BAB II

LANDASAN TEORI

2.1 Point to Point Over Ethernet (PPPOE)

Point to Point Over Ethernet (PPPOE) protokol jaringan untuk mengenkapsulasi Point-to-Point Protocol (PPP) frame dalam frame Ethernet. Hal ini digunakan terutama dengan layanan DSL di mana pengguna individu terhubung ke modem DSL over Ethernet dan di dataran jaringan Ethernet Metro. Ini dikembangkan oleh UUNET, Redback Networks dan Wind River Systems dan menyediakan dalam informasi RFC 2516 (Mamakos, L. 1999).

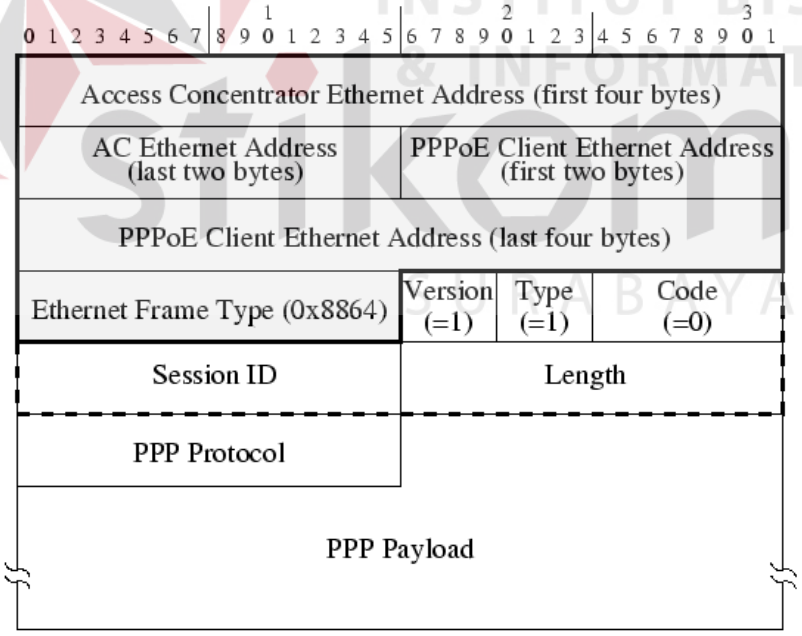
2.2 Manfaat PPPOE

Kerja standar untuk protokol PPPOE diterbitkan oleh IETF pada tahun 1999. IETF spesifikasi untuk PPPOE adalah RFC 2516 (Mamakos, L. 1999). PPPoE memperluas kemampuan asli PPP dengan memungkinkan koneksi point to point virtual atas arsitektur jaringan multipoint Ethernet. PPPOE adalah protokol yang banyak digunakan oleh ISP untuk menyediakan *digital subscriber line* (DSL) kecepatan tinggi layanan Internet, layanan yang paling populer adalah ADSL. Kesamaan antara PPP dan PPPOE telah menyebabkan adopsi luas dari PPPoE sebagai pilihan protokol untuk menerapkan kecepatan tinggi akses Internet. Penyedia layanan dapat menggunakan server otentikasi yang sama untuk sesi PPP dan PPPOE untuk menghasilkan penghematan biaya. PPPOE menggunakan metode standar enkripsi, otentikasi, dan kompresi yang ditentukan oleh PPP. PPPOE dikonfigurasi sebagai titik ke titik sambungan antara dua Port Ethernet. Sebagai sebuah protokol tunneling, PPPOE digunakan sebagai landasan yang efektif untuk transportasi paket IP pada layer jaringan. IP disalut melalui sambungan PPP dan menggunakan PPP sebagai virtual dial up hubungan antara poin pada jaringan. Dari perspektif pengguna, PPPOE sesi dimulai dengan menggunakan koneksi perangkat lunak pada mesin klien atau router. Inisiasi sesi PPPoE melibatkan identifikasi alamat perangkat remote *Media Access Control Address* (MAC). Berikut adalah keuntungan yang akan diperoleh jika metode PPPoE diterapkan :

1. Terdapat user authentication.
2. Interface PPPOE server yang terhubung dengan PPPOE client tidak memiliki IP karena PPPOE bekerja pada layer 2 OSI dengan tujuan menghindari terjadinya serangan *Denial of Service* (DoS) dan IP detection kepada server utama.
3. Fasilitas cut-off oleh PPPoE untuk user yang menggunakan program tambahan peningkat bandwidth (seperti download accelerator). Penggunaan internet setiap usernya dipantau secara oleh administrator sistem. Secara default PPPoE akan melakukan cut-off (memutuskan) Koneksi user yang lebih tinggi (burst mode) dari koneksi yang ditetapkan untuk menjaga kestabilan jaringan.

2.3 Arsitektur PPPOE

Setelah setiap sisi mengetahui alamat Ethernet dan jumlah sesi lain, sesi PPP bisa dimulai. frame PPP dienkapsulasi dalam kerangka sesi PPPOE, yang memiliki Ethernet tipe frame 0x8864 (Mamakos, L. 1999). Sebuah frame sesi PPPOE ditunjukkan gambar 2.1 dibawah ini:

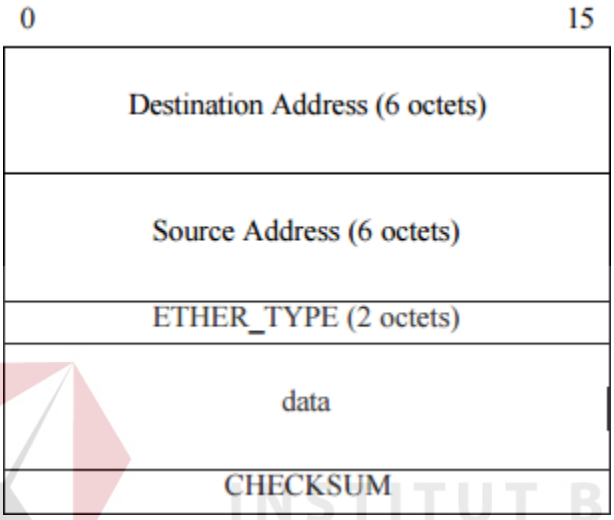


Gambar 2.1 PPPOE sesi frame

2.4 PPPOE label

2.4.1 Struktur frame PPPOE

Frame PPPOE pada dasarnya adalah sebuah frame Ethernet dengan beberapa tambahan enkapsulasi sebagai berkaitan data (Mamakos, L. 1999). gambar 2.2 dibawah ini.



Gambar 2.2 PPPOE frame structure

➢ **Address destination**

Paket alamat tujuan MAC. Pada tahap penemuan, ini mungkin berisi 0xFFFFFFFFFFFF alamat broadcast.

➢ **Source address**

Paket MAC alamat sumber.

➢ **Ether type**

Menunjukkan bahwa frame harus ditafsirkan sebagai PPPOE. Ini memiliki nilai yang sama dengan 0x8863 ditahap penemuan dan 0x8864 dalam tahap sesi.

➢ **Data**

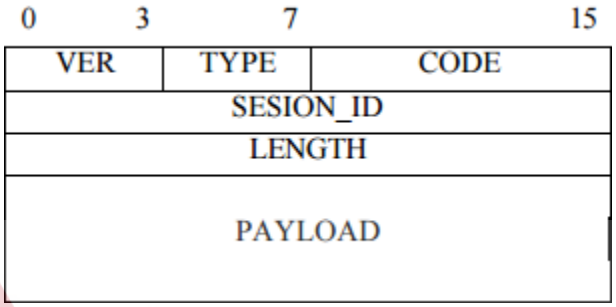
Data frame internet. Struktur data ini untuk PPPOE dijelaskan pada bagian berikutnya.

➢**Checksum**

Data frame internet checksum.

2.4.2 PPPOE frame

Ethernet frame data untuk PPPOE memiliki format (Mamakos, L. 1999) gambar 2.3 berikut:



Gambar 2.3 PPPOE frame

➢**Ver**

Empat bit ini yang menunjukkan versi PPPOE.

➢**Type**

Delapan bit ini yang menunjukkan tipe PPPOE.

➢**Code**

Delapan bit ini yang menunjukkan jenis paket PPPOE tabel 2.1 berikut:

Tabel 2.1 Tipe paket PPPOE

Code	Type of PPPOE packet
0x09	*PPPOE Active Discovery Intiation* (PADI)
0x07	*PPPOE Active Discovery Offer* (PADO)
0x19	*PPPOE Active Discovery Request* (PADR)
0x65	*PPPOE Active Discovery Session*

	Confirmation (PADS)
0xA7	*PPPOE Active Discovery terminate* (PADT)
0x0	Paket dalam tahap sesi

➢**Session ID**

Dua byte mengidentifikasi sesi PPPOE didirikan. Pada tahap penemuan, ini mengambil nilai sama dengan 0 sampai Akses konsentrator memberikan pengenal untuk sesi berlangsung. Sumber dan tujuan alamat bersama-sama unik mengidentifikasi sesi PPPOE.

➢**Payload**

Data PPPOE. Pada tahap sesi ini sebenarnya data protokol PPP. Pada tahap penemuan, yang payload berisi nol atau lebih. Setiap tag terdiri dari dua byte menunjukkan jenis, dua byte menunjukkan panjang dalam byte dan nilai. berbeda digunakan untuk menegosiasikan kondisi pembentukan sesi PPPOE.

2.5 Struktur PPPOE

Sturktur PPPOE yang terdiri dari *PPPOE Active Discovery Initiation* (PADI), *PPPOE Active Discovery Offer* (PADO), *PPPOE Active Discovery Request* (PADR), *PPPOE Active Discovery Session confirmation* (PADS), *PPPOE Active Discovery Terminate* (PADT).

➢ ***Active Discovery Initiation* (PADI)**

PPPOE client mengirimkan sebuah paket PADI ke alamat broadcast. paket ini juga dapat mengisi kolom "nama layanan" jika nama layanan telah dimasukkan pada sifat dial-up networking dari broadband PPPOE terhubung. Jika nama layanan belum masuk, bidang ini tidak dapat dihuni.

➢ ***Active Discovery Offer* (PADO)**

PPPOE Server, atau Akses konsentrator, perlu menanggapi PADI dengan PADO jika akses konsentrator dapat layanan "nama layanan" lapangan yang telah tercatat dalam paket PADI.

Jika tidak ada "nama layanan" lapangan telah terdaftar, akses konsentrator harus menanggapi dengan paket PADO yang memiliki "nama layanan" lapangan diisi dengan nama layanan yang akses konsentrator dapat melayani. Paket PADO dikirim ke alamat unicast dari klien PPPOE.

- ***PPPOE Active Discovery Request* (PADR)**

Ketika paket PADO diterima maka klien PPPoE meresponnya dengan paket PADR. Paket ini dikirim ke alamat unicast dari Akses konsentrator. Klien dapat menerima beberapa paket PADO, tapi klien merespon PADO valid pertama bahwa klien menerima. Jika paket PADI awal memiliki kosong "nama layanan" lapangan diajukan, klien akan mengisi "nama layanan" bidang paket PADR dengan nama layanan pertama yang telah dikembalikan dalam paket PADO.

- ***PPPOE Active Discovery Session confirmation* (PADS)**

Ketika PADR diterima, Access konsentrator menghasilkan identifikasi sesi unik (ID) untuk *Point to Point Protocol* (PPP) sesi akan mengembalikan ID ini untuk klien PPPOE dalam paket PADS. paket ini dikirim ke alamat unicast dari klien.

- ***PPPOE Active Discovery Terminate* (PADT)**

Sinyal dikirim untuk mengakhiri sesi PPPoE. Ini adalah cara yang tepat untuk mengakhiri sesi tetapi bukan penyebab sebenarnya untuk penghentian. Penyebabnya mungkin batas waktu yang mudah, permintaan manual dengan salah satu ujung atau keluar dari kondisi jalur.

2.6 Jenis PPPOE

Apabila menggunakan PPPOE ada empat jenis konfigurasi yang dibawah ini (Wijaya, I. H. 2006) :

1. Konfigurasi virtual private dial up network
2. Konfigurasi interface ethernet
3. Konfigurasi interface dialer
4. Konfigurasi interface ATM

2.7 Definisi berbanding PPPOE client dan PPPOE server

2.7.1 PPPOE client

Mikrotik memiliki kemampuan panggilan pada internet melalui terkoneksi PPPOE yang secara umum menggunakan internet. Jika memungkinkan untuk perangkat lain misalnya router mikrotik. Setelah PPPOE client interface akan terbuka hanya memilih port ethernet dari router mikrotik akan menghubungkan internet dilakukan pasang router pada router lain. Sementara dan menentukan PPPOE untuk mencentang dari penggunaan DNS yang akan memungkinkan mikrotik untuk menggunakan penyedia layanan DNS server.

2.7.2 PPPOE server

Jika menjalankan ISP maka PPPOE metode yang mendapatkan client untuk ke layanan. Pembuatan yang digunakan PPPOE memungkinkan untuk menyingkirkan statis alamat client IP menegakkan manajemen bandwidth dasar. Konfigurasi ini keperluan dilakukan IP pool yang merupakan kisaran alamat IP untuk router mikrotik untuk membagikan ke client. Rentang IP dari IP pool bisa bergantung sama lain yang terpilih. IP pool dilakukan kita dapat melanjutkan untuk menciptakan server PPPOE. PPPOE server akan konfigurasi pilih interface dari router mikrotik yang inginkan untuk bertindak sebagai PPPOE server dalam memasang router pada router lain dengan kartu. Kita sekarang mendapat membuat profil untuk PPPOE untuk digunakan. Profil ini dimana kita akan lakukan beberapa manajemen *bandwidth* dasar. Kita akan menentukan penggunaan IP pool membuat sebelumnya. Membuat sebagai banyak profil yang inginkan semua dengan pembatasan kecepatan *bandwidth* yang berbeda dan hanya menerapkannya pada penggunanya. Setelah profil yang telah dibuat bisa terima untnk menciptakan beberapa pengguna. Ini dilakukan *secret*. Harus memilih *username* dan *password* yang ingin mendedikasikan untuk client juga memilih profil yang telah dibuat dan siap untuk pergi. Membuat sebagai banyak penggunanya.

2.8 Routing mikrotik

2.8.1 Quick set

Mikrotik RouterOS diperkenalkan menu baru yaitu *Quick Set*. Sesuai namanya *Quick set* ini bisa digunakan untuk melakukan konfigurasi Router secara lebih cepat. Jika biasanya dalam melakukan setting Mikrotik kita perlu mengakses banyak menu, dengan *Quick set* kita tidak perlu melakukan itu. Pengaturan standard yang diperlukan untuk terkoneksi ke internet dan untuk distribusi LAN sudah tersedia pada *Quick set* (Towidjojo, R. 2012).

Beberapa lisensi level untuk menjelaskan masing-masing dibawah ini:

- **Level 0**

Lisensi mikrotik ini gratis dan tidak membutuhkan lisensi untuk penggunaannya. Tapi di Level 0 ini penggunaan fitur hanya dibatasi selama 24 jam setelah instalasi dilakukan.

- **Level 1**

Mikrotik level 1 ini hanya dapat difungsikan sebagai routing standar dengan 1 pengaturan. Dengan fungsi yang terbatas itu, mikrotik level 1 ini tidak dibatasi dengan limit waktu untuk penggunaannya.

- **Level 2**

Lisensi level 2 ini oleh mikrotik di skip tanpa ada alasan yang jelas dan dilanjutkan ke lisensi level berikutnya, yaitu lisensi level 3

- **Level 3**

Mikrotik level 1 ditambah dengan kemampuan untuk menajemen router interface ethernet. Mikrotik level 3 ini lebih banyak digunakan sebagai CPE/wireless client (Lisensi Level 3CF-CPE), atau point to point. Mikrotik level 3 ini tidak bisa difungsikan sebagai access point dengan multi client.

➢**Level 4**

Mikrotik level 4 ini merupakan mikrotik level 1 dan 3 ditambah dengan kemampuan untuk mengelola wireless client atau serial interface. Mikrotik level 4 inilah yang paling banyak digunakan karena mempunyai harga yang murah. Mikrotik level 3 ini tidak bisa difungsikan sebagai access point dengan multi client dengan 200 user aktif.

➢**Level 5**

Mikrotik level 5 ini merupakan mikrotik level 1, 3 dan 4 ditambah dengan kemampuan wireless AP. Mikrotik level 5 ini bisa digunakan sebagai aplikasi hotspot dengan 500 user aktif.

➢**Level 6**

Mikrotik level 6 ini merupakan Mikrotik semua level dan tidak memiliki limitasi apapun. Mikrotik level 6 ini bisa digunakan sebagai aplikasi hotspot dengan user aktif yang tak terbatas.

2.8.2 Address list

Deretan angka biner antara 32-bit sampai 128-bit yang dipakai sebagai alamat identifikasi untuk tiap peralatan jaringan yang menggunakan Protocol TCP/IP dan subnet yang mengacu kepada angka biner baik 32bit (IPv4) maupun 128bit (Ipv6) yang digunakan untuk membedakan network ID dengan host ID menunjukkan letak suatu host disuatu jaringan keberadaan di jaringan lokal atau jaringan luar yang sebagai pengelompokan beberapa host dalam satu network. Network untuk lakukan segmen jaringan dengan mendapatkan dinamakan juga sebagai pengelompokan sebuah jaringan dengan batasan yang dirancang dan didefinisikan oleh router. Dalam satu jaringan LAN maka network pasti akan sama maka interface untuk pilihan memasang *ether* yang bertujuan router sama ketika disampaikan pasang router lain.

2.8.3 Dynamic Host Configuration Protocol (DHCP)

Layanan yang secara otomatis memberikan nomor IP kepada komputer yang memintanya. Komputer yang memberikan nomor IP yang sebagai DHCP server sedangkan komputer yang meminta nomor IP yang sebagai DHCP Client. Dengan demikian administrator tidak perlu lagi harus memberikan nomor IP secara manual pada saat konfigurasi TCP/IP tapi cukup dengan memberikan referensi kepada DHCP Server. Pada saat kedua DHCP client dihidupkan maka komputer tersebut melakukan request ke DHCP Server untuk mendapatkan nomor IP. DHCP menjawab dengan memberikan nomor IP yang ada di database DHCP. DHCP Server setelah memberikan nomor IP maka server meminjamkan (lease) nomor IP yang ada ke DHCP Client dan mencoret nomor IP tersebut dari daftar pool. Nomor IP diberikan bersama dengan subnet mask dan default gateway. Jika tidak ada lagi nomor IP yang dapat diberikan, maka client tidak dapat menginisialisasi TCP/IP tidak dapat tersambung pada jaringan.

2.8.3.1 DHCP client

Pengaturan protocol dilakukan di client bahwa mode static atau dynamic didalam DHCP client meminta server untuk memberikan ip, sebelum client mendapatkan IP dynamic untuk client terlebih dahulu merequest ke server yang ada pada jaringan tersebut, dan server melakukan pemeriksaan terhadap client yang meminta IP dynamic, jika sesuai dan diperbolehkan maka server baru mengirimkan IP ke client. system operasi klien jaringan (Windows NT Workstation, Windows 200 Profesional, Windows XP, Windows Vista atau GNU/Linux).

2.8.3.2 DHCP server

DHCP server configurasi protocol (IP address) disediakan oleh server untuk diberikan ke client yang meminta / request ip. (ip address) yang diberikan, ditentukan oleh server pemberian jatah ip bisa dalam hitungan menit, jam, hari dan bulan, juga disertai dengan netmask, gateway dan dns server, itu semua tergantung dari pengaturan di servernya. Beberapa system operasi jaringan seperti Windows NT Server, Windows 200 Server, Windows 2003 Server atau GNU/Linux.

2.8.3.3 Fungsi DHCP

1. DHCP memiliki fungsi utama mendistribusikan IP address secara otomatis kepada setiap client yang terhubung dengan jaringan komputer.
2. DHCP akan memberikan kemudahan bagi seorang network administrator dalam mengelola jaringan komputer, karena alokasi IP address dapat ditentukan secara otomatis dan dalam satu kali kerja.
3. DHCP server selain bisa memberikan IP address secara dinamik, juga bisa memberikan IP address secara statis kepada client yang terhubung ke jaringan komputer.
4. DHCP memberikan kemudahan dalam proses komunikasi data antar komputer.

2.8.3.4 Lakukan membuat cara kerja DHCP

DHCP menggunakan 5 tahapan proses untuk memberikan konfigurasi nomor IP Untuk menjelaskan mengenai cara kerja DHCP setiap tahap proses yang terjadi pada layanan DHCP sebagai dibawah ini :

- **IP Least Request**

Komputer client meminta alamat IP ke server.

- **IP Least Offer**

DHCP server yang memiliki list alamat IP memberikan penawaran kepada komputer client.

- **IP Lease Selection**

Komputer client memilih/ menyeleksi penawaran yang pertama kali diberikan DHCP, kemudian melakukan broadcast dengan mengirim pesan bahwa komputer client menyetujui penawaran ini.

- **IP Lease Acknowledge**

  Pada tahap ini DHCP server menerima pesan tersebut dan mulai mengirim suatu paket acknowledge (DHCPACK) kepada client.

- **Lease Period**

  Pemakaian DHCP Client tersebut dinyatakan selesai, nomor IP tersebut dikembalikan kepada DHCP server, dan server dapat memberikan nomor IP tersebut kepada client yang membutuhkan.

2.8.4 Domain Name Server (DNS)

Distribute database system yang digunakan untuk pencarian *name resolution* (nama komputer) di jaringan yang mengunakan *Transmission Control Protocol/Internet Protocol* (TCP/IP). DNS biasa digunakan pada aplikasi yang terhubung ke Internet seperti web browser atau e-mail, dimana DNS membantu memetakan host name sebuah komputer ke IP address. Dimana setiap komputer di jaringan Internet memiliki *host name* (nama komputer) dan *Internet Protocol* (IP) address. Setiap client yang akan mengkoneksikan komputer yang satu ke komputer yang maka menggunakan host name. Lalu komputer akan menghubungi DNS server kepada mikrotik yang berfungsi agar komputer yang berada dalam jaringan yang membutuhkan diinginkan domain dari sebuah situs. Misalnya (google, yahoo, facebook dan lain-lain). Dilakukan memeriksa *host name* yang berapa IP address. IP address yang digunakan untuk mengkoneksikan komputer dengan komputer lainnya.

2.8.5 Interface list

Beberapa interface list yang menggunakan konfigurasi saat ini keperluan seperti apa membuatnya dan menjelaskan fungsi dibawah ini:

- **Interface**

Untuk melihat status *ether* dari kabel LAN dimasukkan yang telah pasang router dengan router lain dilakukan konfigurasi sudah aktifkan maka menuliskan dari

comment pada *address list* baris sudah bisa isi terdaftarkan judul biar mudah terserah yang bertujuan kita.

➢**Ethernet**

Untuk melihat status *ether* dari kabel LAN dimasukkan yang tetap pasang router dengan router lain tidak berubah dilakukan konfigurasi sudah aktifkan maka tertulis tetap dari *comment* pada *address list* baris sudah bisa isi terdaftarkan judul biar mudah terserah yang bertujuan kita.

➢ ***Ethernet over Internet Protokol*** **(EoIP) tunnel**

Protokol yang membuat sebuah Ethernet tunnel antara dua router di atas koneksi IP. Interface EoIP muncul sebagai interface Ethernet. Ketika fungsi bridging dari router diaktifkan, semua lalu lintas Ethernet (semua protokol Ethernet) akan dijembatani sama seperti jika ada dimana interface Ethernet fisik dan kabel antara dua router (dengan bridging diaktifkan). Pengertian IPIP tunnel adalah sebuah protokol sederhana yang mengenkapsulasi paket IP dalam IP untuk membuat tunnel di antara dua router. IPIP tunnel interface muncul sebagai interface dalam daftar interface. Banyak router, termasuk Cisco dan berbasis Linux, mendukung protokol ini. Maksimum jumlah tunnel yang dapat dibuat EOIP tunnel adalah 65535.

➢**IP tunnel**

Sebuah protokol sederhana yang mengenkapsulasi paket IP dalam IP untuk membuat tunnel di antara dua router. IPIP tunnel interface muncul sebagai interface dalam daftar interface. Banyak router, termasuk Cisco dan berbasis Linux, mendukung protokol ini.

➢***Generic Routing encapsulation*** **(GRE) tunnel**

Sebuah tunnelling protocol yang sebenarnya dikembangkan oleh Cisco System. Dengan menggunakan protokol ini kita dapat melakukan enkapsulasi berbagai protokol yang dibuat untuk kebutuhan link virtual point-to point. Selain GRE Tunnel pada MikroTik juga memiliki tunnelling protocol yang lain seperti EoIP dan IPIP yang mana pembahasannya telah lalu. Baik jenis GRE, EoIP, IPIP yang semua pada

dasarnya dikembangkan sebagai 'stateless tunnel'. Dimana ketika terdapat link tunnel yang down, maka semua trafik yang melewatinya akan terkena drop/blackhole.

➢ ***Virtual Local Area Network*** **(VLAN)**

Virtual Local Area Network (VLAN) adalah lapisan 2 metode yang memungkinkan untuk memiliki beberapa Virtual LAN pada antarmuka fisik tunggal (ethernet, wireless, dll), memberikan kemampuan untuk memisahkan LAN secara efisien. Kita perlu menggunakan RouterOS MikroTik (serta Cisco IOS, Linux dan sistem router lain) untuk menandai paket ini serta untuk menerima dan rute yang ditandai. VLAN bekerja pada OSI Layer 2 mendapat digunakan hanya sebagai antarmuka jaringan lain tanpa batasan.VLAN berhasil melewati jembatan Ethernet biasa. penggunaan VLAN melalui link nirkabel dan menempatkan beberapa interface VLAN pada wireless interface tunggal. Jika perhatikan VLAN bukanlah sebagai terowongan/tunnel tetapi protokol penuh (tidak memiliki ladang tambahan untuk mengangkut MAC address dari pengirim dan penerima) maka pembatasan yang sama berlaku untuk menjembatani atas VLAN untuk antarmuka(interface) nirkabel bridging biasa. Sementara klien nirkabel dapat berpartisipasi dalam VLAN memakai antarmuka nirkabel, tidaklah mungkin untuk memiliki VLAN memakai antarmuka(interface) nirkabel dalam modus stasiun dijembatani dengan interface lain.

