BAB 9 WIDE AREA NETWORKS (WAN)

Tujuan:

Pembahasan ini bertujuan agar siswa dapat :
1. Mengidentifikasi infrastruktur Wide Area Network (WAN)
2. Melakukan Diagnosa permasalahan pada Wide Area Network (WAN)
3. Siswa membuat konfigurasi dari Administrasi Server sebagai pengisi Wide Area Network (WAN)

Pokok Bahasan

Dalam pembahasan ini meliputi:
1. Wide Area Network, meliputi Koneksi WAN, VLAN, VPN, PPP, Frame Relay
2. Diagnosa permasalahan *Wide Area network*
3. Perbaikan / setting ulang *Wide Area network*

9.1. Pendahuluan

WAN (Wide Area Network) merupakan sistem jaringan yang menghubungkan antar Autonomous System (AS). Satu Autonomous System dapat terdiri atas satu jaringan atau lebih. WAN mencakup daerah geografis yang luas, memungkinkan komunikasi antara dua perangkat yang terpisah dengan jarak yang sangat jauh.

Untuk menhubungkan beberapa autonomous system, selain diperlukan media fisik tertentu, juga diperlukan teknologi WAN yang bekerja dengan melakukan komunikasi dengan pengolahan frame.

Pada implementasinya, teknologi WAN dapat bekerja pada lapisan datalink atau gabungan antara lapisan fisik dan datalink. Pada lapisan datalink yang dikerjakan merupakan proses sinkronisasi digital yang juga dilengkapi dengan authentikasi.

Pada lapisan fisik, sejumlah standarisasi pensinyalan yang didefinisikan pada type jalur tertentu dengan kapasitas maksimal data yang dapat dimuatkan pada media telah disediakan untuk membangun Wide Area Network (WAN). Tabel 9.1 menjelaskan standarisasi media yang dapat digunakan untuk membangun Wide Area Network (WAN).

Pada implementasinya macam-macam line type di produksi oleh banyak vendor, satu hal yang membatasi dalam pembuatannya, setiap vendor harus mematuhi aturan standarisasi seperti tercantum pada table 9.1

Tabel 9.1 Standarisasi media WAN dan karakteristiknya

Line Type	Signal Standard	Bit Rate Capacity
56	DS0	56 Kbps
64	DS0	64 Kbps
T1	DS1	1.544 Mbps
E1	ZM	2.048 Mbps
E3	M3	34.064 Mbps
J1	Y1	2.048 Mbps
T3	DS3	44.736 Mbps
OC-1	SONET	51.84 Mbps
OC-3	SONET	155.54 Mbps
OC-9	SONET	466.56 Mbps
OC-12	SONET	622.08 Mbps
OC-18	SONET	933.12 Mbps
OC-24	SONET	1244.16 Mbps
OC-36	SONET	1866.24 Mbps
OC-48	SONET	2488.32 Mbps

Setelah jaringan terhubung dengan menggunakan media fisik tertentu, maka selanjutnya untuk keperluan pertukaran data diperlukan suatu proses yang mengatur pertukaran data melalui aplikasi tertentu. Proses ini selanjutnya dikenal dengan Encapsulasi/Dekapsulasi (*Encapsulation/Decapsulation).*

Encapsulasi adalah proses pemberian informasi (berupa header atauTrailer) data menjadi paket data (PDU = Protocol Data Unit) sebelum dikirimkan ke layer selanjutnya, proses ini terjadi pada proses pengiriman paket data menuju host tujuan.

Proses dari Encapsulation terbagi kedalam lima proses, yaitu :

Tahap 1: Build the Data (PDU = Data). Proses perubahan format aplikasi menjadi PDU yang disebut sebagai DATA, yang dapat dikirimkan melalui media jaringan.

Tahap 2: Package the data for end-to-end transport (PDU = Segments). Proses pengumpulan data yang akan dikirimkan menjadi paket data yang disebut dengan SEGMENT.

Tahap 3: Add the network IP address to the header (PDU=Packets). Pemberian informasi alamat logical (IP Address) asal dan tujuan paket data.

Tahap 4: Add the data link layer header and trailer (PDU=Frames). Pemberian informasi (Frame Header and Trailer) paket data mengenai perangkat jaringan yang terhubung langsung (directly-connected).

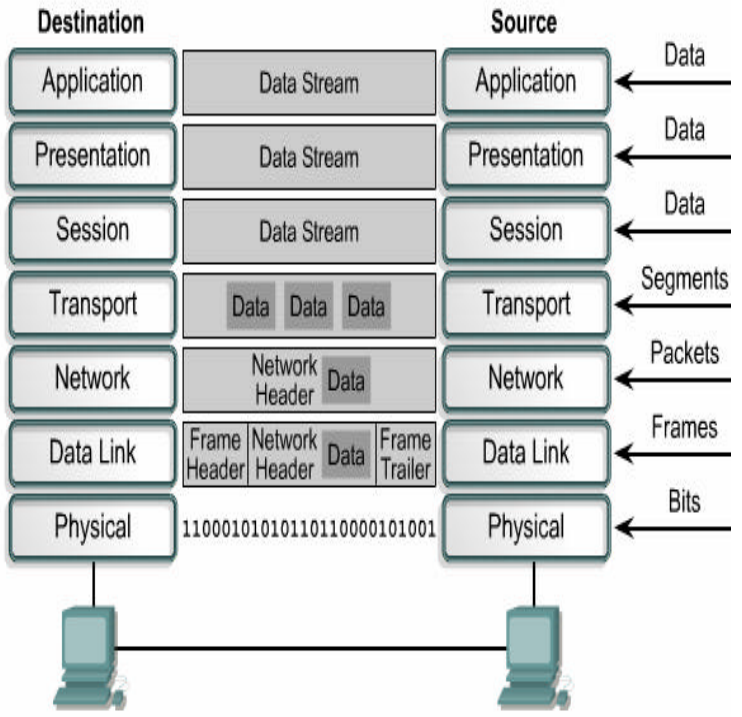
Tahap 5: Convert to bits for transmission (PDU=Bits). Proses konversi paket digital menjadi sinyal-sinyal listrik agar paket data dapat dikirimkan melalui media.

Proses Enkapsulasi terjadi dari Tahap 1 menuju/sampai tahap 5, sedangkan proses kebalikannya yang terjadi pada host tujuan berupa tahap 5 menuju tahap 1 diatas dikenal dengan istilah Dekapsulasi, yaitu terjadi proses pelepasan informasi (berupa header atau trailer) paket data menjadi data.

Proses enkapsulasi terjadi pada proses pengiriman paket data atau proses request pada handshake. Sedangkan proses dekapsulasi terjadi pada proses penerimaan paket data (pada sisi tujuan) atau pada handshake dikenal dengan istilah respon.

Tips :
Simulasi dari analogi teori ini dapat dilihat pada aplikasi network capture dari software wireshark. Pada

software ini dapat dilihat spesifikasi content pada setiap layer meliputi data, header dan trailler-nya.

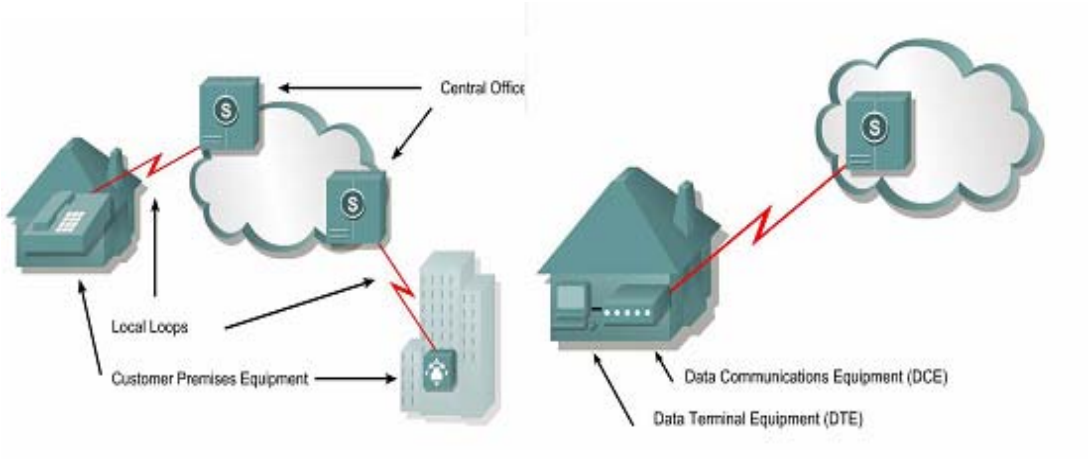


Gambar 9 - 1 PDU Pada OSI Model

WAN dapat menghubungkan banyak LAN serta menyediakan akses ke komputer–komputer atau server pada lokasi lain. Beberapa teknologi WAN antara lain adalah ISDN, DSL, PPP, Frame Relay, T1, E1, T3, E3 dan SONET.

Penyedia layanan jaringan WAN biasa menggunakan istilah-istilah jaringan berikut untuk menggambarkan bagian utama dari jaringan WAN:

1. Customer Premises Equipment (CPE), yaitu peralatan yang dimiliki dan berada di lokasi pelanggan.
2. Data Terminating Equipment (DTE), yaitu perangkat (dapat berupa perangkat tunggal atau berupa sistem) yang berfungsi untuk mengakses jaringan publik yang berada di lokasi pelanggan
3. Local Loop, yaitu jalur yang menghubungkan demarcation dengan lokasi switch yang berada di lokasi Central Office terdekat.
4. Data Circuit Terminating Equipment (DCE), yaitu perangkat (dapat berupa perangkat tunggal atau berupa sistem) yang berfungsi untuk membagi akses jaringan publik kepada pelanggan.
5. Central Office, yaitu perangkat yang menghubungkan pelanggan ke jaringan switching milik provider. Central Office juga biasa di sebut dengan istilah Point Of Presents (POP).



