anda dapat mengaktifkan opsi ini untuk melindungi jaringan Anda. Konfigurasi ini akan memperbolehkan Anda mengatur key (kunci) yang mengenkripsi semua data yang dikirimkan ke *access point*.
  - Jika Anda mengaktifkan WEP, pastikan Anda memasukkan kunci yang sama pada semua sistem yang terpasang pada *access point* Anda.
  - Jika Anda menggunakan LinkSys *router* tapi tidak menggunakan kartu *wireless* (*wireless card*) LinkSys pada sistem di *client*, jangan gunakan auto-key generator. Auto-key generator hanya akan bekerja dengan kartu *wireless* LinkSys.
  - Kebanyakan *access point* menawarkan enkripsi WEP bertingkat yang bervariasi mulai 64 bit hingga 128 bit atau 256 bit. Lebih tinggi akan lebih baik, walaupun konfigurasi yang tinggi dapat mempengaruhi kinerja. Jika WEP diaktifkan,

semua klien harus diatur dengan level enkripsi yang sama dengan *access point* Anda.

#### 9.4 Tahap 3 – Menghubungkan access point ke jaringan kabel

Jika Anda menggunakan *router*, *switch*, atau modem kabel/DSL untuk mengakses Internet, Anda harus menghubungkan *access point* Anda ke perangkat tersebut.

1. Gunakan kabel UTP kategori 5 ke atas yang cukup panjang untuk menghubungkan *access point* ke perangkat *router*, *switch*, atau modem kabel/DSL.
2. Pasangkan salah satu ujung kabel UTP ke Ethernet port berlabel WAN atau Internet yang terletak pada bagian belakang *access point*.
3. Pasangkan ujung kabel yang lain ke Ethernet port pada perangkat yang Anda gunakan untuk berhubungan ke Internet:
  - Untuk menghubungkan ke modem kabel, pasang ke port LAN.
  - Untuk menghubungkan ke *router*, pasang pada port manapun kecuali port yang berlabel WAN.
  - Untuk menghubungkan ke hub atau *switch*, pasang ke port manapun kecuali yang berlabel UPLINK.

#### 9.5 Tahap 4 – Menghubungkan client ke jaringan nirkabel

Nyalakan semua perangkat yang ingin Anda tambahkan ke jaringan nirkabel. Konfigurasi semua klien menurut instruksi di bawah ini. Pastikan semua klien memiliki update terbaru dari sistem operasi dan *servive pack* yang sudah terpasang.

- Pastikan kartu jaringan nirkabel klien dikonfigurasi untuk menggunakan mode Infrastructur atau Access Point (AP) , bukan mode Ad Hoc .
- Pastikan bahwa SSID, channel, dan konfigurasi WEP untuk setiap klien sama dengan konfigurasi pada *access point*.

#### 9.6 Tahap 5 – Menguji koneksi jaringan

Ikuti langkah-langkah di bawah ini untuk memeriksa konfigurasi *access point* Anda:

1. Pastikan *access point* Anda dalam keadaan hidup dan semua perangkat wireless berada dalam jangkauan *access point*.

2. Umumnya kartu jaringan nirkabel memiliki program yang secara otomatis akan mencari jaringan nirkabel. Menggunakan klien *wireless* apapun, scan jaringan. Kemudian pilih nama jaringan dan aktifkan hubungan ke *access point*. Jika koneksi jaringan tidak didapat, coba beberapa solusi berikut ini :
  - Cabut steker *access point* untuk beberapa menit dan pasangkan kembali, kemudian uji kembali koneksi jaringan Anda.
  - Pastikan perangkat Anda cukup dekat dengan *access point*, jika tidak geser agar mendekati *access point*.
  - Pastikan tidak ada benda yang menghalangi jangkauan *access point*.
  - Sesuaikan antena *access point* atau antena adapter dari perangkat Anda (jika ada).
  - Pastikan semua perangkat memiliki *channel* dan SSID yang sama.
  - Pastikan semua perangkat menggunakan konfigurasi enkripsi yang tepat.
  - Periksa konfigurasi LAN dan WAN

Untuk pengujinya, lakukan langkah-langkah berikut ini:

- Pastikan *access point* menyala dan semua perangkat *wireless* berada dalam jangkauan *access point*.
- *Restart* (atau nyalakan) semua perangkat yang terhubung ke jaringan dan periksa apakah Anda dapat terhubung ke jaringan.
- Semua perangkat *wireless* yang telah dikonfigurasi dengan baik seharusnya secara otomatis terhubung ke jaringan ketika Anda menggunakan aplikasi yang mengakses jaringan atau Internet. Jika Anda tidak terhubung, coba beberapa solusi berikut ini:
  - Periksa konfigurasi TCP/IP pada perangkat *wireless* – contohnya, apakah menggunakan DHCP, atau alamat IP ditentukan secara manual?
  - Matikan perangkat *wireless* dan nyalakan kembali.
  - Untuk sistem yang menggunakan DHCP, klik **Start** ketikkan ipconfig /release. Kemudian klik **Start** dan ketikkan ipconfig /renew.
  - Periksa *access point* apakah konfigurasinya sesuai dengan konfigurasi pada dokumen instalasi *access point*.

Jika Anda dapat melihat komputer lain pada jaringan Anda tapi tidak dapat mengakses Internet, berarti konfigurasi LAN Anda sudah tepat tetapi konfigurasi WAN (ISP) Anda tidak tepat. Buka router configuration utility atau browser address.

- Matikan *router* dan modem kabel, tunggu beberapa menit, kemudian nyalakan kembali keduanya.
- Tentukan domain atau DNS server yang berbeda pada konfigurasi WAN.
- Jika perlu, kosongkan nama domain pada konfigurasi WAN.
- Atau minta alamat IP yang baru untuk WAN Anda. Beberapa router configuration utility memiliki tombol untuk tugas ini.
- Periksa dokumentasi *router* dan hubungi ISP jika Anda tidak dapat memecahkan masalah ini.

Jika Anda dapat mengakses Internet tetapi tidak dapat melihat komputer lain yang berada di jaringan Anda, berarti konfigurasi ISP dan TCP/IP Anda sudah benar tapi konfigurasi klien LAN Anda mungkin salah. Lakukan langkah berikut:

- Matikan perangkat dan nyalakan kembali.
- Periksa Network ID, workgroup, domain, atau AppleTalk Zone dan lihat apakah konfigurasi Anda sama dengan komputer lain pada jaringan yang sama.

## Bab 10

### Konfigurasi Jaringan di Windows 10

#### Tujuan:

1. Dapat mengkonfigurasi jaringan di windows 10
2. Setting IP Address
3. Sharing file lewat jaringan LAN

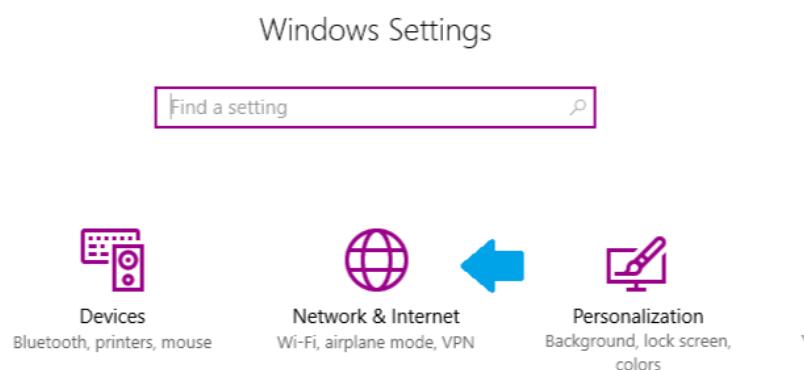
#### 10.1 Setting IP Address dan jaringan LAN pada Window 10

1. Pertama, Klik Start atau jendela windows 10 >> Kemudian klik **Settings**.



Gambar 34. Menu setting windows 10

2. Pada halaman settings, Klik **Network and Internet**



Gambar 35. Tampilan Network dan internet

### 3. Lalu pilih **Ethernet**



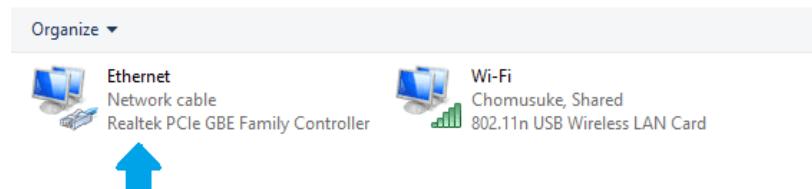
Gambar 36. Menu Ethernet windows 10

### 4. Pada bagian **Ethernet**, kemudian klik “**Change Adapter Setting**”



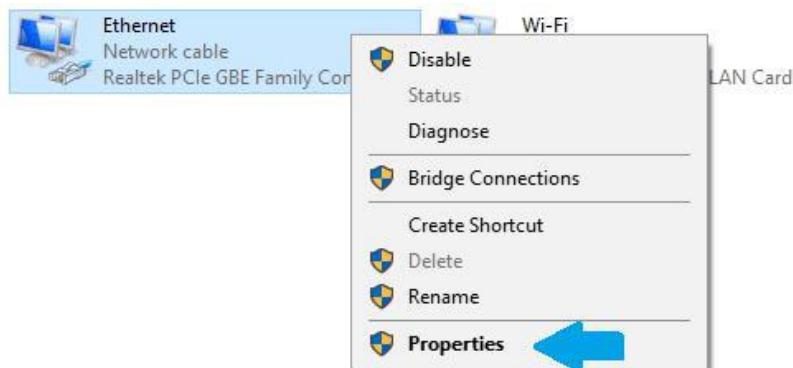
Gambar 37. Change adapter setting

### 5. Kemudian, disini Anda akan menemukan koneksi untuk lannya. Biasanya namanya “Local Area”, ‘Realtek PCI’ dan sebagainya.



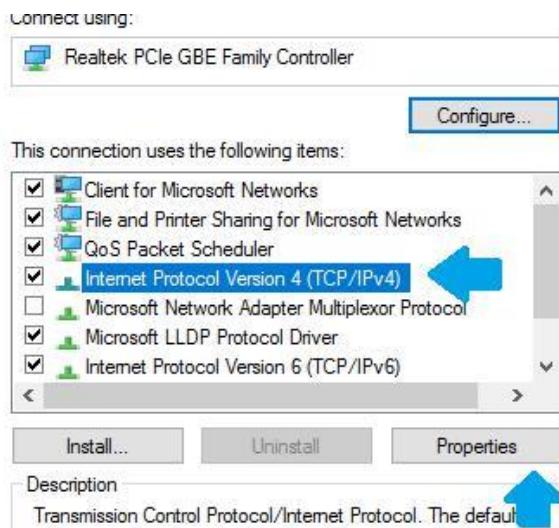
Gambar 38. Tampilan Adapter LAN

6. Klik kanan pada perangkat network kemudian pilih **Properties**



Gambar 39. Pilih Properties pada popup menu

7. Pada jendela **Local Area Connection Properties** Anda pilih **Internet Protocol Version 4 (TCP/IPv4)** dan klik pada **Properties**



Gambar 40. Local Area Network Properties

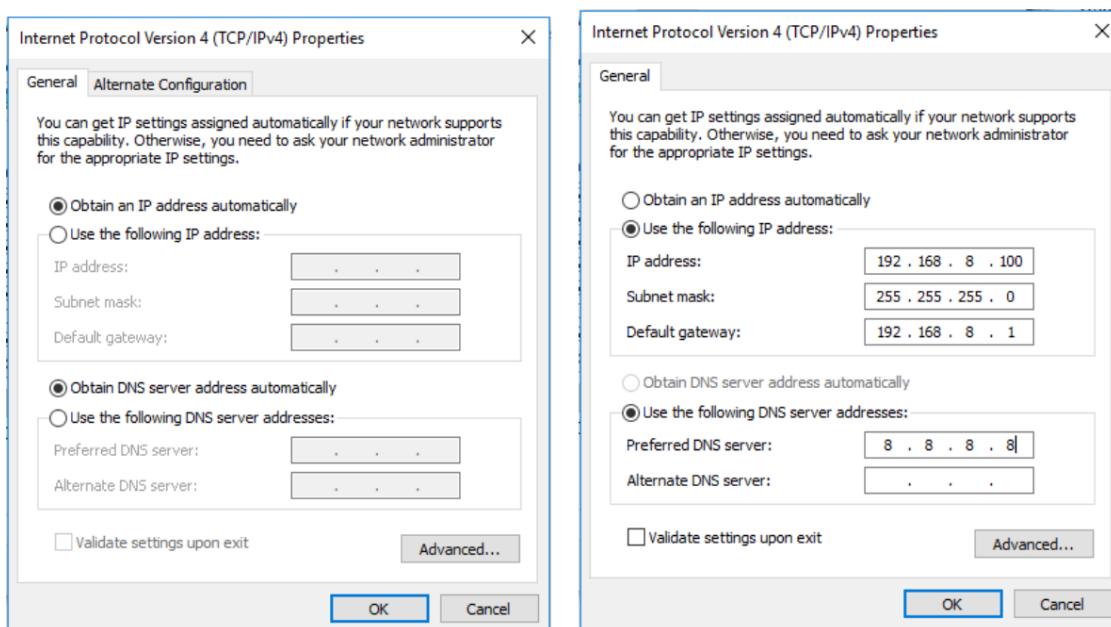
8. Pada jendela **Internet Protocol Version 4 (TCP/IPv4) Properties** masukkan konfigurasi IP address. Adapun yang perlu dimasukkan adalah:

- IP Address, untuk mengalamanan jaringan
- Subnet mask, untuk menentukan Network ID dan Host ID
- Default Gateway, adalah IP address dari komputer atau device yang digunakan untuk jalan keluar ke jaringan lain atau ke internet. Apabila

Anda langsung terhubung langsung ke modem maka biasanya IP address gateway adalah IP address modem.

- Preferred DNS Server, adalah IP address dari DNS server yang Anda gunakan. Dimana DNS digunakan untuk menerjemahkan nama domain menjadi IP address. Tanpa DNS Anda tidak bisa menggunakan nama domain, seperti yahoo.com, detik.com, nurulfikri.com, dan lain-lain. IP DNS Server umumnya didapatkan dari penyedia jasa internet.
- Alternate DNS Server, sama seperti Preferred DNS Server tetapi sebagai cadangan apabila Preferred DNS Server mati atau putus.

Konfigurasi IP address sendiri bisa menggunakan dua cara Automatic atau Manual. Bila Anda ingin menggunakan automatic Anda pilih pada "Obtain an IP address automatically" maka IP address di atas akan didapatkan dari DHCP server. Apabila Anda ingin menggunakan konfigurasi secara manual maka Anda pilih "Use the following IP address" dan Anda harus memasukkan IP address secara manual.



Gambar 41. Setting IP Address dengan Otomatis (DHCP) dan Setting IP Address dengan Manual (static)

9. Setelah itu Anda klik **OK** dan pada jendela **Local Area Connection Properties** Anda klik **OK** lagi atau **Close**. Perlu diingat sebelum Anda melakukan penutupan jendela **Local Area Connection Properties** maka konfigurasi IP address belum dijalankan.

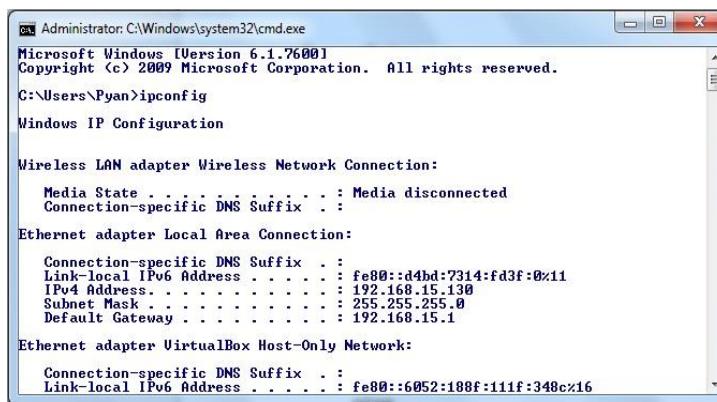
## 10.2 Pengujian jaringan pada windows 10

Setelah Anda mensetting IP address maka Anda bisa melakukan pengujian pada jaringan Anda dengan menggunakan fasilitas-fasilitas pada DOS di Windows 7, yaitu:

- ipconfig, digunakan untuk melihat konfigurasi jaringan di Windows 7 Anda.

Contoh penggunaan:

Ipconfig atau ipconfig /all



```
C:\> Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>Users\Pyan>ipconfig
Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
  Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . . . . . :
    Link-local IPv6 Address . . . . . : fe80::d4bd:7314:fd3f:0%11
    IPv4 Address . . . . . : 192.168.15.130
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.15.1
  Ethernet adapter VirtualBox Host-Only Network:
    Connection-specific DNS Suffix . . . . . :
    Link-local IPv6 Address . . . . . : fe80::6052:188f:111f:348c%16
```

Gambar 42 Hasil dari perintah ipconfig

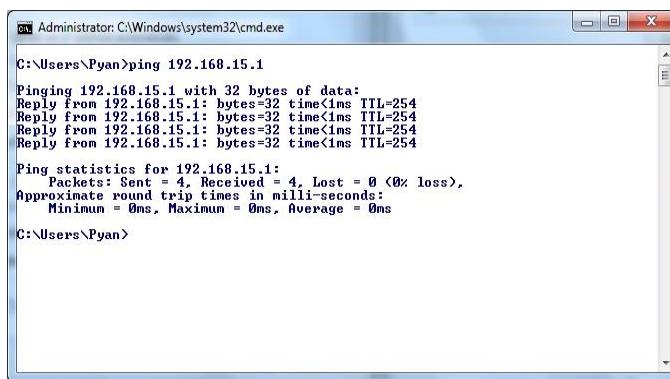
- ping, digunakan untuk melakukan pengecekan koneksi komputer di jaringan.