➢ ***Virtual Router Redundancy Protocol*** **(VRRP)**

Virtual Router Redundancy Protocol (VRRP) Sebuah protokol pemilihan yang menyediakan availabelity tinggi untuk router. Sejumlah router dapat berpartisipasi dalam satu atau lebih router virtual. Satu atau lebih alamat IP mungkin ditugaskan ke router virtual.

➢ **Bonding**

Teknologi yang memungkinkan agregasi dari beberapa interface ethernet menjadi sebuah satu link virtual, sehingga bisa mendapatkan kecepatan data/bandwidth yang lebih besar dan bisa menjadi link failover.

➢ ***Long Term Evolution*** **(LTE)**

Long Term Evolution (LTE) Sebuah nama baru dari layanan yang mempunyai kemampuan tinggi dalam sistem komunikasi bergerak (mobile). Merupakan langkah menuju generasi ke4 (4G) dari teknologi radio yang dirancang untuk meningkatkan kapasitas dan kecepatan jaringan telepon mobile. Dimana generasi sebelumnya dikenal sebagai 3G.

2.8.6 Route list

Routing merupakan sebuah mekanisme pengiriman paket data yang ditransmisikan dari satu network ke network yang lain. Pada sebuah router, biasanya mempunyai sebuah tabel routing atau lebih yang menyimpan informasi jalur routing yang akan digunakan ketika ada pengiriman data yang melewati router. Pada kasus tertentu untuk menuju ke suatu tujuan, router tidak hanya memiliki satu gateway, misalnya karena router harus menghubungkan banyak jaringan yang memiliki segmen yang berbeda.

2.8.7 Firewall

Perangkat yang berfungsi untuk memeriksa dan menentukan paket data yang dapat keluar atau masuk dari sebuah jaringan. Dengan kemampuan tersebut maka firewall berperan dalam melindungi jaringan dari serangan yang berasal dari *outside network* (jaringan luar). Firewall mengimplementasikan packet filtering dan dengan demikian menyediakan fungsi keamanan yang digunakan untuk mengelola aliran data dari dan melalui router. Sebagai contoh, firewall difungsikan untuk melindungi jaringan lokal (LAN) dari kemungkinan serangan yang datang dari Internet. Selain untuk melindungi jaringan, firewall juga difungsikan untuk melindungi komputer user atau host.

➢ **Filter rules**

Merupakan salah satu firewall pada mikrotik yang digunakan untuk menentukan apakah suatu paket data dapat masuk atau tidak kedalam sistem router mikrotik paket data yang akan ditangani fitur filter ini adalah paket data yang ditunjukan pada salah satu interface router.

➢ ***Network Area Translation*** **(NAT)**

Suatu cara untuk menghubungkan lebih dari satu computer ke jaringan internet dengan memakai satu alamat IP. Cara ini dipakai lantaran ketersediaan alamat IP yang terbatas dikeperluan akan *security* (keamanan) jaringan lokal, serta keringanan dan fleksibilitas dalam administrasi jaringan. NAT bekerja dengan mengalihkan satu paket data dari satu alamat IP ke alamat IP yang lain. Saat satu paket diarahkan maka NAT akan mengingat dari lokasi mana asal paket serta kemana maksud paket itu. Ketika ada paket kembali maka NAT dapat mengirimkannya ke asal paket. Dengan kata lain host hanya dapat menerima paket yang di kirim atau yang diperintahnya hingga komunikasi mampu berjalan dengan baik. Jaringan *local Area Network* (LAN) yang memakai NAT disebut dengan natted jaringan. Di MikroTik NAT dapat dipakai untuk komunikasi internal serta komunikasi eksternal. Tujuannya pengalihan data bisa dikerjakan untuk paket yang datang dari jaringan natted (internal) ke jaringan luar (eksternal) atau dari jaringan luar menuju jaringan natted. Atau kita sebut saja komunikasi dua arah dari serta ke jaringan natted (internal).

➢ **Mangle**

Mangle untuk menandai paket/koneksi, kemudian kita gunakan untuk bandwidth management. Kita juga bisa membuat mangle untuk melakukan filtering. Firewall filter tidak dapat melakukan penandaan pada paket atau koneksi, akan tetapi kita bisa kombinasikan mangle dan firewall filter. Kita ditandai terlebih dahulu paket atau koneksi dengan mangle, kemudian kita definisikan di firewall filter.

➢ **Service ports**

Nomor yang sudah ada daftar nama jaringan protokol yang menggunakan port.

➢ **Connections**

Untuk melihat status alamat sumber dan alamat tujuan dengan menggunakan protokol yang butuh diinginkan sesuai router pasang dengan router lain lakukan konfigurasi sudah ada aktifkan.

➢**Address lists**

Digunakan untuk memberikan sebuah nama pada sebuah IP address atau sekelompok ip address yang fungsin untuk mempermudah admin dalam memanage firewall yang digunakan. Terlihat dalam konfigurasi diatas setiap ada sources address yang dimasukan, selalu menuliskan IP address. Dengan adanya fitur address list admin hanya perlu menuliskan address list dari IP address yang sudah ada. Berikut perintah untuk membuat address list.

➢**Layer 7 protocols**

Kita bisa menerapkan filtering pada layer 7 menggunakan firewall filter. Di mikrotik, penambahan regexp bisa dilakukan di menu Layer 7 Protocol. Setelah menambahkan regexp, dilakukan filtering dengan mendefinisikan Layer 7 Protocol pada rule filter yang membuat. Perlu diketahui bahwa penggunaan regexp, akan membutuhkan recource CPU yang lebih tinggi dari rule biasa.

2.8.8 Point to Point Protocol (PPP)

Point to Point Protocol (PPP) yang menggunakan konfigurasi saat ini keperluan seperti apa membuatnya dan menjelaskan fungsi dibawah ini:

➢**Interface**

Membuat tambahan menu konfigurasi saat ini yang diperlukan.

➢**PPPOE Server**

Point to Point Protocol over Ethernet (PPPOE) server protokol menyediakan manajemen pengguna yang luas, manajemen jaringan dan manfaat akuntansi untuk ISP dan administrator jaringan. Saat PPPOE digunakan terutama oleh ISP untuk mengontrol koneksi client untuk xDSL dan modem kabel serta jaringan Ethernet biasa. PPPOE merupakan perpanjangan dari Point standar Point Protocol (PPP). Perbedaan antara mereka dinyatakan dalam metode transportasi: PPPOE mempekerjakan Ethernet bukannya koneksi modem serial. PPPOE digunakan untuk membagikan alamat IP untuk klien berdasarkan otentikasi dengan username (dan juga jika diperlukan, oleh workstation) sebagai lawan workstation hanya otentikasi di

mana alamat IP statis atau DHCP digunakan. Disarankan untuk tidak menggunakan alamat IP statis atau DHCP pada interface yang sama seperti PPPOE untuk alasan keamanan. Klien dan server PPPOE bekerja selama setiap tingkat Layer2 Ethernet antarmuka pada router - wireless 802.11 (Aironet, Cisco, WaveLAN, Prism, Atheros), 10/100/1000 Mbit / s Ethernet, RadioLan dan EoIP (Ethernet over IP tunnel).

- **Secret**

Membuat pendaftaran identitas lokasi area dilakukan nama tempat akan menuliskan diperlukan password dan juga celluar ID yang membutuhkan alamat lokal untuk alamat mengendalikan yang bertujuan kita disampaikan PPP profiles.

- **Profiles**

Membuat pendaftaran identitas lokasi area dilakukan nama tempat akan tertulis untuk bisa alamat lokal untuk alamat mengendalikan sendiri searah bertujuan kita.

- **Active connections**

Membuat pendaftaran nama sudah ada bisa aktifkan.

2.9 Internet Protocol Version 4 (IPv4)

Internet Protocol Version 4 (IPv4) yang merupakan jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IP versi 4. IP versi ini memiliki keterbatasan yakni hanya mampu mengalamati sebanyak 4 miliar host komputer di seluruh dunia. Alamat IP versi 4 umumnya diekspresikan dalam notasi desimal bertitik, yang dibagi ke dalam empat buah oktet berukuran 8-bit. Karena setiap oktet berukuran 8-bit, maka nilainya berkisar antara 0 hingga 255 (terdapat beberapa pengecualian nilai).

2.9.1 Representasi alamat

Alamat IP versi 4 umumnya diekspresikan dalam notasi desimal bertitik (dotted-decimal notation), yang dibagi ke dalam empat buah oktet berukuran 8-bit. Dalam beberapa buku referensi, format bentuknya adalah w.x.y.z. Karena setiap oktet berukuran 8-bit, maka nilainya berkisar antara 0 hingga 255 (meskipun begitu, terdapat beberapa

pengecualian nilai). Alamat IP yang dimiliki oleh sebuah *host* dapat dibagi dengan menggunakan subnet mask jaringan terdiri dari 2 dibawah ini:

- Network Identifier/NetID atau Network Address (alamat jaringan) yang digunakan khusus untuk mengidentifikasikan alamat jaringan di mana host berada. Dalam banyak kasus, sebuah alamat network identifier adalah sama dengan segmen jaringan fisik dengan batasan yang dibuat dan didefinisikan oleh router IP. Meskipun demikian, ada beberapa kasus di mana beberapa jaringan logis terdapat di dalam sebuah segmen jaringan fisik yang sama dengan menggunakan sebuah praktek yang disebut sebagai multinetting. Semua sistem di dalam sebuah jaringan fisik yang sama harus memiliki alamat network identifier yang sama. Network identifier juga harus bersifat unik dalam sebuah internetwork. Jika semua node di dalam jaringan logis yang sama tidak dikonfigurasikan dengan menggunakan network identifier yang sama, maka terjadilah masalah yang disebut dengan routing error.
- Host Identifier/HostID atau Host address (alamat host) yang digunakan khusus untuk mengidentifikasikan alamat host (dapat berupa workstation, server atau sistem lainnya yang berbasis teknologi (TCP/IP) di dalam jaringan.

2.9.2 Jenis alamat

Beberapa alamat IPv4 yang dibawah ini:

- **Alamat Unicast**

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

- **Alamat Broadcast**

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

- **Alamat Multicast**

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

2.9.3 Kelas IPv4

Beberapa lima kelas dari kelas A, kelas B, kelas C, kelas D dan kelas E yang dibawah ini:

- **Kelas A**

Digunakan untuk jaringan WAN, Ip address nya pada bagian pertama antara 0-127, dan yang merupakan Net ID nya yaitu 1 bagian yang pertama. Subnet mask nya 255.0.0.0.

- **Kelas B**

Biasanya digunakan untuk jaringan MAN, Ip address nya pada bagian pertama antara 128-191, dan yang merupakan network ID nya yaitu 2 bagian pertama. Subnet masknya 255.255.0.0.

- **Kelas C**

Biasanya digunakan untuk jaringan LAN, Ip address nya pada bagian pertama antara 192-223, dan yang merupakan network ID nya yaitu 3 bagian pertama. Subnet masknya 255.255.255.0.

- **Kelas D**

Biasanya digunakan untuk keperluan multicasting. IP address nya pada bagian pertama antara 224-247. Dalam multicasting tidak dikenal network ID dan host ID.

- **Kelas E**

Biasanya digunakan untuk keperluan umum. IP address nya pada bagian pertama antara 248-255.

2.9.4 Subnet mask

Istilah teknologi informasi dalam bahasa Inggris yang mengacu kepada angka biner 32 bit yang digunakan untuk membedakan network ID dengan host ID, menunjukkan letak suatu host, apakah berada di jaringan lokal atau jaringan luar. RFC 950 mendefinisikan penggunaan sebuah subnet mask yang disebut juga sebagai address mask sebagai sebuah nilai 32-bit yang digunakan untuk membedakan network identifier dari host identifier di dalam sebuah alamat IP. Bit-bit subnet mask yang didefinisikan, adalah sebagai berikut :

- Semua bit yang ditujukan agar digunakan oleh network identifier diset ke nilai 1.
- Semua bit yang ditujukan agar digunakan oleh host identifier diset ke nilai 0.

Setiap host di dalam sebuah jaringan yang menggunakan TCP\IP membutuhkan sebuah subnet mask meskipun berada di dalam sebuah jaringan dengan satu segmen saja. Entah itu subnet mask default (ketika memakai sering network identifier berbasis kelas) ataupun subnet mask yang dikustomisasi (diperlukan menggunakan untuk membuat subnet atau supernet) harus dikonfigurasi di dalam setiap node TCP\IP.

2.10 Definisi dua berbanding TCP dan UDP menggunakan PORT

2.10.1 Transmission Control Protocol (TCP)

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

Karakteristik dari TCP yang dibawah ini:

1. Reliable berarti data ditransfer ke tujuannya dalam suatu urutan seperti ketika dikirim.
2. Berorientasi sambungan (*connection-oriented*): Sebelum data dapat ditransmisikan antara dua host, dua proses yang berjalan pada lapisan aplikasi harus melakukan negosiasi membuat sesi koneksi terlebih dahulu. Koneksi TCP ditutup dengan menggunakan proses terminasi koneksi TCP (*TCP connection termination*).
3. Full-duplex: Untuk setiap host TCP, koneksi yang terjadi antara dua host terdiri atas dua buah jalur, yakni jalur keluar dan jalur masuk. Dengan menggunakan teknologi lapisan yang lebih rendah yang mendukung full-duplex, maka data pun dapat secara simultan diterima dan dikirim. Header TCP berisi nomor urut (*TCP sequence number*) dari data yang ditransmisikan dan sebuah acknowledgment dari data yang masuk.
4. Memiliki layanan *flow control*: Untuk mencegah data terlalu banyak dikirimkan pada satu waktu, yang akhirnya membuat "macet" jaringan internetwork IP, TCP mengimplementasikan layanan *flow control* yang dimiliki oleh pihak pengirim yang secara terus menerus memantau dan membatasi jumlah data yang dikirimkan pada satu waktu. Untuk mencegah pihak penerima untuk memperoleh data yang tidak dapat disangganya sebagai *buffer*, TCP juga mengimplementasikan flow control dalam pihak penerima, yang mengindikasikan jumlah buffer yang masih tersedia dalam pihak penerima.

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

Beberapa kegunaan dari TCP yang dibawah ini:

1. Menyediakan komunikasi logika antar proses aplikasi yang berjalan pada host yang berbeda.
2. Protokol transport berjalan pada end systems.
3. Pengiriman file (file transfer). *File Transfer Protocol* (FTP) memungkinkan pengguna komputer yang satu untuk dapat mengirim ataupun menerima file ke komputer jaringan. Karena masalah keamanan data, maka FTP seringkali memerlukan nama pengguna (*username*) dan password, meskipun banyak juga FTP yang dapat diakses melalui tidak bisa password sebagai *anonymous*.
4. Remote login. Network terminal Protokol (telnet) memungkinkan pengguna komputer dapat melakukan log in ke dalam suatu komputer didalam suatu jaringan. Jadi hal ini berarti bahwa pengguna menggunakan komputernya sebagai perpanjangan tangan dari komputer jaringan.
5. Computer mail. Digunakan untuk menerapkan sistem elektronik mail.
6. *Network File System* (NFS). Pelayanan akses file-file jarak jauh yg memungkinkan klien-klien untuk mengakses file-file pada komputer jaringan jarak jauh walaupun file tersebut disimpan secara lokal.
7. Remote execution. Memungkinkan pengguna komputer untuk menjalankan suatu program didalam komputer yg berbeda. Biasanya berguna jika pengguna menggunakan komputer yg terbatas, sedangkan ia memerlukan sumber yg banyak dalam suatu system komputer. Ada beberapa jenis remote execution, ada yg berupa perintah-perintah dasar saja, yaitu yang dapat dijalankan dalam system komputer yg sama dan ada pula yg menggunakan "prosedure remote call system", yg memungkinkan program untuk memanggil subroutine yg akan dijalankan di system komputer yg berbeda. (sebagai contoh dalam Berkeley UNIX ada perintah "rsh" dan "rexec").
8. Name servers. Nama database alamat yg digunakan pada internet.

Header TCP

Ukuran TCP header paling kecil (ketika tidak ada tambahan opsi TCP) adalah 20 byte.

Aplikasi yang menggunakan TCP

- ***World Wide Web* (WWW)**

World Wide Web (WWW) Aplikasi ini pada prinsipnya mirip dengan aplikasi gopher, yakni penyediaan database yang dapat diakses tidak hanya berupa text, namun dapat berupa gambar/image, suara, video. penyajiannya pun dapat dilakukan secara live. Dengan demikian, jenis informasi yang dapat disediakan sangat banyak dan dapat dibuat dengan tampilan yang lebih menarik. Hal ini dimungkinkan karena Web menggunakan teknologi hypertext. Karena itu, protokol yang digunakan untuk aplikasi ini dikenal dengan dinamakan *HyperText Transfer Protocol* (HTTP).

- **Archie**

Aplikasi FTP memungkinkan kita mentransfer file dari manapun di seluruh dunia. Hal itu dengan anggapan bahwa kita telah mengetahui lokasi di mana file yang kita cari berada. Namun jika kita belum mengetahui di mana file yang kita cari berada, kita memerlukan aplikasi untuk membantu kita mencari di mana file tersebut berada.

Cara kerja Archie dapat dijelaskan sebagai berikut. Server Archie secara berkala melakukan anonymous ftp ke sejumlah FTP Server dan mengambil informasi daftar seluruh file yang ada pada FTP Server. Daftar ini disusun berdasarkan letak file dalam direktori/sub direktori, sehingga mudah untuk menemukan file tersebut. File-file yang berisi daftar file tiap FTP Server ini merupakan database dari Archie Server. Jika ada query ke Archie Server yang menanyakan suatu file, server mencari dalam daftar tadi dan mengirimkan seluruh jawaban yang berkaitan dengan file tersebut. Informasi yang diberikan adalah alamat FTP Server yang memiliki file tersebut dan letak file dalam struktur direktori.

- ***Wide Area Information Services* (WAIS)**

Wide Area Information Service (WAIS) merupakan salah satu servis pada internet yang memungkinkan kita mencari melalaui materi yang terindeks dan menemukan

dokumen/artikel berdasarkan isi artikel. Jadi pada dasarnya, WAIS memberikan layanan untuk mencari artikel yang berisi kata-kata kunci yang diajukan sebagai dasar pencarian.

Aplikasi WAIS biasanya berbasis text. Untuk membuat suatu dokumen dapat dicari melalaui WAIS Server, harus dibuat terlebih dahulu index dari dokumentasi. Setiap kata dalam dokumen tersebut diurut dan dihitung jumlahnya. Jika ada query dari client, index akan diperiksa dan hasilnya, yakni dokumen yang memiliki kata-kata ditampilkan. Karena kemungkinan ada banyak dokumen yang memiliki kata-kata yang kita ajukan, maka beberapa dokumen yang memiliki kata kunci diberi skor/nilai. Dokumen yang paling banyak mengandung kata-kata kunci akan mendapat skor tertinggi. Dengan demikian, user mendapatkan informasi kemungkinan terbesar dari bebarapa dokumen yang mengandung kumpulan kata yang diajukannya.

- **FAX Internet**

Mesin FAX sebagai pengirim dan penerima berita tertulis melalaui telepon saat ini hampir dimiliki oleh semua kantor. Melalaui gateway Internet FAX, pengiriman FAX dapat dilakukan melalaui e-mail. Gateway akan menerjemahkan pesan e-mail dan menghubungi mesin FAX tujuan melalui jalur telepon secara otomatis. Tentu saja, akses untuk ini terbatas (*private*).

2.10.2 User Datagram Protocol (UDP)

User Datagram Protocol (UDP) merupakan salah satu protokol lapisan transpor TCP/IP yang mendukung komunikasi yang tidak andal (*unreliable*), tanpa koneksi (*connectionless*) antara host-host dalam jaringan yang menggunakan TCP/IP.

Karakteristik dari UDP yang terdiri dari 4 jenis dibawah ini:

1. *Connectionless* (tanpa koneksi): Pesan-pesan UDP akan dikirimkan tanpa harus dilakukan proses negosiasi koneksi antara dua host yang hendak berukar informasi.
2. *Unreliable* (tidak andal): Pesan-pesan UDP akan dikirimkan sebagai datagram tanpa adanya nomor urut atau pesan *acknowledgment*. Protokol lapisan aplikasi

yang berjalan di atas UDP harus melakukan pemulihan terhadap pesan-pesan yang hilang selama transmisi. Umumnya, protokol lapisan aplikasi yang berjalan di atas UDP mengimplementasikan layanan keandalan mereka masing-masing, atau mengirim pesan secara periodik atau dengan menggunakan waktu yang telah didefinisikan.

3. UDP menyediakan mekanisme untuk mengirim pesan-pesan ke sebuah protokol lapisan aplikasi atau proses tertentu di dalam sebuah host dalam jaringan yang menggunakan TCP/IP. HeaderUDP berisi field *Source Process Identification* dan *Destination Process Identification*.
4. UDP menyediakan penghitungan checksum berukuran 16-bit terhadap keseluruhan pesan UDP.

Beberapa kegunaan dari UDP yang terdiri dari 4 jenis dibawah ini:

1. Protokol yang berat ringan (*lightweight*): Untuk menghemat sumber daya memori dan prosesor, beberapa protokol lapisan aplikasi membutuhkan penggunaan protokol yang ringan yang dapat melakukan fungsi-fungsi spesifik dengan saling bertukar pesan. Contoh dari protokol yang ringan adalah fungsi query nama dalam protokol lapisan aplikasi *Domain Name System*.
2. Protokol lapisan aplikasi yang mengimplementasikan layanan keandalan: Jika protokol lapisan aplikasi menyediakan layanan transfer data yang andal, maka kebutuhan terhadap keandalan yang ditawarkan oleh TCP pun menjadi tidak ada. Contoh dari protokol seperti ini dalam *Trivial File Transfer Protocol* (TFTP) dan *Network File System* (NFS)
3. Protokol yang tidak membutuhkan keandalan. Contoh protokol ini adalah protokol *Routing Information Protocol* (RIP).
4. Transmisi broadcast: Karena UDP merupakan protokol yang tidak perlu membuat koneksi terlebih dahulu dengan sebuah host tertentu, maka transmisi broadcast pun dimungkinkan. Sebuah protokol lapisan aplikasi dapat mengirimkan paket data ke beberapa tujuan dengan menggunakan alamat multicast atau broadcast. Hal ini kontras dengan protokol TCP yang hanya dapat mengirimkan transmisi one-to-one. Contoh: query nama dalam protokol NetBIOS Name Service.

Header UDP

Header UDP diwujudkan sebagai sebuah header dengan 4 buah field memiliki ukuran yang tetap.

Aplikasi yang menggunakan UDP

- *Domain Name System* (DNS) 53
- *Simple Network Management Protocol*, (SNMP) 161, 162
- *Trivial File Transfer Protocol* (TFTP) 69
- SunRPC port 111.

2.10.3 Port TCP dan Port UDP

Masing-masing Port TCP dan Port UDP akan menjelaskan tabel 2.2 dibawah ini:

- **Port TCP**

Port TCP mampu mengindikasikan sebuah lokasi tertentu untuk menyampaikan segmen TCP yang dikirimkan yang diidentifikasi dengan TCP Port Number. Nomor di bawah angka 1024 merupakan port yang umum digunakan dan ditetapkan oleh *Internet Assigned Number Authority* (IANA). Port TCP merupakan hal yang berbeda dibandingkan dengan port UDP, meskipun mereka memiliki nomor port yang sama. Port TCP merepresentasikan satu sisi dari sebuah koneksi TCP untuk protokol lapisan aplikasi, sementara port UDP merepresentasikan sebuah antrean pesan UDP untuk protokol lapisan aplikasi. Protokol lapisan aplikasi yang menggunakan port TCP dan port UDP dalam nomor yang sama juga tidak harus sama. Misalnya protokol *Extended Filename Server* (EFS) menggunakan port TCP dengan nomor 520, dan protokol *Routing Information Protocol* (RIP) menggunakan port UDP juga dengan nomor 520. Jelas, dua protokol tersebut sangatlah berbeda bahwa untuk menyebutkan sebuah nomor port, sebutkan juga jenis port yang digunakannya PORTtcp-1

- **Port UDP**

UDP juga memiliki saluran untuk mengirimkan informasi antar host, yang disebut dengan UDP Port. Untuk menggunakan protokol UDP, sebuah aplikasi harus

menyediakan alamat IP dan nomor UDP Port dari host yang dituju. Sebuah UDP port berfungsi sebagai sebuah multiplexed message queue, yang berarti bahwa UDP port tersebut dapat menerima beberapa pesan secara sekaligus. Setiap port diidentifikasi dengan nomor yang unik, seperti halnya TCP, tetapi meskipun begitu, UDP Port berbeda dengan TCP Port meskipun memiliki nomor port yang sama.