Gambar 9 - 2 Komponen WAN

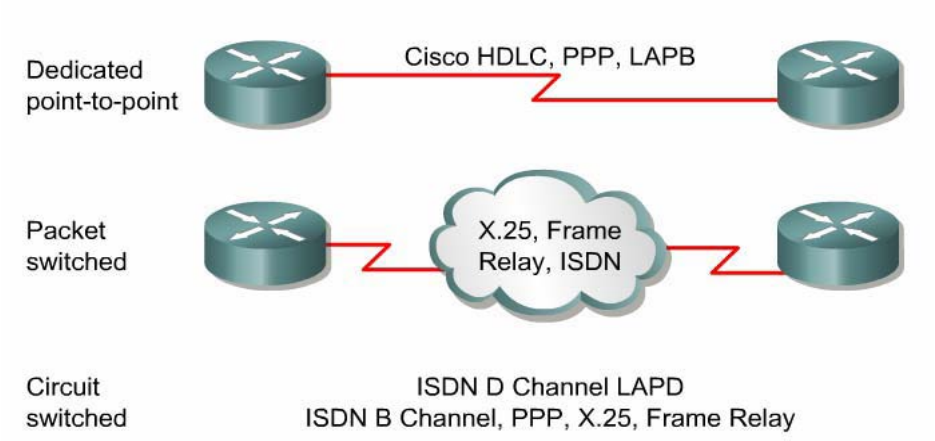
9.2. KONEKSI WIDE AREA NETWORK

Dalam membangun jaringan WAN, maka yang harus dibentuk pertama adalah membangun koneksi antar terminal yang berfungsi sebagai komponen WAN. Koneksi tersebut dibangun dengan memberikan pengaturan signaling, namun karena perangkat yang dihubungkan terpisah dalam jarak geografis yang relatif jauh, maka diperlukan suatu jaringan komunikasi data, yang selanjutnya dikenal dengan istilah teknologi WAN.

Teknologi WAN terdiri dari beberapa jenis koneksi, antara lain (Lihat gambar 9.2):

1. Leased Line (dedicated point – to-point)
2. Circuit Switched
3. Packet Switched

Sedangkan pada implementasinya dapat digunakan konsep Point to Point Protocol (PPP), Frame Relay dan Digital Subscriber Line (DSL).

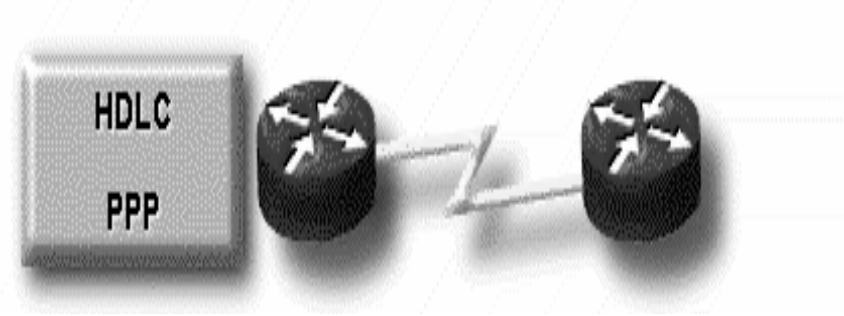


Gambar 9 - 3 Teknologi WAN

9.2.1. Dedicated Point to Point.

Merupakan link point to point atau koneksi dedicated. Koneksi ini tidak memerlukan proses call setup terlebih dahulu ketika hendak mengirimkan data antar DTE. Mekanisme pengiriman pada koneksi leased line dilakukan secara synchronous serial.

Koneksi ini dapat terjadi pada jaringan switching sederhana, jaringan yang dibangun mempunyai banyak koneksi secara fisik, namun untuk operasi dalam satu waktu hanya ada satu fungsi koneksi. Jalur untuk koneksi ini biasanya di-multiplexing-kan, baik dengan menggunakan teknik Frequency Division Multiplexing (FDM) maupun Time Division Multiplexing (TDM). Penerapan di lapangan diimplementasikan dengan menggunakan konsep HDLC dan PPP.

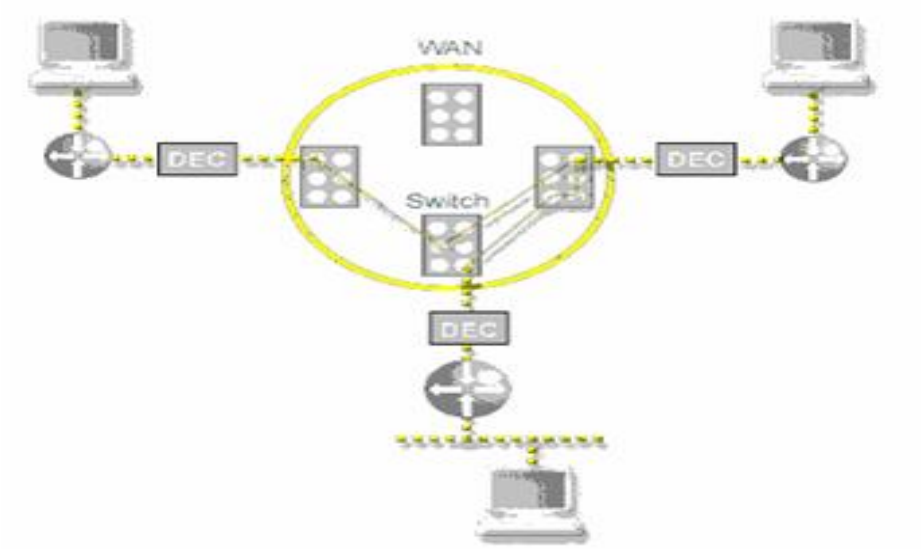


Gambar 9 - 4 Dedicated Point-to-Point link

9.2.2. Circuit Switching.

Pada teknik ini, sebelum pengiriman data dilakukan, terlebih dahulu harus dilakukan proses pembentukan koneksi dengan melakukan prosedur call setup.

PSTN dan ISDN merupakan sistem yang menerapkan koneksi circuit switching ini.

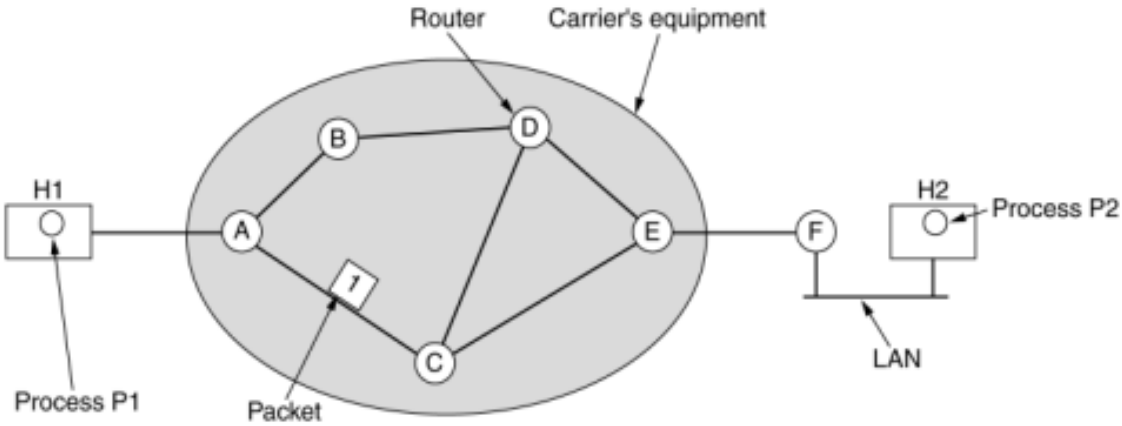


Gambar 9 - 5 Circuit Switch

9.2.3. Packet Switching.

Teknik ini adalah metode WAN switching yang mengijinkan user untuk membagi bandwidth dengan pengguna lain untuk menghemat biaya. Teknologi ini merupakan pengembangan dari teknologi Leased Line. Mekanisme pengiriman data di lakukan secara Synchrounous Serial.

Pada beberapa konsep, teknik ini dikenal dengan konsep *Store and Forward,* dengan teknis penyampaian data dari host pengirim ke host penerima akan dapat terjadi apabila terjadi hubungan antara keduanya baik secara langsung sesuai dengan urutan hop yang direncanakan dalam konsep routingnya, maupun secara tidak langsung dengan mengirimkan data ke tujuan melalui router lain sebagai perantaranya, yang jelas target penyampaian data pada host tujuan harus terjadi.



Gambar 9 - 6 Packet Switch

9.2 Protokol WAN

Infrastruktur untuk teknologi WAN dapat beroperasi dengan adanya Protokol WAN. Teknologi WAN akan dapat beroperasi disesuaikan dengan Protokol WAN yang cocok, perangkat yang membentuknya, dan spesifikasi perangkat dari vendornya.

Saat ini terdapat beberapa jenis protokol yang digunakan untuk menyediakan mekanisme pengiriman data melalui jaringan WAN. Diantaranya adalah:

1. Protokol HDLC (High Level Datalink Control)
2. PPP (Point to Point Protocol)
3. Protokol X.25 Protocol dan LAPB (Link Access Procedure Balanced)
4. Frame Relay
5. ISDN

Dalam fungsinya untuk mendukung internetworking, maka pengamatan terhadap kinerjanya akan berorientasi pada arsitektur komunikasi data baik OSI maupun TCP/IP. Hal ini terjadi karena setiap perangkat yang dipergunakan untuk komunikasi internetworking harus distandarisasi dibawah ISO melalui OSI, dan kinerjanya harus dapat mengikuti proses enkapsulasi/ dekapsulasi baik yang dianalisa melalui arsitektur OSI maupun TCP/IP.

