PRAKTIKUM
DESAIN DAN MANAJEMEN JARINGAN KOMPUTER

Nama	**Aliyah Rizky Al-Afifah Polanda**	**No. Modul**	**04**
NPM	**2206024682**	**Tipe**	**Tugas Pendahuluan**

1. WAN (*Wide Area Network*) merupakan jaringan komputer yang mencakup area yang luas, terdiri dari 2 atau lebih LAN (*Local Area Network*). Jaringan dibangun dengan *leased telecommunication circuits*, dimana terdapat *router* di kedua sisi yang berfungsi untuk menghubungkan LAN di kedua sisi tersebut. WAN bertujuan untuk menyediakan komunikasi antara perangkat-perangkat yang berada di lokasi berjauhan.

   Alasan penggunaan WAN adalah sebagai berikut:

   a. Konektivitas jarak jauh. WAN mencakup area geografis yang luas, sehingga dapat meningkatkan jangkauan klien untuk mengirimkan data dengan cepat dan efisien.
   b. Sumber daya sentral. WAN menyediakan akses jarak jauh ke data tesimpan, sehingga data organisasi/perusahaan dapat disimpan secara terpusat. Akses ke sumber daya ini dapat diberikan ke cabang, dapat memastikan keamanan data.
   c. Kolaborasi global. WAN memungkinkan adanya kolaborasi dan pertukaran data antara tim yang tergabung dalam suatu proyek tanpa terbatas oleh batasan lokal.
   d. Skalabilitas. WAN dapat diperluas sesuai kebutuhan, sehingga dapat menyesuaikan dengan pertumbuhan dari suatu organisasi/perusahaan.
   e. Kemudahan manajemen. Pemeliharaan jaringan dalam WAN dapat dilakukan secara efisien dari satu titik pusat.

   Referensi:

   - "WAN Full Form," geeksforgeeks.org, Jul. 2023. [Online]. Available: https://www.geeksforgeeks.org/wan-full-form/. [Accessed Mar. 12, 2024].

2. Istilah-istilah dalam WAN:

   a. *Customer Premises Equipment* (CPE).

      Merupakan perangkat telekomunikasi yang berada di lokasi fisik klien dan terhubung dengan lokasi penyedia layanan WAN. Contoh CPE adalah *router* DSL. CPE berfungsi untuk mengatur dan mengelola koneksi WAN didalam gedung atau kantor klien.

b. *Data Communication Equipment* (DCE).

Perangkat DCE menyediakan *interface* yang menghubungkan klien ke WAN. Memiliki fungsi untuk membangun, memelihara, dan mengakhiri sesi komunikasi antara klien dengan tujuannya. DCE mencakup perangkat-perangkat yang digunakan penyedia layanan untuk mendukung transmisi data, seperti CSU/DSU..

c. *Data Terminal Equipment* (DTE).

Perangkat DTE berfungsi untuk meneruskan data dari *host* di LAN untuk transmisi melalui WAN. Cara kerjanya dengan mengubah informasi dari *host* dan informasi yang diterima menjadi sinyal. DTE tidak melakukan transmisi data, tetapi membutuhkan perantara agar transmisi data melalui WAN dapat tercipta.

d. *Demarcation Point*.

Merupakan titik yang membatasi tanggung jawab penyedia layanan terhadap LAN, yang berarti tanggung jawab klien dimulai. Titik ini adalah titik pertemuan antara perangkat penyedia layanan dengan CPE, sehingga dapat digunakan untuk memisahkan jaringan mana yang bersifat publik dan mana yang bersifat pribadi.

e. CSU/DSU.

CSU (*Channel Service Unit*)/DSU (*Data Service Unit*) merupakan perangkat yang digunakan untuk menghubungkan DTE dengan saluran komunikasi WAN. Bekerja dengan mengubah *data frame* dari LAN ke *frame* yang sesuai untuk WAN, serta sebaliknya. CSU bertanggung jawab untuk mengontrol kecepatan transmisi data, sedangkan DSU bertanggung jawab untuk melakukan konversi data.