2.10.4 Tabel Port TCP dan UDP

Tabel 2.2 TCP dan UDP

TCP	Bersifat TCP	UDP	Bersifat UDP
Beroperasi berdasarkan konsep koneksi.	**Dapat diandalkan** Jika sambungan terputus ketika mengirim sebuah pesan maka server akan meminta bagian yang hilang. Jadi tidak akan terjadi data yang korup ketika mentransfer sebuah data.	Tidak berdasarkan konsep koneksi, jadi harus membuat kode sendiri.	**Tidak dapat diandalkan** Jika mengirimkan suatu pesan atau data, kita tidak akan tahu apakah sudah terkirim atau belum dan apakah sebagian dari pesan tersebut hilang atau tidak ketika proses pengiriman. Jadi akan ada kemungkinan terjadinya data yang korup.
Jaminan pengiriman-penerimaan data akan reliable dan teratur.	**Berurutan** Ketika mengrimkan dua pesan secara berurutan / satu demi satu. TCP akan mengirimkannya secara berurutan. Tidak perlu khawatir data tiba	Tidak ada jaminan bahwa pengiriman dan penerimaan data akan reliable dan teratur, sehingga paket data mungkin dapat kurang,	**Tidak berurutan** Ketika mengrimkan dua pesan secara berurutan / satu demi satu. Tidak dapat dipastikan

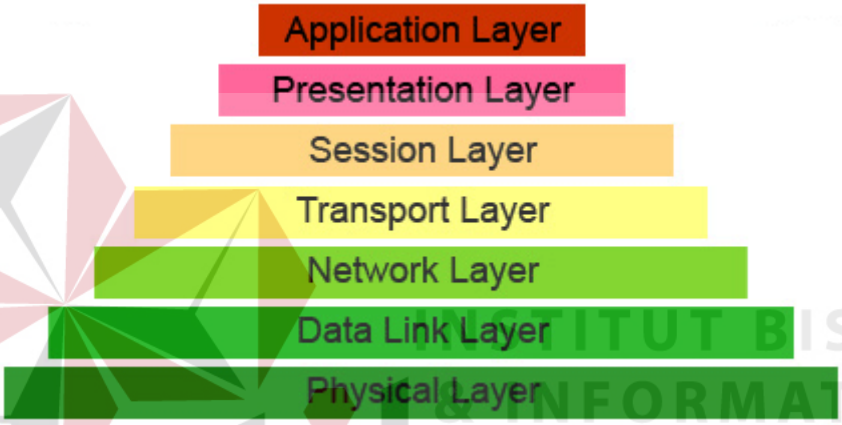
	dengan urutan yang salah.	terduplikat, atau bahkan tidak sampai sama sekali.	data mana yang akan datang terlebih dahulu.
Secara otomatis memecah data ke dalam paket-paket.	**Berorientasi sambungan (*connection oriented*)** Sebelum data dapat ditransmisikan antara dua host, dua proses yang berjalan pada lapisan aplikasi harus melakukan negosiasi untuk membuat sesi koneksi terlebih dahulu. Koneksi TCP ditutup dengan menggunakan proses terminasi koneksi TCP (*TCP connection termination*).	Pemecahan ke dalam paket-paket dan proses pengirimannya dilakukan secara manual.	**tanpa koneksi (*Connectionless*)** Pesan-pesan UDP akan dikirimkan tanpa harus dilakukan proses negosiasi koneksi antara dua host yang hendak berukar informasi.
Tidak akan mengirimkan data terlalu cepat sehingga memberikan jaminan koneksi internet dapat menanganinya.	**Keras berat (Heavyweight)** Ketika tingkat level terendah dari TCP tercapai dalam urutan yang salah, permintaan pengiriman ulang data harus dikirm. dan bagian lainya harus dikembalikan semua. Sehingga membutuhkan proses untuk menyatukannya.	Harus membuat kepastian mengenai proses transfer data agar tidak terlalu cepat sehingga internet masih dapat menanganinya.	**Ringan berat (Lightweight)** Tidak ada permintaan pesan, tidak ada terk koneksi dan yang lainnya, hanya menjalankan dan melupakannya. Ini berarti itu jauh lebih cepat dan kartu jaringan / OS hanya melakukan sedikit

			pekerjaan untuk menerjemahkan kembali data dari paket.
Mudah untuk digunakan, transfer paket data seperti menulis dan membaca file.	**Streaming** Data /paket dibaca sebagai satu alur data. tanpa mengetahui batas setiap data berakhir dan data yang lain mulai. Ada kemungkinan beberapa paket data dibaca per satu panggilan data. **Contoh:** World Wide Web (Apache TCP port 80), e-mail (SMTP TCP port 25 Postfix MTA), File Transfer Protocol (FTP port 21) and Secure Shell (OpenSSH port 22) dan lain-lain.	Jika paket ada yang hilang, perlu dipikirkan di mana letak kesalahan yang terjadi dan mengirim ulang data yang diperlukan.	**Datagrams** Paket dikirim secara individu dan dijamin utuh ketika tiba. Satu paket dibaca per satu panggilan. **Contoh:** *Domain Name System* (DNS UDP port 53), stream aplikasi media sebagai IPTV atau nonton, *Voice over IP* (VoIP), *Trivial File Transfer Protocol* (TFTP) dan online multiplayer games dan lain-lain.

2.11 Arsitektur 7 layer Open System Interconnection

Standar komunikasi yang diterapkan di dalam jaringan komputer. Standar itulah yang menyebabkan seluruh alat komunikasi dapat saling berkomunikasi melalui jaringan. Model referensi *Open System Interconnection* (OSI) menggambarkan bagaimana informasi dari suatu software aplikasi di sebuah komputer berpindah melewati sebuah media jaringan ke suatu software aplikasi di komputer lain. Model referensi OSI secara konseptual terbagi ke dalam 7 lapisan dimana masing-masing lapisan memiliki fungsi jaringan yang spesifik.

Model *Open Systems Interconnection* (OSI) diciptakan oleh *International Organization for Standardization* (ISO) yang menyediakan kerangka logika terstruktur bagaimana proses komunikasi data berinteraksi melalui jaringan. Standard ini dikembangkan untuk industri komputer agar komputer dapat berkomunikasi pada jaringan yang berbeda secara efisien. Terdapat 7 layer pada model OSI. Setiap layer bertanggung jawab secara khusus pada proses komunikasi data. Misalnya, satu layer bertanggungjawab untuk membentuk koneksi antar perangkat, sementara layer lainnya bertanggungjawab untuk mengoreksi terjadinya "error" selama proses transfer data berlangsung gambar 2.4 dibawah ini.



Gambar 2.4 Arsitektur 7 layer *Open System Interconnection* (OSI)

2.12 Menjelaskan 7 layer OSI

2.12.1 Application layer

Spesifikasi untuk lingkup dimana aplikasi jaringan berkomunikasi dengan layanan jaringan. Menyediakan jasa untuk aplikasi pengguna. Layer ini bertanggung jawab atas pertukaran informasi antara program komputer, seperti program e-mail, dan service lain yang jalan di jaringan, seperti server printer atau aplikasi komputer lainnya. Berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan.

Protokol yang lapisan aplikasi dibawah ini:

- ***Hyper Text Transfer Protocol* (HTTP)**

Protokol yang dipergunakan untuk mentransfer dokumen dan web dalam sebuah web browser, melalui www. HTTP juga merupakan protokol yang meminta dan menjawab antar klien dan server.

- ***File Transfer Protocol* (FTP)**

Protokol internet yang berjalam dalam layer aplikasi yang merupakan standar untuk mentransfer file komputer antar mesin-mesin dalam sebuat jaringan internet.

- ***Network File System* (NFS)**

Jaringan protokol yang memungkinkan pengguna di klien komputer untuk menngakses file melalui jaringan dengan cara yang sama dengan bagaiman penyimpanan lokal yang diaksesnya.

- ***Domain Name System* (DNS)**

Protokol yang digunakkan untuk memberikan suatu nama domain pada sebuah alamat IP agar lebih mudah diingat.

- ***Post Office Protocol 3* (POP3)**

Protokol yang digunakan untuk mengambil mail dari suatu mail transfer agent yang akhirnya mail tersebut akan di dowbload kedalam jaringan local.

- ***Multipurpose Internet Mail Exension* (MIME)**

Protokol yang digunakan untuk mengirim file binary dalam bentuk teks.

- ***Server Messange Block* (SMB)**

Protokol yang digunakan untuk mentransfer server-server file ke DOS dan Windows.

- ***Network News Transfer Protocol* (NNTP)**

Protokol yang digunakan untuk menerima dan mengirim newsgroup.

- ***Dynamic Host Configuration Protocol* (DHCP)**

  Layanan yang memberikan no IP kepada komputer yang meminta nya secara otomatis.

2.12.2 Presentation layer

Mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan.

Protokol yang lapisan presetasi dibawah ini:

- **TELNET**

  Protokol yang digunakan untuk akses remote masuk ke suatu host, data berjalan secara lain teks.

- ***Simple Mail Transfer Protocol* (SMTP)**

  Salah satu protokol yang biasa digunakan dalam pengiriman e-mail di internet atau untuk mengirimkan data dari komputer pengirim e-mail ke server e-mail penerima.

- ***Simple Network Management Protocol* (SNMP)**

  Protokol yang digunakan dalam suatu manajemen jaringan.

2.12.3 Session layer

Mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Selain itu, di level ini juga dilakukan resolusi nama.

Protokol yang lapisan sesi dibawah ini:

- **NETBIOS**

  Berfungsi sebagai penyiaran pesan maksud nya memungkinkan user mengirim pesan tunggal secara serempak ke komputer lain yang terkoneksi.

- ***NETBIOS Extended User Interface* (NETBEUI)**

Berfungsi sama dengat NETBIOS hanya sedikit di kembangkan lagi dengan menambahkan fungsi yang memungkinkan bekerja dengan beragam perangkat keras dan perangkat lunak.

- ***AppleTalk Data Stream Protocol* (ADSP)**

Berfungsi protokol ini memantau aliran datadiantara dua komputer dan untuk memeriksa aliran data tersebut tidak terputus.

- ***Printer Access Protocol* (PAP)**

Berfungsi printer Postscript untuk akses pada jaringan AppleTalk dan untuk mengendalikan bagaimana pola komunikasi antar node.

- ***Session Protocol Data Unit* (SPDU)**

Berfungsi mendukung hubungan antara dua session service user.

2.12.4 Transport layer

Memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu, pada level ini juga membuat sebuah tanda bahwa paket diterima dengan sukses (acknowledgement), dan mentransmisikan ulang terhadap paket-paket yang hilang di tengah jalan.

Protokol yang lapisan transport dibawah ini:

- ***Transmission Control Protocol* (TCP)**

Protokol yang menyediakan layanan penuh lapisan transport untuk aplikasi.

- ***User Datagram Protocol* (UDP)**

Protokol connectionless dan proses-to-procces yang hanya menambahkan alamat port, cheksum error control dan panjang informasi data pada layer di atasnya.

2.12.5 Network layer

Mendefinisikan alamat-alamat IP, membuat header untuk paket-paket, dan kemudian melakukan routing melalui internetworking dengan menggunakan router dan switch layer tiga.

Protokol yang lapisan network dibawah ini:

- ***Internetworking Protocol* (IP)**

  Mekanisme transmisi yang digunakan untuk menstransportasikan data ke dalam paket yang disebut datagram.

- ***Address Resolution Protocol* (ARP)**

  Protokol yang digunakan untuk mengetahui alamat IP berdasarkan alamat fisik dari sebuah komputer.

- ***Reverse Address Resolution Protocol* (RARP)**

  Protokol yang digunakan untuk mengetahui alamat fisik melalui IP komputer.

- ***Internet Control Message Protocol* (ICMP)**

  Mekanisme yang digunakan oleh sejumlah host untuk mengirim notifikasi datagram yang mengalami masalah pada hostnya.

- ***Internet Group Message Protocol* (IGMP)**

  Protokol yang digunakan untuk memberi fasilitas message yang simultan kepada group penerima.

2.12.6 Data link layer

Menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai frame. Selain itu, pada level ini terjadi koreksi kesalahan, flow control, pengalamatan perangkat keras (seperti halnya Media Access Control Address (MAC Address)), dan menetukan bagaimana perangkat-perangkat jaringan seperti hub, bridge, repeater, dan switch layer 2 beroperasi. Spesifikasi IEEE 802, membagi level ini menjadi

dua level anak, yaitu lapisan Logical Link Control (LLC) dan lapisan *Media Access Control* (MAC).

Protokol yang lapisan datalink dibawah ini:

- ***Point to Point Protocol* (PPP)**

  Protokol yang digunakan untuk point to point pada suatu jaringan.

- ***Serial Line Internet Protocol* (SLIP)**

  Protokol yang digunakan untuk point to point pada suatu jaringan.

2.12.7 Physical layer

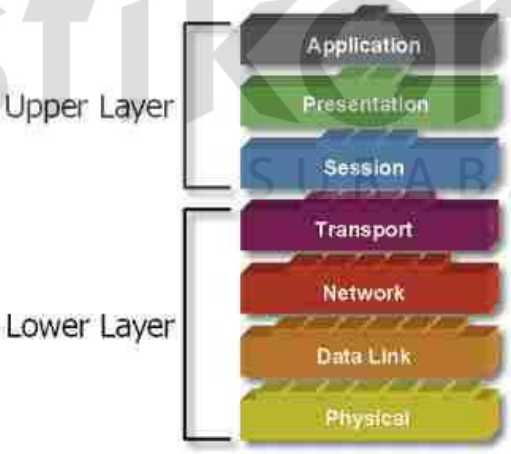
Mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya Ethernet atau Token Ring), topologi jaringan dan pengabelan. Selain itu, level ini juga mendefinisikan bagaimana Network Interface Card (NIC) dapat berinteraksi dengan media kabel atau radio.

Protokol yang lapisan physical dibawah ini:

Tidak mempunyai protokol yan spesifik di layer ini, bertanggung jawab atas proses data menjadi bit dan mentransfernya melalui media, seperti kabel, dan menjaga koneksi fisik antar sistem, pada layer ini hanya mengirimkan bit bit data.

2.13 Arsitektur dan definisi upper layer dan lower layer pada 7 layer OSI

Model Layer OSI dibagi dalam dua kelompok antara *upper layer* dan *lower layer*. Bagaimana cara menjelaskan keduanya bagi lapisan antara *upper layer* dan *lower layer* dimulai dengan *Upper layer* untuk melakukan fungsi tertentu aplikasi seperti manajemen koneksi, sesuai merancang & format, komposisi struktur, pesan encoding dan enkripsi. Lapisan aplikasi mengidentifikasi mitra komunikasi, membatasi atau mengizinkan paparan data dan menangani masalah privasi terkait. transfer file, email, jaringan dan perangkat lunak layanan adalah bagian dari lapisan ini. lapisan atas memerlukan arsitektur menjadi terbuka karena protokol aplikasi yang terus berkembang sedangkan *lower layer* dengan fungsi tertentu lebih jaringan seperti routing, flow control dan menangani. lapisan bawah memerlukan empat lapisan yang tersisa seperti yang disebutkan di awal lapisan yaitu fisik, link layer Data, Jaringan lapisan dan lapisan Transport. Semua ini secara vertikal mendaki lapisan mendukung lainnya di transferensi terbaik dan pemahaman dari data yang berguna dan berkomunikasi perintah untuk lapisan atas. Setiap protokol lapisan memanfaatkan layanan yang disediakan oleh lapisan bawah berikutnya dan menyediakan layanan peningkatan ke lapisan atas hirarki gambar 2.5 dibawah ini.



Gambar 2.5 Arsitektur upper layer dan lower layer pada OSI

- **Upper layer**

menjelaskan berinteraksi dengan pengguna dan menerapkan aplikasi yang berjalan melalui jaringan. Protokol yang berjalan pada lapisan yang lebih tinggi kurang peduli dengan rincian tingkat rendah dari bagaimana data akan dikirim dari satu tempat ke tempat lain selalu bergantung pada lapisan bawah untuk menyediakan pengiriman data. Lapisan tersebut hampir selalu diimplementasikan sebagai perangkat lunak yang berjalan pada komputer atau perangkat keras lainnya.

Upper layer akan dibagi 3 kelompok dibawah ini:

1. Physical
2. Datalink
3. Network

- **Lower layer**

utamanya yang bersangkutan dengan format, pengkodean dan transmisi data melalui jaringan. Jika tidak peduli bahwa banyak tentang apa data atau memungkinkan perlu digunakan untuk hanya tentang bergerak di sekitar. Mereka diimplementasikan dalam hardware dan software, dengan transisi dari perangkat keras ke perangkat lunak terjadi sebagai melanjutkan naik dari lapisan 1 ke lapisan 4.

Lower layer akan dibagi 4 kelompok dibawah ini:

1. Transport
2. Session
3. Presentation
4. application

2.14 Komponen jaringan dan protokol layer

Masing-masing model OSI disampaikan gambar 2.5 akan terdiri dari 7 lapisan dalam jenis protokol tabel 2.3 application layer, tabel 2.4 presentasi layer, tabel 2.5 session layer, tabel 2.6 transport layer, tabel 2.7 network layer, tabel 2.8 data link layer, tabel physical lyer 2.9 dibawah ini:

2.15.1 Tabel application layer

Tabel 2.3 Application layer

Network components	Protocols
Gateway	DNS, FTP
	TFTP, BOOTP
	SNMP, RLOGIN
	SMTP, MIME
	NFS, FINGER
	TELNET, NCP
	APPC, AFP
	SMB

2.15.2 Tabel presentation layer

Tabel 2.4 Presentation layer

Network components	protocols
Gateway	
Redirector	

2.15.3 Tabel session layer

Tabel 2.5 Session layer

Network components	Protocols
Gateway	NetBIOS
	Names pipes
	Mail slots
	RPC

2.15.4 Tabel transport layer

Tabel 2.6 Transport layer

Network components	Protocols
Gateway	TCP, ARP, RARP
Advanced cable tester	SPX
Brouter	NWlink
	NetBIOS/NetBEUI
	ATP

2.15.5 Tabel network layer

Tabel 2.7 Network layer

Network components	Protocols
Brouter	IP, ARP, RARP, ICMP, RIP, OSFP
Router	IGMP
Frame relay device	IPX
ATM switch	NWlink
Advanced cable tester	NetBEUI
	OSI
	DDP
	DECnet

2.15.6 Tabel data link layer

Tabel 2.8 Data link layer

Network components	Protocols
Bridge	Media access control - Communicates with the adapter card
Switch	Controls the type of media adapter card - 802.3 CSMA/CD (Ethernet) - 802.4 Token Bus (ARCnet) - 802.5 Token Ring - 802.12 Demand Priority
ISDN router	Logical link control - Error correction and flow

	control - Manages link control and defines SAPS
Intelligent Hub	802.2 logical link control
NIC	
advanced cable tester	

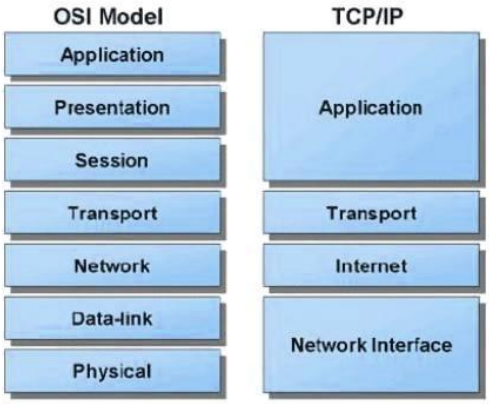
2.15.7 Tabel physical layer

Tabel 2.9 Physical layer

Network components	protocols
Repeater	IEEE 802 (ethernet standard)
Multiplexer	IEEE 802.2 (ethernet standard)
Hubs (passive and active)	ISO 2110
TDR	ISDN
Oscilloscope	
Amplifier	

2.15 Arsitektur Transmission Control Protocol/Internet Protocol

Komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (protocol suite). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini. Data tersebut diimplementasikan dalam bentuk perangkat lunak (software) di sistem operasi. Istilah yang diberikan kepada perangkat lunak ini adalah TCP/IP stack. Arsitektur TCP/IP tidaklah berbasis model referensi tujuh lapis OSI, tetapi menggunakan model referensi DARPA. Seperti diperlihatkan dalam diagram, TCP/IP merngimplemenasikan arsitektur berlapis yang terdiri atas empat lapis. Empat lapis ini, dapat dipetakan (tidak secara langsung) terhadap model referensi OSI. Empat lapis ini, kadang-kadang disebut sebagai DARPA Model, Internet Model, atau DoD Model, mengingat TCP/IP merupakan protokol yang awalnya dikembangkan dari proyek ARPANET yang dimulai oleh Departemen Pertahanan Amerika Serikat. Bentuk model OSI dengan TCP/IP gambar 2.6 dibawah ini:



Gambar 2.6 *Transmission Control Protocol/Internet Protocol* (TCP/IP)

2.15.1 Application layer

Bertugas untuk melayani permintaan data atau servis bahwa aplikasi pada layer ini menunggu di portnya masing-masing pada suatu antrian untuk diproses. Beberapa ciri-ciri layer dibawah ini:

1. *Network Terminal Protocol* (TELNET) untuk menyediakan remote login dalam jaringan.
2. *File Transfer Protocol* (FTP) yang menggunakan file transfer.
3. *Simple Mail Transfer Protocol* (SMTP) penggunaan untuk mengirimkan e-mail (electronic mail).
4. *Domain Name Service* (DNS) untuk memetakan IP Address ke dalam nama tertentu.
5. *Routing Information Protocol* (RIP) untuk protokol routing.
6. *Open Shortest Path First* (OSPF) untuk protokol routing.
7. *Network File System* (NFS) untuk berbagi/sharing file dalam suatu jaringan terhadap berbagai host.
8. *Hyper Text Transfer Protokol* (HTTP) diprotokol yang digunakan untuk web browsing.

2.15.2 Transport layer

Sebuah sambungan antara host penerima dan pengirim sebelum kedua host maka berkomunikasi dan seberapa sering kedua host ini akan mengirim *acknowledgment* dalam

sambungan ini satu sama lainnya. Transport layer hanya terdiri dari dua macam protokol dibawah ini:

1. *Transmission Control Protocol* (TCP)
2. *User Datagram Protocol* (UDP)

2.15.3 Internet layer

Berisi protokol yang mempunyai tanggung jawab dalam pengalamatan dan enkkapsulasi paket data jaringan. Pada internet layer terdiri dari 4 macam dibawah ini:

1. IP
2. ARP
3. ICMP
4. IGMP

2.15.4 Network layer

Gabungan dari Network, Data Link dan Physical Layer. Network Acces Layer menyediakan media bagi sistem untuk mengirimkan data ke device lain yang terkoneksi secara langsung.

2.16 Routing

2.16.1 Open Shortest Path First (OSPF)

protokol routing otomatis (Dynamic Routing) yang mampu menjaga, mengatur dan mendistribusikan informasi routing antar network mengikuti setiap perubahan jaringan secara dinamis. Pada OSPF dikenal sebuah istilah Autonomus System (AS) yaitu sebuah gabungan dari beberapa jaringan yang sifatnya routing dan memiliki kesamaan metode serta policy pengaturan network yang semuanya dapat dikendalikan oleh network administrator. kebanyakan fitur ini diguakan untuk management dalam skala jaringan yang sangat besar. karena itu untuk mempermudah penambahan informasi routing dan meminimalisir kesalahan distribusi informasi routing maka OSPF bisa menjadi sebuah solusi (Towidjojo, R. 2012).

2.16.2 Konfigurasi OSPF

OPSF merupakan protokol routing yang menggunakan konsep hirarki routing, dengan kata lain OSPF mampu membagi-bagi jaringan menjadi beberpa tingkatan. Tingakatan-tingkatan ini diwujudkan dengan menggunakan sistem pengelompokan yaitu area. OSPF memiliki beberapa tipe area untuk menjadi dua dibawah ini:

- **Bakcbone area**

Area ini memiliki area ID 0.0.0.0 dan merupakan area yang diharapkan dapat melakukan forward paket data (IP Packet) menjalankan. Area ini wajib ada jika ternyata hanya akan ada satu area (single area). Jika ternyata dalam jaringan akan dibuat beberapa area maka backbone wajib ada karena berfungsi menghubungkan area yang lain. End user atau host tidak boleh ditempatkan pada backbone area.

- **Regular area**

Area selain backbone (non backbone area) dan berfungsi menghubungkan end user. Jika dalam satu jaringan ada dua regular area maka kedua area ini harus melewati backbone area untuk berkomunikasi

2.16.3 Interface

Penggunaan router ini harus isi pendaftaran untuk menghubungkan interface semuanya pasang bagian ether atau satu pasang bagian ether yang inginkan konfigurasi sesuaikan router ini maka terlihat status sudah aktifkan.

2.16.4 Instances

Router yang terdapat name dan router ID untuk menjelaskan dua tahap yaitu name itu membuat nama biasa yang digunakan router dan switch sedangkan router ID untuk membuat interface dimana mengkonfigurasi router ID pada kedua router. Konfigurasi ini bisa tapi tidak dilakukan. Karena konfigurasi router ID tidak bisa lakukan oleh router OSPF tetap akan memiliki router ID. Router ID yang akan digunakan oleh router OSPF dalam IP address tertinggi pada interfacenya. Router ID yang menggunakan IP address dalam komputer sendiri yang sebagai router ID. diKarenakan IP address kelebihan nilainya dari kedua sisi router pada sasaran *network* pada interface masing-masing.

Router ID akan digunakan sebagai identitas dari setiap LSA yang dibuat oleh router OSPF. Router OSPF tetap akan mencari IP address untuk menjadikan router ID. Sehingga bisa ditentukan router ID. Bukan router yang mencari sendiri router ID.

2.16.5 Network

Setiap router memiliki dua *network* misalnya router yang memiliki router dalam komputer dan kedua sisi router. Jika *network* yang dimiliki oleh router sendiri. Ini dapat lakukan dua router pada konfigurasi advertise *network* pada setiap router. Sebenarnya sebelum melakukan konfigurasi advertise *network* membuat area khusus jaringan single area tanpa OSPF maka area yang digunakan backbone area. Backbone area akan memiliki identitas atau area ID dari backbone nilai 0.0.0.0. setelah konfigurasi advertise *network* dapat terhubung satu sama lainnya. Agar *network* mencapai kondisi convergence. Setelah hasil konfigurasi dengan lakukan pemeriksaan tabel routing maupun melakukan ping antar yang IP address dalam berbanding komputer dengan komputer sendiri.

2.16.6 Area

Router akan mengimplementasikan single area dengan ospf mendapatkan langsung lakukan konfigurasi advertise *network* pada saat konfigurasi router ID telah selesai maka implementasi multi area dengan OSPF jika konfigurasi regular area perlu dilakukan terlebih dahulu sebelum melakukan advertise *network*. Router harus membutuhkan area tidak ketahui yang sebagai regular area dengan identitas nomor area ID maka konfigurasi regular area ini hanya keperluan kedua sisi router ini disebabkan kedua router ini yang akan terhubung ke area tidak ketahui yang diperintah mendapatkan digunakan untuk membuat regular area pada router sendiri.

2.16.7 Area ranges

Tabel routing yang besar dan memuat banyak *network* address akan banyak menguras resource dari router karena router harus menyediakan cukup memori untuk menampung tabel routing. Begitu juga pada saat akan melakukan monitoring maupun troubleshoot administrator jaringan akan relatf sulit membaca tabel routing karena berisi banyak *network* address. Apalagi pekerjaan troubleshooting itu harus dilakukan

menjumlahkan router. Teknik *summarization* maka ukuran tabel routing dapat dibuat lebih ringkas dan ramping. Sehingga masalah resource dan troubleshooting yang dapat dihindari. Tentunya penerapan summarization tidak boleh mengorbankan konektifitas jaringan. Jangan sampai ada beberapa *network* yang tidak terhubung hanya karena penerapan summarization. Karena dibutuhkan perencanaan yang sempurna pada saat akan menerapkan *summarization*. Bagaimana teknik *summarization* maka keberadaan area disini untuk mendapatkan berapa *network* tidak bisa ketahui yang dikelola oleh kedua sisi router lain. Beberapa *network* adalah *network* masing-masing yang dikelola oleh router bersama-sama. Router masing-masing adalah internal router dari area tidak diketahui yang terhubung ke router sendiri.