9.2.1 Protokol HDLC (High Level Datalink Control)

HDLC merupakan sebuah protokol yang bekerja pada lapisan datalink. Pertama kali dibuat oleh ISO, merupakan sebuah protokol yang menetapkan metode enkapsulasi data pada koneksi fisik kabel serial dengan data rate 9600 bps. .HDLC biasa digunakan pada jenis koneksi leased line dan mekanisme autentikasi tidak harus digunakan.

HDLC merupakan enkapsulasi default dari sistem router Cisco. Akan tetapi HDLC yang digunakan oleh router Cisco adalah HDLC yang dibuat sendiri oleh Cisco. Hal ini dikarenakan HDLC yang dikeluarkan oleh ISO memiliki kelemahan, yaitu masih bersifat *single protocol*. Sedangkan HDLC yang dibuat oleh Cisco memiliki kemampuan *multiprotocol.* HDLC mampu mengenkapsulasi beberapa jenis data yang menggunakan *routed protocol (IP, IPX, dsb)* atau protokol layer 3 dan pengirimannya dilakukan secara simultan.

HDLC dapat diimplementasikan pada interface serial yang terdapat pada dedicated router dari vendor Cisco, dengan menggunakan perintah:

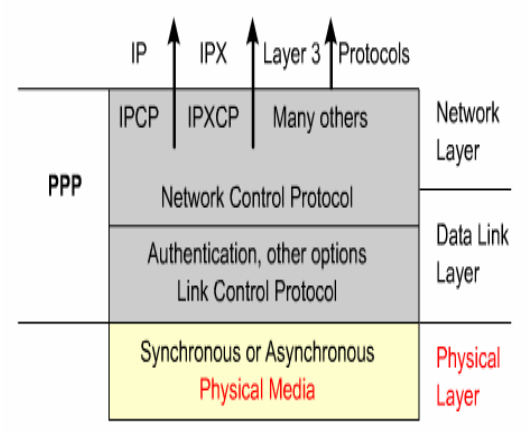
```
Router(config)    # int s0
Router(config-if) #encapsulation hdlc
```

Untuk memeriksa apakah HDLC sudah terpasang pada interface serial, dapat digunakan perintah **show interface serial0,** perhatikan bagian yang menerangkan adanya HDLC Encapsulation.

9.2.2 PPP (Point to Point Protocol)

PPP (Point to Point Protocol) merupakan protokol data link layer yang dapat digunakan pada media asynchrounous serial atau synchrounous serial. PPP pada dasarnya merupakan pengembangan dari protokol SLIP (Serial Line Interface Protocol), yaitu sebuah protokol standard point to point yang menggunakan protokol TCP/IP.

PPP memiliki kemampuan untuk melakukan proses autentikasi dan bersifat *multiprotocol*, sehingga menjadi solusi yang banyak digunakan untuk komunikasi WAN. Segmentasi protokolnya dapat dilihat pada gambar 9.4



Gambar 9 - 7 Fungsi Kerja PPP dari model Referensi

Pada gambar 9.4 terlihat untuk mendukung fungsi kerja PPP, maka terdapat dua lapisan yang terlibat, yaitu Lapisan Datalink dan Network.

Lapisan Physical bertugas untuk menyediakan media yang diperlukan untuk menghubungkan antar router baik dengan menggunakan Media Synchronous maupun Asiynchronous.

Lapisan Network bertugas memberikan layanan traffic menggunakan NCP (Network Control Protocol) dan memberikan layanan traffic secara logika dengan menggunakan protocol IP, IPX dan protocol layer 3 lainnya.

Lapisan Datalink yang mempunyai peranan dominan, terkait dengan beberapa komponen PPP, diantaranya :

1. HDLC merupakan sebuah metoda untuk melakukan enkapsulasi datagram melalui jalur serial.
2. LCP (Link Control Protocol) merupakan sebuah metoda dari penetapan, pemeliharaan dan pemutusan hubungan point to point.
3. NCP (Network Control Protocol) merupakan sebuah metoda dari pembentukan dan pengkonfigurasian protokol-protokol lapisan jaringan. PPP dirancang untuk melakukan pengiriman secara simultan melalui beberapa protokol jaringan.
   NCP digunakan untuk melakukan komunikasi dari beberapa protokol jaringan yang dienkapsulasi oleh PPP.

Protokol LCP memiliki beberapa kemampuan, diantaranya:

- Autentikasi. Untuk keamanan hubungan, PPP menyediakan kemampuan autentikasi.
- Compression, digunakan untuk meningkatkan kinerja proses pengiriman data. Stacker dan Predictor merupakan dua jenis protokol yang mendukung PPP dalam proses kompresi data.
- Error Detection. PPP menggunakan protokol Quality Magic untuk menjamin kehandalan data yang dikirim.
- Multilink, memecahkan data yang akan dikirim, kemudian dikirimkan melalui dua atau lebih jalur secara paralel dan sisi penerima melakukan proses penyusunan data.

Ketika koneksi hendak dibentuk oleh PPP, biasanya ada tiga fase yang biasa dilakukan yaitu:

1. Fase Pembentukan Jalur. Paket LCP dikirimkan oleh setiap device untuk mengkonfigurasi dan menguji jalur.
2. Fase Autentikasi (jika digunakan).
3. Fase Protokol lapisan jaringan. PPP menggunakan NCP untuk mengijinkan beberapa protokol layer network dienkapsulasi dan dikirimkan melalui sebuah PPP.

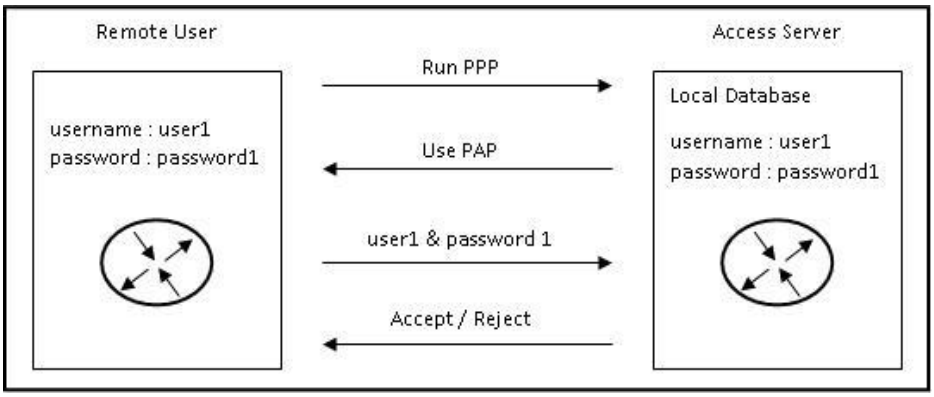
Ada dua metoda autentikasi yang disediakan oleh PPP yaitu:

1. PAP
2. CHAP

1. **Password Authentication Protocol (PAP)**

   Metode autentikasi ini kurang begitu aman dibanding metoda CHAP. Password dikirimkan dalam bentuk clear text.

Dalam metoda PAP, salah satu router (remote router) mengirimkan username dan password dalam bentuk clear text ke router lainnya (akses server). Handshake untuk pembentukan link PPP terjadi setelah hubungan router secara fisik terbangun, dilanjutkan dengan penentuan enkapsulasi PPP, diakhiri sampai enkapsulasi PPP disetujui dengan authetikasi yang telah ditentukan (PAP/CHAP). Proses ini diilustrasikan pada gambar 9.5.



Gambar 9 - 8 Handshake Password Authentication Protocol (PAP)

Kemudian router akses server akan mengautentikasi dan memutuskan apakah menerima hubungan tersebut atau menolaknya tergantung pada informasi username dan password yang terdapat di database lokal dengan username dan password yang diajukan oleh remote router.
Gambar 9.5 memperlihatkan implementasi penggunaan protokol PPP dengan menggunakan autentikasi PAP.

Implementasi PPP dengan autentikasi PAP dapat dilakukan dengan cara menghubungkan kedua router point to point-nya melalui jaringan PSTN/ISDN. Konfigurasi pada kedua router dapat dilakukan dengan:

Router 1:

```
Router(config) # hostname ROUTER1
Router(config)# username ROUTER2
                password DUA
Router(config) # interface serial0
Router(config-if) # encapsulation ppp
Router(config-if)# ppp authentication
                pap
Router(config-if) # ppp pap sent-
                username ROUTER1
                password SATU
```

Router 2:

```
Router(config) # hostname ROUTER2
Router(config) # username ROUTER1
                 password SATU
Router(config) # interface serial0
Router(config-if) # encapsulation ppp
Router(config-if) # ppp
                 authentication pap
Router(config-if) # ppp pap sent-
                 username ROUTER2
                 password DUA
```

Secara umum, konfigurasi PPP dengan menggunakan autentikasi PAP dapat dilakukan dengan beberapa perintah, yakni:

1. Menetapkan nama remote user yang berhubungan dengan router lokal, dengan perintah:

```
Router(config-if) # username
<remote user> password
<password koneksi>
```

2. Pemasangan jenis enkapsulasi PPP dengan perintah:

```
Router(config-if) # encapsulation ppp
```

3. Tentukan jenis autentikasi PAP, dengan perintah:

```
Router(config-if) # ppp authentication pap
```

4. Kirimkan nama user lokal dan password yang terdaftar di database router lain untuk melakukan proses autentikasi, dengan perintah:

```
Router(config-if) # ppp pap sent-
                 username local_user
                 password
                 password_koneksi
```

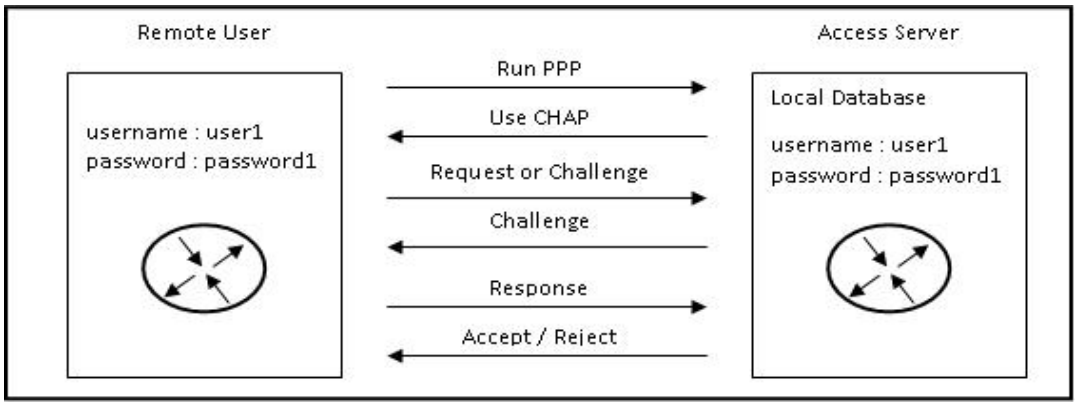
2. Challenge Authentication Protocol (CHAP)

Metoda autentikasi CHAP lebih aman dibandingkan PAP. Sebelum data dikirimkan terlebih dahulu dienkripsi. Gambar 9.6 memberi ilustrasi proses autentikasi dengan metode CHAP. Setelah hubungan PPP ditetapkan, akses server mengirimkan sebuah sinyal Challenge ke remote user.