Sintaks perintah:

ping <ip\_address>

Contoh penggunaan:

ping 192.168.15.1



```
C:\> Administrator: C:\Windows\system32\cmd.exe
C:\>Users\Pyan>ping 192.168.15.1

Pinging 192.168.15.1 with 32 bytes of data:
Reply from 192.168.15.1: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.15.1:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>Users\Pyan>
```

Gambar 43 Hasil dari perintah ping

Pesan-pesan error pada perintah ping:

- Request timed out, komputer tujuan mati atau terputus.

- Destination host unreachable, konfigurasi IP address belum di set atau gateway belum di konfigurasi dan Anda mengakses komputer di jaringan lain.
- Hardware Error, kabel yang terhubung langsung dengan komputer Anda terputus atau tidak tersambung.
- nslookup, digunakan untuk pengecekan DNS. Dimana nslookup akan menampilkan IP address dari suatu domain. Bila error maka DNS belum diset atau DNS server dalam keadaan mati.

Sintaks perintah:

nslookup [options] host server

Contoh penggunaan:

nslookup google.co.id

nslookup yahoo.com



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Pyan>nslookup google.co.id
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:  google.co.id
Addresses: 2404:6800:4003:806::2003
           74.125.200.94

C:\Users\Pyan>nslookup yahoo.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:  yahoo.com
Addresses: 2001:4998:44:204:a7
           2001:4998:c:a66::2:4008
           2001:4998:58:c02::a9
           98.139.188.149
           98.138.253.109
           206.198.36.45

C:\Users\Pyan>
```

Gambar 44. Hasil dari perintah nslookup

- Tracert atau traceroute adalah perintah untuk menunjukkan rute yang dilewati paket untuk mencapai tujuan. Ini dilakukan dengan mengirim pesan Internet Control Message Protocol (ICMP) Echo Request Ke tujuan dengan nilai Time to Live yang semakin meningkat.

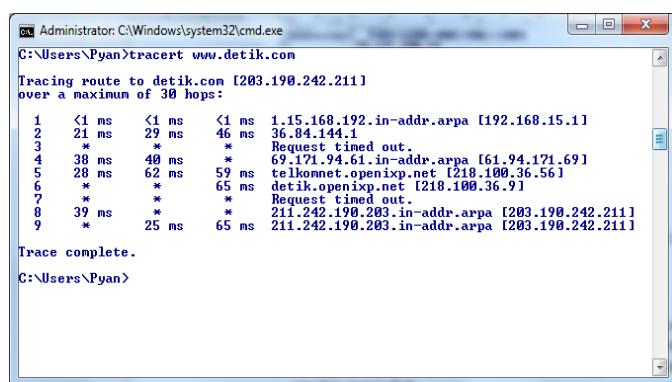
Rute yang ditampilkan adalah daftar interface router (yang paling dekat dengan host) yang terdapat pada jalur antara host dan tujuan. Contoh penggunaan tracert "tracert www.detik.com" disitu akan terlihat beberapa hop atau lompatan router mana saja yg dilewati dari komputer kita menuju www.detik.com.

Sintaks perintah:

tracert [options] target

Contoh penggunaan:

tracert www.detik.com



```

Administrator: C:\Windows\system32\cmd.exe
C:\Users\Pyan>tracert www.detik.com
Tracing route to detik.com [203.190.242.211]
over a maximum of 30 hops:
  1  <1 ms    <1 ms    <1 ms  1.15.168.192.in-addr.arpa [192.168.15.1]
  2  21 ms     29 ms    46 ms  36.84.144.1
  3  *          *          * Request timed out.
  4  38 ms     40 ms    *          69.171.94.61.in-addr.arpa [69.171.94.61]
  5  28 ms     62 ms    59 ms  telkomnet.openixp.net [218.100.36.56]
  6  *          *          65 ms  detik.openixp.net [218.100.36.91]
  7  *          *          * Request timed out.
  8  39 ms     *          *          211.242.198.203.in-addr.arpa [203.190.242.211]
  9  *          25 ms    65 ms  211.242.198.203.in-addr.arpa [203.190.242.211]