2.16.8 Virtual link

Seluruh area OSPF harus terhubung langsung dengan backbone area tidak ketahui melalui ABR. Virtual link dapat digunakan saat suatu area tidak bisa terhubung langsung ke backbone area. Penggunaan virtual link tidak disarankan kecuali sebagai solusi sementara. Virtual link tidak bisa menggunakan stub area untuk transit.

2.16.9 Neighbors

Router membuat informasi dalam periksa sudah aktif untuk menyelesaikan berada router masing-masing.

2.16.10 NBMA neighbors

Media berjenis Nonbroadcast multiaccess ini secara fisik merupakan sebuah serial line biasa yang sering ditemui pada media jenis Point-to- Point. Namun secara faktanya, media ini dapat menyediakan koneksi ke banyak tujuan, tidak hanya ke satu titik saja.

2.16.11 Sham link

Router ospf sham link akan penggunaan konfigurasi *source* address dan *destination* address menunjukkan arah yang keberadaan router maka diperlukan cost berapa yang inginkan saat ini juga menghubungkan dipilihan backbone atau area agar mudah tidak bisa lepas dari router yang terjadi tidak bisa koneksi antara router dari router lain sehingga bisa berkomunikasi satu sama lain maka router ospf sham link sudah bisa

aktif selama berlangsung untuk informasi pendaftaran yang menyampaikan router OSPF sham link.

2.16.12 Link State Advertisements (LSA)

Paket kecil dari informasi routing yang dikirim antar router. LSA akan dikirim antar router. LSA akan dikirim ke router yang terhubung langsung. Saat terjadi perubahan jaringan. jika ada router yang mati maka router yang terhubung langsung akan mengupdate LSAnya. Masing-masing router membangun database topologi yang berisi informasi LSA. Link state protokol akan melakukan flood atau pembanjiran dengan menggunakan alamat multicast. Kemudian router yang mendapatkan informasi perubahan itu akan mengirimkan lagi updatenya ke router tetangga yang terhunbung langsung. Namun informasi LSA ini tidak akan terkirim lagi ke si pengirim pertama.

2.16.13 Routes

Router membuat informasi dalam periksa sudah aktif yang keberadaan router masing-masing yang menyampaikan dikerjakan dalam konfigurasi OSPF sesuai memasang router ini.

2.16.14 Autonomous System Border Routers (ASBR)

Sekelompok router yang membentuk jaringan yang masih berada dalam satu hak administrasi, satu kepemilikan, satu kepentingan, dan dikonfigurasi menggunakan policy yang sama dalam dunia jaringan komunikasi data sering disebut dengan istilah *Autonomous System* (AS). Biasanya dalam satu AS router di dalamnya dapat bebas berkomunikasi dan memberikan informasi. Umumnya, routing protocol yang digunakan untuk bertukar informasi routing adalah sama pada semua router di dalamnya. Jika menggunakan OSPF maka semuanya tentu juga menggunakan OSPF. Di mana sebuah segmen jaringan tidak memungkinkan untuk menggunakan OSPF sebagai routing protokolnya. Misalkan kemampuan router yang tidak memadai, atau kekurangan sumber daya manusia yang paham akan OSPF, dan banyak lagi. Oleh sebab itu, untuk segmen ini digunakanlah routing protocol *Interior Gateway Protocol* (IGP) lain seperti misalnya RIP. Karena menggunakan routing protocol lain, maka oleh jaringan OSPF segmen jaringan ini dianggap sebagai AS lain. OSPF sudah menyiapkan satu tipe router yang

memiliki kemampuan ini. OSPF mengategorikan router yang menjalankan dua routing protokol di dalamnya, yaitu OSPF dengan routing protokol IGP lainnya seperti misalnya RIP, IGRP, EIGRP, dan IS-IS, kemudian keduanya dapat saling bertukar informasi routing, disebut sebagai Autonomous System Border Router (ASBR).

Router ASBR dapat diletakkan di mana saja dalam jaringan, namun yang pasti router tersebut haruslah menjadi anggota dari Area 0-nya OSPF. Hal ini dikarenakan data yang meninggalkan jaringan OSPF juga dianggap sebagai meninggalkan sebuah area. Karena adanya peraturan OSPF yang mengharuskan setiap area terkoneksi ke backbone area, maka ASBR harus diletakkan di dalam backbone area.

2.16.15 Area border routers

Router yang terletak pada perbatasaan dari satu atau lebih area OSPF yang menghubungkan area-area tersebut ke beckbone jaringan. ARB juga dapat disebut sebagai anggota beckbone OSPF dan area tempat router tersebut dipasang. Router ini memelihara tabel routing yang menjelaskan topologi beckbone dan topologi area-area lain.

2.17 Mikrotik Router OS

Merupakan sistem operasi dan perangkat lunak yang diperuntukkan sebagai network router. Didesain untuk memberikan kemudahan bagi penggunanya. Administrasinya bisa dilakukan melalui *Windows Application* (WinBox). Selain itu instalasi dapat dilakukan pada Standard komputer *Personal Computer* (PC). PC yang akan dijadikan router mikrotik tidak memerlukan resource yang cukup besar untuk penggunaan standard, misalnya hanya sebagai gateway. Sistem Operasi yang mampu membuat sebuah PC mempunyai fungsi seperti layaknya Router, Firewall, Bridge, HotSpot, proxy Server, Bandwidth Management dan beberapa fungsi server lainnya. Tidak seperti OS lainnya, RouterOS support terhadap berbagai jenis Driver hardware dan apabila ada hardware yang tidak support terhadap Mikrotik RouterOS, maka kita tidak dapat menambah /menginstall driver tambahan seperti halnya Sistem Operasi. Untuk keperluan beban yang besar (network yang kompleks, routing yang rumit) disarankan untuk mempertimbangkan pemilihan resource PC yang memadai.

Mikrotik dalam bentuk perangkat lunak yang dapat diinstal pada komputer (PC) melalui files patch. setelah mengunduh file image Mikrotik RouterOS dari website resmi mikrotik website dari www.mikrotik.com. Untuk dapat menggunakannya secara full time segala membeli lisensi key dengan catatan satu lisensi hanya untuk satu harddisk. sistem operasi dari perangkat keras mikrotik yaitu router board.

2.18 Fitur mikrotik

Beberapa fitur yang diberikan oleh mikrotik dibawah ini:

1. Address List : Pengelompokan IP Address berdasarkan nama.
2. Asynchronous : Mendukung serial PPP dial-in / dial-out, dengan otentikasi CHAP, PAP, MSCHAPv1 dan MSCHAPv2, Radius, dial on demand, modem pool hingga 128 ports.
3. Bonding : Mendukung dalam pengkombinasian beberapa antarmuka ethernet ke dalam 1 pipa pada koneksi cepat.
4. Bridge : Mendukung fungsi bridge spinning tree, multiple bridge interface, bridging firewalling.
5. Data Rate Management : QoS berbasis HTB dengan penggunaan burst, PCQ, RED, SFQ, FIFO queue, CIR, MIR, limit antar peer to peer.
6. DHCP : Mendukung DHCP tiap antarmuka; DHCP Relay; DHCP Client, multiple network DHCP; static and dynamic DHCP leases.
7. Firewall dan NAT : Mendukung pemfilteran koneksi peer to peer, source NAT dan destination NAT. Mampu memfilter berdasarkan MAC, IP address, range port, protokol IP, pemilihan opsi protokol seperti ICMP, TCP Flags dan MSS.
8. Hotspot : Hotspot gateway dengan otentikasi RADIUS. Mendukung limit data rate, SSL ,HTTPS.
9. IPSec : Protokol AH dan ESP untuk IPSec; MODP Diffie-Hellmann groups 1, 2, 5; MD5 dan algoritma SHA1 hashing; algoritma enkirpsi menggunakan DES, 3DES, AES-128, AES-192, AES-256; Perfect Forwarding Secresy (PFS) MODP groups 1, 2,5.
10. ISDN : mendukung ISDN dial-in/dial-out. Dengan otentikasi PAP, CHAP, MSCHAPv1 dan MSCHAPv2, Radius. Mendukung 128K bundle, Cisco HDLC, x751, x75ui, x75bui line protokol.

11. M3P : MikroTik Protokol Paket Packer untuk wireless links dan ethernet.
12. MNDP : MikroTik Discovery Neighbour Protokol, juga mendukung *Cisco Discovery Protokol* (CDP).
13. Monitoring / Accounting : Laporan Traffic IP, log, statistik graph yang dapat diakses melalui HTTP.
14. *Network Time Protokol* (NTP) untuk server dan clients; sinkronisasi menggunakan system GPS.
15. *Poin to Point Tunneling Protocol* (PPTP), PPPoE dan L2TP Access Consentrator; protokol otentikasi menggunakan PAP, CHAP, MSCHAPv1, MSCHAPv2; otentikasi dan laporan Radius; enkripsi MPPE; kompresi untuk PPoE; limit data rate.
16. Proxy : Cache untuk FTP dan HTTP proxy server, HTTPS proxy; transparent proxy untuk DNS dan HTTP; mendukung protokol SOCKS; mendukung parent proxy; static DNS.
17. Routing : Routing statik dan dinamik; RIP v1/v2, OSPF v2, BGP v4.
18. SDSL : Mendukung Single Line DSL; mode pemutusan jalur koneksi dan jaringan.
19. Simple Tunnel : Tunnel IPIP dan *Ethernet over IP* (EoIP).
20. *Simple Network Monitoring Protocol* (SNMP) mode akses read-only.
21. Synchronous : V.35, V.24, E1/T1, X21, DS3 (T3) media types; sync-PPP, Cisco
22. HDLC; Frame Relay line protokol; ANSI-617d (ANDI atau annex D) dan Q933a (CCITT atau annex A); Frame Relay jenis LMI.
23. Tool : Ping, Traceroute; bandwidth test; ping flood; telnet; SSH; packet sniffer; Dinamik DNS update.
24. UPnP : Mendukung antarmuka *Universal Plug and Play* (UPnP).
25. VLAN : Mendukung Virtual LAN IEEE 802.1q untuk jaringan ethernet dan wireless; multiple VLAN; VLAN bridging.
26. VoIP : Mendukung aplikasi voice over IP.
27. VRRP : Mendukung Virtual Router Redudant Protocol.
28. WinBox : Aplikasi mode GUI untuk meremote dan mengkonfigurasi MikroTik RouterOS.

2.19 Quality Of Service

Quality Of Service (GOS) Suatu pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari suatu layanan. Pada jaringan berbasis IP, IP QoS mengacu pada performansi dari paket IP yang lewat melalui satu atau lebih jaringan. QoS didesain untuk membantu end user menjadi lebih produktif dengan memastikan bahwa end user mendapatkan performansi yang handal dari aplikasi berbasis jaringan. QoS mengacu pada kemampuan jaringan untuk menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda-beda. Contohnya Sebagai contoh komunikasi suara (VoIP atau *IP Telephony*) serta video streaming dapat membuat pengguna frustrasi ketika paket data aplikasi akan dialirkan ke atas jaringan dengan bandwidth yang tidak cukup dengan latency yang tidak dapat diprediksi, atau jitter yang berlebih. Fitur *Quality of Service* (QoS) ini dapat menjadikan *bandwidth*, *latency*, dan *jitter* dapat diprediksi dan dicocokkan dengan kebutuhan aplikasi yang digunakan di dalam jaringan.

2.20 Dua alat komponen mikrotik

2.21.1 RB951G-2HND

RB951G-2HnD merupakan seri wireless routerboard keluaran mikrotik yang berfungsi sebagai router sekaligus *Accsess Point* (AP) gigabit yang dirancang khusus untuk *Small Office Home Office* (SOHO). Produk ini menggunakan atheros *Central Processing Unit* (CPU) jenis terbaru dengan daya prosesor 600MHz dan RAM 128MB. Dilengkapi dengan lima buah port gigabit ethernet 10/100/1000, 1 port *Unisersal Serial Bus* (USB) 2.0, dan wireless AP berdaya tinggi 2.4GHz 1000mW 802.11b/g/n dengan antenna built-in. Produk ini tidak memiliki fungsi output *Protocol Over Ethernet* (POE) seperti yang ada pada produk RB951Ui-2HnD. Bentuk gambar 2.7 dan tabel 2.10 dibawah ini:

Gambar 2.7 Mikrotik RB951G-2HnD

Tabel 2.10 Spesifikasi RB951G-2HnD

Spesifikasi produk	
Nama produk	RB951G-2HnD
CPU	Atheros AR9344 600MHz CPU
Memori	128MB DDR2 onboard memory
LED's	Power, aktifitas NAND, LED 5 port Ethernet, LED aktifitas wireless
Power In	PoE : 8-30V DC pada Ether 1 (Non 802.3af). Jack : 8-30V DC
Dimensi	113x138x29mm
Berat	Tanpa PSU dan kemasan : 232g Kemasan : 420g
Temperatur ketika beroperasi	-20C +70C
Sistem Operasi	MikroTik RouterOs, lisensi level 4
Isi kemasan	RouterBoard dalam casing plastik, power adaptor 24V 0.8A
Antena	internal Dual-Chain 2 x 1.5dbi

2.21.2 RB941-2ND TC

RB941-2nD-TC (Hap Lite) merupakan seri wireless routerboard keluaran mikroyik yang berfungsi sebagai router sekaligus *Accsess Point* (AP) dirancang khusus untuk *Small Office Home Office* (SOHO). prosesor 650Mhz, *Random Access Memory* (RAM) 32 MB, dan sudah dilengkapi dengan RouterOS level 4. Kapasitas besar storage media hanya 16MB NAND dan memiliki ethernet portsebanyak 4 Fast-Ethernet. produk juga tidak dilengkapi dengan fitur POE-In dan POE-Out sehingga supply daya terbatas. Bentuk gambar 2.8 dan tabel 2.11 dibawah ini:

Gambar 2.8 Mikrotik RB941-2nD-TC (Hap Lite)

Tabel 2.11 Spefisikasi RB941-2nd TC

Spesifikasi produk	
Nama produk	RB941-2nD-TC (Hap Lite)
CPU	QCA9531-BL3A-R 650MHz
Memori	32MB DDR RAM
Internet	4x 10/100 Mbit/s Ethernet with Auto-MDI/X
Kartu wireless	Onboard dual chain 2.4GHz 802.11b/g/n QCA9531 modul wireless ; 10kV ESD pelindung dimasing-masing RF port, WPS mendukung
Extra	Reset switch
LED's	Power LED, 4x Internet LED, user LED
Power In	Kemasan dengan 5v DC 0.7A power adapter

Dimensi	113x89x28mm
Berat	Tanpa PSU dan kemasan : 232g Kemasan : 420g
Temperatur ketika beroperasi	-20C to +70C
Sistem Operasi	MikroTik RouterOs, lisensi level 4
Isi kemasan	RouterBoard dalam casing plastik, power adaptor MicroUSB 5v
Antena	2x2 MIMO PIF antennas, max gain 2.5dBi

2.21 Alat komponen

2.22.1 Unshielded Twisted Pair (UTP)

- **Kelebihan kabel UTP**

1. Kabel *Unshielded Twsited Pair* (UTP) cenderung memiliki harga yang terjangkau dibandingkan dengan harga kabel jaringan lain.
2. Proses instalasi yang mudah dan tidak rumit menjadi kelebihan lain yang dimiliki kabel UTP, sehingga banyak orang yang menggunakannya. Proses pemeliharaan kabel jaringan UTP cukup mudah, cocok dan banyak digunakan untuk di dalam ruangan.
3. Kabel UTP memiliki konektor dan kabel relative kecil, sehingga kabel ini cukup fleksibel dengan kemudahan ketika proses crimping. Oleh sebab itu kabel UTP terkenal dengan proses instalasi yang mudah.

- **Kelemahan kabel UTP**

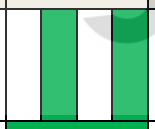
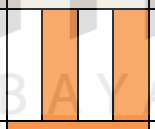
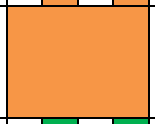
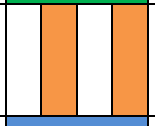
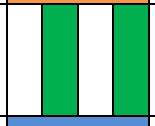
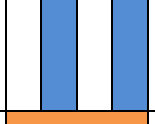
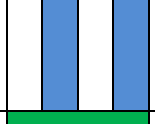
1. Kabel jaringan UTP tidak memiliki perlindungan berupa aluminium foil sehingga sangat rentan terhadap interferensi gelombang elektromagnetik yang berasal dari perangkat lain.
2. Jarak jangkauan yang terbatas dengan kisaran 100 meter, sehingga kalah dengan jenis kabel lain termasuk kabel fiber optik dan kabel coaxial.
3. Transmisi data yang dimiliki kabel UTP cenderung lambat, sehingga kebanyakan orang memilih kabel fiber optik yang terkenal akan kecepatannya.

2.22.2 Kabel UTP

Kabel UTP merupakan untuk saling menghubungkan jaringan internet dan terdiri dari 8 buah pin kabel kecil yang berwarna untuk menjadi satu dan setiap pin kabel mempunyai warna yang berbeda beda. kabel UTP biasanya dipasang dengan koneltor RJ-45 yang akan dihubungkan ke LAN Card atau perangkat jaringan yang mempunyai port RJ-45. Kecepatan kabel UTP 10% lebih cepat dibandingkan dengan kabel coaxial. Pada kabel UTP dikenal dengan standart pengurutan kabel yang digunakan untuk standarisasi urutan pemasangan kabel. Pemasangan urutan Kabel UTP umumnya mengikuti aturan standart international yaitu EIA/TIA 568A dan EIA/TIA 568B. EIA merupakan sinonim atau kepanjangan dari Electronic Industries Alliance dan TIA merupakan sinonim atau

kepanjangan dari Telecommunication Industry Association. EIA/TIA merupakan standarisasi internasional stuktur kabel untuk telekomunikasi. Kabel yang paling sering kita temui adalah jenis UTP, SFTP. Banyak yang menganggap EIA/TIA hanyalah standart untuk kabel jenis ethernet padahal EIA/TIA lebih global untuk telekomunikasi termasuk transfer voice suara (PABX). EIA/TIA 568A dan EIA/TIA 568B menjelaskan spesifikasi kabel UTP sebagai aturan dalam instalasi jaringan komputer. EIA/TIA menggunakan istilah kategori untuk membedakan beberapa tipe kabel UTP mendapatkan beberapa jenis kategori kabel UTP ini yang menunjukkan kualitas yang menjumlahkan kerapatan lilitan pairnya maka kabel UTP harus pemasangan urutan kabel UTP umumnya mengikuti aturan standart internasional yaitu EIA/TIA 568A dan EIA/TIA 568B. Dilihat tabel urutan pemasangan T568A dan T568B dari *crossover* dan *straight* tabel 2.12 dibawah ini:

Tabel 2.12 Kabel UTP dengan standar T568A dan T568B

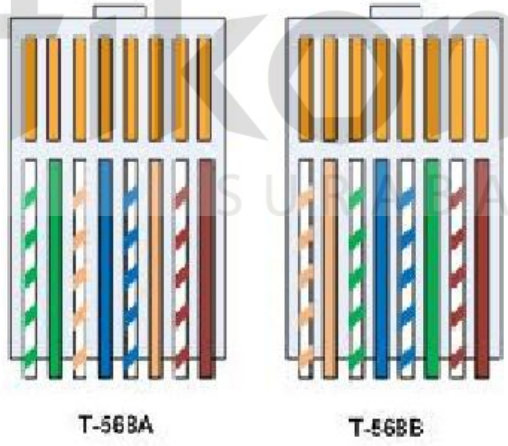
T568A				T568B			
RJ45 PIN#	Warna kawat (T568A)	Diagram kawat (T568A)	10 base – T signal 100 base –TX signal	RJ45 PIN#	Warna kawat (T568B)	Diagram kawat (T568B)	10 base – T signal 100 base –TX signal
1	Putih Hijau		TD+ (data kirim+)	1	Putih Orange		RD+ (data terima+)
2	Hijau		TD- (data kirim-)	2	Orange		RD- (data terima-)
3	Putih Orange		RD+ (data terima +)	3	Putih Hijau		TD+ (data kirim +)
4	Biru		NC (tidak dipakai)	4	Biru		NC (tidak dipakai)
5	Putih Biru		NC (tidak dipakai)	5	Putih Biru		NC (tidak dipakai)
6	Orange		RD- (data terima -)	6	Hijau		TD- (data kirim -)

7	Putih Coklat		NC (tidak dipakai)	7	Putih Coklat		NC (tidak dipakai)
8	Coklat		NC (tidak dipakai)	8	Coklat		NC (tidak dipakai)

Dari dua standar diatas dapat kita lihat pada standar T-568B di dapat dengan menukar urutan kabel ke-1 dengan ke-3 dan urutan ke-2 dengan ke-6 pada standar T568A yang dikenal dengan rumus 1-3 2-6.

- **Crossover cable (kabel silang)**

  Kabel memasangkan berbeda tidak diaturkan sesuai yang penggunaan untuk komunikasi antar komputer termasuk switch/hub. Penggunaan untuk mengcascade hub sering diperlukan jenis hub baru sudah bisa dicascade dengan kabel lurus. Kabel jenis ini pada sebelah kanan dan sebelah kiri yang menggunakan standar warna berbeda maka mulai dari sebelah kiri standar T568A dan sebelah kanan T568B gambar 2.9 dibawah ini.

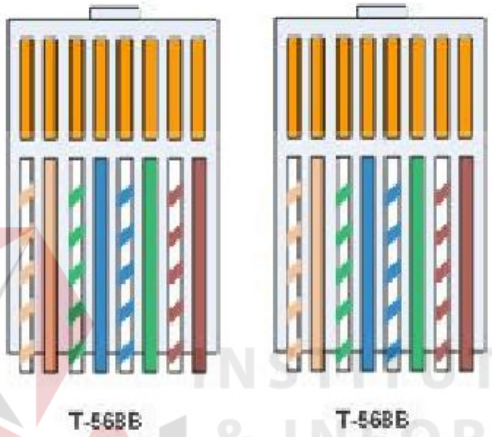


Gambar 2.9 Kabel UTP *crossover* dengan sebelah kiri T568A dan sebelah kanan T568B

- **Straight cable (kabel lurus)**

  Kabel memasangkan sama diaturkan sesuai yang penggunaan untuk menghubungkan beberapa unit komputer melalui perantara hub/switch yang berfungsi sebagai konsentrator maupun repeater. Pada jenis masing-masing ujung

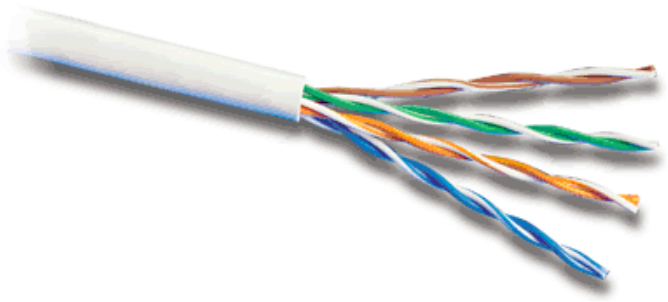
kabel harus menggunakan standar yang sama maka mulai dari sebelah kiri standar T568B dan sebelah kanan T568B. kabel UTP akan digunakan straight pada jaringan lokal biasanya bentuk topologi *star* dengan hub/switch sebagai pusatnya. Switch harus sesuai dengan kecepatan Ethernet Card yang digunakan masing-masing komputer. Perbedaan kecepatan pada NIC dan Switch akan menyebabkan kedua perangkat tidak dapat saling berkomunikasi secara maksimal gambar 2.10 dibawah ini:



Gambar 2.10 Kabel UTP *straight* dengan sebelah kiri T568B dan sebelah kanan T568B

2.22.3 Fungsi kabel UTP

Kabel UTP ini bisa digunakan sebagai salah satu kabel untuk jaringan berbasis lokal *Local Area Network* (LAN) di dalam suatu sistem network/jaringan komputer, dan pada umumnya, kabel UTP ini memiliki impedansi yang kurang lebih sekitar 100 ohm, dan itu juga dibagi menjadi ke dalam beberapa kategori, di mana kategori tersebut berdasarkan kemampuannya dalam menghantarkan suatu data. Kabel UTP dapat bermacam macam sesuai dengan kategori dari kabel gambar 2.11 dibawah ini:



Gambar 2.11 Kabel UTP

1. CAT 1 khususnya kabel UTP Category 1 [Cat1] adalah jenis kabel UTP dengan kualitas transmisi yang terendah, didesain untuk mendukung komunikasi suara analog saja.
2. CAT 2 khususnya kabel UTP Category 2 [Cat2] adalah jenis kabel UTP memiliki kualitas transmisi yang lebih baik dibandingkan dengan kabel UTP Cat1, jenis atau kategori ini didesain untuk mendukung komunikasi data dan juga suara digital. Kabel ini bisa mentransmisikan data sampai 4 megabit/detik.
3. CAT 3 khususnya kabel UTP Category 3 [Cat3] adalah kabel UTP dengan kualitas transmisi yang lebih baik dibandingkan dengan kabel UTP Category 2, jenis atau kategori ini didesain untuk mendukung komunikasi data dan suara pada kecepatan hingga 10 megabit per detik.
4. CAT 4 khususnya kabel UTP Category 4 [Cat4] adalah suatu jenis kabel UTP dengan kualitas transmisi yang jauh lebih lebih baik jika dibandingkan dengan kabel UTP Category 3 (Cat3) atau sebelumnya, didesain untuk mendukung komunikasi data dan juga suara sampai kecepatan 16 megabit/detik.
5. CAT 5 khususnya kabel UTP Category 5 [Cat5] adalah suatu jenis kabel UTP dengan kualitas transmisi yang lebih baik jika dibandingkan dengan kabel UTP Category 4 (Cat4) atau yang sebelumnya, didesain untuk mendukung komunikasi data dan komunikasi suara pada kecepatan sampai 100 megabit/detik.
6. CAT 6 khususnya kabel UTP Category 6 [Cat6] adalah jenis standar kabel UTP dengan sertifikasi resmi paling tinggi.