Remote user merespon dengan memberikan username dan password yang telah dienkripsi dengan menggunakan metode MD5 (Message Digest 5).

Kemudian akses server menerima respon dari remote user dan membandingkan hasil enkripsi remote user dengan hasil enkripsi yang dimiliki akses server. Jika hasilnya sama, maka autentikasi diterima dan hubungan bisa dibentuk.

Implementasi PPP dengan autentikasi CHAP dapat dilakukan dengan cara menghubungkan kedua router point to point-nya melalui jarinngan PSTN/ISDN.



Gambar 9 - 9 Handshake PPP dengan CHAP

Konfigurasi pada kedua router

Router 1:

```
Router(config) # hostname ROUTER1
Router(config) # username ROUTER2
                password PASS
Router(config) # interface serial0
Router(config-if) # encapsulation ppp
Router(config-if) # ppp authentication chap
```

Router 2:

```
Router(config) # hostname ROUTER2
Router(config) # username ROUTER1
                password PASS
Router(config) # interface serial0
Router(config-if) # encapsulation ppp
Router(config-if) # ppp authentication chap
Router(config-if) # ppp chap hostname
                ROUTER2
Router(config-if) # ppp chap password PASS
```

Secara umum, konfigurasi PPP dengan menggunakan autentikasi CHAP dapat dilakukan dengan menggunakan perintah-perintah berikut:

1. Menetapkan nama remote user yang dapat berhubungan dengan router lokal. Caranya dengan menggunakan perintah:

```
Router(config) # username <remote user>
password <password koneksi>
```

2. Pemasangan jenis enkapsulasi PPP dengan menggunakan perintah:

```
Router(config-if) # encapsulation ppp
```

3. Menentukan jenis autentikasi CHAP, dengan perintah:

```
Router(config-if) # ppp authentication pap
```

4. Pada salah satu router, tentukan username dan password

koneksinya, dengan menggunakan cara mengirimkan nama user lokal dan password yang terdaftar di database router lain untuk melakukan proses autentikasi, dengan menggunakan perintah:

```
Router(config-if) # ppp chap hostname
                    local_router
Router(config-if) # ppp chap password
                    password_koneksi
```

Konfigurasi PPP yang telah kita lakukan dapat diverifikasi dengan menggunakan perintah-perintah berikut:

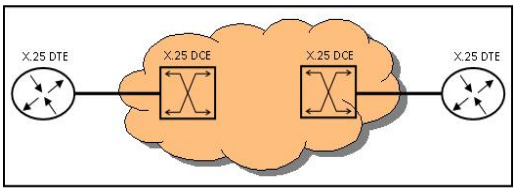
- **show running-config**, menampilkan perintah-perintah yang kita gunakan untuk konfigurasi PPP.

- **show interface serial,** memastikan apakah enkapsulasi PPP sudah terpasang pada interface serial. Perhatikan bagian yang menyebutkan ***Encapsulation ppp.***

9.2.3 Protokol X.25 dan LAPB (Link Access Procedure Balanced)

Pendekatan tradisional packet switching memungkinkan penggunaan X.25 yang tidak hanya menentukan interface user dari jaringan WAN, akan tetapi juga mempengaruhi desain internal jaringan, dengan beberapa pendekatan:

- Packet-packet control panggilan, yang diperlukan untuk mensetup dan membubarkan sirkuit virtual, dibawa pada channel yang sama pada sirkuit virtual yang sama sebagai paket data. Akibatnya, diperlukan pensinyalan *inband*.
- Multiplexing sirkuit virtual menempati layer 3 model komunikasi OSI.
- Baik layer 2 maupun layer 3 mencakup mekanisme kendali aliran dan koreksi kesalahan.



Gambar 9 - 10 Link X.25

X.25 merupakan sebuah protokol standar yang mendefinisikan hubungan antara sebuah terminal dengan jaringan packet switching. X.25 didesain untuk dapat melakukan pengiriman dan penerimaan data melalui jalur analog. Protokol X.25 beroperasi pada layer network, sedangkan layer datalink dikelola oleh protokol LAPB (Link Access Procedure Balanced) yang menyediakan kehandalan dan mekanisme *sliding windows.*

DTE dan DCE pada X.25 mengidentifikasi tanggung jawab dari dua station yang terpasang pada jaringan X.25. Protokol X.25 mengimplementasikan virtual circuit diantara X.25 DTE dan X.25 DCE. X.25 DTE biasanya berupa router, sedangkan X.25 DCE biasanya bertindak sebagai fungsi pembatas ke jaringan data publik dengan sebuah switch/concentrator. Jenis virtual circuit yang disediakan oleh X.25 ada dua jenis yaitu SVC (Switched Virtual Circuit) dan PVC (Permanent Virtual Circuit).

Bentuk pengalamatan dari X.25 didefinisikan oleh ITU-T yang dikenal dengan pengalamatan X.121, yang terdiri dari:
- 4 digit pertama menetapkan DNIC (Data Network Identification Code).
- Maksimal 10 atau 11 digit menetapkan NTN (Network Terminal Number).

Implementasi penggunaan protokol X.25 pada jaringan SVC Switched Virtual Circuit) di router dapat dilakukan dengan cara:
1. Mendefinisikan jenis enkapsulasi (default: DTE):

```
Router(config-if) # encapsulation x25 [
                    dce | dte ]
```

2. Menetapkan alamat x.121:

```
Router(config-if) # x25 address x.121-
                    address
```

3. Memetakan alamat network layer protocol (mis, IP, IPX) dengan alamat x.121

```
Router(config-if) # x25 map protocol
                    address x.121-address
```

Implementasi penggunaan protokol X.25 pada jaringan PVC (Permanent Virtual Circuit) di router dapat dilakukan dengan cara:
1. Mendefinisikan jenis enkapsulasi (default: DTE):

```
Router(config-if) # encapsulation x25 [dce
                    | dte ]
```

2. Menetapkan alamat x.121:

```
Router(config-if) # x25 address x.121-
                    address
```

3. Memetakan alamat network layer protocol (mis, IP, IPX) dengan alamat x.121:

```
Router(config-if) # x25 pvc
                    circuit_number protocol
                    address x.121-address
```

Konfigurasi X.25 yang telah dilakukan dapat diverifikasi dengan menggunakan perintah-perintah:
- **show running-config**, menampilkan perintah-perintah yang telah digunakan untuk mnenerapkan konfigurasi X.25
- **show interface-serial**, memastikan apakah enkapsulasi X.25 sudah terpasang pada interface serial.

9.2.4 Frame Relay

Jaringan Frame Relay dirancang untuk dapat menampilkan kualitas koneksi yang lebih efektif dibandingkan dengan X.25. Protokol Frame Relay mendefinisikan proses pengiriman data melalui sebuah jaringan data publik, dengan sifat koneksi yang connection oriented.

Overhead (header) yang diberikan oleh encapsulasi Frame relay mempunyai kapasitas yang lebih kecil dibanding dengan header dari encapsulasi X.25, hal ini akan menyebabkan kualitas koneksi Frame relay dinilai lebih baik

Frame Relay mempunyai kelemahan yaitu berkurangnya kemampuan flow control dan error correction antar jalur router – link frame relay, akan tetapi kemampuan ini tersedia pada lapisan diatasnya.

Frame relay mempunyai kelebihan, yaitu dapat menyediakan proses komunikasi yang ringan. Fungsi protokol yang diperlukan pada interface pemakai jaringan menjadi berkurang saat terjadi proses encapsulasi frame relay, akibatnya delay lebih rendah dan laju penyelesaian komunikasi yang lebih tinggi dapat terjadi.

Rekomendasi ITU-T I.233 menunjukkan bahwa Frame Relay dapat digunakan pada akses dengan kecepatan sampai 2Mbps.

Sama halnya dengan X.25, Frame Relay memiliki kemampuan membentuk beberapa Virtual Circuit melalui sebuah jalur pengiriman dengan memasangkan identitas koneksi ke setiap pasang device DTE yang terhubung. Teknik pemberian identifikasi ini dikenal dengan istilah DLCI (Datalink Connection Identifier).

Ketika device switch pada service provider menerima frame dari DTE melalui LMI (Local Management Inteface), maka switch akan menganalisis DLCI dan mengirim frame ke port yang sebelumnya telah ditetapkan. LMI adalah signaling yang terpasang antara CPE (DTE) dengan Switch Frame Relay, Identitas DLCI yang memetakan pengenal koneksi tiap interface akan disimpan pada table yang dibentuk oleh switch frame relay pada service provider. Nomor ini selanjutnya akan dipetakan secara statis maupun dinamis dengan alamat network layer dengan menggunakan protokol IARP (Inverse Address Resolution Protocol).