Referensi:

- B. Priya. “What are the differences between DTE and DCE?” tutorialspoint.com, Mar. 20233. [Online]. Available: https://www.tutorialspoint.com/what-are-the-differences-between-dte-and-dce. [Accessed Mar. 12, 2024].
- K. T. Hanna. “customer premises equipment,” techtarget.com. [Online]. Available: https://www.techtarget.com/searchnetworking/definition/customer-premises-equipment. [Accessed Mar. 12, 2024].
- K. Stone. “What is Demarcation Point or Demarc?” getvoip.com, Dec. 2020. [Online]. Available: https://getvoip.com/library/what-is-demarcation-point/. [Accessed Mar. 12, 2024].
- P. Kirvan. “CSU/DSU (Channel Service Unit/Data Service Unit)” techtarget.com. [Online]. Available: https://www.techtarget.com/searchnetworking/definition/CSU-DSU. [Accessed Mar. 12, 2024].

3. *Private* WAN *infrastructure* merupakan jaringan yang dimiliki oleh suatu organisasi atau perusahaan secara pribadi. Kepemilikan pribadi ini berarti organisasi/perusahaan memiliki kontrol pernuh atas infrastruktur WAN tersebut.

   Keuntungan dari *private* WAN adalah:

   - Organisasi/perusahaan memiliki kontrol penuh atas manajemen jaringan, sehingga jaringan dapat dioptimalisasi sesuai kebutuhan spesifik organisasi/perusahaan.
   - Organisasi/perusahaan dapat menerapkan langkah-langkah keamanan yang ketat dalam jaringan. Selain itu akses ke jaringan dapat dibatasi sesuai keperluan masing-masing komponen dalam organisasi/perusahaan.
   - Kinerja dari *private* WAN dapat lebih diandalkan dan efisien, karena organisasi/perusahaan memegang kendali langsung dalam pengelolaan jaringan.

   Public WAN *infrastructure* merupakan jenis jaringan telekomunikasi yang dirancang untuk menghubungkan beberapa LAN secara bersamaan dalam area geografis yang luas. Karena digunakan secara bersamaan, maka *public* WAN menjadi kurang aman dibandingkan dengan *private* WAN. *Public* WAN disediakan oleh pihak ketiga atau penyedia layanan jaringan. Contoh dari *public* WAN adalah internet dan layanan *cloud*.

   Keuntungan dari *public* WAN adalah:

   - *Public* WAN menyediakan akses global, dimana organisasi/perusahaan dapat beroperasi dan berkomunikasi tanpa batas.
   - Penggunaan *public* WAN dapat mengurangi biaya investasi, karena *public* WAN digunakan secara bersama dengan organisasi/perusahaan lain.
   - Memiliki kemudahan untuk mengatur skala jaringan saat menggunakan *public* WAN.

   Referensi:

   - R. Sturt. “What are private WAN technologies?” netify.com, Jan. 2019. [Online]. Available: https://www.netify.com/learning/private-wan-options. [Accessed Mar. 12, 2024].
   - W. Dillon. “What Does ‘Public WAN (Wide Area Network)’ Mean?” techterminologies.com. [Online]. Available: https://techterminologies.com/definitions/public-wan-wide-area-network/. [Accessed Mar. 12, 2024].

4. PPP (*Point to Point Protocol*) merupakan protokol yang bekerja pada *data link layer* dan digunakan untuk mengirimkan *multiprotocol* data antara dua *host* yang terhubung secara langsung. PPP menjadi protokol yang paling umum digunakan untuk akses *point-to-point* serta banyak digunakan dalam

implementasi koneksi *dial-up* dan jaringan *remote*. Protokol ini dapat digunakan dalam *link* sinkronus atau asinkronus.

Tiga komponen dalam PPP adalah sebagai berikut:

a. Encapsulation.