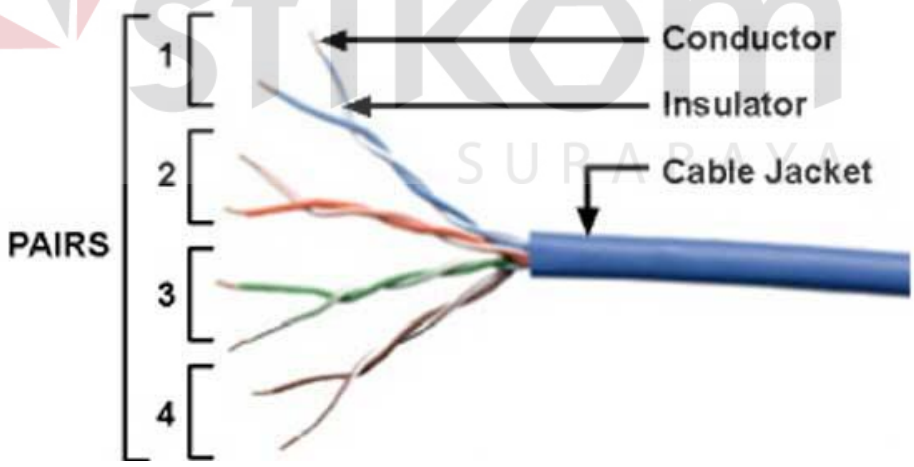
7. CAT 7 khususnya kabel UTP Category 7 [Cat7] adalah jenis kabel premium yang sangat cocok sekali sebagai media yang high traffic berbagai macam aplikasi dalam 1 kabel (single cable). Maksimum data yang terkirim sampai 10 Gbit/detik, dengan frekuensi 1000 Mhz.

2.22.4 Jenis kabel UTP

Kabel utp standar yang spesifikasi khususnya EIA/TIA 568. Berdasarkan setiap jenisnya maka kabel ini harus disusun sesuai dengan mengaturkan. Bertujuan agar kabel mendapatkan difungsikan dengan LAN. Pada jenis kabel straight harus memastikan spesifikasi kabel yang terpasang sama pada ujung satu dan yang lain. Kabel jenis ini umumnya digunakan untuk menghubungkan komponen tertertu seperti switch dan router, PC dan switch, serta PC dan HUB.

2.22.5 Karakteristik kabel jaringan twisted pair

Twisted Pair yang menggunakan beberapa kawat tembaga bersama-sama digabung dengan pasangannya dan tiap-tiap kawat tembaga dilapisi oleh isolator yang memiliki warna berbeda gambar 2.12 dibawah ini:



Gambar 2.12 Struktur komponen dasar kabel Twisted Pair

Lebih menjelaskan twisted pair mendapat gambar diatas. Ketiga contoh gambar diatas untuk menjelaskan dibawah ini:

- **Conductor**

  Conductor merupakan kawat tembaga yang terletak di tengah-tengah dan berfungsi sebagai media konduktor listrik.

- **Insulator**

  Tiap-tiap kawat tembaga dilapisi oleh insulator yang memiliki warna berbeda, dimana fungsi lapisan yang satu ini adalah untuk melindungi kawat tembaga agar tidak bersentuhan langsung dengan kawat tembaga lainnya saat menggabungkan.

- **Cable Jacket**

Di bagian paling luar, terdapat cable jacket yang berfungsi sebagai pelindung kabel Twisted Pair itu sendiri terhadap gangguan dari luar.

Selain tiga komponen di atas. Twisted Pair secara umum dapat klasifikasi dibawah ini :

1. Bagian dalam kabel jaringan Twisted Pair terdiri dari dua kawat tembaga yang dibagi menjadi 8 dawai dan dikelompokkan lagi menjadi 4 pasang (pair), lalu dipilin menjadi satu.
2. Kabel jaringan Twisted Pair memiliki kecepatan transmisi 10-100Mbps.
3. Panjang kabel maksimal yang diizinkan yaitu 100 meter (pendek).
4. Kabel jaringan Twisted Pair hanya bisa menangani satu kanal data (yang bekerja pada baseband).
5. Instalasi jaringan komputer menggunakan kabel Twisted Pair membutuhkan sebuah hub untuk membangun sebuah LAN yang baik.
6. Media dan ukuran konektor kecil.
7. Konektor kabel jaringan Twisted Pair biasanya menggunakan konektor RJ-11 atau RJ-45 untuk koneksinya.
8. Pemeliharaan kabel jaringan Twisted Pair terkenal mudah.
9. Kerusakan yang terjadi pada salah satu saluran kabel jaringan Twisted Pair tidak akan mengganggu jaringan secara keseluruhan.

2.22.6 RJ45

Registered Jack (RJ) 45 konektor kabel Ethernet yang digunakan dalam jaringan komputer LAN maupun jaringan komputer tipe lainnya. Standard peralatan pada jaringan yang mengatur tentang pemasangan kepala konektor dan urutan kabel, yang digunakan untuk menghubungkan 2 atau lebih peralatan telekomunikasi (Telephone Jack) ataupun peralatan jaringan (Computer Networking). Menghubungkan kabel UTP dengan kartu jaringan, diperlukan sebuah konektor yang bernama 8P8C, atau biasa disebut sebagai konektor Registered Jack seri 45 (RJ-45). Terdapat dua standar pengurutan warna kabel pada saat dimasukkan ke dalam konektor RJ-45 untuk tempatnya T568-A dan T568-B gambar 2.13 dibawah ini:

Gambar 2.13 *Register Jack* (RJ) 45

2.22.7 Crimping

Kegiatan memasangkan kabel UTP dengan konektor RJ-45 dinamakan crimping. Memerlukan sebuah tang khusus yang bernama crimp tool, atau biasa dinamakan tang crimper. Alat ini gunanya untuk mematikan atau menanam konektor ke kabel UTP. Sekali kerapatan kabel UTP sudah tidak bisa dilepas lagi dari konektor RJ-45 termasuk cara lakukan memotong kabelnya gambar 2.14 dibawah ini:

Gambar 2.14 Crimping

2.22.8 Menjelaskan kabel UTP dengan *crossover* dan *straight*

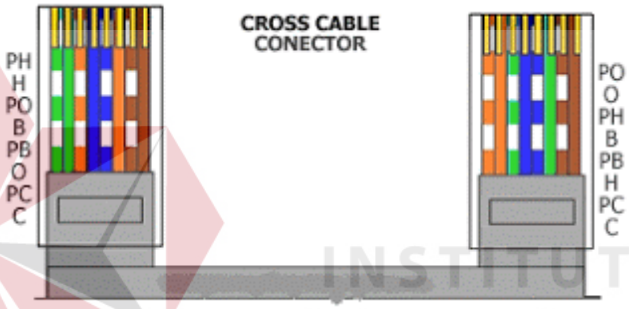
Kabel Unshielded Twisted Pair (UTP) merupakan kabel yang digunakan sebagai media transmisi yang digunakan di dalam jaringan Local Area Network (LAN) pada sistem network/jaringan komputer. LAN merupakan suatu Jenis Jaringan Komputer dengan mencakup wilayah lokal. Dengan menggunakan berbagai perangkat jaringan yang cukup sederhana dan populer, seperti menggunakan kabel UTP (Unshielded Twisted-Pair), Hub, Switch, Router, dan lain sebagainya. Berbanding kabel UTP dalam LAN dengan crossover dan straight untuk perangkat-perangkat jaringan membutuhkan sambungan yang berbeda-beda sesuai dengan karakter perangkat yang akan dihubungkan. Kabel UTP harus mengikuti aturan standarisasi internasional dinamakan EIA/TIA khususnya kabel UTP dengan menggunakan *crossover* dan *straight* dalam urutan T568A dan T568B maka keduanya harus UTP memasangkan untuk berbeda dan sama. Tujuannya harus menjelaskan kabel UTP dengan LAN untuk memasangkan antara *crossover* dan *straight* mendapatkan dua macam jenis sambungan dibawah ini:

- **Crossover**

Kabel *crossover* yang menggunakan untuk menghubungkan perangkat jenis yang berbeda. Sebuah kabel *crossover* yang terdiri dari 5 bermacam-macam jenis untuk bisa memasukkan mendukung komputer, switch, hub, router. Perangkat-perangkat jaringan lokal dimanapun untuk menjelaskan dibawah ini:

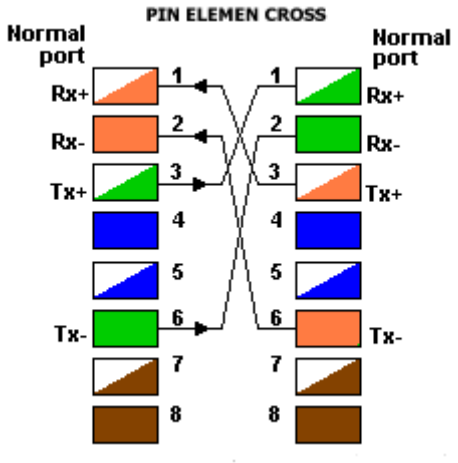
1. Menghubungkan 2 buah komputer secara langsung
2. Menghubungkan 2 buah switch
3. Menghubungkan 2 buah hub
4. Menghubungkan switch dengan hub
5. Menghubungkan komputer dengan router

Kabel UTP yang dipasangkan berbeda menggunakan *crossover* dalam urutan T-568A dan T-568B untuk dihubungan sebelah kiri digunakan T-568A dan sebelah kanan digunakan T-568B gambar 2.15 dibawah ini.



Gambar 2.15 Konector kabel UTP dengan LAN didalam urutan T-568A dan T-568B.

Bentuk pin elemen crossover yang menggunakan kabel UTP dengan urutan EIA/TIA 568A dan EIA/TIA 568B akan mengubahkan dua bagian kategori yaitu sebelah kiri digunakan urutan T568A dan sebelah kanan digunakan urutan T568B. Terkecuali pasangan tidak mengaturkan dalam berbanding dua macam yaitu warna putih orange, orange dan warna putih hijau, hijau dikatakan kategori warna dimulai warna putih orange untuk RD+ (data terima +) dan orange untuk RD- (data terima -) sedangkan warna putih hijau TD+ (data kirim+) dan warna hijau TD- (data kirim-) yang menganggapi tak terhingga dalam keadaaan kondisi *crossover* jaringan tidak urutan terkoneksi semakin baik gambar 2.16 dibawah ini.



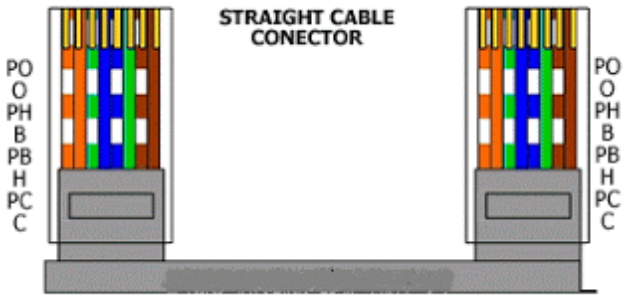
Gambar 2.16 Bentuk pin elemen *crossover* dengan urutan T-568A dan T-568B berbeda

- **Straight**

Kabel *straight* yang menggunakan untuk menghubungkan perangkat jenis yang berbeda. Sebuah kabel *straight* yang terdiri dari 5 bermacam-macam jenis untuk bisa memasukkan mendukung komputer, switch, hub, router, modem cable/DSL. Perangkat-perangkat jaringan lokal untuk menjelaskan dibawah ini:

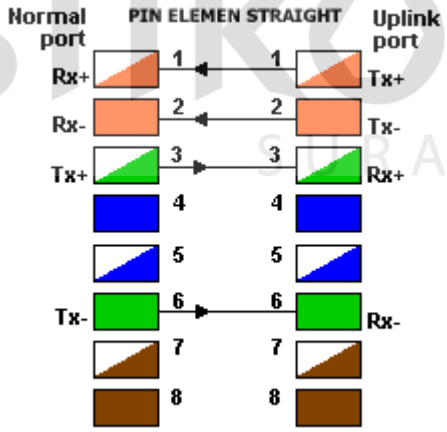
1. Menghubungkan antara komputer dengan switch
2. Menghubungkan komputer dengan LAN pada modem cable/DSL
3. Menghubungkan router dengan LAN pada modem cable/DSL
4. Menghubungkan switch ke router
5. Menghubungkan hub ke router

Kabel UTP yang dipasangkan sama menggunakan *straight* dalam urutan T568B keduanya seperti sama untuk dihubungan sebelah kiri digunakan T568B dan sebelah kanan digunakan T-568A gambar 2.17 dibawah ini.



Gambar 2.17 Konector kabel UTP dengan LAN didalam urutan T568B.

Bentuk pin elemen crossover yang menggunakan kabel UTP dengan urutan EIA/TIA 568A bagian kiri dan kanan maka mengubahkan dua bagian kategori yaitu sebelah kiri digunakan urutan T568B dan sebelah kanan digunakan urutan T568B. Terkecuali pasangan mengaturkan dalam berbanding dua macam yaitu warna putih orange, orange dan warna putih hijau, hijau dikatakan kategori warna dimulai warna putih orange untuk RD+ (data terima +) dan orange untuk RD- (data terima -) sedangkan warna putih hijau TD+ (data kirim+) dan warna hijau TD- (data kirim-) yang menganggapi terhingga dalam keadaaan kondisi *straight* jaringan urutan terkoneksi semakin sempurna gambar 2.18 dibawah ini.



Gambar 2.18 Bentuk pin elemen *straight* dengan urutan T-568B keduanya yang sama

2.22.9 Cara memasang kabel UTP dengan kabel crossover dan kabel straight

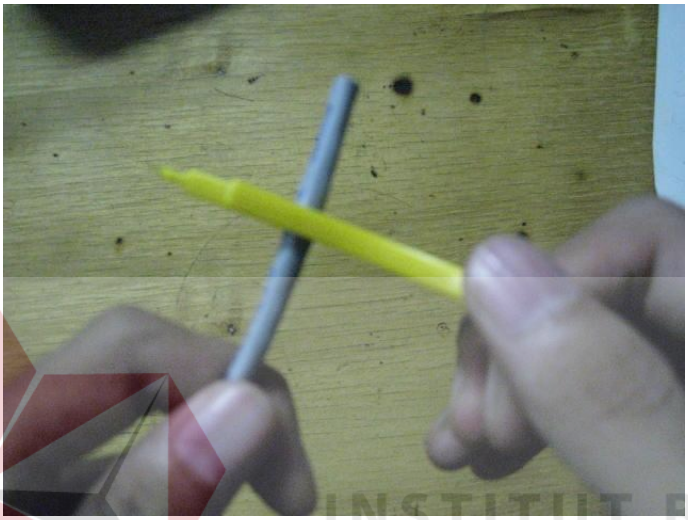
Disiapkan kabel UTP untuk membuat antara *crossover* dan *straight* gambar 2.19 dibawah ini.

Gambar 2.19 Kabel UTP

Potong kulit kabel UTP dalam bagian paling luar mendapat *cable jacket* yang berfungsi sebagai pelindung kabel Twisted Pair gambar 2.20 dibawah ini.

Gambar 2.20 Potong kulit

kabel UTP Potonglah ujung kabel UTP sehingga rata kemudian kupas bagian paling luar cable jacket yang berfungsi sebagai pelindung kabel Twisted Pair itu sendiri. kabel kira-kira sepanjang 2 cm dengan menggunakan pengupas kabel yang biasanya ada pada crimping tool (bagian yang seperti 2 buah silet saling berhadapan yang dapat untuk mengupas) gambar 2.21 dibawah ini.

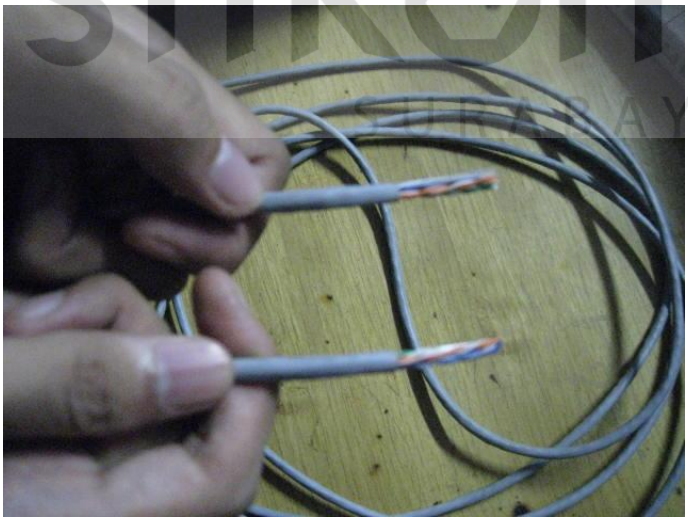


Gambar 2.21 Potong kulit putaran dengan kabel UTP

Kabel UTP sudah lepaskan bagian luar *cable jacket* yang terlihat *insulator* terdiri dari 8 buah pin kabel kecil yang berwarna untuk menjadi satu dan setiap pin kabel mempunyai warna yang berbeda beda. kabel UTP akan segera memotong bagian luar insulator untuk sebelah kiri dan sebelah kanan gambar 2.22 dibawah ini.

Gambar 2.22 Kabel UTP dalam tipis bagian (1)

Setelah kabel UTP dipotong bagian luar akan menghasilkan keduanya sama *insulator* antara sebelah kiri dan sebelah kanan gambar 2.23 dibawah ini.

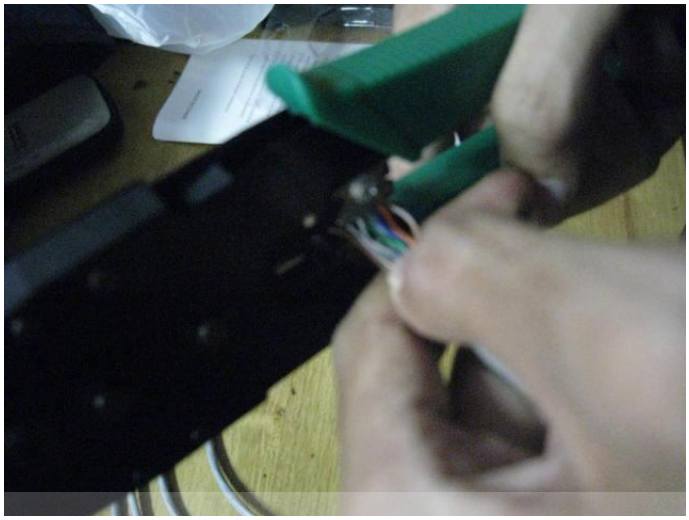


Gambar 2.23 Kabel UTP dalam tipis bagian (2)

Bentul crimping membuat kabel UTP sudah dipotong bagian luar akan menghasilkan keduanya sama *insulator* tinggal *conductor* dalam kawat tembaga yang terletak ditengah keatas maka dirapat tipis warna agar mudah bisa lepas untuk segera dipotong secepat mungkin gambar 2.24 dibawah ini.

Gambar 2.24 Crimping

Setelah sudah dipotong *insulator* akan susunan kabel warna tipis tersusun kabel dengan cara menekan bagian yang dekat dengan pisau kecil lalu merapatkan kabel warna *conductor* supaya susunan mudah lepas saat dipegang kabel *conductor* warna akan lakukan dipotong maka terlihat rata. Keduanya *insulator* harus dipotong terlihat sebelah kiri dan sebelah kanan gambar 2.25 dibawah ini.



Gambar 2.25 Crimping dengan kabel UTP

Setelah keduanya *insulator* melihat sebelah kiri dan sebelah kanan akan terjadi hasil seperti gambar 2.26 dibawah ini.

Gambar 2.26 Crimping sudah potong kabel UTP

Kabel UTP akan lakukan memasangkan antara *crossover* dan *straight* untuk menjelaskan dimulai *crossover* akan diperlihatkan tabel menghubungkan dari kiri dan kanan yang berbeda dengan urutan T568B dan T568A dalam bagian kiri Potongan satu (P1) dan Potongan dua (P2) sedangkan *straight* akan diperlihatkan tabel menghubungkan dari kiri

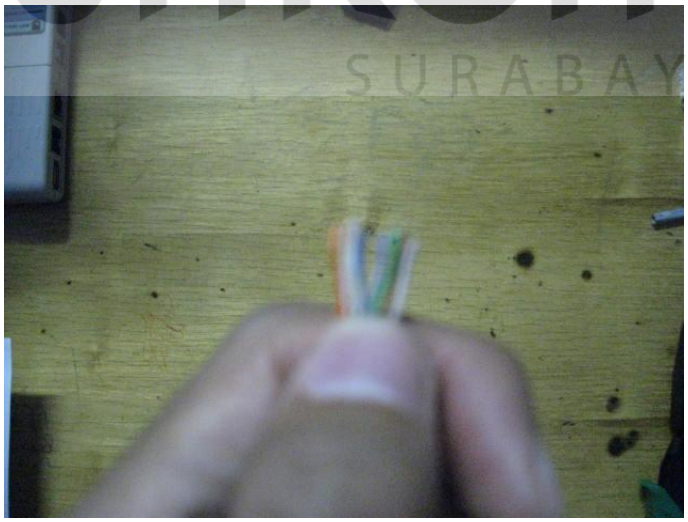
dan kanan yang sama dengan T568B dan T568B dalam bagian kanan Potongan satu (P1) dan Potongan dua (P2). Keduanya *crossover* dan *straight* akan membuat memotong segera lakukan pengujian sudah selesai tabel 2.13 dibawah ini.

Tabel 2.13 Kabel *Unshielded Twisted Pair* (UTP) antara *crossover* dan *straight*

Kabel Unshielded Twisted Pair (UTP)			
Crossover		**Straight**	
Kiri dan kanan yang berbeda		**Kiri dan kanan yang sama**	
T568B	**T568A**	**T568B**	**T568B**
Potongan satu (P1)	**Potongan dua (P2)**	**Potongan satu (P1)**	**Potongan dua (P2)**
Putih orange	Putih hijau	Putih orange	Putih orange
Orange	Hijau	Orange	Orange
Putih hijau	Putih orange	Putih hijau	Putih hijau
Biru	Biru	Biru	Biru
Putih biru	Putih biru	Putih biru	Putih biru
Hijau	Orange	Hijau	Hijau
Putih coklat	Putih coklat	Putih coklat	Putih coklat
Coklat	Coklat	Coklat	Coklat

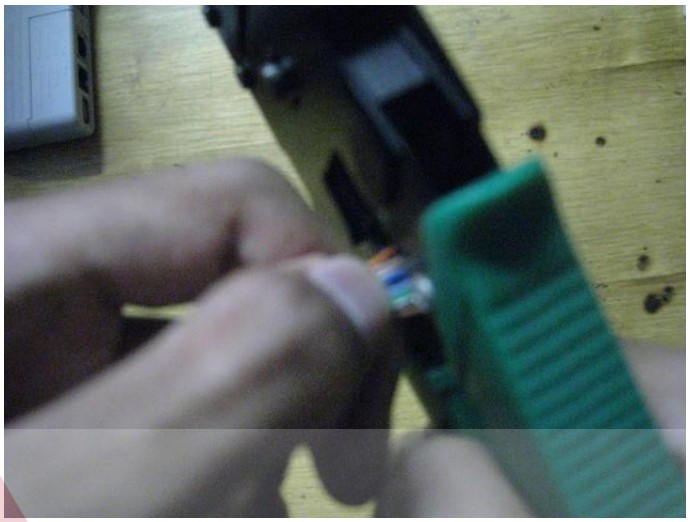
- **Crossover**

Sebelah kiri kabel UTP dengan *crossover* bagian kabel warna akan ditahan *insulator* dengan urutan urutan T568B yang terletak *conductor* dilakukan Potongan Satu (P1) gambar 2.27 dibawah ini.



Gambar 2.27 P1 kabel UTP dengan *crossover* bagian (1)

Kemudian sebelah kiri *crossover* akan dipegang *insulator* lakukan alat crimping untuk potong kecil dalam terlelak *conductor* gambar 2.28 dibawah ini.

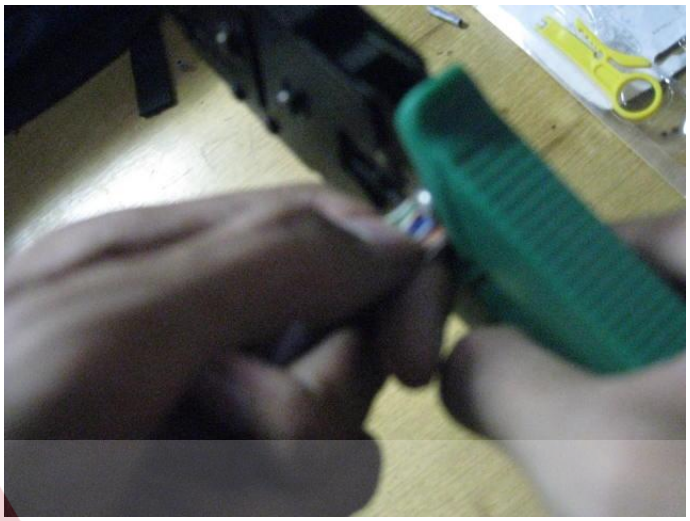


Gambar 2.28 P1 kabel UTP dengan *crossover* untuk crimping bagian (1)

Sebelah kanan kabel UTP dengan *crossover* bagian kabel warna akan ditahan *insulator* dengan urutan urutan T568A yang terletak *conductor* dilakukan Potongan Satu (P2) gambar 2.29 dibawah ini.

Gambar 2.29 P2 kabel UTP dengan *crossover* bagian (2)

Kemudian sebelah kanan *crossover* akan dipegang *insulator* lakukan alat crimping untuk potong kecil dalam terlelak *conductor* gambar 2.30 dibawah ini.



Gambar 2.30 P2 kabel UTP dengan *crossover* untuk crimping bagian (2)

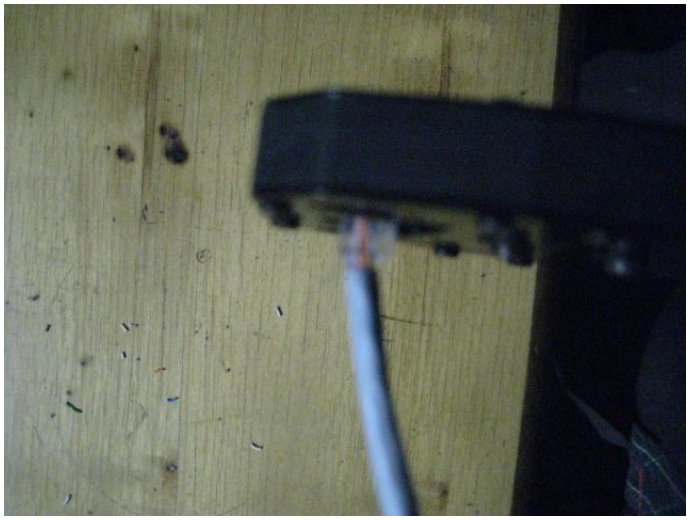
Setelah *crossover* keduanya bagian sebelah kiri dan kanan akan terlihat rapi keadaan kondisi baik gambar 2.31 dibawah ini.