Berikut ini akan diuraikan contoh konfigurasi frame relay pada beberapa perangkat router. Device dedicated router yang diproduksi oleh vendor Cisco dapat mendukung tiga jenis LMI, yaitu:

- Cisco
- Ansi
- Q933a

Konfigurasi Frame Relay pada jaringan router Cisco dapat dilakukan dengan cara:

1. Tentukan interface yang akan dihubungkan dengan frame relay
2. Berikan konfigurasi alamat network layer (IP Address)
3. Pilih jenis enkapsulasi yang akan digunakan:

```
Router(config-if) # encapsulation frame
                    relay [cisco | ietf]
```

*) Catatan:

- Enkapsulasi Frame Relay **Cisco** merupakan nilai default. Dipilih, jika pasangan komunikasinya menggunakan Router Cisco
- Enkapsulasi Frame Relay ietf dipilih jika pasangan komunikasinya router non-Cisco.

4. Tentukan jenis LMI yang digunakan:

```
Router(config-if) # frame-relay lmi-type
                    [cisco | ansi | a933a]
```

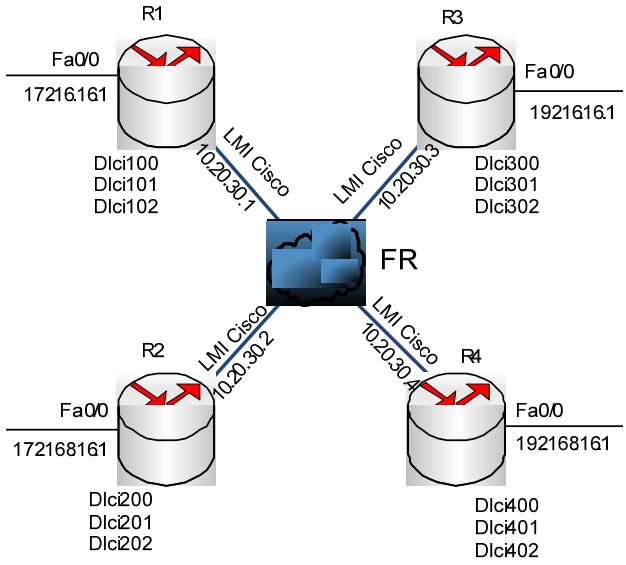
5. Menetapkan nomor DLCI yang digunakan :

Router(config-if) # frame-relay interface-dlci [*number-dlci]*

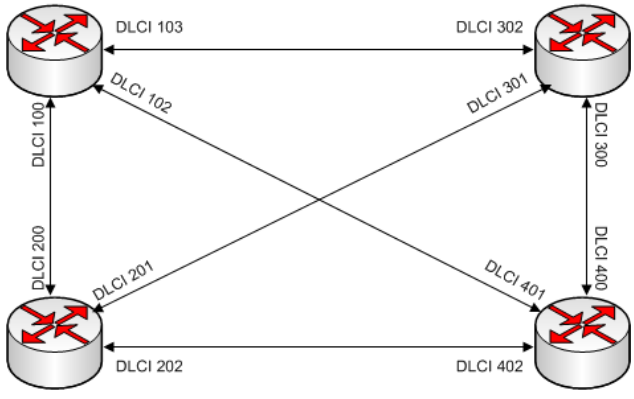
Router(config-if) # frame-relay map [*ip address dlci number broadcast]*

6. Konfigurasi pemetaan alamat jika hendak menggunakan cara pemetaan statis, maka digunakan perintah:

Sebagai ilustrasi implementasi Frame Relay, diperlihatkan pada gambar 9.8.



(a)



(b)

Gambar 9 - 11 Link Frame Relay

(a) Topologi implementasi Frame Relay, (b) Konfigurasi DLCI

Gambar 9.8 (a) memperlihatkan topologi implementasi Frame Relay yang terdiri atas empat buah router yang tergabung dalam satu awan frame relay.

Gambar 9.8 (b) menunjukkan konfigurasi DLCI untuk keperluan pengalamatan Frame Relay pada setiap router.

Untuk membangun topologi sesuai gambar 9.8, maka yang harus dilakukan pada setiap router adalah :

1. Konfigurasi network pada interface yang digunakan untuk frame relay.
2. Set Clock rate, disesuaikan dengan media yang digunakan. Apabila digunakan serial, clock rate dapat di set 4800.
3. Set encapsulation frame relay, untuk memfungsikan frame relay sebagai enkapsulasi lapisan datalink nya.
4. Set DLCI Number untuk masing-masing jalur, disesuaikan dengan perencanaan.

Contoh untuk konfigurasi pada R1, dapat digunakan sintaks seagai berikut :

```
Router(config)#hostname R1
R1(config)#int s2/0
R1(config-if)#ip address 10.20.30.1
            255.255.255.0
R1(config-if)#clock rate 4800
R1(config-if)#encapsulation frame-relay
R1(config-if)# frame-relay interface-dlci
            100
R1(config-if)# frame-relay interface-dlci
            101
R1(config-if)# frame-relay interface-dlci
            102
R1(config-if)#no shutdown
```

Konfigurasi untuk Router 2, 3 dan 4 dapat disesuaikan dengan topologi, dan urutan sesuai konfigurasi router 1 diatas.

Konfigurasi Frame Relay yang telah dilakukan dapat diverifikasi dengan menggunakan perintah:

- **Show frame-relay pvc,** menampilkan statistic trafic data pada virtual circuit. Responnya perhatikan statistik interface yang digunakan untuk frame relay (DLCI, DLCI Usage, PVC Status dan jenis interface yang digunakan).
- **Show interface serial,** memastikan enkapsulasi Frame relay sudah terpasang atau belum. Responnya perhatikan baris yang menyatakan "Encapsulation FRAME-RELAY"
- **Show running-config**, menampilkan perintah-perintah yang telah digunakan untuk menerapkan konfigurasi frame relay. Responnya perhatikan bagian yang menyebutkan:
  - encapsulation frame-relay
  - frame relay lmi-type [ ]
  - frame-relay interface-dlci [ ]
- **Show frame-relay map**, menampilkan pemetaan antara DLCI number dan alamat network layer. Responnya perhatikan angka yang menunjukkan alamat DLCI dan alamat network layer / ip address, dan metode penetapan nomor DLCI-nya (static/dynamic).

Jaringan Frame Relay memiliki sifat NBMA (*Non Broadcast Multi Access*). Jaringan frame relay yang menerapkan pemasangan beberapa PVC terhadap sebuah interface di router akan menimbulkan masalah

dengan aturan *split horizon*. Akan tetapi masalah tersebut dapat diatasi dengan cara:

1. Me-non-aktifkan aturan *split horizon*. Hanya saja jika cara ini dilakukan, maka akan menimbulkan masalah baru yaitu terjadi routing loop jika terjadi perubahan topologi.
2. Membentuk sub interface. Sebuah interface dibentuk seolah-olah terdiri dari beberapa interface secara logika (virtual), dalam beberapa implementasi dikenal dengan istilah aliasing. Cara ini merupakan cara yang paling efektif untuk menangani masalah *split horizon* yang terjadi pada jaringan NBMA, khususnya frame relay.

Langkah untuk membentuk sub interface pada sebuah interface:

1. Tentukan interface yang akan dibentuk menjadi sub interface
2. Hilangkan network layer address yang ada, apabila telah memiliki alamat, maka frame tidak akan diterima oleh subinterface.

```
Router(config-if) # no ip address
```

3. Konfigurasikan enkapsulasi frame relay

4. Pilih sub interface yang akan dikonfigurasi:

```
Router(config-if) # interface serial
                    nomor-port.nomor-
                    subinterface
```

Contoh konfigurasi untuk implementasinya dapat di lihat pada kotak perintah disamping:

```
Router(config) # interface serial0
Router(config-if) # no ip address
Router(config-if) # encap frame-relay
Router(config-if) # int s0.2 point-to-point
Router(config-subif) # ip address
                    192.168.100.1
                    255.255.255.0
Router(config-subif) #  frame-relay
                    interface-dlci 100
Router(config-if) # int s0.3 multipoint
Router(config-subif) # ip address
                    192.168.200.1
                    255.255.255.0
Router(config-subif) #  frame-relay
                    interface-dlci 200
Router(config-subif) #  frame-relay
                    interface-dlci 300
```

Dalam implementasinya, jaringan Frame Relay dapat menggunakan topologi:

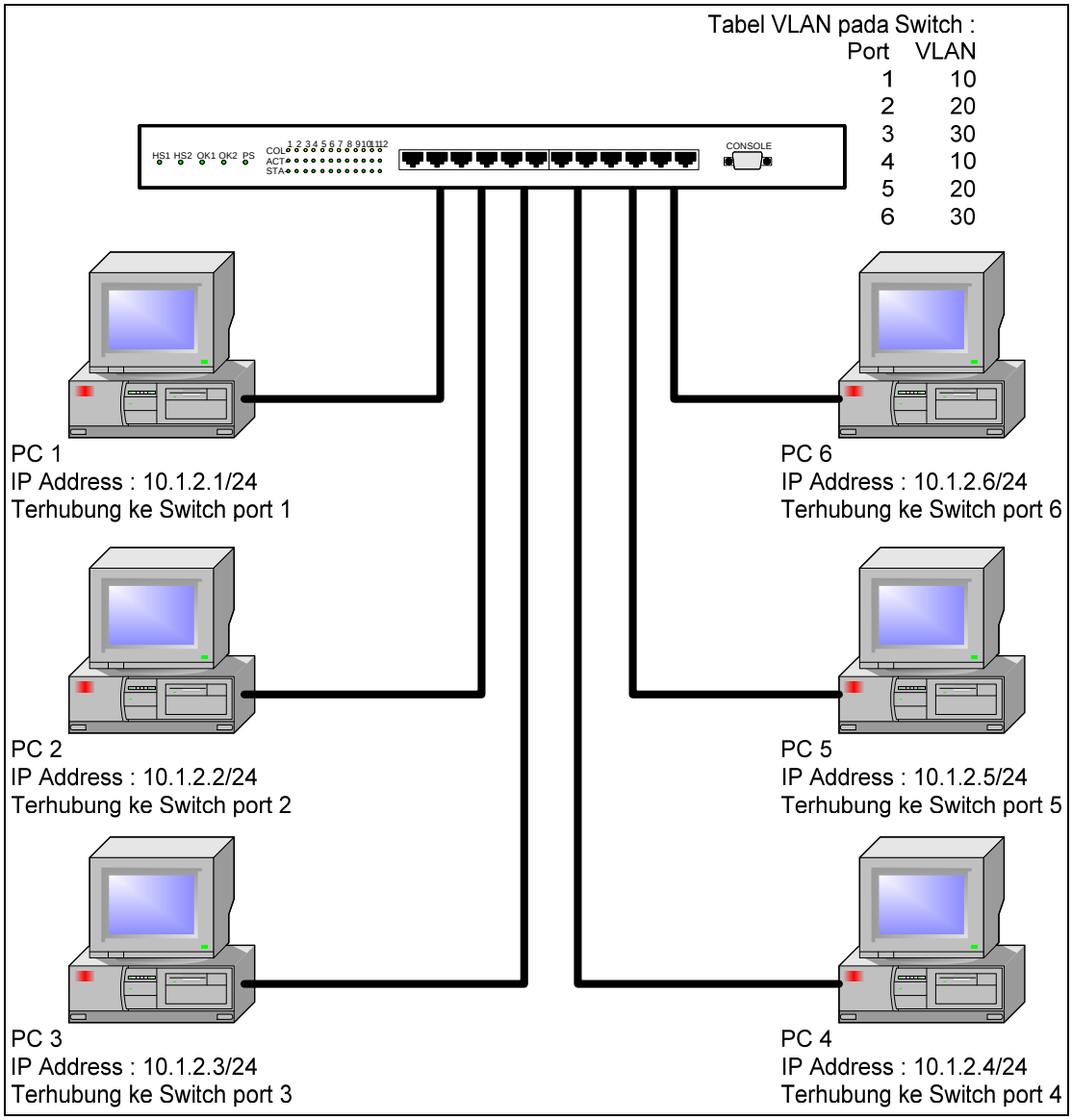
- Star
- Full Mesh
- Partial Mesh

9.3 Virtual LAN (VLAN)

Virtual LAN (VLAN) adalah sebuah konsep yang menggabungkan beberapa broadcast domain menjadi satu collision domain. Penerapan

konfigurasi Virtual LAN (VLAN) dapat dilakukan pada Manageable Switch.

Port diberikan identitas VLAN ID untuk komunikasi dengan port yang lainnya. Port dengan VLAN ID yang sama dikatakan berada dalam satu broadcast domain. Sebaliknya apabila antar port berbeda identitas VLAN ID-nya maka berbeda pula broadcast domainnya (tidak dapat saling berkomunikasi), walaupun berada pada fisik manageable switch yang sama dan host yang terhubung pada port tersebut mempunyai identitas Network Address yang sama pula.



Gambar 9 - 12 Implementasi VLAN

Secara default, dari vendor semua port pada manageable switch tergabung dalam satu VLAN ID, sehingga sebelum diberikan konfigurasi VLAN ID untuk masing-masing port, maka masing-masing host yang terhubung pada masing-masing port secara otomatis dapat berkomunikasi sampai konfigurasi VLAN diberikan.

Gambar 9.9 memperlihatkan implementasi VLAN pada suau manageable switch yang dengannya terhubung enam PC dari network yang sama, akan tetapi berbeda kelompok VLAN.

Sebelum implementasi VLAN, semua PC dapat saling terkoneksi karena semuanya tergabung dalam network 10.10.10.0/24, namun setelah implmentasi VLAN dengan tiga kelompok VLAN (Vlan 10,20 dan 30), maka hanya PC yang sama VLAN ID nya saja yang dapat saling berkomunikasi.

PC 1 yang terkoneksi ke port 1 hanya dapat berkomunikasi dengan PC 4 yang terkoneksi ke port 4, karena keduanya sama-sama menggunakan VLAN ID 10.

PC 2 yang terkoneksi ke port 2 hanya dapat berkomunikasi dengan PC 5 yang terkoneksi ke port 5, karena keduanya sama-sama menggunakan VLAN ID 20.

PC 3 yang terkoneksi ke port 3 hanya dapat berkomunikasi dengan PC 6 yang terkoneksi ke port 6, karena keduanya sama-sama menggunakan VLAN ID 30.

Dengan implementasi ini, terlihat bahwa VLAN dapat membatasi koneksi antar host yang secara network (broadcast domain) terdapat dalam satu kelompok, namun berbeda kelompok collision domain (VLAN Group).

9.4 Virtual Private Networks (VPN)

Virtual Private Networks (VPN) merupakan solusi untuk membuat koneksi LAN melalui internetwork. Penerapan konfigurasinya dilakukan pada router yang keduanya terhubung pada internetwork dengan menggunakan protokol yang sama untuk keperluan VPN. Pada beberapa aplikasi komunikasi, metoda ini dikenal dengan istilah *Tunneling*.

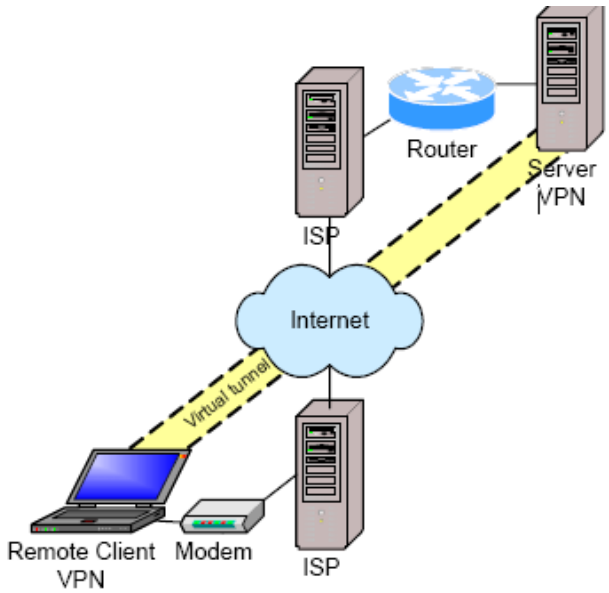
Untuk membuat link point to point antar router yang melakukan koneksi dengan memanfaatkan *Virtual Private Networks (VPN)* diperlukan satu alamat jaringan.

VPN berfungsi untuk mengijinkan dua jaringan atau komputer untuk berkomunikasi satu sama lain melalui suatu media yang relatif tidak menjamin/aman. Dalam banyak implementasi, media yang menghubungkannya adalah internet.

Gambar 9.10 memperlihatkan dua host (Server VPN dan Remote Klien VPN) terhubung ke Internet melalui Gateway/ISP masing-masing. Karena keduanya terhubung ke internet, maka antara keduanya dapat saling berkomunikasi, hanya saja untuk melakukan komunikasinya harus ditempuh dengan melalui banyak lompatan/hop routing, dikarenakan melalui banyak router dari masing-masing ISP,

Dengan implementasi VPN, maka jumlah lompatan/hop routing dapat disederhanakan, dimana antara pasangan VPN (Server dan klien) hanya terhubung dengan satu lompatan/hop routing saja, selain itu

juga dengan implementasi VPN, data yang di kirim-terima kan akan relatif lebih aman, dengan diterapkannya encryption/key management didalamnya.



Gambar 9 - 13 Implementasi VPN

9.4.1 Protokol Tunneling VPN

Ada beberapa protokol *tunneling* yang dapat digunakan pada VPN, diantaranya:

- L2F – Protokol Forwarding pada Layer 2. Bekerja pada link layer OSI model dan tidak memiliki encryption. Selanjutnya peranan protokol ini digantikan oleh L2TP.
- PPTP - *Point-to-Point Tunneling Protocol* (RFC 2637) bekerja pada link layer, tidak memiliki encryption /key management didalamnya.
- L2TP – *Layer 2 Tunneling Protocol*. (RFC 2661), menggabungkan L2F and PPTP dan bekerja pada link layer, tidak memiliki encryption/key management didalamnya.
- IPSec - *Internet protocol security*, dikembangkan oleh IETF, diimplementasikan pada layer 3. Merupakan kumpulan satuan keamanan berupa pengalamatan untuk kemanan data, integrity, authentication, dan key management, dalam penggunaan-nya untuk tunneling, tidak diterapkan key management.
- Socks – diterapkan pada application layer

9.4.2 Keamanan VPN

Dalam implementasi tunneling, VPN memerlukan keamanan baik yang berupa *authentification, confidentiality, data integrity* maupun

key management, untuk mengamankan data yang dikirimkan melintasi media transmisi publik. Proses pengamanannya meliputi:

- Authentication, untuk menjamin data terkirim dari pengirim ke penerima yang dikehendaki.
- Confidentiality, mengamankan data dari penyadapan pihak ketiga.
- Data integrity, memastikan data tidak mengalami perubahan oleh pihak lain sebelum tiba di tujuan.
- Access control, mengamankan data dari campur tangan pihak yang tidak diberikan hak akses.