Bertanggung jawab untuk melakukan enkapsulasi pada datagram untuk dapat ditransmisikan melalui lapisan fisik tertentu. Hal ini sangat penting dalam PPP karena PPP sendiri memungkinkan data dari protokol jaringan yang berbeda untuk ditransmisikan melalui jalur yang sama.

b. **Link Control Protocol** (LCP).

Memiliki tugas untuk membangun, memelihara, dan mengakhiri tautan transmisi. LCP juga menyertakan *Authentication Protocol* yang mendukung fitur otentikasi pengguna. Dua protokol dalam mengautentikasi pengguna adalah PAP (*Password Authentication Protocol*) dan CHAP (*Challenge Handshake Authentication Protocol*).

c. **Network Control Protocols** (NCPs).

Merupakan seperangkat protokol yang digunakan untuk memfasilitasi enkapsulasi data yang berasal dari *network layer* ke PPP *frames*. Dengan ini, hanya protokol yang diaktifkan yang dapat digunakan pada koneksi tertentu. Beberapa contoh dari NCPs adalah IPCP (Int*ernet Protocol Control Protocol*), IPXCP (*Internetwork Packet Exchange Control Protocol*), dan IPV6CP (IPV6 *Control Protocol*).

Referensi:

- R. Rathor. “Point-to-Point Protocol (PPP)” tutorialspoint.com, Sep. 2023. [Online]. Available: https://www.tutorialspoint.com/point-to-point-protocol-ppp. [Accessed Mar. 12, 2024].
- “PPP Protocol,” javatpoint.com. [Online]. Available: https://www.javatpoint.com/ppp-protocol. [Accessed Mar. 12, 2024].

5. Tahap pembentukan sesi PPP:

a. *Link establishment*.

Pembentukan koneksi antara dua *host* dilakukan dengan menggunakan LCP. LCP memeriksa apakah *host* di ujung lainnya siap untuk membangun koneksi. Selanjutnya, terjadi negosiasi parameter antara kedua *host*. Contoh parameter adalah kecepatan transmisi dan opsi enkripsi. Setelah negosiasi berhasil, maka koneksi telah berhasil dibangun.

b. *Authentication*.

Melibatkan penggunaan *Authentication Protocol* untuk memverifikasi identitas kedua *host*. Protokol yang dapat digunakan adalah PAP dan CHAP. PAP menggunakan pertukaran *username* dan *password*, sedangkan CHAP menggunakan *challenge* dan *response* untuk memverifikasi identitas *host*.

c. *Network layer protocol negotiation*.

Setelah proses otentikasi berhasil, NCP akan digunakan untuk menentukan protokol *network layer* yang akan digunakan di atas koneksi PPP. Jika semua tahap telah dilakukan, maka *link* PPP akan terus aktif, hingga adanya penutupan *link* oleh *frame* LCP dan NCP tertentu atau adanya kejadian eksternal, seperti intervensi pengguna.

Referensi:

- "PPP link establishment process," techhub.hpe.com. [Online]. Available: https://techhub.hpe.com/eginfolib/networking/docs/routers/hsr6800/5200-3506_l2-wan_cg/content/482615503.htm. [Accessed Mar. 12, 2024].

6. LQM (*Link Quality Monitoring*) merupakan upaya untuk memantau kualitas, yaitu rasio kehilangan dan kerusakan paket, *link* PPP secara *real time*. Jika LQM pada PPP tidak diaktifkan, maka satu *host* hanya akan mengirimkan *keepalives* ke *host* lainnya secara berkala. Jika LQM diaktifkan, maka *Link Quality Reports* (LQRs) akan dikirimkan sebagai ganti dari *keepalives*, yang bertujuan untuk memantau *link*. Hasil pengukuran LQM dapat berada dibawah persentase penutupan (*close-percentage*), dan *link* yang memiliki hasil tersebut dua kali secara berturut-turut akan ditutup.