Gambar 2.31 P1 dan P2 kabel UTP dengan *crossover* bagian (3)

Setelah *crossover* sudah dipotong sebelah kiri akan lakukan dipegang *insulator* yang terletak *conductor* untuk masukkan kabel ke konektor RJ45 sampai ujung-ujung kabel terlihat dibagian depan konektor RJ-45. Kalau masih belum coba terus ditekan sambil dipastikan posisi kabel tidak berubah gambar 2.32 dibawah ini.

Gambar 2.32 P1 kabel UTP dengan *crossover* untuk RJ45 bagian (1)

Setelah *crossover* bagian sebelah kiri akan lakukan dipegang *insulator* yang terletak *conductor* untuk masukkan kabel ke konektor RJ45 sampai ujung-ujung kabel terlihat dibagian depan konektor RJ45. Sebuah alat crimping untuk lakukan yakin posisi kabel tidak berubah dan kabel sudah masuk dengan baik ke konektor RJ-45 selanjutnya masukan konektor RJ45 akan merapat. Ketika konektor dalam kondisi di dalam crimping dipastikan kembali kabel sudah sepenuhnya menyentuh bagian RJ45 dengan cara mendorong kabel ke dalam RJ45. Kemudian bisa menekan crimping sekuat tenaga supaya semua pin RJ45 masuk dan menembus pelindung kabel UTP yang kecil. Apabila kurang kuat menekan kemungkinan kabel UTP tidak tersobek oleh pin RJ45 sehingga kabel tidak. Apabila pembungkus bagian luar tidak masuk kedalam konektor RJ45 apabila kabel warna sering bergerak kemungkinan besar posisi kabel akan bergesar dan bahkan copot gambar 2.33 dibawah ini.



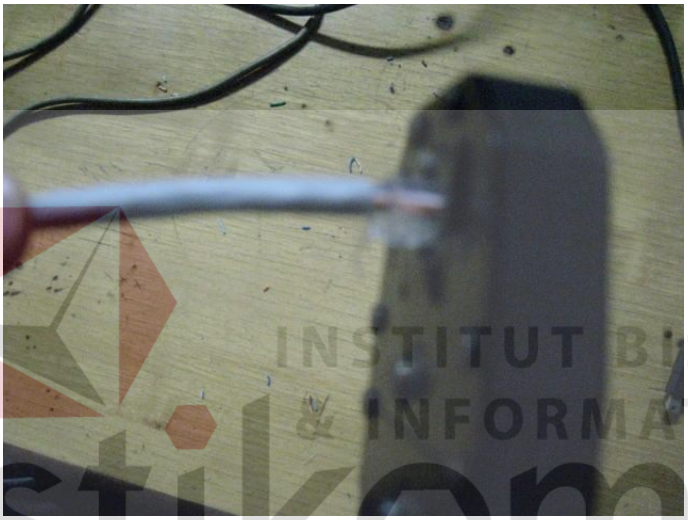
Gambar 2.33 P1 kabel UTP dengan *crossover* untuk crimping dalam RJ45 bagian (1)

Setelah *crossover* sudah dipotong sebelah kanan akan lakukan dipegang *insulator* yang terletak *conductor* untuk masukkan kabel ke konektor RJ45 sampai ujung-ujung kabel terlihat dibagian depan konektor RJ45. Kalau masih belum coba terus ditekan sambil dipastikan posisi kabel tidak berubah gambar 2.34 dibawah ini.

Gambar 2.34 P2 kabel UTP dengan *crossover* untuk RJ45 bagian (2)

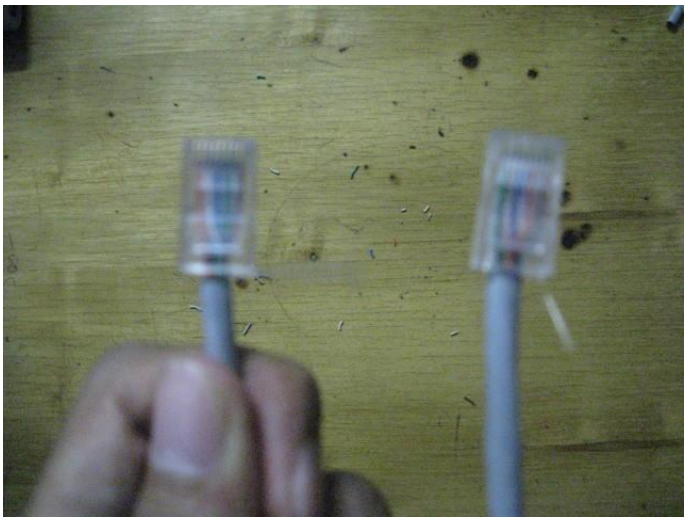
Setelah *crossover* bagian sebelah kanan akan lakukan dipegang *insulator* yang terletak *conductor* untuk masukkan kabel ke konektor RJ45 sampai ujung-ujung kabel terlihat dibagian depan konektor RJ45. Sebuah alat crimping untuk lakukan yakin posisi kabel tidak

berubah dan kabel sudah masuk dengan baik ke konektor RJ45 selanjutnya masukan konektor RJ45 akan merapat. Ketika konektor dalam kondisi di dalam crimping dipastikan kembali kabel sudah sepenuhnya menyentuh bagian RJ45 dengan cara mendorong kabel ke dalam RJ45. Kemudian bisa menekan crimping sekuat tenaga supaya semua pin RJ45 masuk dan menembus pelindung kabel UTP yang kecil. Apabila kurang kuat menekan kemungkinan kabel UTP tidak tersobek oleh pin RJ45 sehingga kabel tidak. Apabila pembungkus bagian luar tidak masuk kedalam konektor RJ45 apabila kabel warna sering bergerak kemungkinan besar posisi kabel akan bergesar dan bahkan copot gambar 2.35 dibawah ini.



Gambar 2.35 P2 kabel UTP dengan *crossover* untuk crimping dalam RJ45 bagian (2)

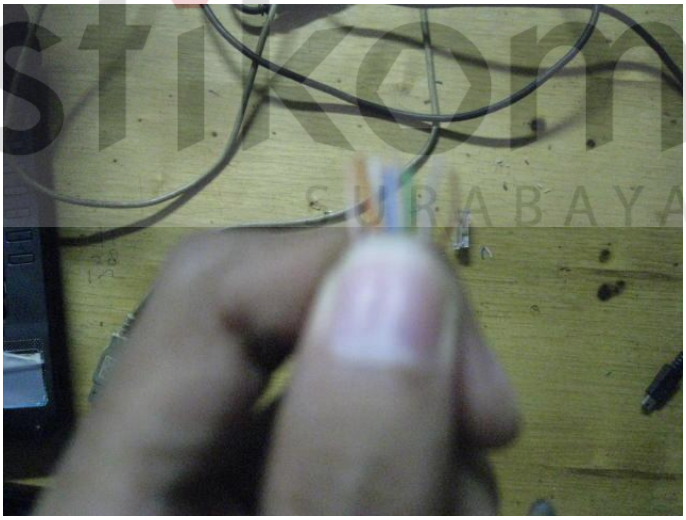
Setelah *crossover* bagian sebelah kiri dan sebelah kanan maka apabila sudah yakin memasang kabel UTP ke RJ-45 yang terlihat rapi sudah selesai gambar 2.36 dibawah ini.



Gambar 2.36 P1 dan P2 kabel UTP dengan *crossover* proses sudah selesai

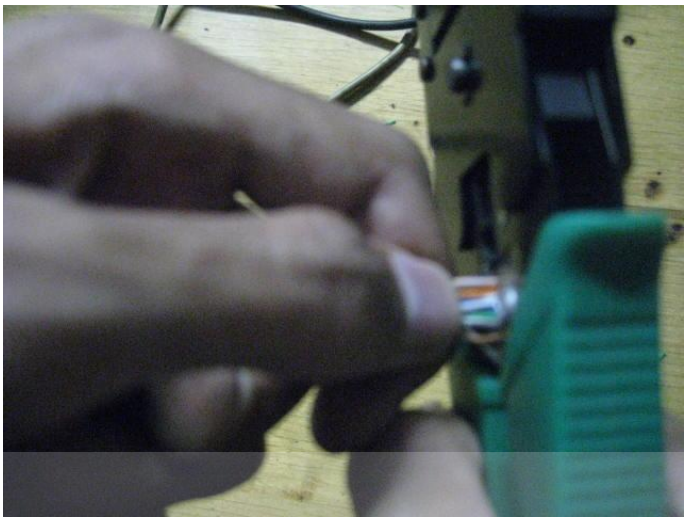
- **Straight**

Sebelah kiri kabel UTP dengan *straight* bagian kabel warna akan ditahan *insulator* dengan urutan urutan T568B yang terletak *conductor* dilakukan Potongan Satu (P1) gambar 2.37 dibawah ini.



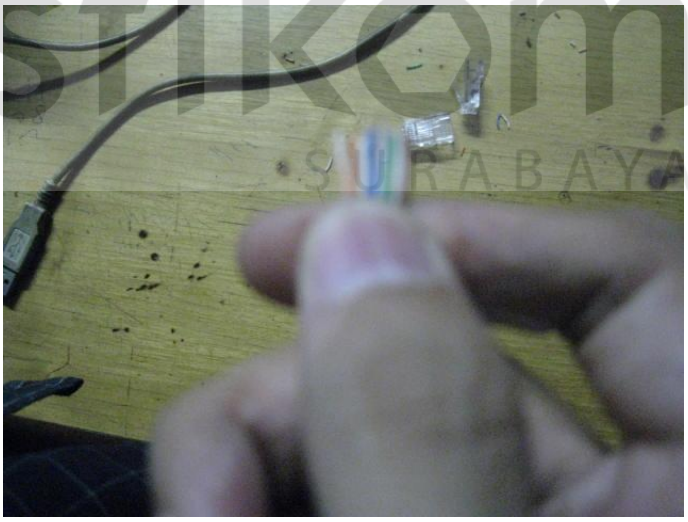
Gambar 2.37 P1 kabel UTP dengan *straight* bagian (1)

Kemudian sebelah kiri *straight* akan dipegang *insulator* lakukan alat crimping untuk potong kecil dalam terlelak *conductor* gambar 2.38 dibawah ini.



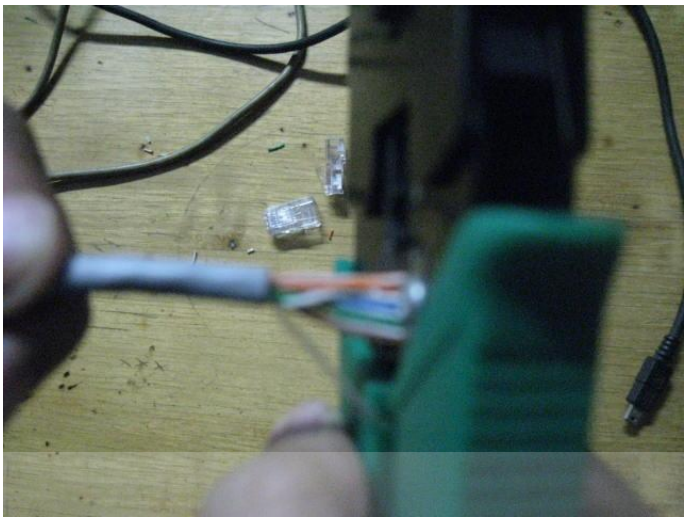
Gambar 2.38 P1 kabel UTP dengan *straight* untuk crimping bagian (1)

Sebelah kanan kabel UTP dengan *straight* bagian kabel warna akan ditahan *insulator* dengan urutan urutan T568B yang terletak *conductor* dilakukan Potongan Satu (P2) gambar 2.39 dibawah ini.



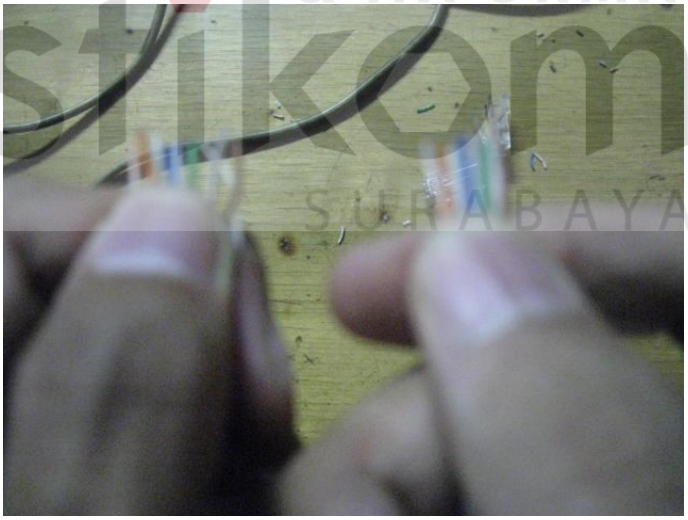
Gambar 2.39 P2 kabel UTP dengan *straight* bagian (2)

Kemudian sebelah kiri *straight* akan dipegang *insulator* lakukan alat crimping untuk potong kecil dalam terlelak *conductor* gambar 2.40 dibawah ini.



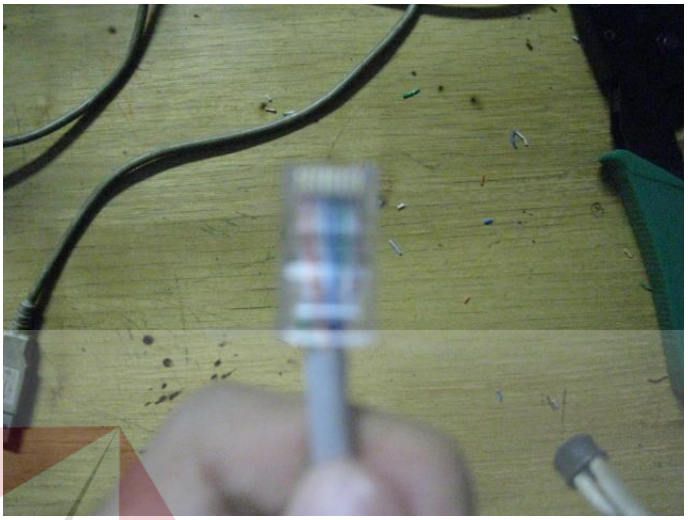
Gambar 2.40 P2 kabel UTP dengan *straight* untuk crimping bagian (2)

Setelah *straight* keduanya bagian sebelah kiri dan kanan akan terlihat rapi keadaan kondisi baik gambar 2.41 dibawah ini.



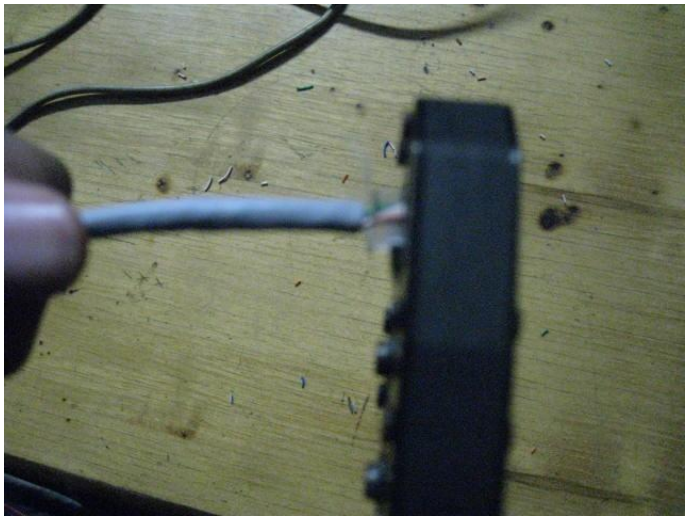
Gambar 2.41 P1 dan P2 kabel UTP dengan *straight* bagian (3)

Setelah *straight* sudah dipotong sebelah kiri akan lakukan dipegang *insulator* yang terletak *conductor* untuk masukkan kabel ke konektor RJ45 sampai ujung-ujung kabel terlihat dibagian depan konektor RJ45. Kalau masih belum coba terus ditekan sambil dipastikan posisi kabel tidak berubah gambar 2.42 dibawah ini.



Gambar 2.42 P1 kabel UTP dengan *straight* untuk RJ45 bagian (1)

Setelah *straight* bagian sebelah kiri akan lakukan dipegang *insulator* yang terletak *conductor* untuk masukkan kabel ke konektor RJ45 sampai ujung-ujung kabel terlihat dibagian depan konektor RJ45. Sebuah alat crimping untuk lakukan yakin posisi kabel tidak berubah dan kabel sudah masuk dengan baik ke konektor RJ45 selanjutnya masukan konektor RJ-45 akan merapat. Ketika konektor dalam kondisi di dalam crimping dipastikan kembali kabel sudah sepenuhnya menyentuh bagian RJ45 dengan cara mendorong kabel ke dalam RJ45. Kemudian bisa menekan crimping sekuat tenaga supaya semua pin RJ45 masuk dan menembus pelindung kabel UTP yang kecil. Apabila kurang kuat menekan kemungkinan kabel UTP tidak tersobek oleh pin RJ45 sehingga kabel tidak. Apabila pembungkus bagian luar tidak masuk kedalam konektor RJ45 apabila kabel warna sering bergerak kemungkinan besar posisi kabel akan bergesar dan bahkan copot gambar 2.43 dibawah ini.



Gambar 2.43 P1 kabel UTP dengan *straight* untuk crimping dalam RJ45 bagian (1)

Setelah *straight* sudah dipotong sebelah kanan akan lakukan dipegang *insulator* yang terletak *conductor* untuk masukkan kabel ke konektor RJ45 sampai ujung-ujung kabel terlihat dibagian depan konektor RJ45. Kalau masih belum coba terus ditekan sambil dipastikan posisi kabel tidak berubah gambar 2.44 dibawah ini.

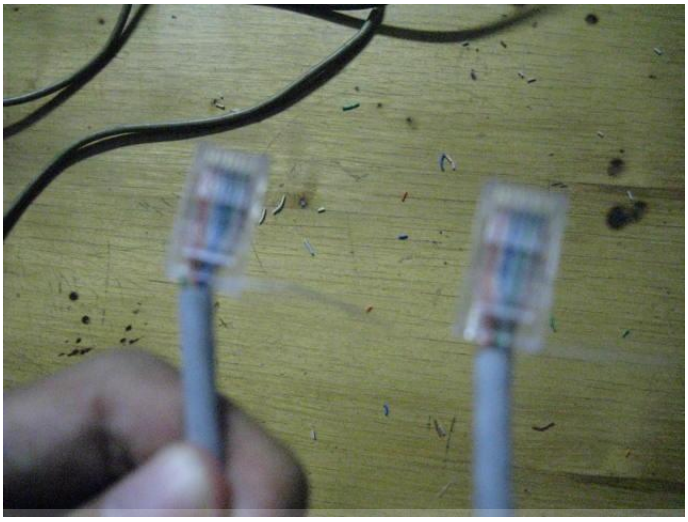
Gambar 2.44 P2 kabel UTP dengan *straight* untuk RJ45 bagian (2)

Setelah *straight* bagian sebelah kanan akan lakukan dipegang *insulator* yang terletak *conductor* untuk masukkan kabel ke konektor RJ45 sampai ujung-ujung kabel terlihat dibagian depan konektor RJ45. Sebuah alat crimping untuk lakukan yakin posisi kabel tidak berubah dan kabel sudah masuk dengan baik ke konektor RJ45 selanjutnya masukan konektor

RJ-45 akan merapat. Ketika konektor dalam kondisi di dalam crimping dipastikan kembali kabel sudah sepenuhnya menyentuh bagian RJ45 dengan cara mendorong kabel ke dalam RJ45. Kemudian bisa menekan crimping sekuat tenaga supaya semua pin RJ45 masuk dan menembus pelindung kabel UTP yang kecil. Apabila kurang kuat menekan kemungkinan kabel UTP tidak tersobek oleh pin RJ45 sehingga kabel tidak. Apabila pembungkus bagian luar tidak masuk kedalam konektor RJ45 apabila kabel warna sering bergerak kemungkinan besar posisi kabel akan bergesar dan bahkan copot gambar 2.45 dibawah ini.

Gambar 2.45 P2 kabel UTP dengan *straight* untuk crimping dalam RJ45 bagian (2)

Setelah *straight* bagian sebelah kiri dan sebelah kanan maka apabila sudah yakin memasang kabel UTP ke RJ-45 yang terlihat rapi sudah selesai gambar 2.46 dibawah ini.



Gambar 2.46 P1 dan P2 kabel UTP dengan *straight* proses sudah selesai

2.22.10 Memeriksa kabel UTP dengan kabel LAN crossover dan kabel straight

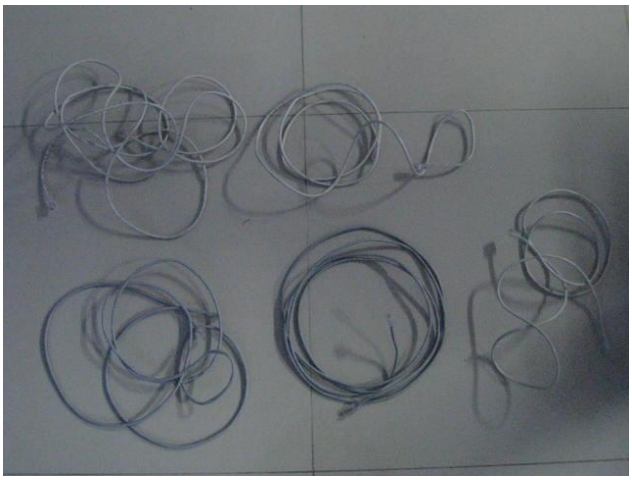
Kemudian setelah *crossover* dan *straight* keduanya untuk melangkah proses membuat sudah selesai. Sebuah alat Cable Tester RJ45/RJ11/USB/BNC LAN Cable Cat5 Cat6 Wire Tester akan lakukan menguji apakah kegiatan crimping dalam konektor RJ45 maka keduanya *crossover* dan *straight* yang telah menghasilkan benar bahawa diuji dibagian LAN *tester* akan memasukkan posisi kiri dan kanan. Pada perangkat ini terdapat dua bagian dan pada masing-masing bagian terdapat delapan lampu LED yang menunjukkan urutan nomor gambar 2.47 dibawah ini.

Gambar 2.47 Network Cable Tester RJ45/RJ11/USB/BNC
LAN Cable Cat5 Cat6 Wire Tester

Kabel UTP *crossover* untuk menyampaikan dilangkah tahap membuatnya sudah selesai tinggal memasukkan LAN *tester* dari sebelah kiri dan sebelah kanan maka lakukan menguji apakah kegiatan crimping dalam konektor RJ45 akan menghasilkan benar bahawa diuji dibagian LAN *tester* akan memasukkan posisi kiri dan kanan. Ternyata crossover mendapatkan dua bagian dan pada masing-masing bagian terdapat delapan lampu LED yang menunjukkan urutan nomor pin yang menandai non-parallel berarti tidak mengaturkan sesuai urutan T568B dan T568A dalam keadaan kondisi semakin baik jadi lihat gambar 2.48 dibawah ini.

Gambar 2.48 Scanner kabel UTP dengan *crossover* bagian (1)

Akhirnya kabel UTP *crossover* untuk membutuhkan 5 buah yang menyampaikan setiap dilangkah tahap membuatnya sudah diselesaikan gambar 2.49 dibawah ini.

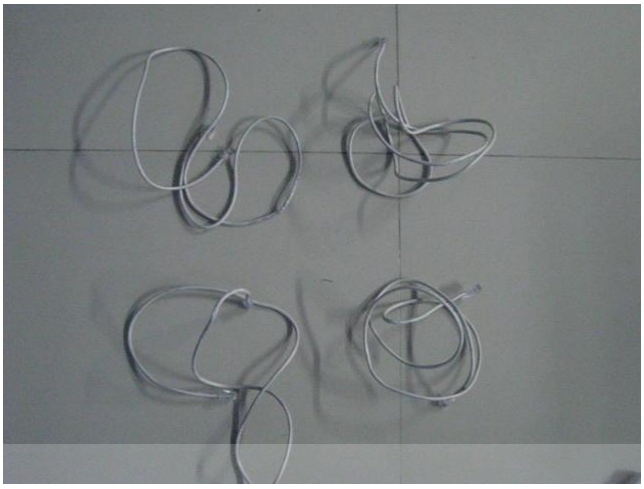


Gambar 2.49 Kabel UTP dengan crossover 5 buah bagian (2)

Kabel UTP *crossover* untuk menyampaikan dilangkah tahap membuatnya sudah selesai tinggal memasukkan LAN *tester* dari sebelah kiri dan sebelah kanan maka lakukan menguji apakah kegiatan crimping dalam konektor RJ45 akan menghasilkan benar bahawa diuji dibagian LAN *tester* akan memasukkan posisi kiri dan kanan. Ternyata crossover mendapatkan dua bagian dan pada masing-masing bagian terdapat delapan lampu LED yang menunjukkan urutan nomor pin yang menandai connected berarti mengaturkan sesuai urutan T568B bersama dalam keadaan kondisi semakin lancar gambar 2.50 dibawah ini.

Gambar 2.50 Scanner kabel UTP dengan *straight* bagian (1)

Akhirnya kabel UTP *straight* untuk membutuhkan 5 buah yang menyampaikan setiap dilangkah tahap membuatnya sudah diselesaikan untuk melihat gambar 2.51 dibawah ini.