Dalam penanganan user terkait dengan key management atau sistem autentikasinya maka dapat diterapkan dua protokol key management, yaitu:

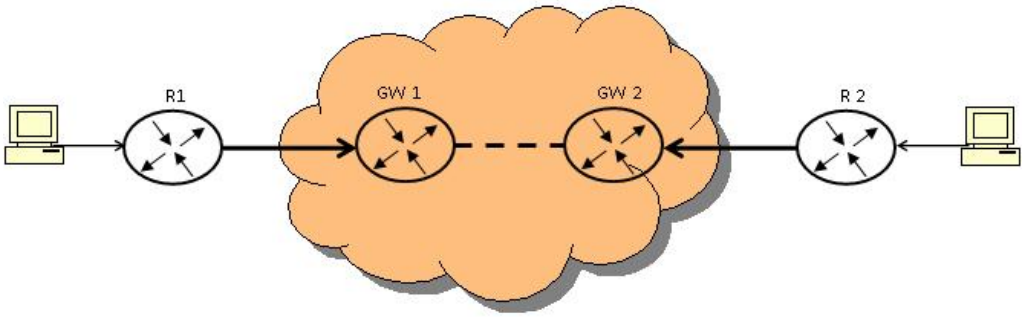
1. Radius (Remote Authentication Dial-In User Service), menggunakan PPTP atau L2TP Tunnelling.
2. ISAKMP/Oakley

.

9.4.3 Membangun VPN

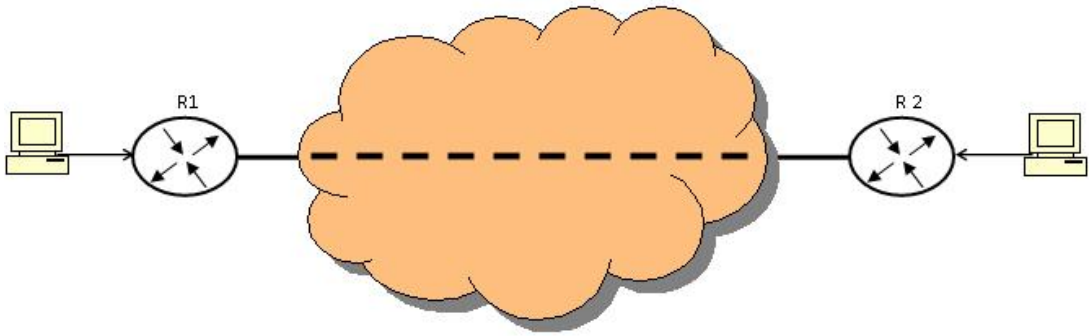
Untuk membangun link VPN berikut beberapa hal yang harus dilakukan :

1. Membuat topologi perencanaan VPN
   - Gambar 9.11 menunjukan Topologi awal sebelum implementasi VPN.



Gambar 9 - 14 Topologi Sebelum Implementasi VPN

- Topologi setelah implementasi VPN



Gambar 9 - 15 Topologi Sesudah Implementasi VPN

2. Membangun PC Router dengan menggunakan sistem operasi jaringan tertentu (dalam implementasi ini akan digunakan s\istem operasi Linux)
   - Mempersiapkan PC untuk Router dengan memasang dua buah network interface card.
   - Instalasi sistem operasi jaringan dilengkapi dengan fungsi IP Forwarding.
   - Instalasi/aktivasi kernel untuk keperluan penambahan device virtual/VPN. (untuk linux dapat diaktivasi device GIF).
   - Memberi Konfigurasi Network (IP Address dan Routing) pada kedua network interface card sesuai dengan networknya (Local dan Internet Gateway).

Router 1:

```
# ifconfig eth0 192.168.100.2
  netmask 255.255.255.0
# ifconfig eth1 202.10.20.2 netmask
  255.255.255.240
# route add default gw 202.10.20.1
```

Router 2:

```
# ifconfig eth0 192.168.200.2
    netmask 255.255.255.0
# ifconfig eth1 202.100.200.2
    netmask 255.255.255.240
# route add default gw
    202.100.200.1
```

Mengkonfigurasi alamat *tunneling* pada device GIF, dengan membuat virtual link.

Pada Router 1:

```
# ifconfig gif0 create
# ifconfig gif0 tunnel 202.10.20.2
    202.100.200.2
# ifconfig gif0 inet 192.168.100.1
    192.168.100.2 netmask 0xffffffff
```

Pada Router 2:

```
# ifconfig gif0 create
# ifconfig gif0 tunnel 202.100.200.2
    202.10.20.2
# ifconfig gif0 inet 192.168.100.2
    192.168.100.1 netmask 0xffffffff
```

Untuk melakukan verifikasi terhadap konfigurasi yang telah diberikan, dapat di cek dengan menggunakan perintah:

```
# ifconfig gif0
```

Konfigurasi *tunneling* berhasil apabila respon nya:

```
# ifconfig gif0
gif0: flags=8051<UP,POINTOPOINT,
        RUNNING,MULTICAST> mtu
        1280 tunnel inet 202.10.20.2  -->
        202.100.200.2
inet 192.168.100.1 --> 192.168.100.2
        netmask 0xffffffff
```

Selanjutnya pada table routing terdapat opsi routing tambahan berupa penambahan routing static ke remote network melalui interface Tunnel:

```
# netstat -rn
Routing tables
Destination     Gateway       Flags  Use   Netif  Expire
192.168.2.1     192.168.1.1   UH     0     gif0   ...
```

Untuk melewatkan koneksi antar network, maka antar router tersebut harus ditambahkan opsi routing dengan destination remote network melalui ip address *tunneling* pada remote router.

Pada Router 1:

```
# route add –net 20.20.20.0/24
192.168.100.2
```

Pada Router 2:

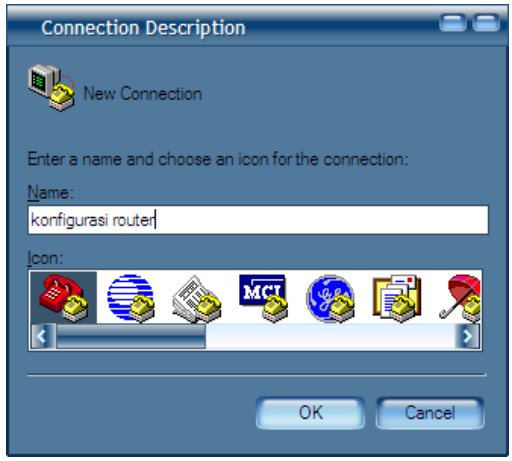
```
# route add –net 10.10.10.0/24
192.168.100.1
```

3. Pengujian dapat dilakukan dengan menggunakan tools monitoring network (*ping* dan *traceroute*). Dengan menggunakan tools *ping*, yakinkan koneksi antara kedua network tersebut sudah terbangun. Dengan menggunakan *traceroute*, yakinkan hop yang dilalui oleh paket data dari local network ke remote network hanya satu hop, yaitu setelah melalui local router selanjutnya packet data langsung disampaikan ke remote router melalui interface *tunnel*.

9.5 Membangun Koneksi.

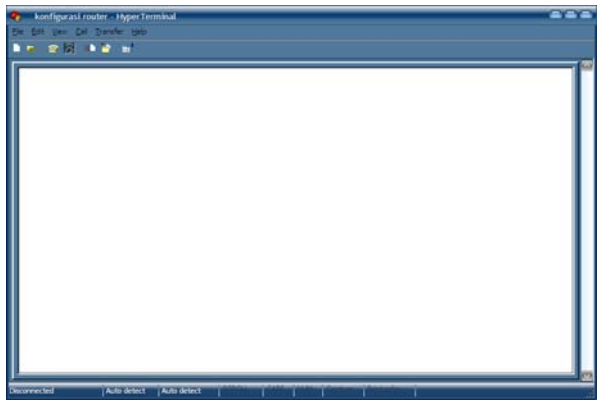
Melakukan kinfogurasi kepada suatu manageable switch atau dedicated router dapat dilakukan dengan beberapa cara, diantaranya:

1. Melalui koneksi hyper terminal (console), dilakukan dengan akses hyper terminal dari program, setelah sebelumnya dibuat koneksi antara host (serial port) dengan switch/router pada port console.



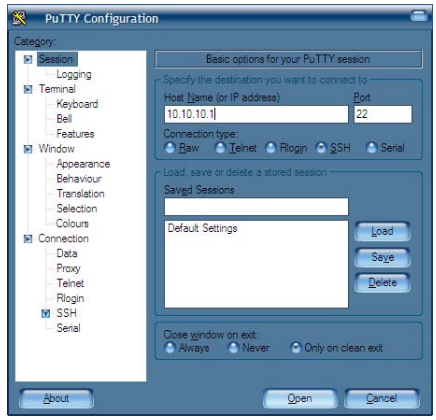
Gambar 9 - 16 Tampilan Awal Konfigurasi Hyper Terminal

- Isi nama koneksi dan pilih salah satu icon koneksi untuk pembuatan shortcut.
- Selanjutnya tentukan port yang digunakan untuk koneksi dan bit rate.
- Selanjutnya apabila berhasil, maka hyper terminal akan menghantarkan kita ke terminal pada remote terminal. Masukan *user – password* untuk aksesnya.
  Untuk sistem tanpa password, maka dapat diberikan eksekusi ”enter” sebagai pengantarnya.