   Beberapa tujuan dari LQM yaitu:

   - Mengukur kualitas *link*. Informasi yang dikumpulkan oleh LQM dapat memberikan gamabaran mengenai seberapa baik atau buruk kualitas dari suatu *link* PPP.
   - Mendeteksi masalah dalam *link*. LQM melakukan pemantauan terhadap link PPP secara kontinu, sehingga LQM dapat digunakan untuk mendeteksi masalah yang muncul, seperti kehilangan paket, dan ketidakstabilan *link*.
   - Penyesuaian protokol. LQM dapat membantu dalam peningkatan konfigurasi protokol PPP sesuai dengan kondisi kualitas *link* yang terdeteksi.

   Dengan menerapkan LQM dalam *link* PPP, maka dapaat tercipta sistem yang lebih andal dan optimal.

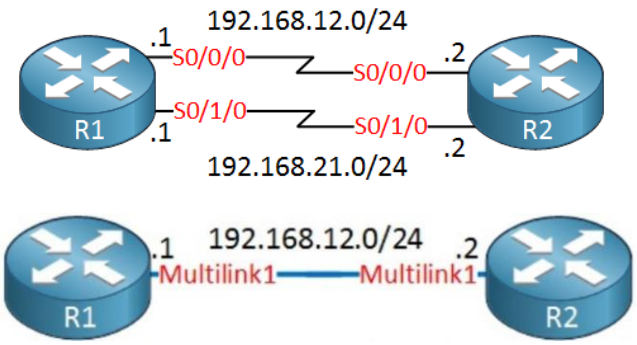
   Referensi:

- "Enabling PPP link quality mentoring." Techhub.hpe.com. [Online]. Available: https://techhub.hpe.com/eginfolib/networking/docs/routers/hsr6800/5200-3506_l2-wan_cg/content/482615515.htm. [Accessed Mar. 12, 2024].

7. Implementasi *load balancing* diantara *router* dapat dilakukan dengan konfigurasi *multilink* PPP (MLPPP). MLPPP memungkinkan untuk membagi *traffic* ke dua atau lebih *link* secara efisien. Konfigurasi MLPPP harus dilakukan di semua *router*. Contoh konfigurasinya adalah:

   Router(config)# interface [nama dan nomor interface]
   Router(config-if)# encapsulation ppp
   Router(config-if)# ppp multilink
   Router(config-if)# ppp multilink group [nomor grup]
   Router(config)#interface multilink [nomor grup]
   Router(config-if)#ip address [alamat IP] [netmask]

   MLPPP merupakan protokol yang menggabungkan beberapa *link* WAN menjadi satu *logical bundle*. Jika salah satu *link* gagal, maka *link* MLPPP tetap aktif dan komunikasi masih dapat berjalan. Hal ini memberikan redundansi antara *link*.



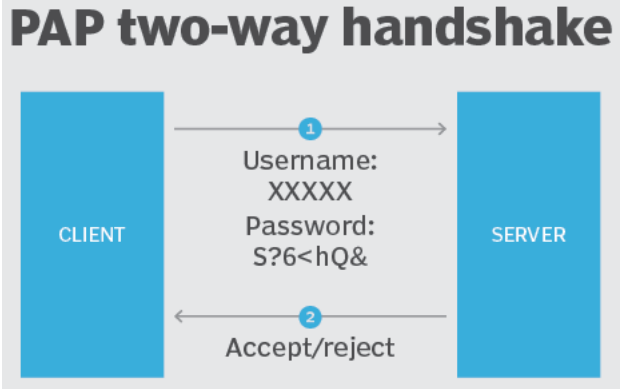
Sumber: https://networklessons.com/cisco/ccna-routing-switching-icnd2-200-105/ppp-multilink

Referensi:

- "What is MLPP?" ipcisco.com. [Online]. Available: https://ipcisco.com/lesson/what-is-mlppp/. [Accessed Mar. 12, 2024].