Trace complete.
C:\Users\Pyan>

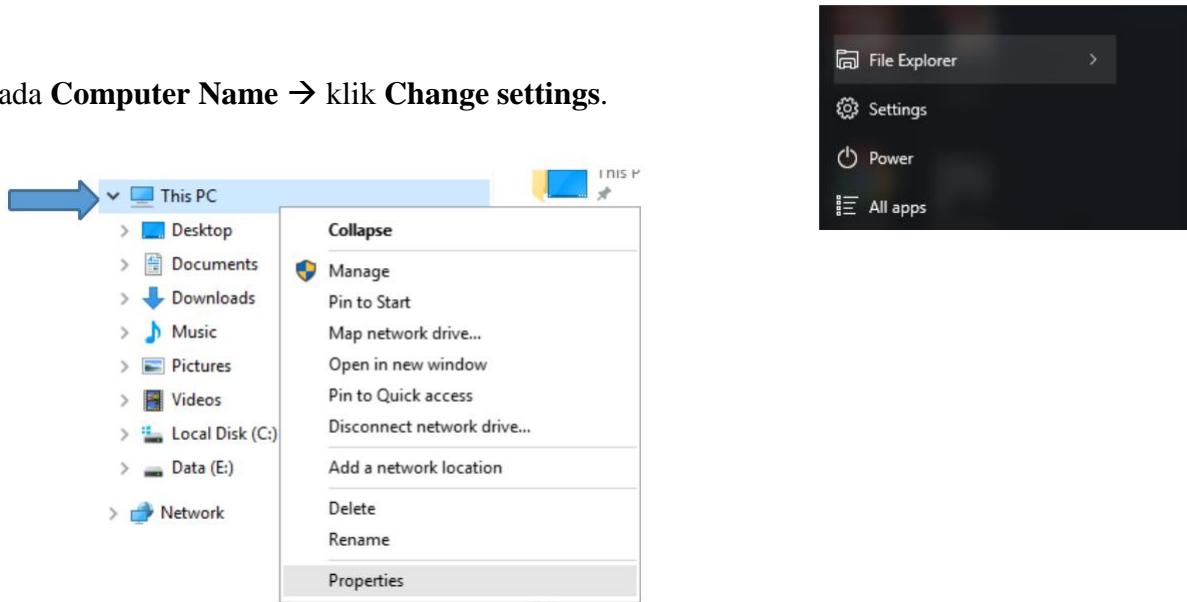
```

Gambar 45 Hasil dari perintah tracert

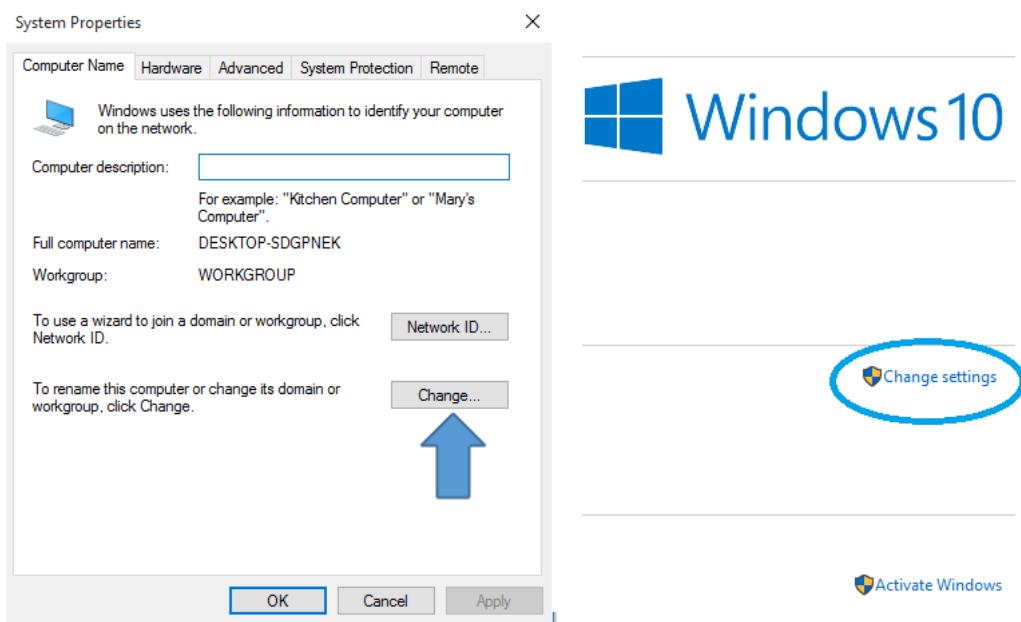
### 10.3 Memberi identitas Komputer sebagai anggota suatu Group dalam Windows 10

Agar komunikasi antar komputer dalam jaringan dapat berjalan dengan efektif, maka anggota grup dalam jaringan tersebut harus memiliki identitas. Untuk mengganti ataupun memberikan identitasnya, dapat dilakukan langkah-langkah berikut ini:

1. Klik **Start** atau jendela windows 10 kemudian pilih **File Explorer**



3. Kemudian pilih **Change Settings** kemudian muncul jendela computer name lalu klik **Change**



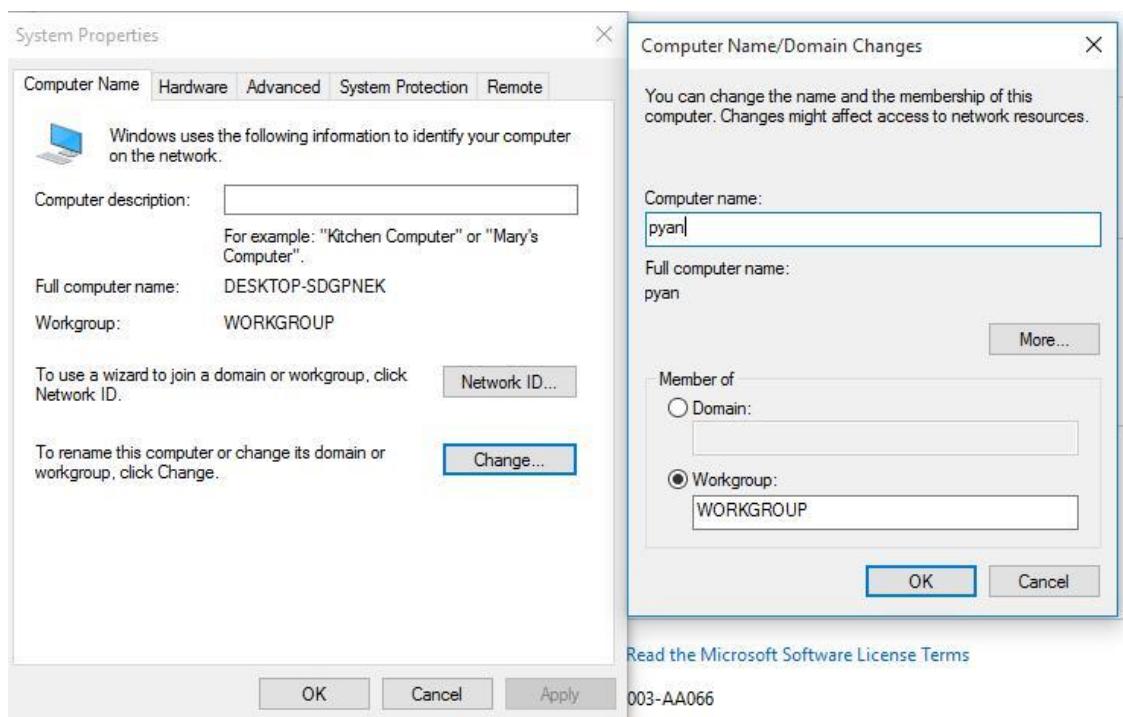
Gambar 46. Change Setting, mengubah nama komputer anda

4. Pada jendela **Computer Name Changes** Anda masukkan nama komputer yang Anda jadikan sebagai pengenal komputer Anda di jaringan. Tulis di bawah **Computer name**. Nama ini bisa digunakan pada saat seseorang hendak mengakses share yang ada di komputer Anda. Usahakan nama komputer ini tidak sama dengan komputer lain di jaringan.

Pada bagian **Member of** terdapat dua bagian, yaitu :

- Domain, Anda pilih ini bila dalam jaringan terdapat komputer yang berperan sebagai *domain controller*. Kegunaan komputer ini sebagai tempat autentikasi yang terpusat di jaringan tersebut. Proses login di setiap komputer akan ditangani oleh komputer ini bila Anda sebagai anggota group suatu domain.
- Workgroup, Anda pilih bila pada jaringan setiap komputer mengatur proses autentikasinya masing-masing. Pengelompokan yang dilakukan oleh workgroup bukan berarti komputer lain tidak bisa mengakses komputer yang berada di luar workgroupnya.

4. Kemudian klik **OK** dan klik **OK** lagi di **System Properties**. Setelah itu Anda diminta untuk restart.



Gambar 47.Penganturan Computer Name

#### 10.4 Share Folder di Windows 10

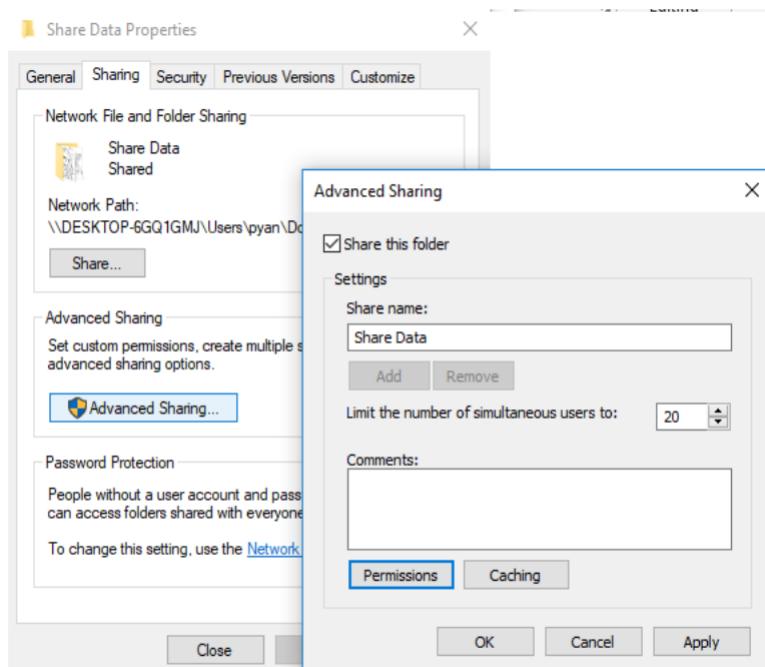
Yang dimaksud dengan *share* di sini adalah anggota dari suatu workgroup dapat menggunakan file yang terdapat di dalam suatu folder dari anggota workgroup lainnya. Penggunaannya itu bisa dalam bentuk menyalin, membaca, menghapus ataupun menambahkan file lain ke dalam folder yang di-*share* tersebut. Ciri suatu file atau folder ataupun printer yang di-*share* adalah adanya gambar berbentuk tangan yang seakan-akan ingin membagikannya kepada anggota jaringan yang lain.

Apabila Anda menginginkan melakukan sharing folder selain yang sudah di-share melalui homegroup, maka langkahnya adalah:

- Jalankan Windows Explorer dengan cara klik ikon Windows Explorer yang terdapat pada kiri bawah desktop
- Pilih folder yang akan di-share. Kemudian klik tombol Share with pada Toolbar lalu pilih Homegroup (Read) atau Homegroup (Read/Write).
- Anda buka Windows Explorer dan buat terlebih dahulu folder yang akan dijadikan tempat menghimpun file-file yang akan di-*share*. Sebagai contoh saya membuat folder data pada partisi C . Untuk membuatnya klik pada drive C pada Windows Explorer

sebelah kanan Anda klik kanan lalu pilih **New Folder**. Ganti nama folder yang baru dibuat menjadi **Share Data**. Masukkan file-file yang ingin di *share*

- Klik kanan pada folder **Share Data** dan pilih tab **Sharing**. Maka akan muncul jendela sharing.
- Apabila belum muncul tampilan untuk share, seperti gambar di bawah, maka Anda klik **Advanced Sharing**

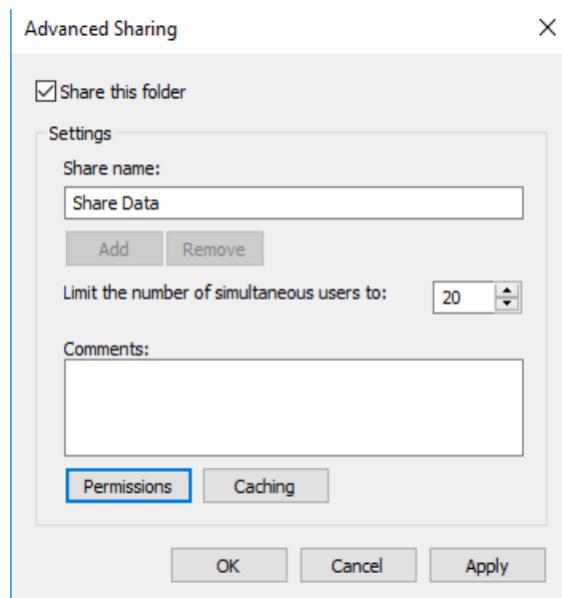


Gambar 48. Jendela Sharing file

Pada jendela Sharing, sharing folder dapat diaktifkan. Anda dapat mulai melakukan share di Windows 10 Anda dengan memberi centang atau cek list pada Share this folder. Share name akan aktif dan Anda bisa memberikan nama share untuk folder tersebut Secara default share yang diberikan untuk komputer lain di jaringan adalah dengan ijin read only, user hanya bisa membaca file yang anda share. Untuk memberikan akses tulis atau akses merubah (read/write) pada file yang Anda share kemudian Anda bisa klik Permissions.

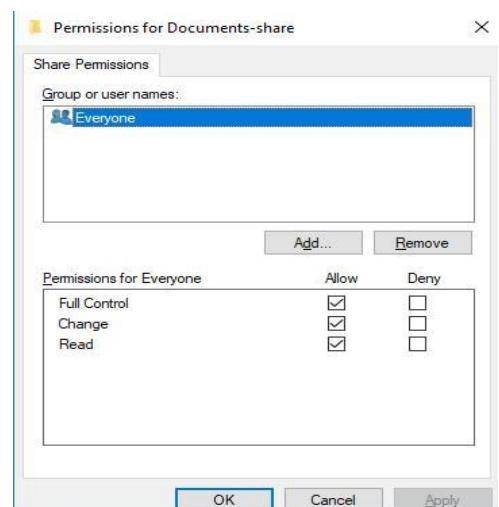
#### 10.4.1 Pengaturan Hak Akses pada Sharing di Windows 10

1. Klik kanan dari folder yang telah Anda share dan pilih Advance Sharing lalu kemudian Anda akan mendapatkan jendela yang berbeda dengan yang sebelumnya. Sekarang muncul tombol **Permissions**.



Gambar 49. Jendela Sharing dengan Permissions

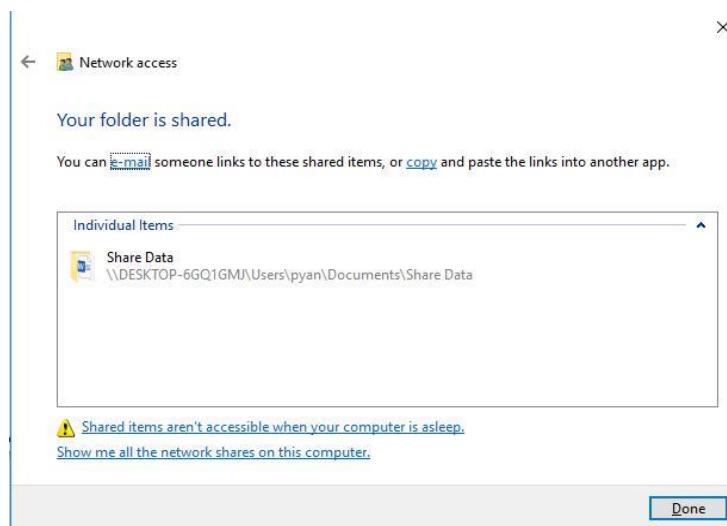
2. Untuk mengatur hak akses Anda klik pada tombol **Permissions**, dan muncul-lah jendela Permission Anda. Apabila Anda belum mengatur hak akses pada komputer Anda maka user yang ada hanyalah **Everyone**. Berarti share Anda dapat digunakan oleh semua user di jaringan
3. Untuk setiap user yang ada di komputer ini. Anda dapat mengatur permission untuk setiap user. Hak akses sebagai berikut:



Gambar 50. Pengaturan Permission

- **Full control**, artinya Anda diberikan akses penuh dalam menggunakan share tersebut. Seperti membaca isi file, mengubah isi file, bahkan menghapus.
- **Change**, Anda diberikan hak akses untuk mengubah isi file, termasuk juga menghapus file
- **Read**, Anda diberikan hak akses untuk membaca isi file

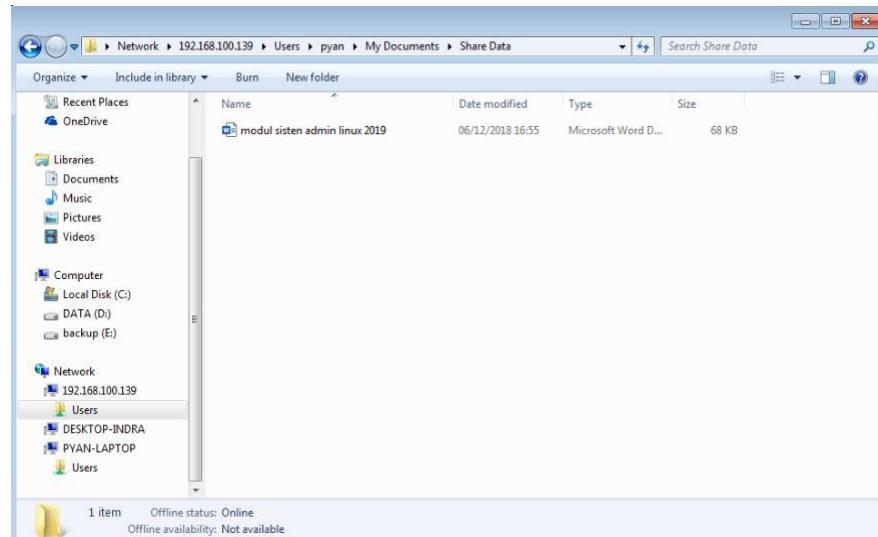
4. Untuk memperbolehkan hanya untuk user-user tertentu saja yang bisa mengakses komputer Anda. Maka user everyone harus dihapus dengan menekan tombol Remove. Setelah itu Anda tambah user yang Anda ingin atur hak aksesnya dengan menekan tombol Add.
5. Pada jendela Select Users or Groups Anda masukkan user atau group yang diperbolehkan mengakses share Anda. Kemudian klik OK.
6. Setelah user-user telah dipilih Anda atur hak akses dari setiap user. Kemudian klik OK.



Gambar 51. Hasil dari sharing file

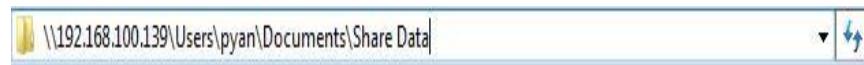
#### 10.4.2. Mengakses file yang dishare dari komputer lain

Untuk mengakses file yang di-share di komputer lain Anda harus mengetahui nama komputer atau nomor IP address dari komputer tujuan. Anda bisa mencari komputer tersebut dari **windows explorer => Network => Nama Komputer => Nama Share**



Gambar 52.Mengakses dari network

Anda juga bisa menggunakan nama komputervatau IP address untuk menuju komputer yang di share secara langsung, yaitu dengan menuliskan \\nama komputer atau \\ip address pada address bar **Windows Explorer**.



Gambar 53. Pengaksesan dari IP Address

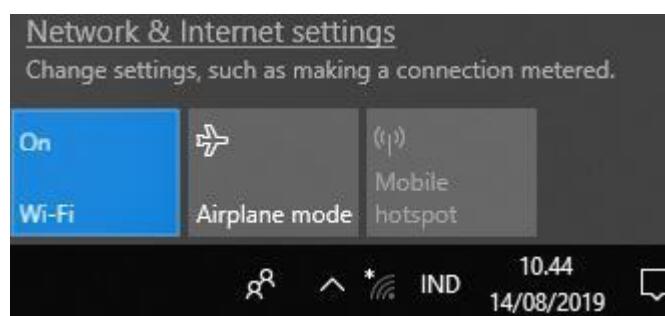
## 10.5 Menggunakan Wifi atau Wireless

1. Install driver untuk wireless device Anda. Wireless device dapat berupa wireless USB, wireless card yang dipasang pada slot PCI atau PCMCIA atau merupakan device onboard (pada notebook).
2. Pastikan komputer Anda berada dalam jangkauan sinyal dari Access Point (hub untuk jaringan wireless) sering disebut dengan hotspot. Untuk menghubungkan jaringan wireless, Anda harus mengetahui nama jaringan wireless (SSID) dan key yang dibutuhkan untuk ke jaringan tersebut. Key untuk jaringan wireless ada beberapa macam :
  - WEP (Wired Equivalent Privacy), algoritma keamanan yang digunakan pada jaringan wireless. Untuk WEP menggunakan key agar menghubungkan komputer ke jaringan wireless. WEP-40 memiliki key dengan standard 64 bit dan WEP-104

memiliki key dengan standard 128 bit. Untuk saat ini WEP dianggap sudah tidak aman karena sangat mudah di-*hack* dengan program tertentu, walaupun begitu WEP masih umum digunakan.

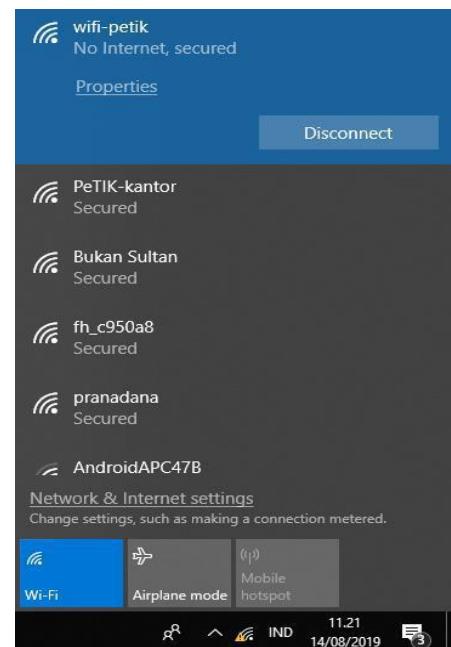
- WPA (Wi-Fi Protected Access) adalah program sertifikasi yang dibuat oleh organisasi Wi-Fi Alliance untuk memberikan dukungan terhadap protokol keamanan yang dibuat oleh Wi-Fi Alliance. WPA dapat menggunakan sistem enkripsi AES dan TKIP. WPA menawarkan sistem keamanan yang lebih baik dibanding dengan WEP.

3. Bila Anda masuk ke dalam suatu jaringan maka terdapat peringatan berikut



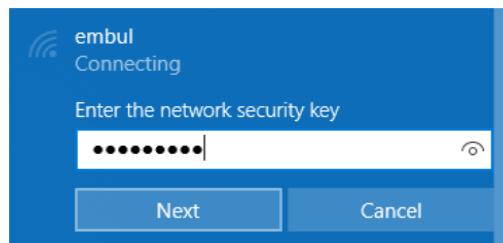
4. Untuk terkoneksi dengan jaringan wireless yang ada Anda bisa melakukannya pada jendela Wireless Network Connection. Untuk membuka jendela tersebut ada 3 cara, yaitu :

- klik pada  gambar dengan mengklik dua kali tombol komputer di kanan bawah yang memiliki gambar signal wireless
- klik **Start** → **setting** → **network and internet** (Wi-fi, airplane mode, VPN) → **Wireless Network Connection** → **Wifi** → **on**
- klik **Start** → **Control Panel** → **Network Connection** → **Network and Internet** → **Network and Sharing Center** → **Change adapter setting** pilih **Wireless**



Gambar 54. Wireless Network Connection

4. Klik dua kali pada jaringan wireless yang hendak Anda gunakan. Apabila menggunakan key maka akan muncul jendela permintaan security key



Gambar 55. Memasukan Security Key

5. Tunggulah beberapa saat untuk dilakukan konfigurasi jaringan. Pada umumnya jaringan wireless menggunakan pengaturan IP address secara otomatis. Apabila ternyata menggunakan konfigurasi secara manual Anda klik pada **Change advanced settings** dan atur IP address seperti biasa.
6. Bila sudah terkoneksi Anda bisa melepas koneksi dengan menekan tombol **Disconnect** di kanan bawah pada gambar



## Bab 11

### Keamanan Jaringan Nirkabel

#### Tujuan

- Memahami pentingnya keamanan jaringan wireless.
- Mengetahui jenis jenis atau cara mengamankan jaringan wireless

#### 11.1 Pengantar Keamanan Jaringan Wireless

Jaringan wireless yang tidak diamankan dapat merugikan kita sebagai pengelola jaringan maupun sebagai pengakses atau pengguna jaringan. Jaringan wireless tanpa pengamanan itu artinya siapa pun dapat menghubungkan peralatan atau komputernya ke AP (Access Point) atau peralatan wireless yang lain. Misalnya Anda mengelola jaringan kantor yang menggunakan AP untuk menghubungkan banyak komputer dan terhubung ke modem untuk mengakses ke internet. Jika tidak ada pengamanan, atau pengamanan lemah, maka orang yang tidak berhak dapat masuk ke jaringan kantor Anda, lalu memanfaatkan akses internet. Bahkan yang lebih bahaya, orang lain itu dapat merusak atau mencuri data kantor yang dishare.

Banyak bentuk pengamanan jaringan wireless, misalnya penyembunyian SSID, penyaringan alamat MAC, penggunaan password WEP, WPA, dan aplikasi otentikasi dengan username dan password untuk login. Berikut ini penjelasan masing-masing contoh jenis keamanan jaringan wireless itu:

#### 11.2 Menyembunyikan SSID

SSID atau ESSID adalah nama yang digunakan untuk peralatan jaringan seperti AP agar bisa dikenali dan mudah diakses oleh peralatan lain. Agar tidak mudah diketahui orang yang tidak berhak atau peralatan lain tidak otomatis dapat terhubung ke jaringan wireless, kita dapat membuat SSID tersembunyi atau hidden. Hampir semua AP mendukung hidden SSID.

### 11.3 Penggunaan Kunci WEP

WEP (*Wired Equivalent Privacy*) merupakan suatu metode pengamanan pada Wi-Fi. Otentikasi pada WEP sebanding dengan jaringan kabel biasa sehingga mode pengamanan WEP sangat lemah. Oleh karena itu, penggunaan WEP biasanya bersamaan dengan metode penyaringan MAC Address. Ada dua metode otentikasi WEP yang pernah dikembangkan dan masih digunakan, yakni Open System dan Shared Key. Meskipun Open System dinilai lebih baik, saat ini keduanya sudah sangat lemah, karena mudah di-crack.

Ada beberapa jenis WEP, di antaranya berdasar jumlah bit enkripsi ada kunci 64 bit, 128 bit, dan 152 bit. Kunci dapat menggunakan bilangan Heksadesimal antar 0 sampai 9, dan A hingga F. Kunci juga dapat menggunakan kode ASCII. Jika menggunakan bilangan heksadesimal, jumlah kunci adalah 10 karakter untuk 64 bit, 26 karakter untuk 128 bit, dan 32 karakter untuk 152 bit. Sedangkan jika menggunakan ASCII, jumlah karakter adalah 5 untuk 32 bit, 13 untuk 128 bit, dan 16 untuk 152 bit. Namun sekali lagi mudahnya algoritma enkripsi WEP ini dipecahkan membuat perbedaan jumlah bit itu tidak terlalu penting, sehingga disarankan saat ini pengamanan wireless beralih menggunakan password WPA/WPA2

### 11.4 Penggunaan Password WPA

Melihat banyaknya kelemahan dan kekurangan pada metode pengamanan WEP, maka diciptakanlah WPA (*Wi-Fi Protected Access*). Yang mana metode ini mengimplementasikan standar IEEE yaitu 802.11i serta sistem enkripsi *TKIP (Temporal Key Integrity Protocol)* atau *AES (Advanced Encryption Standard)* yang jauh lebih aman dibandingkan WEP. TKIP tidak didukung Wi-Fi versi N (802.11n), maka untuk jaringan yang melayani 11bgn, sebaiknya menggunakan AES. AES lebih baru dan lebih aman dibandingkan TKIP.

WPA dan WPA2 mendukung PSK (Pre-Shared Key) atau disebut juga modus Personal dan WPA & WPA 2 Enterprise. WPA &WPA2 Personal sering ditulis sebagai WPAPSK & WPA2PSK. Sedangkan WPA & WPA2 Enterprise menggunakan protokol otentikasi *EAP*

(*Extensible Authentication Protocol*). WPA & WPA2 dapat menggunakan otentikasi dengan server RADIUS.

### 11.5 Penyaringan Alamat Mac

Alamat MAC atau MAC Address adalah sebuah pengalamatan unik yang terdiri dari 48 bit (6 Byte) yang menjadi identitas sebuah device jaringan. Tidak seperti alamat IP, alamat MAC pada setiap device aslinya tidak akan pernah sama. Metode pengamanan dengan penyaringan MAC memungkinkan untuk membatasi client yang mencoba melakukan hubungan ke jaringan wireless. Yaitu dengan memasukkan daftar MAC Address mana saja yang diperbolehkan atau dilarang masuk ke jaringan wireless tersebut.

### 11.6 Penggunaan Program Otentikasi

Merasa kurang aman dengan metode pengamanan penyaringan MAC, WEP, maupun WPA, metode lainnya adalah menggunakan program otentikasi atau disebut juga *captive portal*. Captive portal biasanya dipakai di jaringan terbuka atau hotspot umum, yang tak punya metode otentikasi lain seperti WEP, WPA, atau MAC filter, karena sangat sulit membagikan kunci WEP, WPA, maupun mencatat alamat MAC setiap klien yang dapat sering berganti orang dan komputer.