\

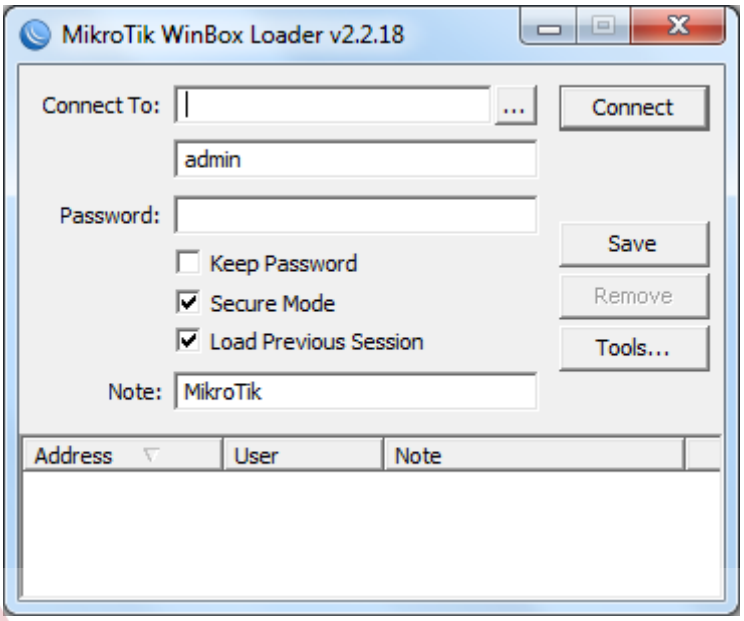
Gambar 2.51 Kabel UTP dengan *straight* 4 buah bagian (2)

2.22 Aplikasi install

2.23.1 Router winbox loader v2.2.18

Setelah aplikasi Winbox Loader v2.2.18 yang menginginkan ketarangan fungsinya. Berikut sedikit penjelasan mengenai tombol dan tulisan pada bidang layar winbox loader pada gambar 2.52 dibawah ini:

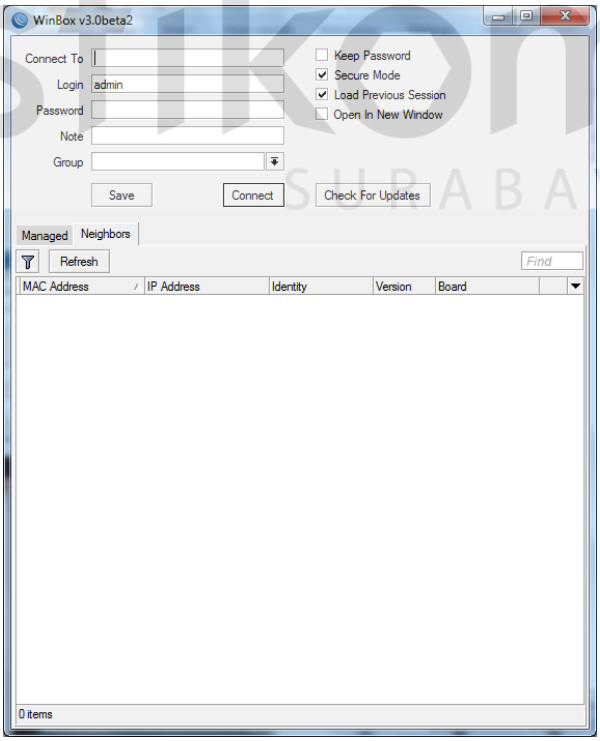
1. *[...]* adalah ditentukan dan ditunjukkan perangkat MikroTik Neighbour Discovery Protocol (MNDP) atau Cisco Discovery Protocol (CDP). Sederhananya untuk menemukan perangkat MikroTik RouterOS yang terhubung ke jaringan.
2. *Connect* adalah digunakan untuk terhubung ke routerOS
3. *Save* adalah digunakan untuk menyimpan alamat, login, password, dan catatan. Entri yang disimpan akan ditampilkan di bagian bawah jendela loader.
4. *Tools* adalah digunakan untuk menjalankan berbagai fungsi, seperti menghapus semua item dari daftar, membersihkan cache pada disk lokal, impor alamat dari file WBX atau ekspor ke file WBX.
5. *Connect to* adalah Tujuan IP atau MAC Address dari Router
6. *Login* adalah username yang digunakan untuk otentikasi.
7. *Password* adalah sandi yang digunakan untuk otentikasi.
8. *Keep* password adalah jika dicentang, sandi tidak disimpan ke dalam daftar.
9. *Secure mode* adalah jika dicentang, winbox akan menggunakan enkripsi TLS untuk mengamankan sesi.
10. *Load previous session* adalah jika dicentang, winbox akan mencoba untuk mengembalikan semua jendela yang dibuka sebelumnya.
11. *Note* adalah deskripsi router yang akan disimpan ke dalam daftar.



Gambar 2.52 Mikrotik winbox loader 2.2.18

2.23.2 Winbox v3.0 beta2

Merupakan aplikasi terbaru winbox versi v3.0 yang menggunakan beta 2 jauh daripada sebelum penggunaan aplikasi lama ini gambar 2.53 dibawah ini.



Gambar 2.53 Winbox v3.0 beta 2

2.23.3 Putty

Sebuah program open source yang menggunakan untuk lakukan client protokol jaringan khususnya RAW, telnet, rlogin, SSH, serial. Dimanakan putty tidak memiliki arti yang masih belum pasti meskipun kata 'tty' suatu nama untuk sebuah terminal dalam sistem operasi Unix. Aplikasi Putty awalnya ditulis untuk Microsoft Windows yang telah berkembang ke berbagai sistem operasi lain. Aplikasi Putty gratis ini dibangun pada awal tahun 1999 setelah digunakan menjadi klien SSH 2 sejak Oktober 2000. Menjelaskan fungsi aplikasi PuTTY harus menjalankan PuTTY pada OS Windows mendapatkan disambungkan lewat khusus mesin Unix. Aplikasi Putty membuka Window. Lalu apakah diketik dalam jendela yang dikirim langsung ke mesin Unix, dan segala sesuatu jawaban dari OS Unix akan dikirim kembali ditampilkan di jendela. Sebuah jaringan digunakan LAN dan wireless bisa lewat akses internet program ini banyak digunakan oleh pengguna komputer tingkat menengah keatas. Biasanya digunakan untuk menyambungkan, mensimulasi, atau mencoba berbagai hal yang terkait dengan jaringan. Bentuk gambar 2.54 dibawah ini:

2.23.3.1 Host name (or IP address)

Membuat alamat tujuan bisa tekan menuliskan disesuaikan ingin nomor atau mungkin website dengan port melalui tipe terkoneksi masing-masing akan terpilih salah satu kita dikerjakan terjadi terminal konfigurasi siap dilaksanakan untuk mengendalikan komputer dari alat komponen misalnya (Mikrotik, cisco).

2.23.3.2 Port

- **Port umum (well known port)**

awalnya berkisar antara 0 hingga 255 tapi kemudian diperlebar untuk mendukung antara 0 hingga 1023. Port number yang termasuk ke dalam well-known port, selalu merepresentasikan layanan jaringan yang sama, dan ditetapkan oleh *Internet Assigned Number Authority* (IANA). Beberapa di antara port-port yang berada di dalam range Well-known port masih belum ditetapkan dan direservasikan untuk digunakan oleh layanan yang bakal ada pada masa depan.

- **Port Terdaftar (Registered Ports)**

Port-port yang digunakan oleh vendor-vendor komputer atau jaringan yang berbeda untuk mendukung aplikasi dan sistem operasi yang mereka buat. Registered port juga diketahui dan didaftarkan oleh IANA tapi tidak dialokasikan secara permanen, sehingga vendor lainnya dapat menggunakan port number yang sama. Range registered port berkisar dari 1024 hingga 49151 dan beberapa port di antaranya dinamakan *Dynamically Assigned Port*.

- **Port Pribadi atau Port Dinamis (Dynamic or Private Ports).**

Memiliki range dari 49152-65535, port ini terutama di gunakan yang memerlukan range port number yang besar

Beberapa contoh port dan fungsinya yang sering digunakan:

1. *File Transfer Protocol* (FTP) sebuah protokol jaringan yang berjalan dalam lapisan aplikasi yang standar pentransferan berkas dari komputer antar mesin-mesin dalam internetwork.
2. *Simple Mail Transfer Protocol* (SMTP) merupakan salah satu protokol yang umum digunakan untuk pengiriman surat elektronik jaringan. Protokol sering yang digunakan untuk mengirimakan data dari komputer.
3. *Hypertext Transfer Protocol* (HTTP) protokol yang menggunakan ditransfer dokumentasi dalam *World Wide Web* (WWW). Protokol sering memakai protokol ringan tidak bisa berstatus dan generik yang dapat dipergunakan berbagai macam tipe dokumentasi.
4. *Post Office Protocol version 3* (POP3) protokol yang digunakan untuk mengambil surat elektronik (email) dari server email.
5. *Internet Message Access Protocol* (IMAP) protokol standar untuk mengakses protokol standar untuk mengakses/ mengambil e-mail dari server. IMAP memungkinkan pengguna memilih pesan e-mail yang akan ia ambil, membuat folder di server, mencari pesan e-mail tertentu, bahkan menghapus pesan e-mail yang ada.

6. 1-19, berbagai protokol, Sebagian banyak port ini tidak begitu di perlukan namun tidak dapat diganggu. Contohnya layanan echo (port 7) yang tidak boleh dikacaukan dengan program ping umum.

Jenis-jenis port dan fungsi-fungsinya.

1. 1-19, berbagai protokol, Sebagian banyak port ini tidak begitu di perlukan namun tidak dapat diganggu. Contohnya layanan echo (port 7) yang tidak boleh dikacaukan dengan program ping umum.
2. 20-FTP-DATA. "Active" koneksi FTP menggunakan dua port: 21 adalah port kontrol, dan 20 adalah tempat data yang masuk. FTP pasif tidak menggunakan port 20 sama sekali.
3. 21-Port server FTP yang digunakan oleh File Transfer Protocol. Ketika seseorang mengakses FTP server, maka ftp client secara default akan melakukan koneksi melalui port 21.
4. 22-SSH (Secure Shell), Port ini ini adalah port standar untuk SSH, biasanya diubah oleh pengelola server untuk alasan keamanan.
5. 23-Telnet server. Jika anda menjalankan server telnet maka port ini digunakan client telnet untuk hubungan dengan server telnet.
6. 25-SMTP, Simple Mail Transfer Protocol, atau port server mail, merupakan port standar yang digunakan dalam komunikasi pengiriman email antara sesama SMTP Server.
7. 37-Layanan Waktu, port built-in untuk layanan waktu.
8. 53-DNS, atau Domain Name Server port. Name Server menggunakan port ini, dan menjawab pertanyaan yang terkait dengan penerjamahan nama domain ke IP Address.
9. 67 (UDP)-BOOTP, atau DHCP port (server). Kebutuhan akan Dynamic Addressing dilakukan melalui port ini.
10. 68 (UDP)-BOOTP, atau DHCP port yang digunakan oleh client.
11. 69-TFTP, atau Trivial File Transfer Protocol.
12. 79-Port Finger, digunakan untuk memberikan informasi tentang sistem, dan login pengguna.

13. 80-WWW atau HTTP port server web. Port yang paling umum digunakan di Internet.
14. 81-Port Web Server Alternatif, ketika port 80 diblok maka port 81 dapat digunakan sebagai port altenatif untuk melayani HTTP.
15. 98-Port Administrasi akses web Linuxconf port.
16. 110-POP3 Port, alias Post Office Protocol, port server pop mail. Apabila anda mengambil email yang tersimpan di server dapat menggunakan teknologi POP3 yang berjalan di port ini.
17. 111-SUNRPC (Sun Remote Procedure Call) atau portmapper port. Digunakan oleh NFS (Network File System), NIS (Network Information Service), dan berbagai layanan terkait.
18. 113-IDENTD atau Auth Port Server. Kadang-kadang diperlukan, oleh beberapa layanan bentuk lama (seperti SMTP dan IRC) untuk melakukan validasi koneksi.
19. 119-NNTP atau Port yang digunakan oleh News Server, sudah sangat jarang digunakan.
20. 123-Network Time Protocol (NTP), port yang digunakan untuk sinkronisasi dengan server waktu di mana tingkat akurasi yang tinggi diperlukan.
21. 137-139-NetBIOS (SMB).
22. 143-IMAP, Interim Mail Access Protocol. Merupakan aplikasi yang memungkinkan kita membaca e-mail yang berada di server dari komputer di rumah / kantor kita, protokol ini sedikit berbeda dengan POP.
23. 161-SNMP, Simple Network Management Protocol. Lebih umum digunakan di router dan switch untuk memantau statistik dan tanda-tanda vital (keperluan monitoring).
24. 177-XDMCP, X Display Management Control Protocol untuk sambungan remote ke sebuah X server.
25. 443-HTTPS, HTTP yang aman (WWW) protokol di gunakan cukup lebar.
26. 465-SMTP atas SSL, protokol server email
27. 512 (TCP)-EXEC adalah bagaimana menunjukkan di netstat. Sebenarnya nama yang tepat adalah rexec, untuk Remote Execution.

28. 512 (UDP)-BIFF, protokol untuk mail pemberitahuan.
29. 513-Login, sebenarnya rlogin, alias Remote Login. Tidak ada hubungannya dengan standar / bin / login yang kita gunakan setiap kali kita log in.
30. 514 (TCP)-Shell adalah nama panggilan, dan bagaimana netstat menunjukkan hal itu. Sebenarnya, rsh adalah aplikasi untuk "Remote Shell". Seperti semua "r" perintah ini melemparkan kembali ke kindler, sangat halus.
31. 514 (UDP)-Daemon syslog port, hanya digunakan untuk tujuan logging remote.
32. 515-lp atau mencetak port server.
33. 587-MSA, Mail Submission Agent. Sebuah protokol penanganan surat baru didukung oleh sebagian besar MTA's (Mail Transfer Agent).
34. 631-CUPS (Daemon untuk keperluan printing), port yang melayani pengelolaan layanan berbasis web.
35. 635-Mountd, bagian dari NFS.
36. 901-SWAT, Samba Web Administration Tool port. Port yang digunakan oleh aplikasi pengelolaan SAMBA berbasis web.
37. 993-IMAP melalui SSL.
38. 995-POP melalui SSL.
39. 1024-Ini adalah port pertama yang merupakan Unprivileged port, yang ditugaskan secara dinamis oleh kernel untuk aplikasi apa pun yang memintanya. Aplikasi lain umumnya menggunakan port unprivileged di atas port 1024.
40. 1080-Socks Proxy Server.
41. 1433-MS SQL Port server.
42. 2049-NFSd, Network File Service Daemon port.
43. 2082-Port cPanel, port ini digunakan untuk aplikasi pengelolaan berbasis web yang disediakan oleh cpanel.
44. 2095-Port ini di gunakan untuk aplikasi webmail cpanel.
45. 2086-Port ini di gunakan untuk WHM, atau Web Host Manager cpanel.
46. 3128-Port server Proxy Squid.
47. 3306-Port server MySQL.

48. 5432-Port server PostgreSQL.
49. 6000-X11 TCP port untuk remote. Mencakup port 6000-6009 karena X dapat mendukung berbagai menampilkan dan setiap tampilan akan memiliki port sendiri. SSH X11Forwarding akan mulai menggunakan port pada 6.010.
50. 6346-Gnutella.
51. 6667-IRCD, Internet Relay Chat Daemon.
52. 6699-Napster.
53. 7100-7101-Beberapa Font server menggunakan port tersebut.
54. 8000 dan 8080-Common Web Cache dan port server Proxy Web.
55. 10000-Webmin, port yang digunakan oleh webmin dalam layanan pengelolaan berbasis web

2.23.3.3 Raw

protokol jaringan yang memungkinkan pertukaran data dengan menggunakan saluran aman antara dua perangkat jaringan. Digunakan terutama pada Linux dan Unix sistem berbasis untuk mengakses akun shell, SSH dirancang sebagai pengganti Telnet dan kerang terpencil tidak aman lainnya, yang mengirim informasi, terutama password, di teks biasa, meninggalkan mereka terbuka untuk intersepsi.

2.23.3.4 Telnet

Telecommunication network (Telnet) sebuah protokol jaringan yang digunakan pada *Local Area Network* (LAN) untuk menyediakan fasilitas komunikasi berbasis teks interaksi dua arah yang menggunakan koneksi virtual terminal. remote login yang dapat terjadi di internet karena ada service dari protocol TELNET. telnet memungkinkan untuk dimasukkan komputer lain secara remote melalui internet. Suatu protokol jaringan yang digunakan jaringan lokal. Telnet menyediakan komunikasi dua arah yang berbasis teks atau terminal emulator antara client dengan server atau dengan bisa memberikan memberikan perintah, untuk menjalankan perintah, untuk merubah konfigurasi, untuk mengendalikan, dan meremote komputer lain (server) melalui komputer pada client. Protocol client server yang memfasilitasi akses remote login ke komputer host dalam jaringan komputer bahwa telnet mendapatkan telnet yang sebagai

virtual atau emulasi terminal yang menggunakan protokol telnet untuk dilakukan akses secara remote pada komputer jika telnet harus diperintah mengisikan bagian dari protokol TCP/IP untuk mengakses komputer remote. Penggunaan putty untuk meremote komputer dengan terhubungnya memakai port serta sebagainya. telnet akan berbanding 2 program antara client dan sever maka keduanya program yang menjelaskan software client yang dijalankan pada komputer yang meminta pelayanan dan software server akan dijalankan oleh komputer yang menghasilkan pelayanan. Penjelasan keduanya program dari client dan server dibawah ini:

- **Client**

1. Membuat koneksi network *Transfer Control Protocol* (TCP) dengan server.
2. Menerima inputan dari user.
3. Menformat kembali inputan dari user kemudian mengubah dalam bentuk format standar dan dikirim ke server.
4. Menerima output dari server dalam format standard.
5. Mengubah format output tadi untuk ditampilkan pada layar.

- **Server**

1. Menginformasikan software jaringan bahwa komputer itu siap menerima koneksi.
2. Menunggu permintaan dalam bentuk format standard.
3. Melaksanakan permintaan tersebut.
4. Mengirim kembali hasil ke client dalam bentuk format standard.
5. Menunggu permintaan selanjutnya.

Fungsi *Telecommunication Network* (Telnet)

telnet untuk mengakses komputer (host/server) dari jauh/remote login. Jika memungkinkan komputer menjadi terminal dari komputer dari komputer lain pada internet. telnet memungkinkan masuk (Log in) sebagai penggunaan komputer jarak jauh menjalankan program komputer layanan yang komputer

- **Kelebihan Telnet**

  Kelebihan menggunakan telnet server dari user interface yang ramah untuk memberikan perintah jarak jauh (istilahnya remote) seolah-olah akan mengeksekusi perintah pada command line pada komputer.

- **Kelemahan Telnet**

  Kekurangan telnet yang penggunaan NTLM authentication tanpa enkripsi sehingga memudahkan pencurian password oleh sniffers. jika administrator sistem disarankan untuk menggunakan SSH pada Linux daripada Telnet Server untuk mengkonfigurasikan sistem.

2.23.3.5 Rlogin

Remote login suatu program emulasi terminal yang similar dengan telnet menawarkan dalam kebanyakan implementasi Unix.

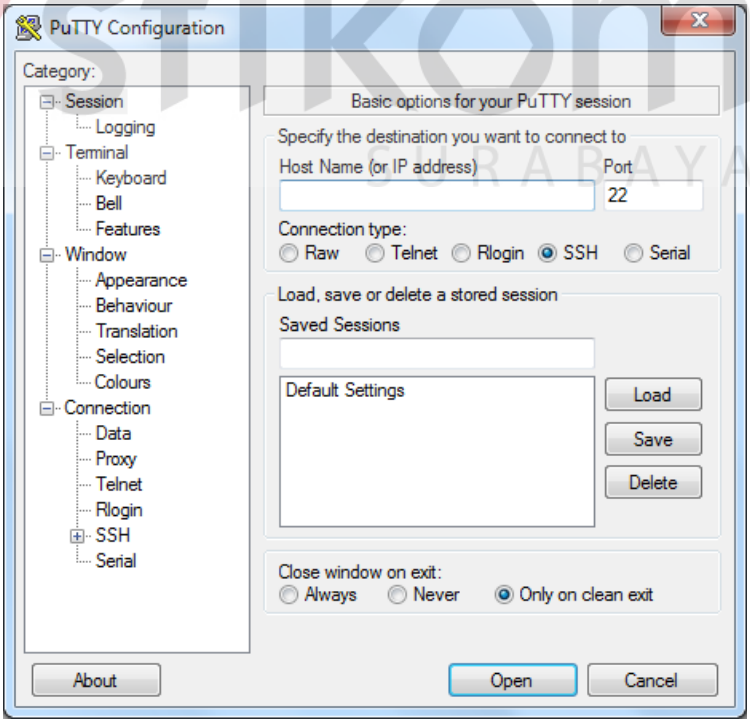
2.23.3.6 Secure shell (SSH)

Secure shell (SSH) merupakan protokol kriptografi yang digunakan untuk komunikasi data yang aman dengan menggunakan antarmuka baris perintah seperti command promt yang dipergunakan untuk mengeskekusi perintah jarak jauh seperti update, upgrade, config, dll pada layanan jaringan antar komputer satu dengan komputer lainnya dengan port standard yang digunakan adalah port 22. aplikasi pengganti remote login seperti telnet, rsh, dan rlogin, yang jauh lebih aman. Fungsi utama aplikasi ini adalah untuk mengakses mesin secara remote. Sama seperti telnet, SSH Client menyediakan User dengan shell untuk remote ke mesin. Tidak seperti telnet SSH menyediakan koneksi enkripsi antara klien dengan server. Penggunaan menggunakan telnet dan ssh seperti perbedaan dengan mengakses website biasa dengan website yang lebih aman (HTTPS). protokol jaringan yang memungkinkan pertukaran data melalui saluran aman antara dua perangkat jaringan. Terutama banyak digunakan pada sistem berbasis Linux dan Unix untuk mengakses akun shell SSH dirancang sebagai pengganti Telnet dan shell remote tak aman lainnya, yang mengirim informasi dalam terutama kata password dalam bentuk teks sederhana yang membuatnya mudah untuk dicegat. protokol jaringan yang memungkinkan pertukaran data

melalui saluran aman antara dua perangkat jaringan (misalnya komputer kita ke VPS). SSH ini karena merupakan protokol jadi bentuknya angka, seperti yang kita tau dalam IP (internet protokol) dan memiliki username password untuk mengakses ke VPS ex: 199.221.xxx.xxx. SSH ini sendiri menjadi pembungkus bagi IP kita yang asli. Enkripsi yang digunakan oleh SSH menyediakan kerahasiaan dan integritas data melalui jaringan yang tidak aman seperti Internet. SSH digunakan sebagai jalur internet gratis, tanpa mengurangi kuota atau pulsa. Ini merupakan salah satu kegunaan SSH yaitu forwarding atau tunneling. Biasanya digunakan alat tambahan seperti inject, proxyfier, proxy, dll.

2.23.3.7 Serial

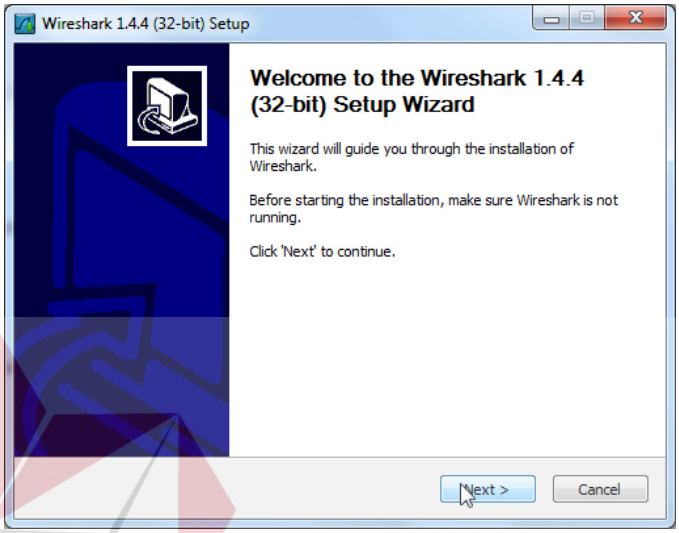
Penggunaan metode penerima kabel serial menggunakan com port dan band rate untuk terkoneksi dan antara satu sama lain harus sama untuk band ratenya agar data yang masuk dapat dibaca. Khususnya mesin cisco dalam menggunakan LAN harus ada kabel cisco untuk digabungkan kabel serial RS232 akan masukan aplikasi putty untuk mengisikan *serial line* com berapa dibutuhkan saat ini dan *port* 9600.



Gambar 2.54 Putty

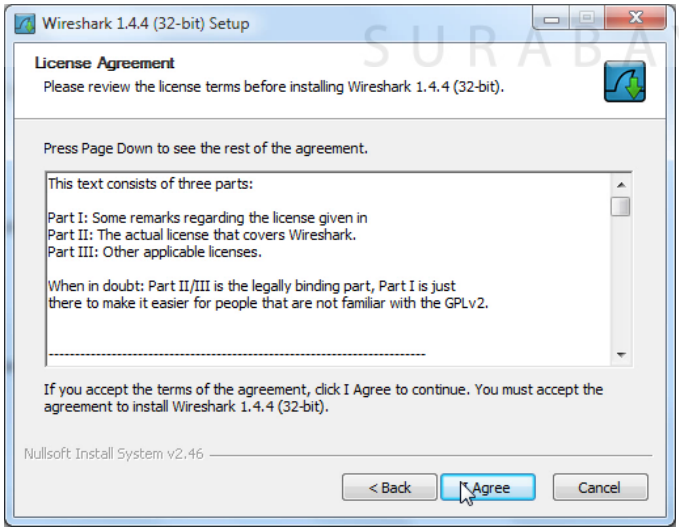
2.23.4 Wireshark

Sebuah aplikasi versi 1.4.4 akan mulai muncul tampilah seperti ini untuk dimulai memasukkan diinstall wireshark lalu klik selanjutnya gambar 2.55 dibawah ini (Sharpe, R. 2008).



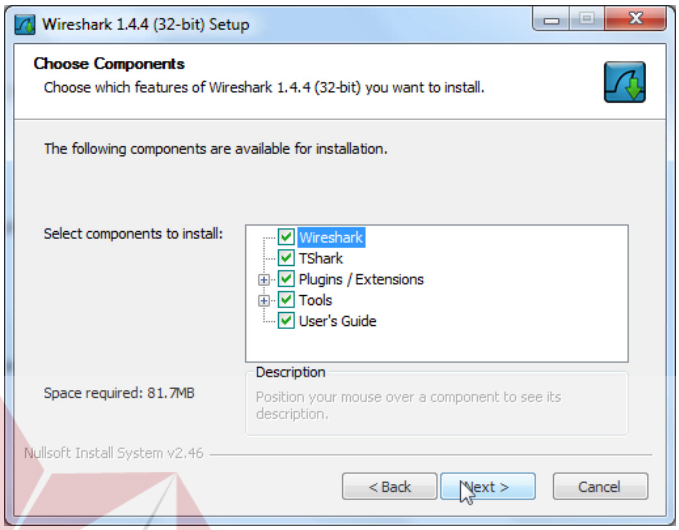
Gambar 2.55 Menginstall wireshark 1.4.4 (1)

Kemudian ada muncul pengumuman bisa lihat instruksi manual cara memakainya maka dimulai keatas sampai terakhir untuk dipahami jika sudah selesai akan ditekan *I agree* selanjutnya gambar 2.56 dibawah ini.