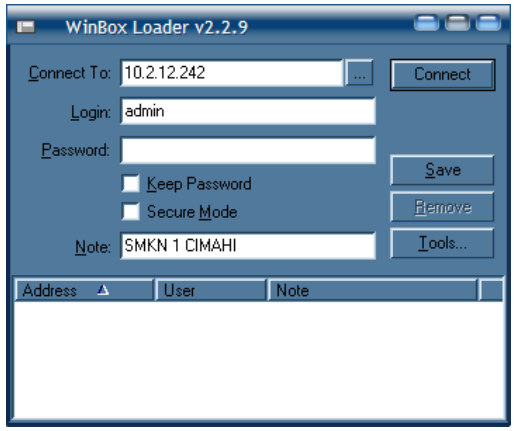


Gambar 9 - 17 Tampilan Remote Terminal Melalui Hyper Terminal

2. Web Base, dengan memanfaatkan protokol http sebagai interface-nya, dilakukan dengan terlebih dahulu menghubungkan host dengan remote host (manageable switch/ dedicated router) yang akan di konfigurasikan, baik dengan melalui network atau secara langsung. Satu syarat yang harus di penuhi adalah alamat yang akan ditempatkan pada address bar browser harus diketahui, dan meyakinkan koneksi antar host tersebut.
3. Remote Terminal, bisa menggunakan Telnet, SSH, winbox, rlogin atau tools remote terminal lainnya. Telnet atau SSH dapat dilakukan melalui software, salah satunya adalah *putty*.



Gambar 9 - 18 Software Putty untuk remote login



Gambar 9 - 19 Winbox Loader untuk Remote Terminal

Atau dapat pula digunakan software winbox tampilannya seprti ditunjukan pada gambar 9.16.

Selain dari dua software diatas masih banyak software remote terminal yang dapat digunakan untuk melakukan pengkonfigurasian suatu host tertentu.

9.6 Diagnosa Permasalahan WAN

Dalam komunikasi jaringan komputer, khususnya Wide Area Network, perlu dilakukan proses monitoring jaringan. Hal ini dimaksudkan agar seorang penanggung jawab jaringan/ autonomous system (AS), biasanya seorang network administrator, dapat melakukan pemantauan terhadap interkoneksi autonomous system yang menjadi tanggung jawabnya.

Dalam hal diagnosa permasalahan WAN, fokus yang harus diperhatikan adalah analisa kinerja jaringan (trafic) yang dapat dilakukan pada software dengan memanfaatkan protokol SNMP dengan memperhatikan dua parameter, yaitu parameter Layanan dan parameter Efisiensi.

Disamping itu hal yang harus diperhatikan adalah *load balancing*

dengan memanfaatkan QoS (Quality of Service).

Analisa kinerja jaringan didefinisikan sebagai suatu proses untuk menentukan hubungan antara 3 konsep utama, yaitu sumber daya (resources), penundaan (delay) dan daya-kerja (throughput).

Obyektif analisa kinerja mencakup analisa sumber daya dan analisa daya kerja. Nilai keduanya ini kemudian digabung untuk dapat menentukan kinerja yang masih dapat ditangani oleh sistem.

Analisa kinerja pada jaringan komputer membicarakan sifat dasar dan karakteristik aliran data, yaitu efisiensi daya-kerja, penundaan dan parameter lainnya yang diukur untuk dapat mengetahui bagaimana suatu pesan diproses di jaringan dan dikirim lengkap sesuai fungsinya.

Analisa Kinerja jaringan komputer dapat didefinisikan sebagai penelitian kuantitatif yang terus menerus terhadap suatu jaringan komunikasi dalam urutan kerja yang tetap berada dalam fungsinya (Terplan, 1987) agar hal-hal berikut dapat terpenuhi, yaitu:

- Dapat menyempurnakan level layanan pemeliharaan.
- Dapat mengenali potensi kemacetan.
- Dapat mendukung pengendalian operasional jaringan, administrasi dan merencanakan kapasitas.

Administrasi jaringan membantu langkah analisa kinerja dalam usaha mengevaluasi kemampuan layanan pada konfigurasi tertentu, selanjutnya akan mendefinisikan indikator kinerja yang penting, merekomendasikan prosedur pelaporan kinerja dan menentukan antarmuka manajemen basis data.

Kriteria penting dari sudut pandang pemakai jaringan adalah **keandalan**, yaitu kriteria pengukuran seberapa mudah suatu sistem terkena gangguan, terjadi kegagalan atau beroperasi secara tidak benar.

Keandalan adalah ukuran statistik kualitas komponen dengan menggunakan strategfi pemeliharaan, kuantitas redudansi, perluasan jaringan secara geometris dan kecenderungan statis dalam merasakan sesuatu secara tidak lenagusng tentang bagaimana suatu paket ditansmisikan oleh sistem tersebut.

Kinerja jaringan dapat diukur berdasarkan kriteria Terplan (1987):

1. Kriteria level pemakai (user level), yaitu waktu respon dan keandalan.
   - Waktu respon yaitu waktu tanggapan saat paket dipancarkan dengan benar.
   - Keandalan yaitu suatu keadaan yang dapat menentukan seberapa berfungsinya sistem pada suatu tugas pengiriman paket.

2. Kriteria level jaringan (network Level), yaitu waktu respon rata-rata. Penentuan waktu respon rata-rata dilakukan dengan 2 langkah, yaitu:
   - Menentukan rata-rata penundaan satu jalur paket melewati jaringan dan antar mukanya sebagai suatu fungsi beban terhadap ukuran paket.
   - Menggunakan informasi dengan penundaan dan pemakaian link untuk menghitung waktu respon rata-rata pemakai.

3. Kriteria kinerja khusus, yaitu daya kerja dan penundaan rata-rata.

9.7 Perbaikan/Setting Ulang WAN

Perbaikan terhadap kerusakan pada bagian jaringan harus secepatnya dilakukan,. Hal termudah yang dilakukan adalah melakukan *restore* terhadap *sistem backup* yang telah disimpan sebelumnya. Akan tetapi proses back up sistem sering terlewatkan oleh pengelola jaringan komputer, sehingga ketika terjadi gangguan pada jaringan maka perbaikannya menjadi sulit.

Satu hal yang harus di perhatikan ketika dilakukan setting ulang adalah **down time**. Ketika dilakukan perbaikan / setting ulang jaringan, user mendapat banyak kerugian akibat terputusnya koneksi.

Seandainya dengan sangat terpaksa harus ada proses mematikan koneksi, maka hal tersebut harus dilakukan dalam waktu yang sesingkat mungkin.

Peranan mesin/ perangkat back up sangat diperlukan untuk menanggulangi recovery apabila terjadi kerusakan pada sistem sehingga mengharuskan dilakukan perbaikan/setting ulang terhadap jaringan.

Perbaikan terhadap satu atau beberapa komponen jaringan komputer dapat dilakukan dengan terlebih dahulu mengelompokan gejala kerusakan yang terjadi baik berdasarkan lokasinya (melokalisasi masalah) dan dilanjutkan dengan mencari inti permasalahannya, apakah masalah terjadi pada daerah media/fisik, konfigurasi jaringan, sistem operasi atau atau apliksi jaringan yang diterapkan.

Setelah hal tersebut dilakukan maka tindakan perbaikan dapat dilakukan dengan objektif terhadap masalah yang terjadi. Penanganan masalah harus dilakukan dengan tidak menimbulkan masalah baru pada jaringan.

Seefektif apapun tindakan perbaikan terhadap suatu masalah yang terjadi sudah tentu akan berdampak pada kualitas koneksi jaringan, misalnya paling tidak jaringan akan mengalami *down time* ketika perbaikan dilakukan.

Untuk menjaga reliabilitas jaringan, maka yang seharusnya dilakukan oleh pengelola jaringan secara teknis adalah melakukan perawatan terhadap kualitas koneksi jaringan, pemeliharaan tidak menunggu sampai satu atau beberapa bagian dari jaringan komputer mengalami masalah.

Perawatan yang dilakukan sebaiknya dilakukan dengan memperhatikan beberapa hal, yaitu :

1. Adanya prosedur yang baku pada jaringan komputer, baik yang terkait dengan topologi dan perangkat jaringannya, maupun aturan terhadap pengelolaan jaringan tersebut, meliputi aturan terhadap personal yang diberi wewenang terhadap pengaturan jaringan secara teknis dan lingkup perubahan teknis jaringan komputer yang dilakukan, setiap perubahan teknis/konfigurasi harus disetujui oleh semua pihak yang berkepentingan terhadap kinerja jaringan tersebut.
2. Perawatan dilakukan secara berkala yang meliputi semua hal yang terkait kinerja

jaringan, mulai dari kualitas fisik/media jaringan, konfigurasi jaringan, reliabilitas sistem operasi yang digunakan, sampai *performance* dari aplikasi yang digunakan untuk memanfaatkan jaringan komputer tersebut.

3. Adanya data perawatan atau dikenal dengan data Maintenance Repair (MR), hal ini berguna sebagai data / referensi apabila di kemudian hari terdapat kebutuhan terhadap kondisi pada kurun waktu tertentu.

9.8 Soal-Soal Latihan

Soal-soal latihan ini diperuntukan bagi siswa yang telah selesai melakukan pemahaman Bab 9 mengenai Wide Area Network (WAN).

Jawablah pertanyaan dibawah ini dengan tepat.

1. Apa yang dimaksud dengan Wide Area Network (WAN)
2. Jelaskan komponen pembentuk Wide Area Network (WAN)
3. Jelaskan tiga jenis koneksi WAN
4. Apa yang dimaksud dengan Protokol WAN, berikan contohnya
5. Jelaskan dua metoda autentikasi yang disediakan oleh PPP.
6. Jelaskan keunggulan CHAP dibanding PAP pada implementasi koneksi PPP.
7. Tuliskan topologi fisik yang dapat dibentuk untuk mengimplementasikan jaringan Frame Relay.
8. Apa yang dimaksud dengan Virtual LAN (VLAN).
9. Apa yang dimaksud dengan Virtual Private Network (VPN).
10. Sebutkan beberapa protokol tunneling yang dapat digunakan pada VPN.
11. Tuliskan prinsip yang digunakan dalam melakukan diagnosa permasalah pada WAN.
12. Tuliskan hal yang harus diperhatikan dalam upaya menjaga kehandalan kualitas koneksi jaringan komputer.