Dengan program tersebut, setiap client akan memiliki user dan password sendiri yang tersimpan pada suatu server. Jika ingin lebih aman dengan kosekuensi lebih repot dalam merawat, selain user dan password setiap client juga bisa diatur untuk harus mendaftarkan MAC Address device mereka untuk dapat mengakses jaringan Wi-Fi tersebut. Metode pengamanan tersebut merupakan implementasi dari 802.11i yang salah satunya disebut RADIUS (Remote Authentication Dial In User Service), yaitu sebuah server yang berisi data otentikasi dan MAC Address untuk semua client yang terdaftar. Salah satu program Open Source untuk captive portal adalah Chillispot. Anda juga dapat menggunakan sistem otentikasi bawaan MikroTik atau program otentikasi lainnya

Prinsip kerja otentikasi atau captive portal biasanya memiliki urutan sebagai berikut:

- Peralatan klien mendapatkan alamat IP dari server DHCP yang ada di AP.

- Setelah mendapatkan IP, semua trafik jaringan diarahkan ke program captive portal untuk otentikasi, sehingga meskipun setiap peralatan wireless telah mendapatkan alamat IP melalui server DHCP, peralatan tidak dapat mengakses fasilitas jaringan sebelum memberikan username dan password yang benar.
- Akses web juga diblokir (*redirect*) ke aplikasi web yang ada di captive portal sehingga pengguna langsung mengetahui halaman login di web untuk memasukkan username dan password-nya.
- Setelah username dan password diterima, peralatan diberi akses sesuai dengan kriteria yang ditentukan oleh program captive portal seperti akses web melalui proxy dan akses internet yang lain.
- Captive portal lengkap seperti yang tersedia pada MikroTik tidak hanya untuk keamanan, tapi juga untuk memudahkan pengelola dalam mengatur bandwidth setiap pengguna, waktu akses, dan lain-lain.

## 11.7 Wireless VPN

VPN adalah fasilitas dalam jaringan publik (internet) yang digunakan sebagai jaringan privat (LAN atau WAN) secara virtual. Kata virtual ini menunjukkan bahwa jaringan privat itu tidak seratus persen privat, karena menggunakan jaringan publik atau internet. Wireless VPN artinya gabungan teknologi wireless LAN dengan teknologi VPN. Dengan cara ini, dua atau lebih komputer dalam jaringan wireless LAN kantor dapat berhubungan melalui internet dengan komputer di tempat atau LAN kantor lain seakan-akan menjadi satu jaringan privat, meskipun hubungan antar wireless LAN itu melalui internet. Dengan menerapkan VPN ini keamanan wireless LAN/WAN juga menjadi lebih baik daripada tanpa VPN. Tidak semua AP (access point) memiliki fasilitas VPN. Salah satu contoh AP atau router untuk wireless yang mendukung VPN adalah produk yang dikeluarkan oleh MikroTik.

## 11.8 Wireless Gateway

Wireless Gateway adalah perangkat penghubung antara wireless LAN dengan internet atau dengan jaringan lain. Selain menjadi perantara, gateway juga menjadi pelindung keamanan bagi komputer yang mengakses internet melalui wireless AP terhadap kemungkinan serangan dari internet. Fungsi wireless gateway ini berarti menyatukan fungsi

AP dan router, dan biasanya juga menyediakan fasilitas firewall. Fungsi firewall adalah mengisolasi komputer terhadap akses yang tidak sah dari internet, meskipun komputer yang tersambung ke wireless LAN tetap dapat mengakses Internet. Contoh AP murah yang mendukung gateway atau router dan firewall adalah TP Link TL-WR941ND seperti yang akan dibahas pada bab berikutnya. Contoh AP mahal yang lengkap mendukung Wireless Gateway adalah beberapa produk dari MikroTik, Linksys/Cisco, dan merek lainnya.

## Bab 12

### Cara Mengamankan Jaringan Wireless

#### Tujuan:

- Setup Access Point dengan beberapa jenis keamanan wireless.
- Menggunakan komputer Windows dan atau Linux untuk mengakses jaringan wireless yang telah dilengkapi beberapa tipe keamanan.

#### 12.1 Pengamanan Jaringan Wireless

Berikut ini contoh-contoh cara mengamankan peralatan jaringan wireless, misalnya AP (Access Point) dengan merek dan tipe tertentu, berdasarkan jenis-jenis pengamanan di atas. Modul pelatihan ini disusun dengan AP merek TP-Link tipe TL-WR941ND. Merek dan tipe AP yang Anda gunakan dalam latihan atau tugas nyata dapat saja berbeda, namun secara umum memiliki fasilitas keamanan yang serupa dengan beberapa fasilitas keamanan AP yang dibahas dalam contoh ini

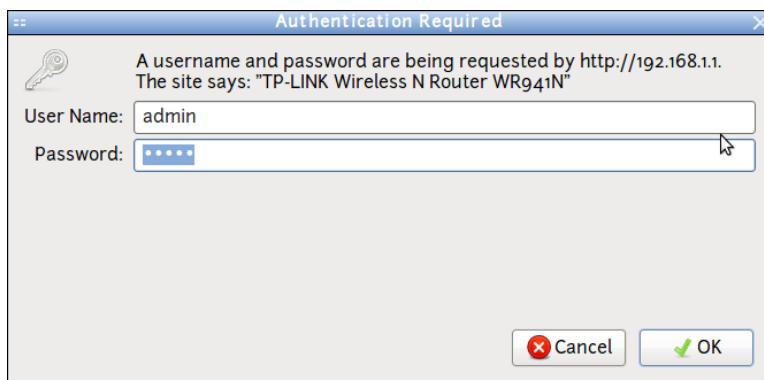


Gambar 56. Contoh Acces Point – TP-Link TL-WR941ND

Sebelum memulai latihan masing-masing jenis pengamanan, berikut ini yang harus diperhatikan:

- Umumnya AP dapat disetup melalui web, sehingga pelatihan ini hanya menekankan cara mengonfigurasi AP melalui browser web, misalnya Firefox.

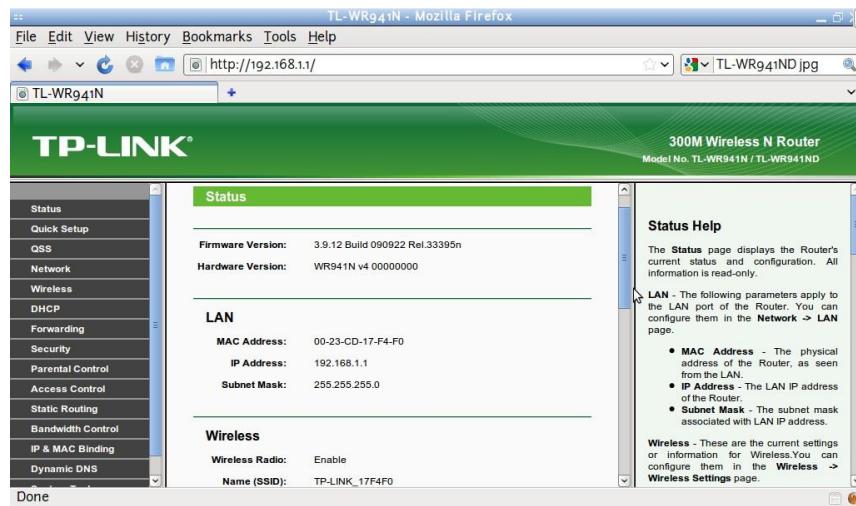
- Pasangkan AP dan sebuah komputer dengan sistem operasi Linux atau Windows melalui kabel UTP secara langsung atau melalui Switch/Hub. Komputer akan digunakan untuk mengatur kemananan AP, sehingga lebih dahulu pastikan jaringan kabel dan atau wireless komputer telah bekerja dengan baik.
- Untuk mengonfigurasi keamanan ini, matikan lebih dahulu jaringan wireless yang ada di laptop, sehingga sambungan hanya melalui jaringan kabel agar tidak terputus ketika sistem keamanan diubah. Namun jika tidak ada jaringan kabel, Anda tetap dapat mengatur melalui jaringan wireless, hanya akan sering terputus setiap kali terjadi perubahan konfigurasi.
- Berikan alamat IP komputer satu kelas dengan jaringan AP. Misalnya AP memiliki alamat bawaan pabrik 192.168.1.1, maka gunakan alamat komputer 192.168.1.2 atau di atasnya hingga 192.168.1.254.
- Gunakan web browser, misalnya Firefox atau Google Chrome, untuk mengakses alamat 192.168.1.1, sehingga tampil jendela halaman login seperti Gambar 2. Jika password belum diubah, gunakan user admin dan password admin. Segera ganti password admin ini agar tidak disalahgunakan oleh orang yang tidak berhak.



Gambar 57. Halaman login untuk setup salah satu contoh AP

- Tampilan halaman utama untuk setup salah satu contoh AP seperti Gambar 47 CATATAN: Jika password pernah diubah dan Anda lupa password-nya, atau Anda lupa alamat IP-nya, lakukan proses me-reset AP dengan cara menyalakan ulang sambil menekan tombol RESET dengan ballpen atau yang

sejenis, tahan hingga proses booting AP selesai (selama satu hingga dua menit, tergantung merek dan tipe AP).

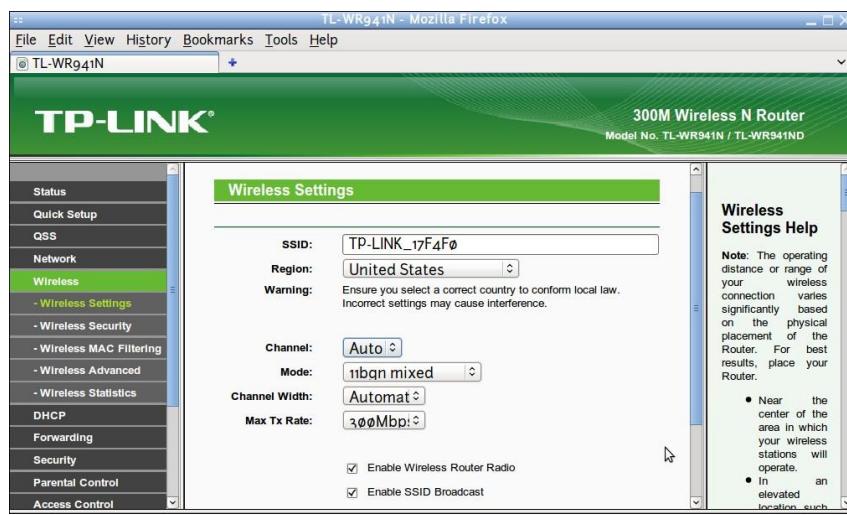


Gambar 58 Halaman utama salah satu contoh AP

- Aktifkan server DHCP pada AP (bila ada), untuk memudahkan pengujian selama pelatihan ini. Jika alamat AP 192.168.1.1, atur server DHCP untuk memberikan alamat di antara 192.168.1.2 hingga 192.168.1.254 (dengan syarat tidak ada jaringan lain yang terganggu karena bentrok alamat IP).

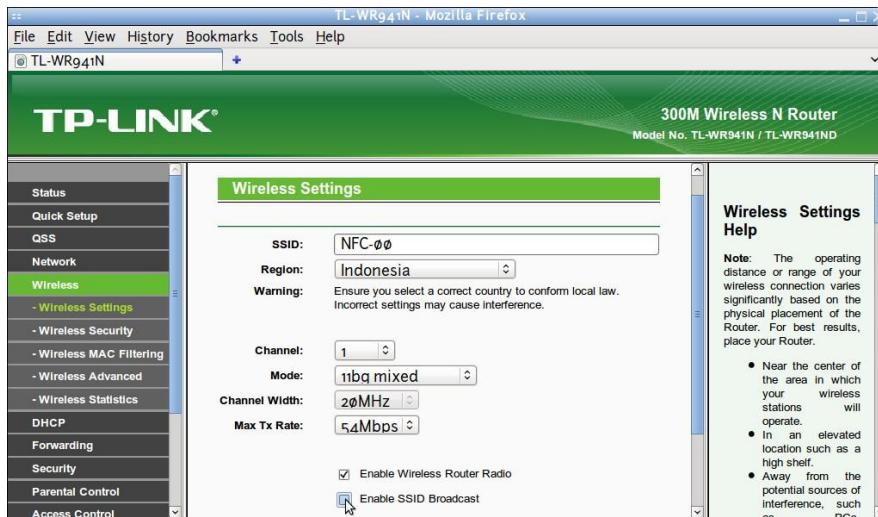
## 12.2 Cara menyembunyikan SSID

- Klik menu Wireless. Dalam contoh ini, SSID bawaan AP dari pabrik adalah **TP-LINK\_17F4F0**, Region United States, Channel Auto, Mode 11bgn mixed, Wireless Router Radio di- enable (aktif), dan SSID Broadcast di-enable (tidak disembunyikan), seperti Gambar 48



Gambar 59. Konfigurasi wireless AP bawaan pabrik

- Untuk memudahkan kita mengingat, kita ubah SSID itu menjadi **NFC-00**, Region Indonesia, Channel diubah menjadi 1 atau yang lain sesuai petunjuk pengajar, Mode 11b atau 11bg atau 11bgn sesuai kemampuan AP yang Anda gunakan, lalu matikan Enable SSID Broadcast yang artinya SSID disembunyikan (hidden), sehingga tampil seperti Gambar 5. Klik Save dan Reboot AP agar perubahan diaktifkan.



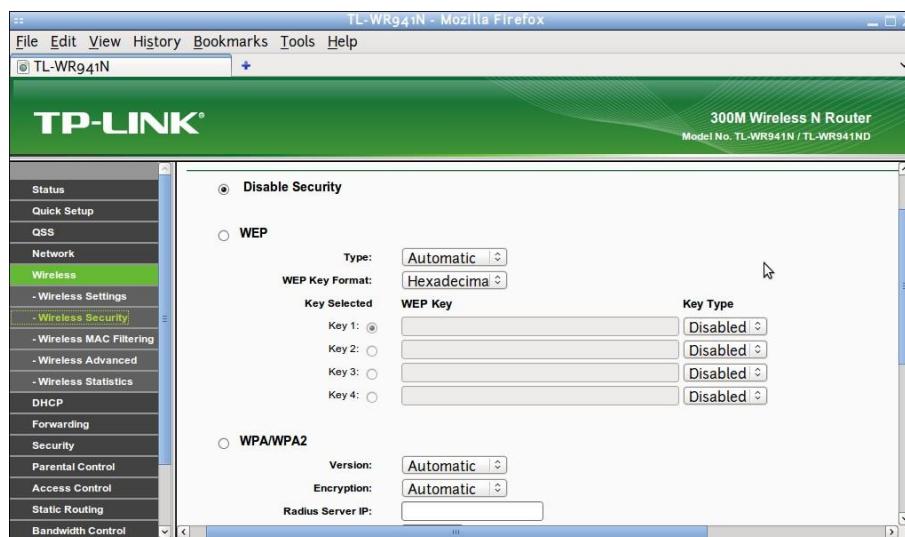
Gambar 60. Konfigurasi wireless AP dengan SSID disembunyikan

- Untuk mencoba hasil pengubahan, lihat dari komputer apakah SSID sudah berubah dan tidak terlihat. Kemudian lakukan setting manual jaringan wireless komputer yang Anda gunakan, dengan memasukkan SSID yang disembunyikan (dalam contoh ini NFC-00) dan berikan alamat IP yang sama dengan alamat IP sebelumnya atau sesuai

petunjuk pengajar. Uji coba sambungan dengan ping ke alamat IP AP, misalnya ping 192.168.1.1.

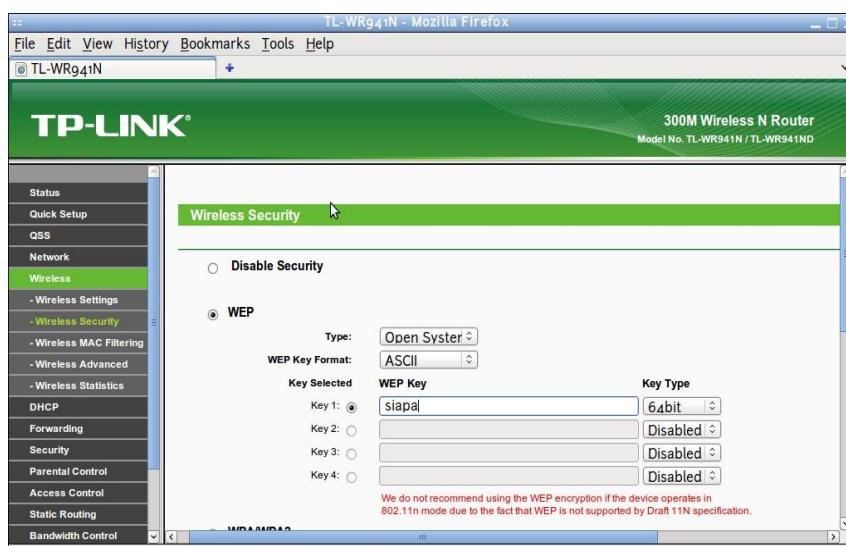
### 12.3 Cara Mengaktifkan WEP

- Kembali ke web browser untuk mengakses alamat IP AP, kembalikan SSID tidak disembunyikan untuk memudahkan uji coba berikutnya. Klik menu Wireless Security, dengan contoh tampilan default dari pabrik belum diberikan pengamanan WEP maupun WPA, atau *Disable Security* seperti Gambar 50



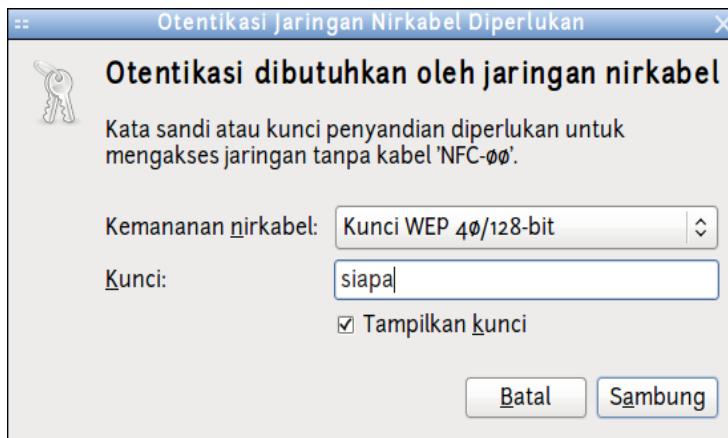
Gambar 61. Keamanan AP masih dimatikan

- Klik pilihan WEP, kemudian masukkan data berikut ini sebagai latihan. *Type Open System*, *WEP Key Format ASCII*, *Key Selected* pilih *Key 1* saja dengan kunci “siapa” menggunakan enkripsi 64 bit. Klik *Save* dan *Reboot AP* agar perubahan diaktifkan.



Gambar 62. Kemanan AP dengan WEP

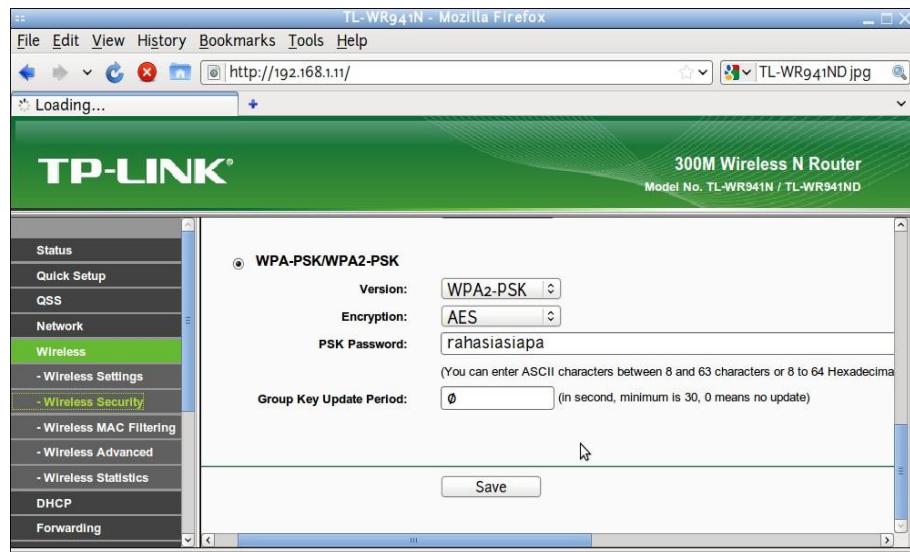
- Untuk mengujinya, gunakan Windows atau Linux untuk menyambung ke jaringan wireless NFC-00. Anda akan ditanyakan kunci WEP. Masukkan kata kunci yang telah dibuat, seperti terlihat di Gambar 52. Contoh ini menggunakan Linux.



Gambar 63. Meminta kunci WEP untuk menyambungkan komputer ke AP

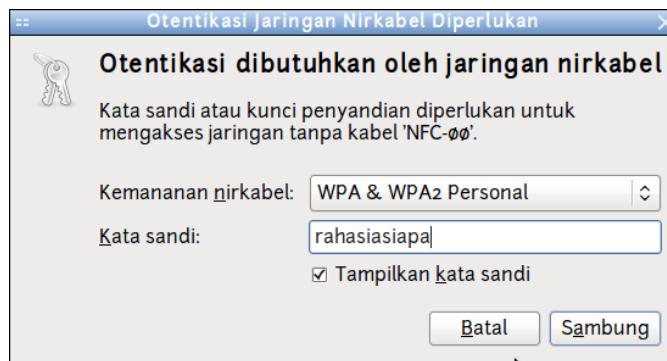
## 12.4 Cara Mengaktifkan WPA

- Coba salah satu pengamanan WPA yang mudah, misalnya WPA-PSK atau WPA2-PSK yang tidak membutuhkan otentikasi server lain seperti RADIUS. Karena enkripsi TKIP tidak didukung Wi-Fi versi 11n, pilih enkripsi AES yang didukung semua versi 11bgn, kemudian masukkan password PSK, misalnya “rahasiasiapa” seperti Gambar 53. Klik Save, lalu Reboot AP untuk mengaktifkannya.



Gambar 64. Kemanan AP dengan WPA2-PSK

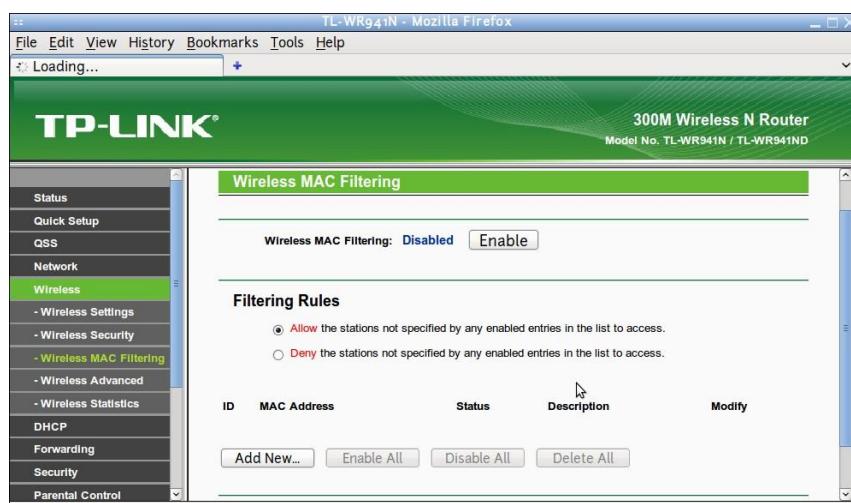
- Uji coba dengan Windows atau Linux untuk menyambungkan komputer dengan AP telah diberi pengamanan dengan WPA.



Gambar 65. Kunci WPA untuk menyambungkan komputer ke AP

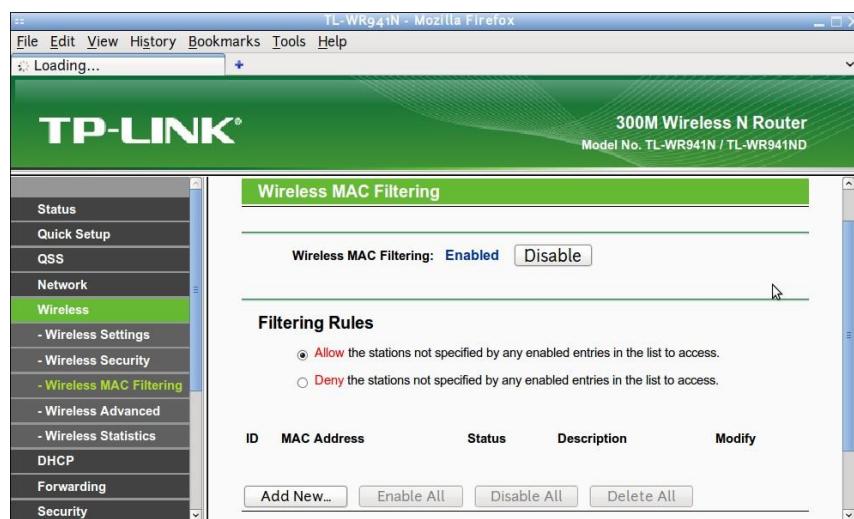
## 12.5 Cara Menyaring Alamat MAC

- Umumnya AP yang ada di pasar saat ini mendukung penyaringan atau MAC Filtering. Kembali akses halaman web AP, menu utama Wireless, pilih Wireless MAC Filtering sehingga tampil di layar seperti Gambar 55



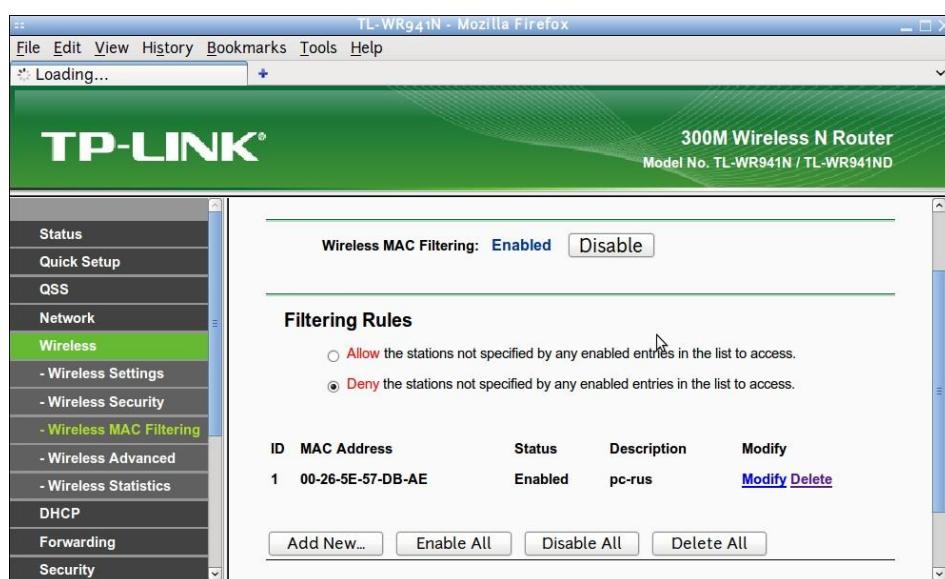
Gambar 66. MAC Filtering belum diaktifkan atau disabled

- Klik Enable dan tunggu beberapa detik. Jika komputer Anda terhubung ke AP ini melalui wireless, kembalikan ke Disabled, agar Anda tetap dapat terhubung ketika mengubah Filtering Rules. Pada posisi awal adalah *Allow the stations not specified by any enabled entries in the list to access.*, yang artinya semua MAC diizinkan mengakses karena tidak masuk ke daftar MAC yang dilarang, sehingga Anda tetap dapat mengakses.



Gambar 67. MAC Filtering sudah diaktifkan belum ada MAC yang dilarang

- Jika dipertahankan Allow seperti di atas, maka semua MAC yang dilarang harus didaftarkan. Jika hanya ingin mendafarkan MAC yang diizinkan, maka pindahkan pilihan ke *Deny the stations not specified by any enabled entries in the list to access*, yang artinya MAC selain yang didaftarkan dilarang.
- Pastikan kembali ke Disabled jika komputer Anda terhubung ke wireless AP ini. Sekarang masukkan MAC komputer Anda ke dalam daftar dengan klik Add New. Penulisan MAC untuk AP TP-Link ini adalah 00:26:5e:57-db:ae, bukan 00:26:5e:57:db:ae. Huruf heksadesimal antara a hingga f dapat menggunakan huruf kecil maupun besar A hingga F. Lihat Gambar 57 yang menunjukkan hanya ada satu MAC yang diizinkan, karena dengan Filtering Rules Deny ini, maka MAC selain yang terdaftar itu dilarang.



Gambar 68. Salah satu alamat MAC didaftarkan mendapat izin akses

## Bab 13

### Pengenalan Mikrotik

#### Tujuan:

- Peserta mengetahui sejarah Mikrotik
- Peserta mengetahui jenis-jenis lisensi RouterOS
- Peserta mengetahui jenis-jenis router Mikrotik

#### 13.1 Apa itu Mikrotik?

Mikrotik berasal dari kata Mikrotiks yang berarti network kecil. Mikrotik adalah perusahaan yang berkantor pusat di Latvia yang bergerak pada bidang teknologi jaringan. Didirikan oleh John Trully dan Arnis Riekstins pada tahun 1995. Memiliki visi untuk merouting seluruh dunia. Awalnya Mikrotik hanya menjual aplikasi router, yaitu RouterOS. Tetapi kemudian juga menjual *hardware-hardware* jaringan yang menggunakan aplikasi RouterOS.

RouterOS merupakan produk utama dari Mikrotik berbasis sistem operasi Linux. Aplikasi ini memungkinkan user mengubah komputer PC menjadi *software* router, memungkinkan fitur-fitur seperti firewall, VPN server dan client, manajemen bandwidth (Quality of Service – QoS), access point wireless dan beberapa fitur-fitur lain. Sistem tersebut juga dapat digunakan sebagai captive-portal berbasis hotspot. Selain itu mendukung aplikasi-aplikasi untuk ISP menengah hingga besar dengan dukungan terhadap protokol routing seperti OSPF, BGP dan VPLS/MPLS. Mendukung koneksi dengan menggunakan FTP, telnet dan SSH.

RouterOS mendukung semua perangkat jaringan yang didukung oleh kernel Linux 2.6.16 kecuali Wireless yang hanya mendukung Wireless dari Atheros dan Prism. Mendukung prosessor AMD dan Intel.

RouterOS dapat dikelola dengan menggunakan beberapa cara dari Web, telnet, SSH dan menggunakan aplikasi manajemen yang disebut Winbox.

### 13.2 Hardware Router - RouterBoard

*Hardware* Mikrotik memiliki beberapa produk seperti perangkat router (RouterBoard) dan interface jaringan. Anda dapat melakukan pemilihan berdasarkan:

- Jenis prosesor, prosesor yang lebih cepat berarti dapat mendukung proses dan fitur yang lebih kompleks dan banyak.
- Memori (RAM), memori digunakan untuk membantu kinerja prosesor dengan menyimpan data-data sementara yang hendak dimasukkan ke dalam memori.
- Jumlah interface:
  - Ethernet, device ethernet dapat dihubungkan dengan koneksi kabel
  - MiniPCI, dapat dihubungkan dengan wireless card. Setiap miniPCI dihubungkan dengan satu perangkat wireless dapat berfungsi untuk menerima atau membagi akses jaringan wireless. Bila memiliki dua atau lebih wireless card berarti routerboard dapat difungsikan untuk wireless repeater.