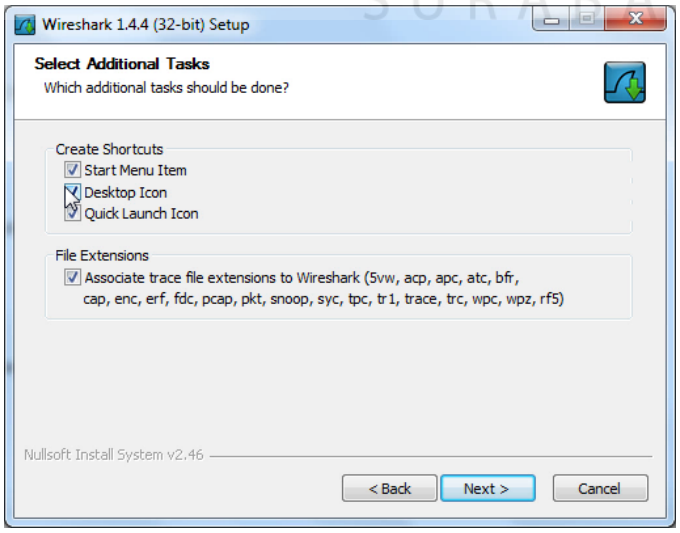
Gambar 2.56 Menginstall wireshark 1.4.4 (2)

Kemudian ada muncul memilih komponen didalam 5 menu kotak centang dari *wireshark*, *tshark*, *plugins/extensions*, *tools*, *user's guide*. Menu 5 kotak centang masing-masing akan ditekan semuanya mengisntall lalu klik selanjutnya gambar 2.57 dibawah ini.



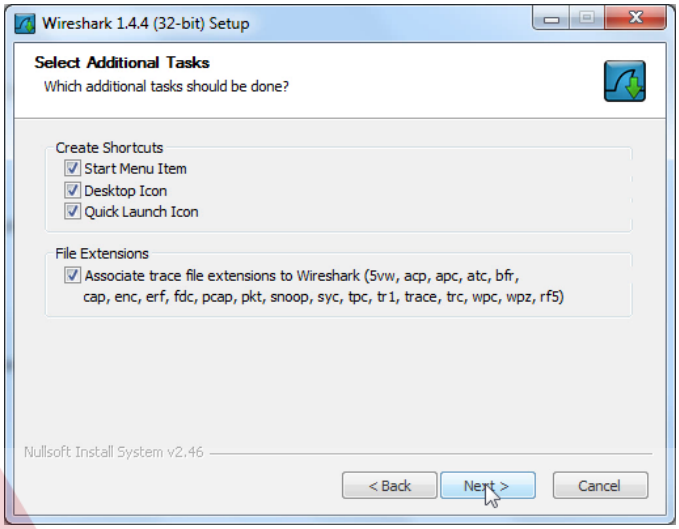
Gambar 2.57 Menginstall wireshark 1.4.4 (3)

kemudian ada muncul dua pilihan menu dalam kotak centang yaitu *create shortcuts* dan *file extension* keduanya harus tekan terlebih dahulu sebelum dimulai *create shortcuts* untuk tiga kotak centang masing-masing akan ditekan semuanya menandai sedangkan untuk *file extensions* ditekan satu menandai yang melengkapi file gambar 2.58 dibawah ini.



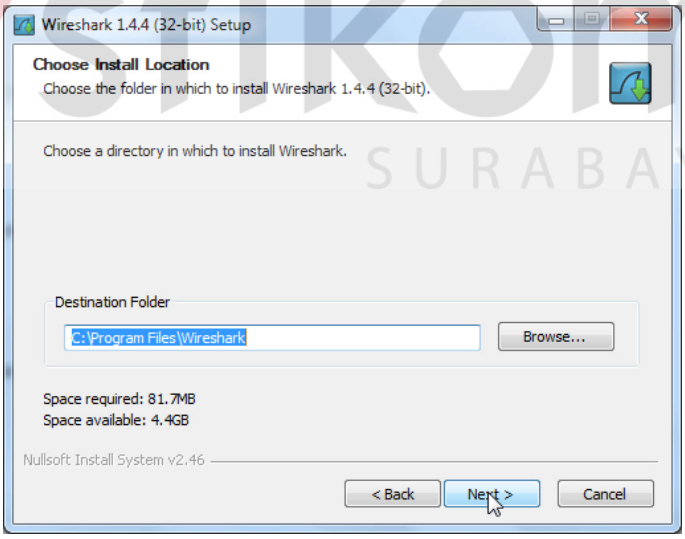
Gambar 2.58 Menginstall wireshark 1.4.4 (4)

setelah keduanya menu *create shortcuts* dan *file extensions* sudah selesai lalu klik selanjutnya gambar 2.59 dibawah ini.



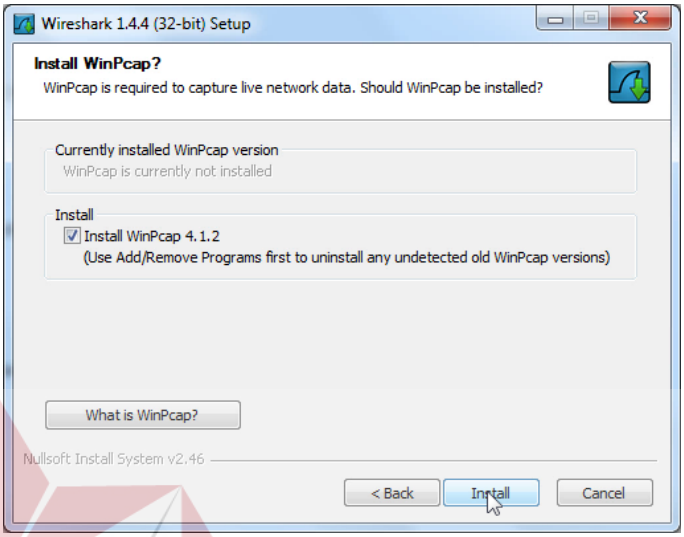
Gambar 2.59 Menginstall wireshark 1.4.4 (5)

Kemudian ada muncul lokasi memilih diinstall akan membuka direktori folder pada browser yang menunjukkan tulisan c:\program files\wireshark dipastikan kapasitas ukuran mencapai 81.7MB lalu klik selanjutnya gambar 2.60 dibawah ini.



Gambar 2.60 Menginstall wireshark 1.4.4 (6)

Setelah tahap menu sudah selesai tinggal aplikasi winpcap 4.1.2 dalam kotak centang maka ditekan menandai lalu finish diakhiri. Beberapa proses menjalankan hasil sudah selesai gambar 2.61 dibawah ini.

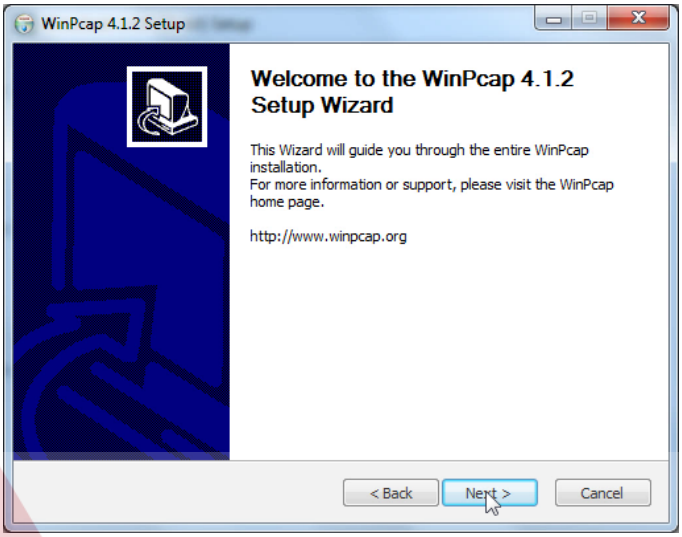


Gambar 2.61 Menginstall wireshark 1.4.4 (7)

Setelah terjadi ada aplikasi terbaru winpcap versi 4.1.2 untuk menjalankan diinstall lalu klik selanjutnya gambar 2.62 dibawah ini.

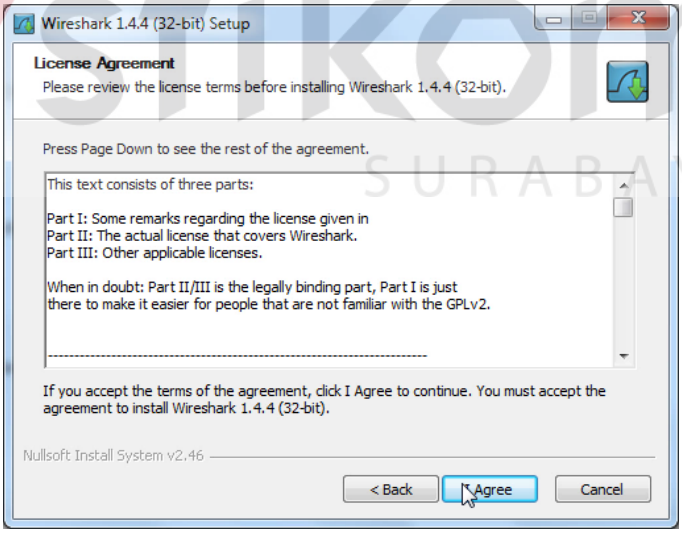
Gambar 2.62 Menginstall wireshark 1.4.4 pada diinstall winpcap 4.1.2 (1)

Sebuah aplikasi winpcap versi 4.1.2 akan mulai muncul tampilah seperti ini untuk dimulai memasukkan diinstall wireshark lalu klik selanjutnya gambar 2.63 dibawah ini.



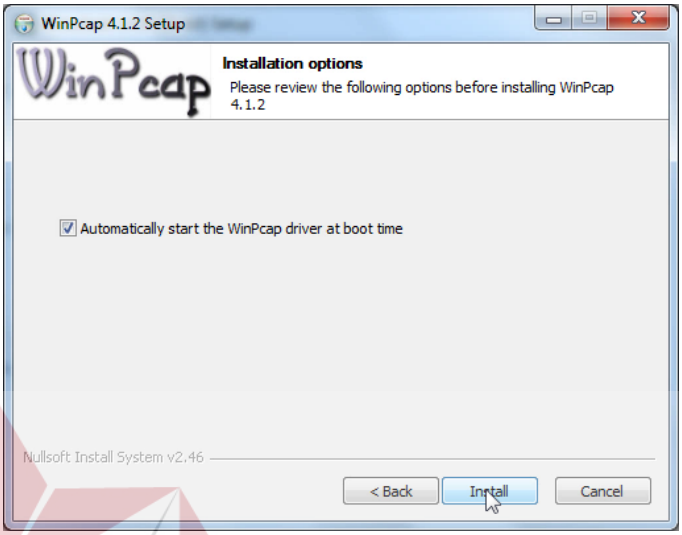
Gambar 2.63 Menginstall wireshark 1.4.4 pada diinstall winpcap 4.1.2 (2)

Kemudian ada muncul pengumuman bisa lihat instruksi manual cara memakainya maka dimulai keatas sampai terakhir untuk dipahami jika sudah selesai akan ditekan *I agree* selanjutnya gambar 2.64 dibawah ini.



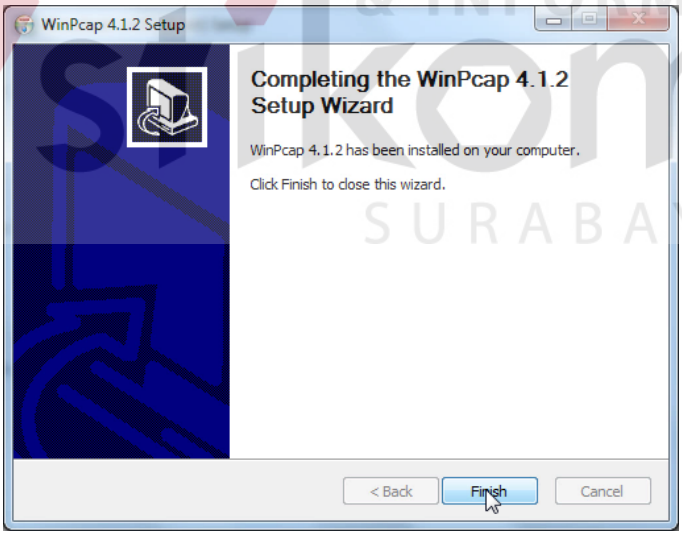
Gambar 2.64 Menginstall wireshark 1.4.4 pada diinstall winpcap 4.1.2 (3)

Kemudian setelah akhir tinggal kotak centang ditekan *automatically start the winpcap driver at boot time* untuk menandai jika sudah selesai lalu finish selanjutnya. Nunggu proses menjalankan dinstall sudah selesai gambar 2.65 dibawah ini.



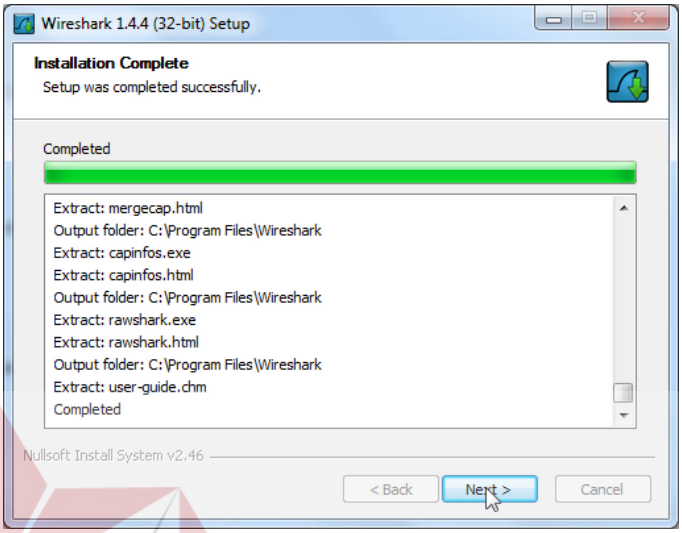
Gambar 2.65 Menginstall wireshark 1.4.4 pada diinstall winpcap 4.1.2 (4)

Setelah aplikasi winpcap 4.1.2 sudah selesai lalu tekan finish gambar 2.66 dibawah ini.



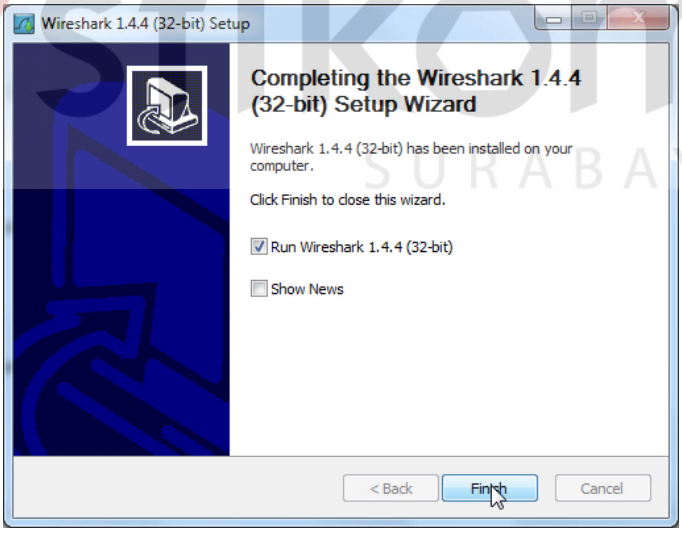
Gambar 2.66 Menginstall wireshark 1.4.4 pada diinstall winpcap 4.1.2 (5)

Kembali melanjutkan proses wireshark yang disampaikan aplikasi winpcap 4.1.2 untuk tahap sudah selesai tinggal akhir ditekan finish selanjutnya. Nunggu proses menjalankan dinstall sudah selesai gambar 2.67 dibawah ini.



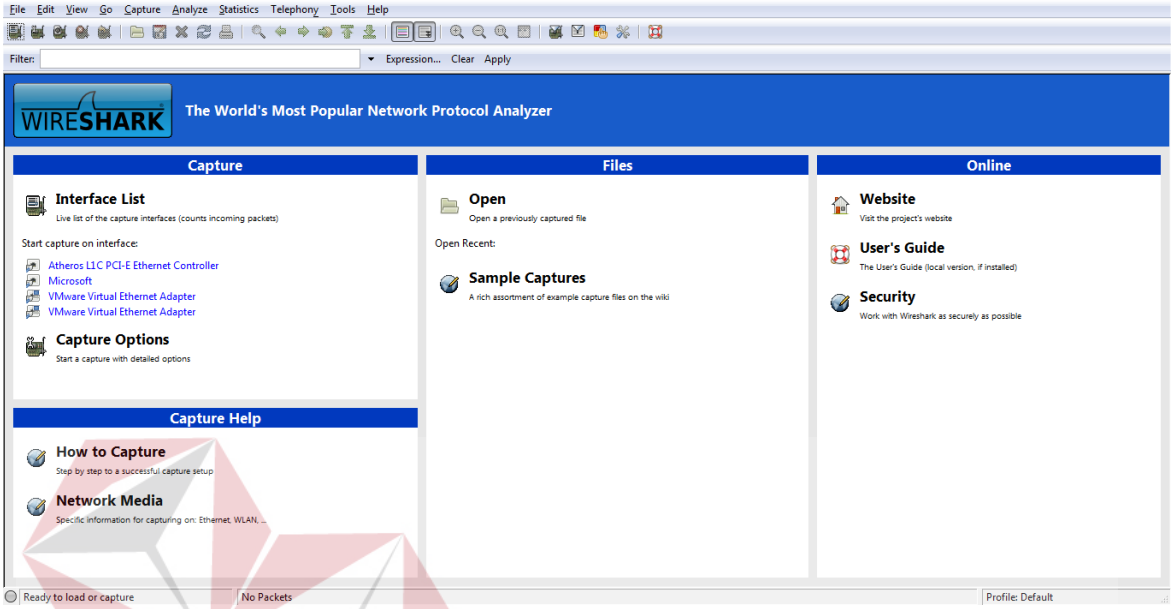
Gambar 2.67 Kembali melanjutkan proses wireshark 1.4.4 sampai winpcap 4.1.2

Setelah aplikasi wireshark versi 1.4.4 sudah selesai dalam kotak centang ditekan *run wireshark 1.4.4 (32 bit)* lalu finish sudah diakhiri gambar 2.68 dibawah ini.



Gambar 2.68 Membuka aplikasi wireshark 1.4.4 (1)

Setelah aplikasi wireshark versi 1.4.4 sudah bisa menjalankan dengan baik gambar 2.69 dibawah ini.



Gambar 2.69 Membuka aplikasi wireshark 1.4.4 (2)

2.23 Menjelaskan dan rumusan

2.24.1 Bandwidth

Istilah yang digunakan untuk menggambarkan berapa banyak informasi dapat dikirim melalui koneksi jaringan komputer. Ini biasanya dilambangkan sebagai bit per detik, atau dengan beberapa denominasi bit yang lebih besar, seperti Megabits per detik, dinyatakan sebagai Mbit/s atau kbit/s. Kualitas data yang ditransfer dipandang sebagai bagian dari pengertian bandwidth yang memperhitungkan apakah data berhasil dikirim atau tidak. Sedangkan bandwidth koneksi mungkin cukup tinggi, jika tingkat kehilangan sinyal juga tinggi, maka throughput dari koneksi akan tetap agak rendah. Sebaliknya, bahkan koneksi bandwidth relatif rendah dapat memiliki throughput yang cukup tinggi jika kualitas sinyal juga tinggi.

- **Rumusan bandwidth**

  Merupakan ukuran kecepatan aliran data yang menyatakan banyaknya informasi yang dapat mengalir dari suatu tempat ke tempat lain dalam suatu waktu tertentu. Sebenarnya bandwidth adalah jumlah bit yang dapat dikirimkan dalam satu detik. Oleh karenanya bandwith memiliki satuan yang dipakai dalam bits per second atau sering disingkat sebagai bps. Cara menghitung bandwidth seperti ini

- **Bandwidth** = $\frac{\sum bit}{s}$

2.24.2 Throughput

Nilai throughput yang minimum mungkin diperlukan. berbeda dengan kunjungan yang paling elastis yang dapat terus mengirimkan data dengan layanan banyak aplikasi inelastis mungkin terdegradasi benar-benar memerlukan throughput minimum tertentu. Jka standar ukuran dengan satuan waktu tertentu dan pada kondisi jaringan tertentu yang digunakan untuk melakukan transfer file dengan ukuran tertentu. Menjumlahkan bit yang dapat dikirimkan dalam satu detik sedangkan throughput walau pun memiliki satuan dan rumus yang sama dengan bandwidth, tetapi throughput lebih pada menggambarkan bandwidth yang sebenarnya (aktual) pada suatu waktu tertentu dan pada kondisi dan jaringan internet tertentu yang digunakan untuk mendownload suatu file dengan ukuran tertentu. (Stallings, W. 2002)

➢**Rumusan throughput**

Merupakan besaran yang menunjukkan laju bit informasi data sebenarnya dari laju bit pada suatu jaringan telekomunikasi. Throughput adalah bandwidth aktual yang terukur pada suatu ukuran waktu tertentu dalam suatu hari menggunakan rute internet yang spesifik ketika sedang melakukan download suatu file. . Kecepatan rata-rata data yang penerima dari node dalam selang waktu pengamatan tertentu. Throughput merupakan bandwidth actual saat ini juga dimana kita sedang melakukan koneksi. Satuan yang dimilikinya sama dengan bandwidth dalam bps.

$$\textbf{Troughput} = \frac{(jumla\ h\ data\ \ yang\ \ dikirim\ )}{(waktu\ \ pengiriman\ \ \ data\ )}$$

2.24.3 Latency (delay)

Istilah serupa yang mengacu pada jumlah waktu yang dibutuhkan sedikit yang akan dikirim dari sumber ke tujuan. Jitter penundaan yang bervariasi dari waktu ke waktu. Salah satu cara untuk melihat latency adalah berapa lama sistem berpegang pada sebuah paket. Sistem yang mungkin merupakan sebuah perangkat tunggal seperti router, atau sistem komunikasi lengkap termasuk router dan link.

➢**Rumusan latency (delay)**

Delay adalah waktu tunda saat paket yang diakibatkan oleh proses transmisi dari satu titik lain yang menjadi tujuannya. Delay diperoleh dari selisih waktu kirim antara satu paket TCP dengan paket lainnya. Untuk menghitung ratarata delay digunakan rumus

$$\textbf{Delay} = \frac{total\ \ delay}{total\ \ packet\ \ yang\ \ diterima}$$

2.24.4 Jitter

Besarnya variasi delay merupakan faktor penting dalam aplikasi real time. semakin besar variasi delay yang diijinkan lagi penundaan nyata dalam memberikan data dan semakin besar ukuran delay penyangga diperlukan pada penerima, secara real time

aplikasi interaktif seperti telekonferensi mungkin memerlukan wajar batas atas jitter. Besarnya nilai jitter akan sangat dipengaruhi oleh variasi beban trafik dan besarnya tumbukan antar paket (congestion) yang ada dalam jaringan IP. Semakin besar beban trafik di dalam jaringan akan menyebabkan semakin besar pula peluang terjadinyacongestion dengan demikian nilai jitter-nya akan semakin besar. Semakin besar nilai jitter akan mengakibatkan nilai QoS akan semakin turun. Untuk mendapatkan nilai QoS jaringan yang baik, nilai jitter harus dijaga seminimum mungkin. (Stallings, W. 2002)

➢ **Rumusan jitter**

variasi waktu dari sinyal periodik dalam elektronik dan telekomunikasi, sering kali dalam kaitannya dengan sumber referensi jam. Jitter dapat diamati dalam karakteristik seperti frekuensi berturut-turut pulses, amplitude sinyal, atau fasa dari sinyal periodik. Jitter mendefiniskan sebagai variasi delay antar paket yang diakibatkan oleh panjang queue dalam suatu pengolahan data dan reassemble paket paket data di akhir pengiriman akibat kegagalan sebelumnya. Delay antrian pada router dapat menyebabkan jitter . Semakin besar beban trafikatau nilai variasi delay di dalam jaringan akanmenyebabkan semakin besar pula peluang terjadinyatumbukan antar paket, sehingga nilai jitter akan semakin besar dan menyebabkan nilai QoS semakinturun. Secara umum jitter merupakan masalah dalam slow speed links. Cara menghitung jitter menggunakan rumus seperti dibawah ini.

$$\textbf{Jitter} = \frac{total\ \ variasi\ \ delay}{total\ \ paket\ \ yang\ \ diteria\ -1}$$

2.24.5 Packet loss

Kegagalan transmisi paket IP mencapai tujuannya. Kegagalan paket tersebut mencapai tujuan, dapat disebabkan oleh beberapa hal yaitu terjadinya overload trafik di dalam jaringan, tabrakan (congestion) dalam jaringan, error yang terjadi pada media fisik, kegagalan yang terjadi pada sisi penerima antara lain bisa disebabkan karena overflow yang terjadi pada buffer. Menurut (Langi, 2008) paket hilang yang menyebabkan kelemahan dari audio dan video pada multimedia *streaming*. pembuangan paket di jaringan (*network loss*) atau pembuangan paket di *gateway/terminal* sampai kedatangan

terakhir (*late loss*). *Network loss* secara normal disebabkan kemacetan (*router buffer overflow*), perubahan rute secara seketika misalnya kegagalan *link*, dan *lossy link*. Kemacetan atau kongesti pada jaringan merupakan penyebab utama dari paket hilang.

➢ **Rumusan packet loss**

perbandingan seluruh paket IP yang hilang dengan seluruh paket IP yang dikirimkan antara pada source dan destination. Salah satu penyebab paket loss adalah antrian yang melebihi kapasitas buffer pada setiap node. Bentuk paket yang hilang selama proses transmisi ke tujuan.

$$\boldsymbol{Packet\ loss} = \frac{(packet\ \ transmitted\ \ -packet\ \ received\ )}{packet\ \ transmitted} * 100\ \%$$