8. PAP (*Password Authentication Protocol*) merupakan protokol otentikasi yang sederhana dan biasanya digunakan pada situs publik. Pada PAP, *password* dikirimkan tanpa enkripsi sehingga protokol ini kurang aman. PAP menggunakan *two-way handshake* untuk otentikasi;
   - Klien mengirimkan *username* dan *password* ke server dalam *request packet*.

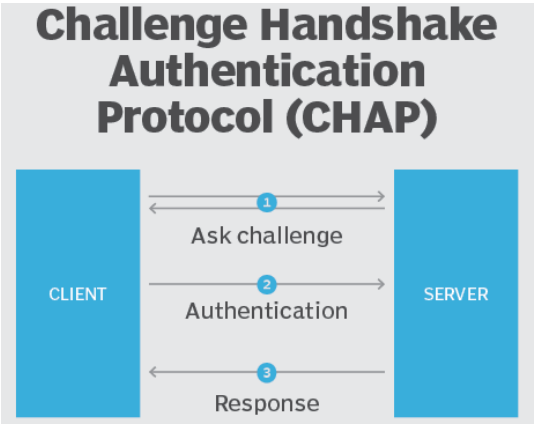
- Server menerima paket dari klien dan membandingkannya dengan informasi yang tersimpan di server. Jika sesuai, maka server akan mengirimkan *authentication-ack response packet* ke klien. Jika tidak sesuai maka server akan mengirimkan *authentication-nak response packet* ke klien.



Sumber: https://www.techtarget.com/searchnetworking/answer/Which-is-most-secure-CHAP-or-PAP

CHAP (*Challenge Handshake Authentication Protocol*) merupakan protokol otentikasi yang melibatkan enkripsi dalam prosesnya, sehingga menjadi protokol yang lebih aman daripada PAP. CHAP menggunakan *three-way handshake* untuk otentikasi:

- Server mengirimkan *challenge* ke klien, *challenge* ini mencakup rangkaian tantangan yang dibuat secara acak.
- Klien menggunakan *password* yang diketahui oleh klien dan server untuk membuat *hash* berdasarkan *challenge* yang diterima.
- Server melakukan dekripsi terhadap *hash* yang diterima dan melakukan verifikasi. Jika sesuai, maka server akan mengirimkan *authentication-success packet* ke klien. Jika tidak sesuai maka server akan mengirimkan *authentication-failure packet* ke klien.



Sumber: https://www.techtarget.com/searchnetworking/answer/Which-is-most-secure-CHAP-or-PAP

Perbedaan antara PAP dan CHAP:

PAP	CHAP
Menggunakan *two-way handshake* dalam prosesnya.	Menggunakan *three-way handshake* dalam prosesnya.
Transmisi *password* dilakukan tanpa enkripsi.	Transmisi *password* dilakukan dengan menerapkan enkripsi.
Kurang aman.	Lebih aman.
Tidak dapat melakukan *mid-session authentication* secara berulang.	Dapat melakukan *mid-session authentication* secara berulang.
Penggunaannya telah berkurang karena masalah keamanan.	Digunakan untuk *remote users* dan *routers*.

Konfigurasi:

a. Konfigurasi PAP:

Router (config)# username [username] password [password]
Router (config)# interface [nama dan nomor interface]
Router (config-if)# ppp authentication pap

b. Konfigurasi CHAP:

Router (config)# username [username] password [password]
Router (config)# interface [nama dan nomor interface]
Router (config-if)# ppp authentication chap

c. Konfigurasi PAP/CHAP:

Router (config)# username [username] password [password]
Router (config)# interface [nama dan nomor interface]
Router (config-if)# ppp authentication pap chap

Referensi:

- "Difference between PAP and CHAP," geeksforgeeks.org, Mar. 2023. [Online]. Available: https://www.geeksforgeeks.org/difference-between-pap-and-chap/. [Accessed Mar. 12, 2024].
- A. Froehlich and M. Tuomenoksa. "The differences between PAP and CHAP," techtarget.com, Jul. 2021. [Online]. Available: https://www.techtarget.com/searchnetworking/answer/Which-is-most-secure-CHAP-or-PAP. [Accessed Mar. 12, 2024].