  - Slot USB, USB dapat dihubungkan dengan flashdisk atau ke modem GPRS/3G/HSDPA/CDMA. Bila dihubungkan ke modem maka dapat difungsikan untuk router 3G.
  - MicroSD, dapat digunakan untuk media penyimpanan tambahan. Digunakan untuk menyimpan cache dari komputer.
- Level Lisensi, level lisensi menentukan fitur-fitur yang diaktifkan dan skalabilitas jaringan.

### 13.3 Lisensi RouterOS

Lisensi RouterOS menentukan fitur-fitur yang diaktifkan dan skalabilitas jaringan. Lisensi dibedakan dalam beberapa level, yaitu:

- Level 0, adalah lisensi yang diberikan pada saat anda baru menginstal image RouterOS. Dalam hal ini anda belum memberikan lisensi apa pun. Pada lisensi ini anda akan diberikan fitur secara full selama 24 jam saja.
- Level 1, adalah free demo tanpa batasan waktu. Untuk mendapatkannya anda harus melakukan registrasi ke Mikrotik.

- Level 3, adalah lisensi untuk perangkat RouterOS yang dapat difungsikan sebagai client atau penerima dari suatu Access Point.
- Level 4, 5, 6 adalah lisensi perangkat RouterOS yang dapat difungsikan sebagai Router dan Access Point (bila memiliki device wireless). Adapun perbedaannya pada jumlah pengguna service VPN dan hotspot.

Level	3	4	5	6		
Upgrade time	dalam 1 versi mayor dan versi berikutnya					
Wireless CPE/PTP	yes					
Wireless AP	no	yes				
Sync Interface	no	yes				
EoIP	1	unlimited				
PPPoE	1	200	500	unlimited		
PPTP & L2TP	1	200	unlimited			
VLAN, Firewall, Queue	unlimited					
Proxy, Radius Client	yes					
Dynamic Routing	RB = yes	yes				
Hotspot Active User	1	200	500	unlimited		
User Manager Active User	10	20	50	unlimited		

Tabel 13-1 Daftar Lisensi Mikrotik

Lisensi dapat anda beli secara terpisah, tetapi cara paling mudah adalah anda membeli perangkat routerboard Mikrotik. Setiap routerboard mikrotik telah disertakan dengan lisensi RouterOS tertentu.

### 13.4 Produk Mikrotik

Berikut ini adalah beberapa produk RouterBoard Mikrotik sebagai pilihan untuk UKM dan perusahaan besar yang dapat dimanfaatkan untuk membangun jaringan komputer yang handal.

- **RB411**

RB411 seri yang didesain apabila anda memperhatikan besar dan harga. Perangkat ini sangat tepat digunakan sebagai access point client. Dapat digunakan untuk SOHO atau menjalankan link backup wireless. Perangkat yang menggunakan lisensi level 3 ini dapat digunakan untuk wireless client access point saja, tetapi untuk yang level 4 dapat digunakan untuk access point untuk small office.

Spesifikasi:

- CPU: Atheros AR7130 300MHz (AR7161 680MHz for AH model)
  - Memory: 32MB DDR SDRAM onboard memory (64MB for RB411AH model)
  - Boot loader: RouterBOOT
  - Data storage: 64MB onboard NAND memory chip
  - Ethernet: One 10/100 Mbit/s Fast Ethernet port with Auto-MDI/X
  - miniPCI: One MiniPCI Type IIIA/IIIB slot
  - Extras: Reset switch, Beeper
  - Serial port: One DB9 RS232C asynchronous serial port
  - LEDs: Power, NAND activity, 5 user LEDs
  - Power options: PoE: 8-28V DC on Ether1 (Non 802.3af). Jack: 8-30V DC
  - Dimensions: 105 mm x 105 mm, Weight: 82 g
  - Power consumption: ~3W without extension cards, maximum – 12 W
  - Operating System: MikroTik RouterOS, Level 3 license without AP some uses Level 4
- **RB433**

RB 433 adalah wireless access point universal. 3 slot mini PCI (dapat diisi dengan kartu wireless) dan 3 port ethernet memberikan anda pilihan yang cukup untuk konektivitas di jaringan. Dengan menggunakan RB 433 anda dapat membuat wireless repeater ditambah access point local, atau access point untuk beberapa sektor. RB433 disertakan dengan CPU Atheros 300 MHz dan telah diinstal dengan lisensi RouterOS level 4.

Spesifikasi:

- CPU: Atheros AR7130 300MHz (AR7161 680MHz for AH model)
- Memory: 64MB DDR SDRAM onboard memory (128MB for AH model)
- Boot loader: RouterBOOT
- Data storage: 64MB onboard NAND memory chip and microSD
- Ethernet: Three 10/100 Mbit/s Ethernet ports with Auto-MDI/X
- miniPCI: Three miniPCI Type IIIA/IIIB slots
- Extras: Reset switch, Beeper
- Serial port: One DB9 RS232C asynchronous serial port
- LEDs: Power, NAND activity, 5 user LEDs

- Power options: PoE: 8-28V DC on Ether1 (Non 802.3af). Jack: 8-30V DC
- Dimensions: 105 mm x 154 mm, Weight: 137g
- Power consumption: ~3W without extension cards, maximum – 25 W, 16W output to cards
- Operating System: MikroTik RouterOS, L4 license. L5 license for AH model
- **RB750**

RB750 adalah router kecil dengan memiliki 5 slot port ethernet. Dengan bentuknya yang kecil dan harganya yang murah dapat digunakan untuk membuat router untuk perusahaan SOHO. Dikarenakan tidak memiliki perangkat wireless maka hanya dapat digunakan untuk menangani jaringan kabel saja. RB750 dengan harganya yang murah dan fiturnya yang lengkap dari RouterOS maka dapat anda gunakan untuk gateway pada kantor skala SOHO, DHCP server, firewall, atau MPLS router.

Spesifikasi:

- CPU: AR7241 400MHz CPU
- Memory: 32MB DDR SDRAM onboard memory
- Boot loader: RouterBOOT
- Data storage: 64MB onboard NAND memory chip
- Ethernet: Five 10/100 Mbit/s Fast Ethernet ports with Auto-MDI/X. Hardware switch chip and port mirror support
- Extras: Reset switch
- Serial port: no serial port
- LEDs: Power, NAND activity, 5 Ethernet LEDs
- Power options: PoE: 8-30V DC on Ether1 (Non 802.3af). Jack: 8-30V DC
- Dimensions: 113x89x28mm. Weight without packaging and cables: 130g
- Power consumption: Up to 3W
- Operating System: MikroTik RouterOS v3, Level4 license
- Package contains: RouterBOARD in a plastic case, power adapter
- **RB751U-2HnD**

RB751U-2HnD adalah router sejenis dengan RB750 yang dilengkapi port wireless. Dengan harga relatif lebih murah dapat digunakan untuk membuat router untuk perusahaan

SOHO. RB751U-2HnD dengan harganya yang murah dan fiturnya yang lengkap dari RouterOS maka dapat anda gunakan untuk gateway pada kantor skala SOHO, DHCP Server, Firewall, MPLS Router, Access Point, 3G Router.

Spesifikasi:

- CPU: AR7241 400MHz CPU
- Memory: 32MB DDR SDRAM onboard memory
- Boot loader: RouterBOOT
- Data storage: 64MB onboard NAND memory chip
- Ethernet: Five 10/100 Mbit/s Fast Ethernet ports with Auto-MDI/X. Hardware switch chip and port mirror support
- Wireless: Wireless Standards 802.11 b/g/n
- Extras: Reset switch
- Port USB: 1 USB
- LEDs: Power, NAND activity, 5 Ethernet LEDs
- Power options: PoE: 8-30V DC on Ether1 (Non 802.3af). Jack: 8-30V DC
- Dimensions: 113x89x28mm. Weight without packaging and cables: 130g
- Power consumption: Up to 3W
- Operating System: MikroTik RouterOS v3, Level4 license
- Package contains: RouterBOARD in a plastic case, power adapter

- **RB800**

RB800 adalah perangkat wireless dengan performa tinggi. Perangkat ini memiliki 4 slot miniPCI, 3 slot Gigabit ethernet, 2 konektor daughterboard, slot miniPCI-e dan slot compact flash. Dua konektor daughterboard memberikan anda untuk mengembangkan jumlah port kabel dan wireless, dikarenakan menggunakan CPU dengan kecepatan tinggi menyebabkan hal tersebut dapat dilakukan. Dengan menggunakan RB800 anda dapat menggunakan sebagai wireless router yang rumit, firewall, dan manager bandwidth, dengan banyak opsi ekspansi. RB800 disertakan dengan lisensi level 6 yang tidak memiliki batasan user, sehingga mudah dalam mengembangkan jaringan anda.

Spesifikasi:

- CPU: MPC8544 800MHz

- Memory: 256MB DDR2 SDRAM onboard memory
  - Boot loader: RouterBOOT
  - Data storage: 512MB NAND memory chip, CF slot on back
  - Ethernet: Three 10/100/1000 Mbit/s Ethernet ports with Auto-MDI/X
  - miniPCI: 4 x miniPCI, 1 x miniPCI-e
  - Expansion: PCI daughterboard port
  - Extras: Reset switch, beeper, 4x fan headers, voltage and temperature sensors
  - Serial port: One DB9 RS232C asynchronous serial port, One serial port header
  - LEDs: Power, 1x User LED
  - Power options: Power over Ethernet: 36-56V DC (including power over datalines)
  - Power jack: 10-56V DC
  - Dimensions: 14 cm x 20 cm (5.51 in x 7.87 in), 285 g
  - Operating System: MikroTik RouterOS, Level6 license
- **RB1100**

Core router performa tinggi dengan menggunakan 13 slot Gigabit ethernet, yang dapat digunakan untuk membuat dua group switch dan menyertakan kapabilitas Ethernet bypass. RB1100 juga memiliki slot SODIMM RAM untuk melakukan penambahan memory, 2 slot microSD, sebuah beeper dan sebuah serial port. RB110 memilki casing aluminium rackmount 1U sehingga bisa dipasang di rak server.

#### Spesifikasi

- CPU: PowerPC MPC8533 1066MHz network CPU with hardware encryption
- Memory: SODIMM DDR Slot, 2GB installed (RouterOS supports up to 1.5GB)
- Boot loader: RouterBOOT, 1Mbit Flash chip
- Data storage: Onboard NAND memory chip
- Ethernet: Thirteen 10/100/1000 Mbit/s Gigabit Ethernet with Auto-MDI/X
- Ethernet: Includes switch to enable Ethernet bypass mode in two ports
- miniPCI: none
- Storage: 512MB NAND, one microSD slot
- Serial port: One DB9 RS232C asynchronous serial port
- Extras: Reset switch, beeper, voltage and temperature sensors

- Power options: IEC C14 standard connector 110/220V
  - Fan: Dual fan with failover support mounted at case back
  - Dimensions: 1U case: 44 x 176 x 442 mm, 1275g. Board only: 365g
  - Operating System: MikroTik RouterOS, Level 6 license
- 
- **R52**

R52 adalah kartu wireless dari Mikrotik. Menggunakan konektor mini PCI. Mendukung wireless dengan IEEE 802.11 a/b/g untuk seri R52. Pada seri 52Hn sampai IEEE 802.11 a/b/g/n. Pada R52 menggunakan daya 65mW dan pada R52H menggunakan daya 350mW untuk meningkatkan jangkauan dan kecepatan dari perangkat wireless.

- **Mikrobit**

Mikrobit merupakan produk RouterBoard unggulan Mikrotik yang digunakan untuk core router dengan performa tinggi, Processor dengan performa tinggi, kualitas bahan lebih baik dan harga cukup mahal. Cocok digunakan untuk perusahaan-perusahaan besar yang menginginkan performa terbaik dan tahan lama.

Berikut jenis-jenis produk dari Mikrobit:

- Aneto: Intel Atom 64 bit D525
- Ainos: Intel Core i3
- Celoica: Intel Core2 Quad Core Q9400/Intel Xeon X3380
- Dinara: Intel Quad Xeon Sandy Bridge (3 GHz)

## Bab 14

### Instalasi dan Koneksi ke Mikrotik

#### Tujuan:

- Peserta dapat melakukan instalasi RouterOS pada PC
- Peserta dapat melakukan koneksi ke RouterOS

#### 14.1 Pendahuluan

Anda bisa menggunakan RouterOS dengan berbagai cara, yaitu:

- Dari Routerboard, ketika anda membeli Routerboard sudah tersedia RouterOS di dalamnya sehingga dapat digunakan secara langsung.
- Dari DOM (Disk On Module), dengan DOM berisi software RouterOS, maka anda bisa memasang DOM sebagai harddisk di komputer anda.
- Dari instalasi ke harddisk, selain pilihan di atas anda bisa menginstall RouterOS dari CD ke dalam komputer anda.

Image CD RouterOS bisa anda dapatkan di situs mikrotik (<http://mikrotik.co.id>), tetapi lisensi yang digunakan adalah lisensi level 0. Lisensi tersebut hanya bisa digunakan 1x24 jam sehingga tidak bisa digunakan untuk produksi. Anda harus meng-*upgrade* lisensi tersebut ke level 4, 5 atau 6.

#### 14.2 Kebutuhan *Hardware*

Kebutuhan *hardware* minimal :

- Pentium II
- RAM 64 Mb
- Harddisk IDE 400 Mb

Walaupun untuk fungsi-fungsi yang membutuhkan komputasi tinggi seperti proxy, radius, hotspot, dll membutuhkan sumber daya yang lebih tinggi terutama pada prosesor dan memori.

### 14.3 Langkah-langkah Instalasi

1. Atur booting komputer anda ke CD pertama kali. Kemudian masukkan CD Mikrotik dan boot komputer anda.
2. Pilih paket yang akan diinstal.



Gambar 71. Pemilihan paket yang akan diinstal

Berikut keterangan paket yang dapat diinstal:

- **system** (mipsle, mipsbe, ppc, x86), berisi fitur router dasar seperti static routing, ip address, sNTP, telnet, API, queue, firewall, web proxy, cache DNS, TFTP, IP pool, SNMP, packet sniffer, tool send email, visualisasi, pengetesan bandwidth, torch, EoIP, IPIP, bridging, VLAN, VRRP, dll.
- **ppp**, MIPPP client, PPP, PPTP, L2TP, PPPoE, client dan server ISDN PPP.
- **dhcp**, client dan server Dynamic Host Control Protocol.
- **advanced-tools**, advanced ping tools. netwatch, ip-scan, sms tool, wake-on-LAN.
- **arlan**, dukungan Aironet Arlan lama.
- **calea**, perangkat pengumpulan data untuk kebutuhan tertentu dikarenakan adanya "Communications Assistance for Law Enforcement Act" di USA.
- **gps**, dukungan terhadap perangkat Global Positioning System
- **hotspot**, manajemen user hotspot.
- **ipv6**, dukungan terhadap pengalaman IPv6.

- **isdn**, dukungan terhadap ISDN.
- **kvm**, virtualisasi KVM.
- **lcd**, dukungan terhadap panel LCD.
- **mpls**, dukungan terhadap Multi Protocol Labels Switching.
- **multicast**, Protocol Independent Multicast (PIM) – Sparse Mode, Internet Group Managing Protocol (IGMP) – Proxy.
- **ntp**, client dan server Network Time Protocol.
- **radiolan**, dukungan terhadap kartu radioLAN.
- **routerboard**, mengakses dan mengelola RouterBOOT, informasi spesifik Routerboard.
- **routing**, protokol routing dinamis seperti RIP, BGP, OSPF dan perangkat routing seperti BFD, filtering untuk route.
- **security**, IPSEC, SSH, Secure WinBox.
- **synchronous**, dukungan untuk FarSync.
- **ups**, APC ups.
- **user-manager**, Mikrotik User Manager.
- **wireless**, dukungan terhadap perangkat wireless.

Anda bisa instal semua paket dengan menggunakan tombol “a” atau tekan tombol “m” untuk instalasi minimal. Bila sudah memilih paket yang akan diinstal klik tombol “i”.

3. Do you want to keep old configuration? Apabila anda memiliki instalasi RouterOS sebelumnya, anda bisa tidak menghapus konfigurasi pada saat instalasi. Apabila anda ingin konfigurasi tidak dihapus klik “y”.
4. Kemudian muncul peringatan bahwa isi harddisk akan dihapus. Untuk melanjutkan tekan tombol “y” pada Continue.