9. Fitur debug ppp negotiation dan debug ppp authentication berguna untuk melakukan *troubleshooting*.
   a. debug ppp negotiation.

      Berfungsi untuk menampilkan informasi mengenai proses negosiasi yang terjadi diantara dua *host* yang ingin membangun *link* PPP. Kegunaannya meliputi pemantauan (pengaturan parameter dan opsi enkapsulasi) dan pemeriksaan setiap langkah dalam proses negosiasi untuk mengidentifikasi potensi masalah dalam konfigurasi.

      Konfigurasi:

      Router(config-if)# debug ppp negotiation

   b. Debug ppp authentication.

      Berfungsi untuk menampilkan informasi mengenai proses otentikasi, seperti jenis otentikasi apa yang digunakan, langkah otentikasi dan hasilnya. Kegunaannya meliputi penyediaan informasi detail mengenai proses otentikasi dan pemberian petunjuk terkait kesalahan otentikasi.

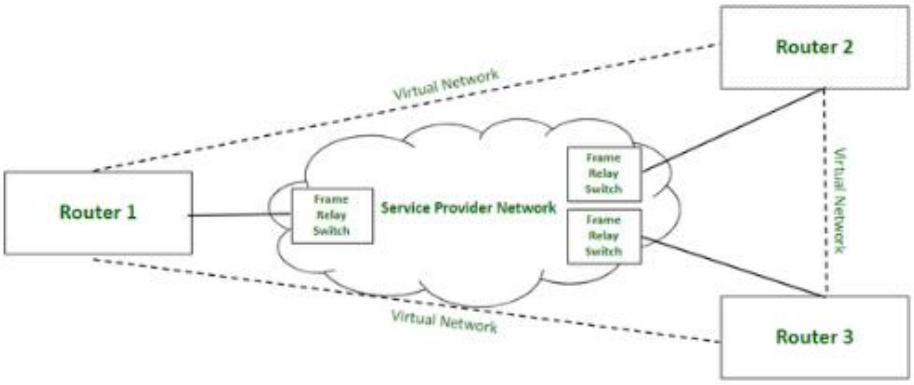
      Konfigurasi:

      Router(config-if)# debug ppp authentication

   Referensi:

   - "Troubleshooting PPP (CHAP or PAP) Authentication," cisco.com. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25646-ppp-authen-ts-fl.html. [Accessed Mar. 12, 2024].
   - "Understanding debug ppp negotiation Output," cisco.com. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25440-debug-ppp-negotiation.html. [Accessed Mar. 12, 2024].

10. *Frame relay* merupakan protokol jaringan *packet-switching* yang bekerja pada *data link layer*. Memiliki fungsi untuk menghubungkan LAN dan mengirimkan data melalui WAN. Mekanisme ini lebih baik daripada PPP yang setiap *link* nya hanya menghubungkan sepasang *node*/*host* saja. *Frame relay* menggunakan enkapsulasi *frame* yang sederhana, memungkinkan *multiple virtual circuits* untuk berbagi *link* fisik yang sama, sehingga dapat mengurangi biaya. Visualisasi penerapan *frame relay* dalam topologi adalah sebagai berikut:



Sumber: https://www.geeksforgeeks.org/how-does-frame-relay-work/

Frame relay bekerja dengan mengirimkan data yang telah dikemas dalam bentuk *frame* melalui *virtual circuit* (dapat dibuat secara permanen (PVC) atau dinamis (SVC)). *Data frame* tersebut melalui *link* fisik yang dapat digunakan bersama, sehingga penggunaan *bandwidth* dapat lebih efisien.

Virtual circuit merupakan jalur *virtual* yang dibuat dalam mekanisme *frame relay*. Terdiri dari dua jenis yaitu:

a. *Permanent Virtual Circuit* (PVC).

   Merupakan *virtual circuit* yang ditetapkan secara permanen untuk menghubungkan dua titik tetap. Digunakan untuk koneksi yang memerlukasn kestabilan dan memerlukan komunikasi konstan antara dua lokasi permanen.

b. *Switched Virtual Circuit* (SVC).

   Merupakan *virtual circuit* yang dibuat hanya saat diperlukan, dapat dihancurkan sesuai kebutuhan komunikasi. Digunakan untuk situasi ketika perlu dibangun koneksi antara dua titik yang berubah-ubah.

Keuntungan dari *virtual circuit* adalah paket akan diterima dalam urutan yang sama dengan urutan saat pengiriman, tidak memerlukan *overhead* untuk setiap paket, dan termasuk sirkuit jaringan yang andal.

Referensi:

- "How does Frame Relay Work?" geeksforgeeks.org, Nov. 2021. [Online]. Available: https://www.geeksforgeeks.org/how-does-frame-relay-work/. [Accessed Mar. 12, 2024].
- "Virtual Circuit in Computer Network," geeksforgeeks.org, May, 2020. [Online]. Available: https://www.geeksforgeeks.org/virtual-circuit-in-computer-network/. [Accessed Mar. 12, 2024].

11. *Data Link Connection Identifier* (DLCI) merupakan angka yang digunakan oleh *frame relay switch* (DCE) untuk mengidentifikasi *router* tujuan dari paket yang masuk. DLCI biasanya ditetapkan oleh penyedia layanan *frame relay*. Setiap DCE akan mengetahui DLCI dari DCE lainnya, yang berada dalam satu *frame relay cloud.* DCE tidak dapat memiliki DLCI yang sama untuk tujuan yang berbeda. Dalam *frame relay*, DLCI digunakan untuk mengidentifikasi *virtual circuit* dan membawa *frame* ke tujuan yang sesuai. Dengan kata lain, DLCI berperan sebagai *identifier* yang membantu mengarahkan *traffic* dalam jaringan *frame relay.*

    Inverse ARP (InARP) merupakan kebalikan dari ARP. InARP menggunakan alamat MAC *layer*-2 untuk menemukan alamat IP *layer*-3. InARP digunakan oleh *frame relay* untuk memetakan DLCI ke alamat IP. *Router* akan menanyakan alamat IP tujuan dengan mencatumkan DLCI untuk *router* tersebut. *Static mapping* merupakan alternatif dari InARP, dimana *administrator* jaringan akan memetakan DLCI ke alamat IP secara manual.

    Referensi:

    - "Data Link Connection Identifier (DLCI)" geeksforgeeks.org, Aug. 2022. [Online]. Available: https://www.geeksforgeeks.org/data-link-connection-identifier-dlci/. [Accessed Mar. 12, 2024].
    - U. Samariya. "ARP, Reverse ARP, Inverse ARP, Proxy ARP, and Gratuitous ARP," tutorialspoint.com, Nov. 2022. [Online]. Available: https://www.tutorialspoint.com/arp-reverse-arp-inverse-arp-proxy-arp-and-gratuitous-arp. [Accessed Mar. 12, 2024].

12. DLCI memiliki rentang 16-1007 (atau hingga 1023 pada beberapa perangkat) untuk koneksi antara klien dengan penyedia layanan *frame relay* dan rentang 1024-15999 untuk koneksi antara dua penyedia layanan *frame relay*. Rentang yang biasanya digunakan tentu saja rentang yang mewakili koneksi klien dengan penyedia layanan *frame relay*, yaitu 16-1007/1023.

    Referensi:

    - "multicast-dlci," juniper.net, Sep. 2018. [Online]. Available: https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/multicast-dlci-edit-interfaces-ni.html. [Accessed Mar. 12, 2024].