```
Do you want to keep old configuration? [y/n]:n
Warning: all data on the disk will be erased!
Continue? [y/n]:y
Creating partition.....
Formatting disk.....
installed system-4.11
installed user-manager-4.11
installed security-4.11
installed routing-4.11
installed routerboard-4.11
installed ntp-4.11
installed ipo6-4.11
installed hotspot-4.11
installed dhcp-4.11
installed ppp-4.11
Software installed.
Press ENTER to reboot
```

Gambar 71. Proses Instalasi Mikrotik

5. Setelah proses instalasi selesai tekan tombol Enter untuk *restart* komputer anda.
6. Setelah diinstal maka anda bisa login langsung ke dalam sistem. Gunakan user admin dan password dikosongkan. Maka instalasi RouterOS telah selesai, anda bisa memulai melakukan konfigurasi router anda.



Gambar 72. Prompt login Mikrotik

```
      MMM      MMM      KKK      TTTTTTTTTTTT      KKK
      MMMMM    MMMMM    KKK      TTTTTTTTTTTT      KKK
      MMM  MMMM  MMM  III  KKK  KKK  RRRRRR  000000  TTT  III  KKK  KKK
      MMM  MM  MMM  III  KKKKKK  RRR  RRR  000  000  TTT  III  KKKKKK
      MMM  MMM  III  KKK  KKK  RRRRRR  000  000  TTT  III  KKK  KKK
      MMM  MMM  III  KKK  KKK  RRR  RRR  000000  TTT  III  KKK  KKK

MikroTik RouterOS 4.11 (c) 1999-2010      http://www.mikrotik.com/

ROUTER HAS NO SOFTWARE KEY
-----
You have 23h45m to configure the router to be remotely accessible,
and to enter the key by pasting it in a Telnet window or in Winbox.
See www.mikrotik.com/key for more details.

Current installation "software ID": 8B8Z-81PL
Please press "Enter" to continue!

[admin@MikroTik] >
```

Gambar 73. Tampilan antarmuka Mikrotik berbasis teks

#### 14.4 Mengelola Perangkat Mikrotik

Perangkat Mikrotik dapat dikelola dengan berbagai cara, diantaranya:

- Webbox, adalah aplikasi berbasis web yang digunakan untuk mengelola perangkat Mikrotik. Webbox dapat diakses dengan menggunakan web browser diarahkan pada IP address perangkat komputer. Webbox memiliki fitur yang tidak terlalu lengkap sehingga hanya tepat untuk pengaturan-pengaturan yang sederhana.
- Winbox, adalah aplikasi berbasis desktop untuk sistem operasi Microsoft Windows yang digunakan untuk melakukan pengaturan perangkat Mikrotik. Aplikasi ini memiliki fitur yang lengkap untuk melakukan segala pengaturan perangkat Mikrotik.
- Remote Terminal (telnet/SSH), seperti perangkat jaringan lainnya RouterOS dapat dikontrol dengan menggunakan aplikasi remote terminal telnet dan SSH. Dengan menggunakan remote terminal anda akan terhubung dengan Command Line Interface dari RouterOS.

#### 14.5 Bekerja dengan Winbox

Aplikasi Winbox dapat anda unduh secara gratis pada alamat <http://www.mikrotik.co.id/download.php> atau <https://mikrotik.com/download>.

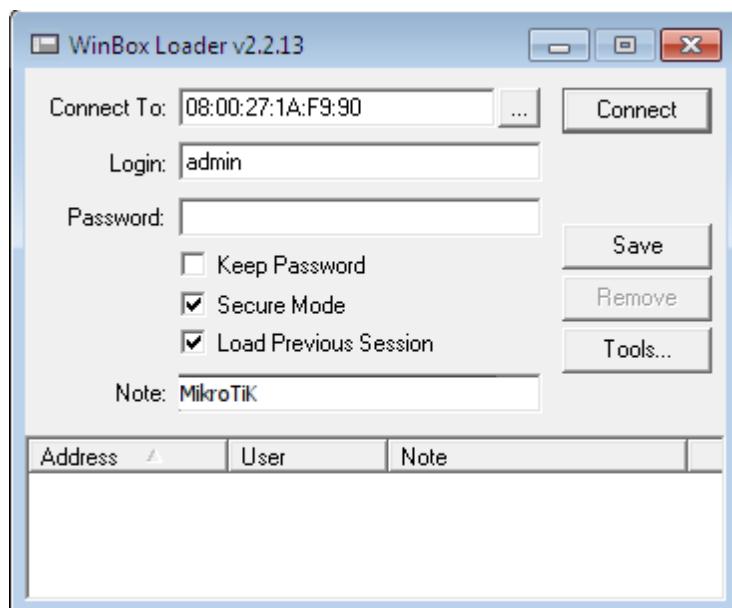
Untuk melakukan pengaturan Mikrotik, jalankan aplikasi Winbox kemudian melakukan login dengan memasukkan username dan password. Pada saat muncul tampilan jendela Winbox klik tanda (...) pada Connect to dan pilih MAC Address atau IP address dari perangkat Mikrotik anda.

Agar bisa mengakses perangkat Mikrotik menggunakan Winbox, anda harus terhubung secara langsung dengan menggunakan kabel atau berada pada network segmen yang sama.

Apabila anda mengkonfigurasi perangkat Mikrotik tersebut untuk pertama kali maka setiap perangkat memiliki konfigurasi IP address, username dan password default, yaitu:

- IP address: 192.168.88.1/24
- Username: admin
- Password: <kosong>

Perlu diperhatikan bahwa Winbox menggunakan port jaringan 8291, oleh karena itu harus diperhatikan agar port tersebut dapat diakses melalui jaringan.



Gambar 74 Proses login melalui Winbox

## Bab 15

### Konfigurasi Dasar Mikrotik

#### Tujuan:

- Peserta dapat melakukan konfigurasi dasar perangkat Mikrotik
- Peserta dapat melakukan pengaturan DHCP
- Peserta dapat melakukan backup konfigurasi

#### 15.1 Konfigurasi hostname

Hostname digunakan sebagai pengenal perangkat Mikrotik anda. Daripada menggunakan IP address maka hostname lebih mudah dimengerti dan dihapalkan. Untuk mengganti hostname pada RouterOS caranya sebagai berikut:

1. Klik System → Identity
2. Ubah nama identity router anda.



Gambar 76. Mengatur hostname perangkat Mikrotik

Konfigurasi melalui *command line*:

```
[admin@MikroTik] > /system identity edit value-name=MyRouter
```

#### 15.2 Konfigurasi Jaringan

Konfigurasi jaringan dapat dilakukan dengan dua cara, yaitu:

- Pengaturan secara manual, berarti anda harus melakukan pengaturan jaringan secara mandiri. Agar dapat terhubung ke internet maka konfigurasi yang perlu dilakukan adalah:

- IP Address, digunakan untuk pengalaman komputer anda di jaringan.  
Konfigurasi ini harus diikuti dengan pengaturan netmask.
- Default Route atau gateway, digunakan untuk mengkonfigurasi perangkat berikutnya yang harus dilewati untuk ke jaringan luar atau ke internet.
- DNS, digunakan untuk menerjemahkan nama domain, seperti yahoo.com menjadi IP address.
- Pengaturan secara otomatis, berarti perangkat anda akan mendapatkan IP address dari server DHCP secara otomatis, sehingga anda tidak melakukan konfigurasi IP address secara manual. Untuk itu anda harus mengkonfigurasi perangkat anda sebagai DHCP client.

Misalkan anda akan melakukan konfigurasi perangkat Mikrotik sehingga memiliki konfigurasi sebagai berikut:

- IP address: 192.168.123.1
- Netmask: 255.255.255.0
- Gateway: 192.168.1.1
- DNS: 180.131.144.144 & 180.131.145.145

- **Konfigurasi IP address**

Untuk melakukan konfigurasi IP address caranya sebagai berikut:

1. Klik IP → Addresses. Kemudian klik tombol + untuk menambah IP address.
2. Pada Address masukkan 192.168.1.123/24. 24 adalah prefix. Prefix didapatkan dari netmask yang digunakan oleh IP address anda. Sebagai contoh:
  - Netmask 255.255.255.0 prefixnya 24
  - Netmask 255.255.0.0 prefixnya 16
  - Netmask 255.0.0.0 prefixnya 8
3. Kemudian pada Interface, anda pilih NIC dari perangkat yang ingin diberikan IP tersebut. Sebagai contoh digunakan perangkat ether1.



Gambar 77. Konfigurasi IP Address

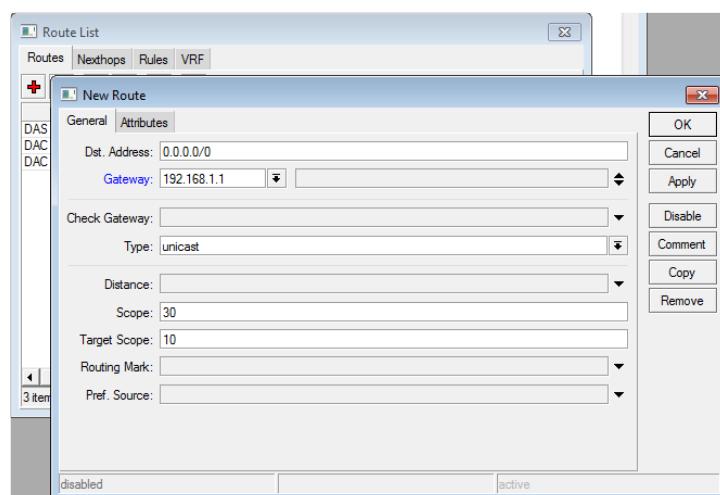
Konfigurasi Command Linenya adalah:

```
[admin@MikroTik] > /ip address add address=192.168.1.123/24 interface=ether1
```

- **Konfigurasi Default Route**

Untuk melakukan konfigurasi default route, lakukan langkah berikut:

1. Klik IP → Routes. Kemudian klik tombol +.
2. Masukkan pada Dst. Address dengan 0.0.0.0/0. Dst Address menunjukkan jaringan atau IP address tujuan dari lalu lintas jaringan anda. Untuk default route maka tujuannya selalu ke 0.0.0.0/0. Pada Gateway anda masukkan IP address dari perangkat perantara dari komputer anda ke jaringan luar. Apabila anda menghubungkan modem ADSL ke perangkat jaringan anda untuk bisa mengakses internet, maka interface modem yang menuju ke LAN akan digunakan IP addressnya sebagai gateway pada perangkat Mikrotik.



Gambar 78. Konfigurasi Default Route

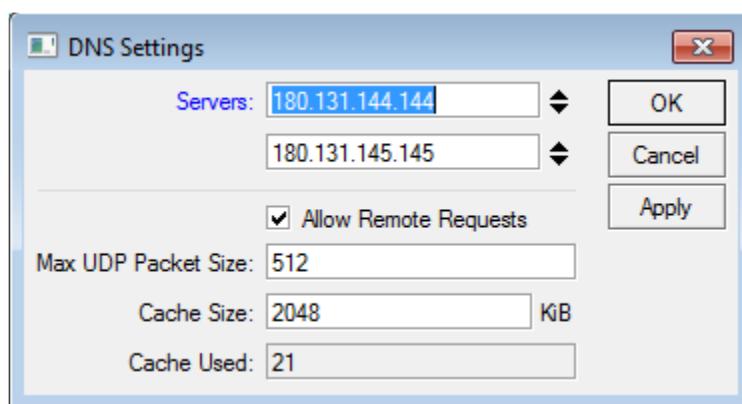
Konfigurasi Command Linenya:

[admin@MikroTik] > /ip route add dst-address=0.0.0.0/0 gateway=192.168.1.1

- **Konfigurasi DNS**

Untuk melakukan konfigurasi DNS sebagai berikut:

1. Klik IP → DNS. Kemudian pilih Settings
2. Pada jendela DNS Settings pada server masukkan IP dari DNS server yang anda pergunakan. Untuk menambah DNS server kedua klik tombol segitiga ke bawah dan tuliskan DNS server kedua pada text box yang muncul. Dalam contoh pada Servers dimasukkan nilai 180.131.144.144 dan 180.131.145.145.



Gambar 79. Konfigurasi DNS

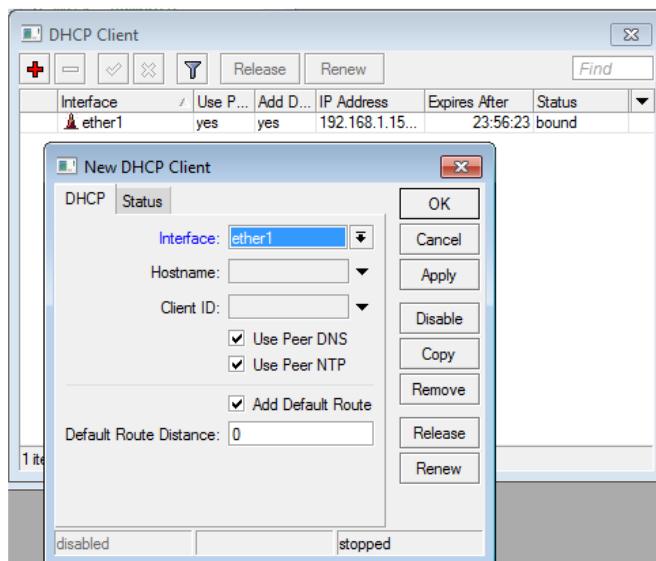
Konfigurasi Command Linenya:

[admin@MikroTik] > /ip dns set servers=180.131.144,180.131.145.145

- **Konfigurasi DHCP Client**

Untuk melakukan konfigurasi DHCP client anda hanya perlu mendaftarkan interface anda untuk mendapatkan IP address secara otomatis. Caranya:

1. Klik IP → DHCP Client. Kemudian klik + untuk mendaftarkan interface anda sebagai DHCP client.
2. Pada Interface maka anda masukkan NIC yang akan mendapatkan IP address secara otomatis. Dalam hal ini NIC yang digunakan adalah ether1.

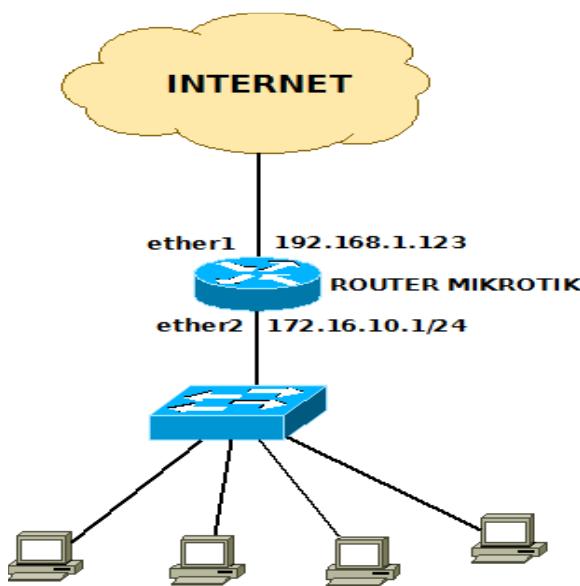


Gambar 80 Konfigurasi DHCP Client

Konfigurasi Command Linenya:

```
[admin@MikroTik] > /ip dhcp-client add interface=ether1 disabled=no
```

### 15.3 Sharing Internet

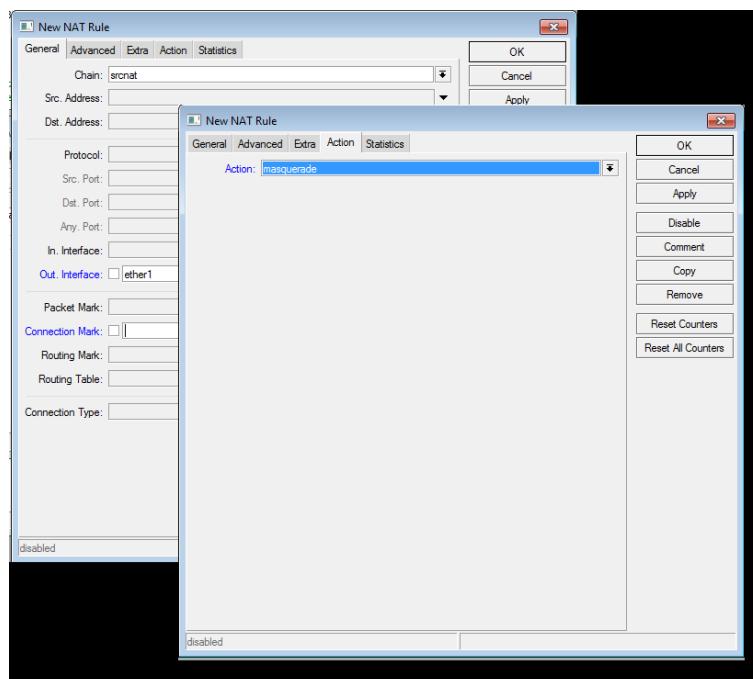


Salah satu fungsi dari router Mikrotik adalah sebagai pembagi jaringan internet yang dimilikinya ke perangkat yang lainnya. Untuk itu paling tidak router tersebut harus memiliki paling tidak dua NIC. Dikarenakan minimal satu koneksi digunakan untuk akses internet, sedangkan yang lainnya untuk membagi akses internet ke perangkat lain di LAN.

Seperti pada gambar di atas terlihat bahwa router dihubungkan dengan menggunakan dua kabel yang pertama terhubung ke interface ether1 yang mengarah ke internet dan yang lainnya terhubung ke interface ether2 yang mengarah ke komputer-komputer di LAN. Maka yang perlu dilakukan adalah anda harus mengatur IP address dari kedua interface. Untuk ether1 anda harus pastikan dapat terkoneksi

ke internet. Kemudian lakukan sharing internet dengan menggunakan fungsi source-NAT dari firewall. Caranya sebagai berikut:

1. Klik IP → Firewall. Pilih tab NAT dan kemudian tekan tombol +.
2. Pilih Chain srcnat dan Out Interface ether1 (berarti adalah device yang ke internet).
3. Kemudian klik tab Action dan ubah Action menjadi masquerade.



Gambar 81 Konfigurasi Sharing Internet

Berdasarkan konfigurasi di atas berarti anda akan mengganti Source IP dari paket yang melewati router anda dengan IP address dari out interface anda, sehingga paket tersebut dapat dikembalikan lagi ke komputer asalnya apabila paket telah sampai ke server tujuan di internet.

Konfigurasi Command Linenya:

```
[admin@MikroTik] > /ip firewall nat add chain=srcnat out-interface=ether1
action=masquerade
```

## 15.4 DHCP Server

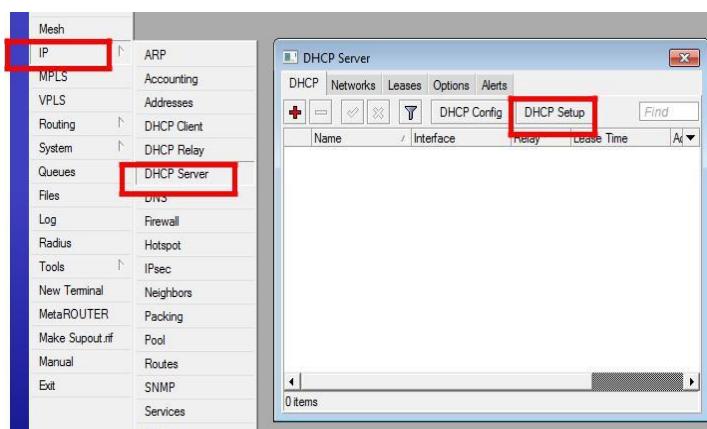
DHCP (Dynamic Host Configuration Protocol) digunakan untuk pemberian IP address secara mudah. DHCP server akan memberikan konfigurasi IP address ke client yang telah dikonfigurasikan dengan pengaturan jaringan (IP address, default gateway, domain name, DNS server dan server WINS) secara otomatis. Ketika client meminta IP address dari server, server

akan memberikan IP address sesuai dengan MAC address dari client. IP address yang dialokasikan untuk suatu client DHCP untuk jangka waktu tertentu disebut juga DHCP lease. RouterOS dapat diimplementasikan sebagai DHCP server dan client dan sesuai dengan standard RFC 2131.

RouterOS mendukung untuk menjadi server untuk setiap interface Ethernet. Agar DHCP server dapat bekerja maka anda harus mengatur IP pool (range IP address yang dialokasikan ke client – jangan masukkan IP address DHCP server ke dalam pool) dan DHCP network.

Langkah konfigurasi DHCP server sebagai berikut:

1. Klik IP → DHCP Server, kemudian pilih DHCP Setup.



Gambar 82 Konfigurasi DHCP server

2. Pada DHCP Server Interface masukkan interface yang akan digunakan untuk memberikan IP address secara otomatis. Interface yang digunakan untuk membagikan akses DHCP harus memiliki IP address yang bersifat statis.
3. Pada DHCP Address Space masukkan nomor jaringan dari LAN anda.
4. Pada Gateway for DHCP Network masukkan IP address dari gateway yang digunakan di jaringan. Bila anda menggunakan router Mikrotik anda sebagai gateway maka masukkan IP address dari interface anda yang menuju ke LAN.
5. Pada Address to Give Out masukkan jangkauan IP address yang akan diberikan ke client. Hal ini akan menentukan jumlah client dari DHCP server anda. Misalkan anda berikan 172.16.10.2-172.16.10.254 berarti jumlah client yang mungkin terhubung adalah 253 komputer.
6. Pada DNS Server masukkan DNS Server yang akan diberikan ke komputer-komputer di jaringan.

7. Pada Lease Time masukkan berapa lama konfigurasi IP address akan dipinjamkan ke komputer client. Apabila suatu client terkoneksi melewati lease time, maka harus meminta konfigurasi IP address yang baru.

Konfigurasi Command Linenya adalah:

```
[admin@MikroTik] > /ip dhcp-server setup
```

**Select interface to run DHCP server on**

**dhcp server interface: ether2**

**Select network for DHCP addresses**

**dhcp address space: 172.16.10.0/24**

**Select gateway for given network**

**gateway for dhcp network: 172.16.10.1**

**Select pool of ip addresses given out by DHCP server addresses to give out:**

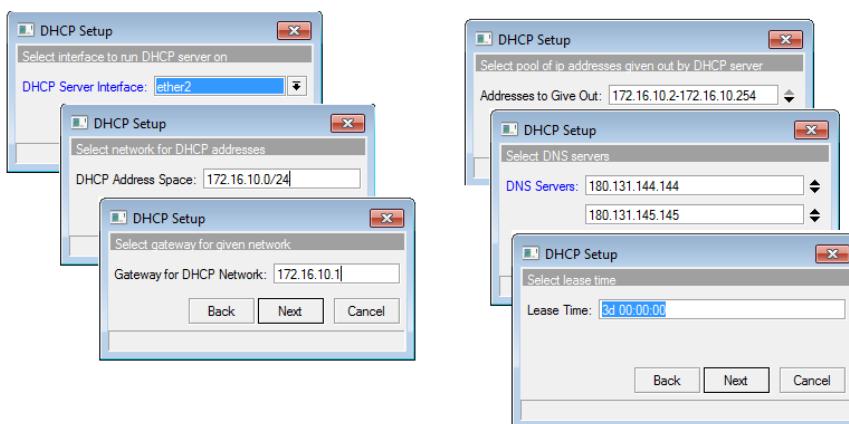
**172.16.10.2-172.16.10.254**

**Select DNS servers**

**dns servers: 180.131.144.144,180.131.145.145**

**Select lease time**

**lease time: 3d**



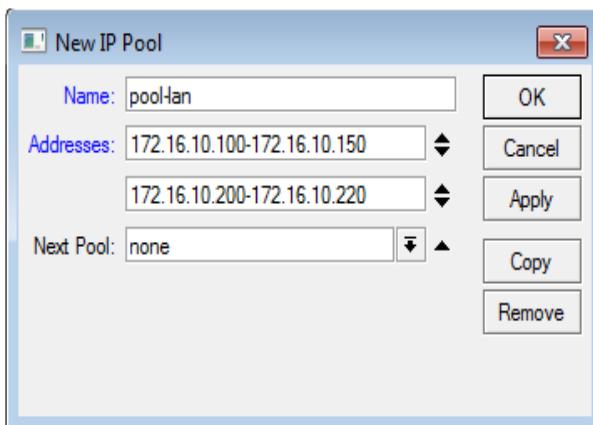
Gambar 83 Step by step konfigurasu DHCP server

- **Menambah IP Pool**

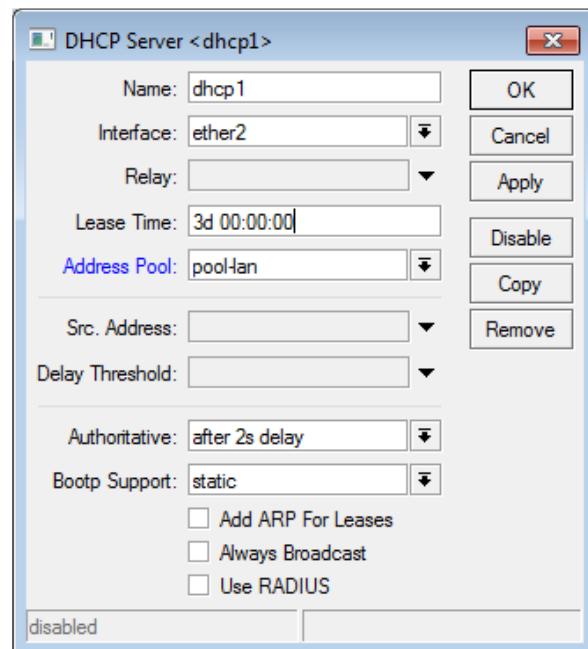
Suatu ketika mungkin anda hendak ingin mengganti konfigurasi jangkauan IP address yang hendak diberikan ke client. Untuk itu anda bisa mengatur IP pool dari DHCP server anda. Langkahnya sebagai berikut:

1. Klik IP → Pool. Kemudian klik + untuk menambahkan pool baru.

2. Pada Name masukkan nama pool Anda, misalkan pool-lan. Pada Addresses diisi dengan jangkauan IP address yang akan diberikan kepada client di jaringan. Anda bisa menambahkan jangkauan yang terpisah dengan menekan segitiga ke bawah pada Addresses untuk menambahkan jangkauan IP address baru. Contoh penulisan Addresses adalah 172.16.10.100-172.16.10.150.
3. Untuk mengubah konfigurasi DHCP dengan pool baru, klik IP → DHCP Server. Kemudian klik dua kali pada konfigurasi dhcp yang hendak diganti. Untuk mengubah pool, masukkan nama pool pada bagian Address Pool.



Gambar 84 Konfigurasi IP pool



Gambar 85 Penambahan pool pada DHCP Server

Konfigurasi Command Linenya adalah:

```
[admin@MikroTik] > /ip pool add name=pool-oke ranges=172.16.10.100-
172.16.10.150, 172.16.10.200-172.16.10.220
```

- **Membuat Static Lease**

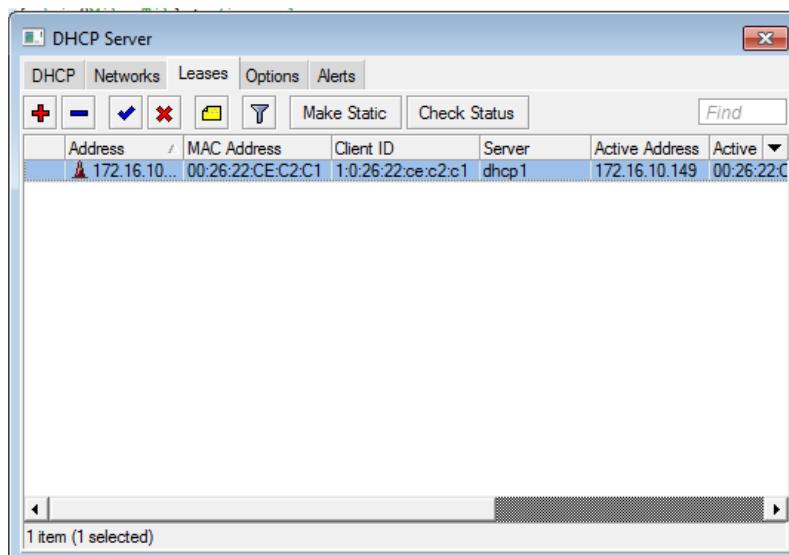
Dengan menggunakan DHCP maka IP address dari komputer akan diberikan oleh server. Hal ini mengakibatkan IP address yang diberikan bisa berbeda dari waktu ke waktu. Pada router Mikrotik anda dapat memberikan IP yang sama untuk suatu komputer. Untuk memberikan IP address yang sama untuk beberapa komputer anda bisa membuat static lease untuk setiap komputer tersebut. Static lease akan menyebabkan IP address yang sama dipetakan ke MAC

address suatu komputer. Dengan fasilitas ini maka akan mempermudah pengelolaan jaringan dan pengenalan komputer di jaringan.

Ada beberapa cara melakukan static lease, yaitu dengan menambahkan static lease atau dengan mengubah dynamic lease menjadi static lease.

#### 15.4..1 Mengubah Dynamic Lease menjadi Static Lease

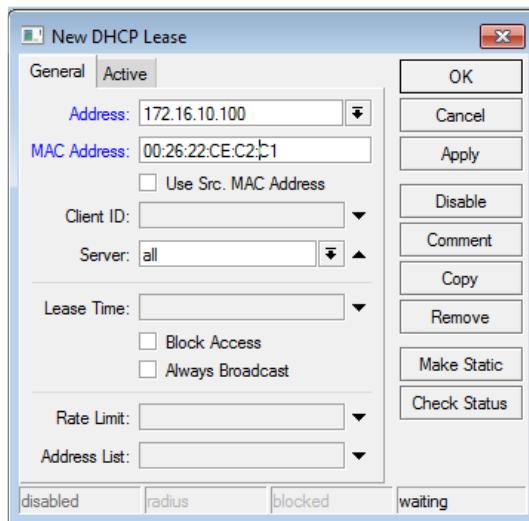
1. Klik IP → DHCP Server → Klik tab Leases
2. Klik salah satu mapping IP address dan MAC address yang ada di daftar leases dan klik tombol Make Static. Maka mapping tersebut menjadi permanen.



Gambar 86 Konfigurasi Leases

#### 15.4..2 Menambahkan Static Lease

1. Klik IP → DHCP Server → Klik tab Leases. Kemudian klik tombol +.
2. Pada Addresses masukkan IP address yang hendak diberikan kepada Client dan pada MAC Address masukkan MAC address dari interface yang dimiliki oleh client. Bila ingin konfigurasi ini menjadi permanen klik Make Static.



Gambar 87 Penambahan leases baru

Konfigurasi Command Linenya:

1. Pertama cek lease yang ada:

```
[admin@MikroTik] > /ip dhcp-server lease print
```

Flags: X - disabled, R - radius, D - dynamic, B - blocked

#	ADDRESS	MAC-ADDRESS	HO.. SERVER RA..	STATUS
0	172.16.10.149	00:26:22:CE:C2:C1	to.. dhcp1	bound
1	172.16.10.100	00:26:22:CE:C2:C1		

2. Kemudian pilih nomor lease yang ada di sebelah paling kiri untuk dibuat menjadi static

```
[admin@MikroTik] > /ip dhcp-server lease make-static numbers=1
```

## 15.5 Backup dan Restore Konfigurasi

Setiap perangkat jaringan pasti memiliki umurnya masing-masing atau memiliki kerusakan akibat mati lampu, petir, dll. Oleh karena itu membackup konfigurasi dari perangkat tersebut perlu sekali dilakukan. Bila tidak seorang network administrator mungkin perlu mengkonfigurasi perangkat tersebut secara manual satu persatu. Hal ini tentu saja memakan waktu yang cukup lama. Terlebih lagi apabila anda mendaftarkan daftar user yang cukup banyak atau memiliki konfigurasi firewall yang rumit.

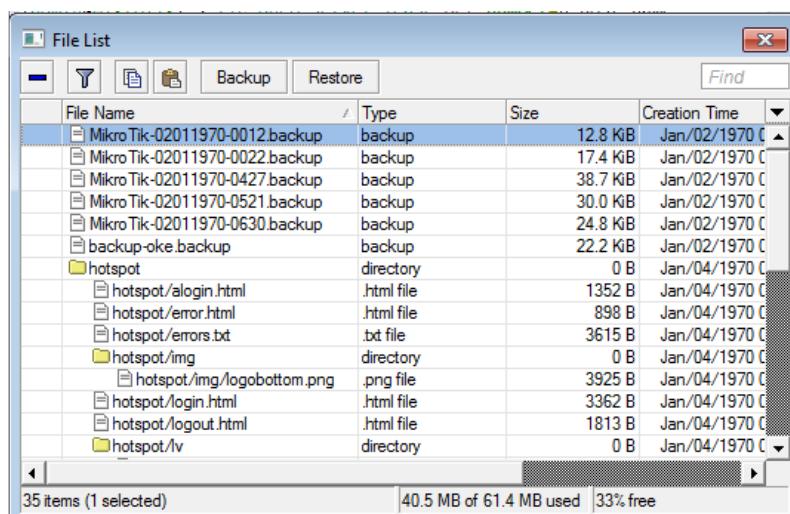
Selain itu backup juga perlu dilakukan apabila anda hendak mengubah konfigurasi perangkat anda dengan konfigurasi baru. Konfigurasi baru belum tentu selalu ideal dan lebih

baik, bisa saja menyebabkan konflik atau error pada konfigurasi yang lama. Penghapusan konfigurasi-konfigurasi lama pun bisa terjadi.

RouterOS telah menyediakan fasilitas backup di dalam sistem operasinya. Proses backup dapat dilakukan secara penuh (full) atau secara parsial. Secara parsial berarti anda hanya membackup konfigurasi tertentu saja, misalkan konfigurasi firewall saja. Pembackuan secara parsial juga dapat dilakukan untuk kepentingan analisa, dikarenakan perintah-perintah yang anda eksekusi di dalam router dapat diamati satu persatu.

- **Backup Penuh**

Untuk melakukan pembackuan secara penuh pada Winbox klik tombol **Files**, kemudian klik **Backup**.

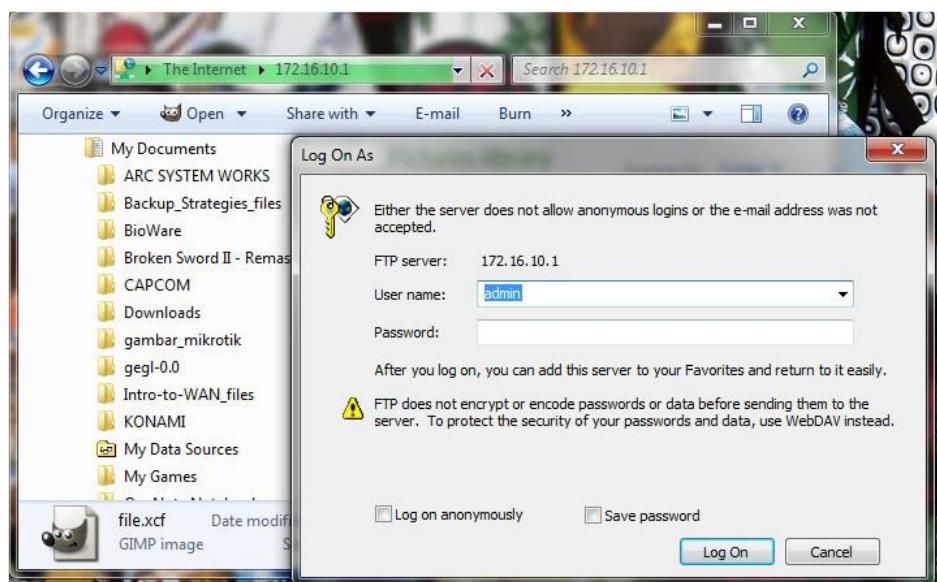


Gambar 88 Daftar file dalam Mikrotik

Konfigurasi Command Linenya:

```
[admin@MikroTik] > /system backup save name=backup-full
```

Hasil backup konfigurasi dapat diambil dengan melakukan *drag and drop* nama file ke desktop anda atau anda bisa akses melalui FTP. Untuk mengakses file backup dari FTP di Windows, buka Windows Explorer pada address bar tuliskan `ftp://<ip_address_router>` sebagai contoh: `ftp://172.16.10.1` apabila anda masih menggunakan user default maka `user=admin` dan `password=<kosong>`. Backup konfigurasi dapat disimpan di dalam komputer anda untuk menjaga apabila terjadi ketidak sengajaan penghapusan konfigurasi atau sebab lain.



Gambar 89 Mengakses Mikrotik menggunakan FTP

Untuk melakukan restore, letakkan file backup ke router menggunakan FTP atau drag and drop ke **Files** kemudian klik tombol **Restore**. Perlu diperhatikan bahwa restore akan menghapus semua konfigurasi anda yang sebelumnya.

Pada command line perintahnya adalah:

```
[admin@MikroTik] > /system backup load name=backup-full.backup
```

- **Backup Parsial**

Backup parsial dilakukan melalui command line interface. anda bisa remote menggunakan telnet atau SSH, selain itu anda juga bisa menggunakan command line dari Winbox di New Terminal. Sebagai contoh untuk melakukan backup konfigurasi firewall jalankan perintah berikut:

```
[admin@MikroTik] > /ip firewall export file=firewall-konf
```

File akan tersimpan pada daftar file router sebagai firewall-konf.rsc anda bisa atur dengan drag and drop file atau menggunakan FTP.

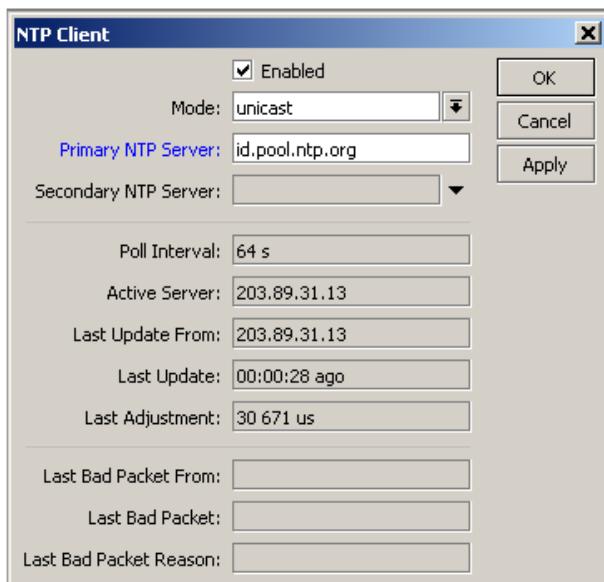
Untuk melakukan restore anda tidak bisa menggunakan cara yang sama dengan backup penuh, anda harus membuka file dengan notepad dan *copy and paste* pada terminal yang anda buka.

## 15.6 Konfigurasi NTP

Perangkat Routerboard Mikrotik tidak memiliki baterai yang menyimpan konfigurasi jam seperti pada motherboard suatu komputer. Oleh karena itu setiap kali perangkat dimatikan maka jam pada perangkat akan kembali pada konfigurasi semula. Hal ini menyebabkan jam pada perangkat bisa menjadi tidak akurat, untuk itu dibutuhkan NTP.

NTP (Network Time Protocol) adalah protokol yang didesain untuk mensinkronisasi jam dari komputer melalui suatu jaringan. NTP akan melakukan sinkronisasi jam sesuai dengan konfigurasi timezone yang anda atur dan akan disesuaikan dengan server NTP yang berada pada internet. Server NTP ini akan mensinkronkan jam sesuai dengan standard jam internasional yaitu GMT, sehingga perangkat anda akan memiliki waktu yang akurat. Untuk pengaturannya sebagai berikut:

1. Klik System → NTP Client
2. Centang pada Enabled, pilih Mode: unicast dan Primary NTP Server: id.pool.ntp.org. anda bisa gunakan server lain untuk melakukan sinkronisasi waktu.



Gambar 90 Konfigurasi NTP

Konfigurasi Command Linenya:

```
[admin@MikroTik] > /system ntp client set enabled=yes primary-
ntp=id.pool.ntp.org
```

## DAFTAR PUSTAKA

1. Toto Harjendro, Modul Pengantar Komputer dan Internet. LP3T Nurul Fikri, 2010
2. Rusmanto, Modul Wireless LAN Security, LP3T Nurul Fikri,2010
3. Dudi Fitriahadi, Modul Membangun Jaringan Komputer berbasis Windows. LP3 STT NF, 2016
4. Wahyu Januar , Modul Pengantar Komputer dan Jaringan, NF Computer, 2018
5. Dudi Fitriahadi, Modul Mikrotik, PeTIK,2019
6. All IT Ebook, CompTIA A+
7. I Putu Agus Eka Pratama, Handbook Jaringan Komputer, Informatika, 2014
8. <https://id.wikipedia.org/wiki/Inframerah>
9. <https://id.wikipedia.org/wiki/WiMAX>