PRAKTIKUM
DESAIN DAN MANAJEMEN JARINGAN KOMPUTER

Nama	**Aliyah Rizky Al-Afifah Polanda**	**No. Modul**	**03**
NPM	**2206024682**	**Tipe**	**Tugas Pendahuluan**

1. NAT (*Network Address Translation*) merupakan suatu proses untuk menerjemahkan satu atau lebih alamat IP lokal/privat ke satu atau lebih alamat IP global/publik, proses ini juga dilakukan sebaliknya. Tujuan dilakukannya NAT adalah untuk menyediakan akses internet bagi *local hosts*. Dengan NAT, banyak perangkat di jaringan lokal dapat mengakses internet menggunakan satu alamat IP publik. Selain itu, NAT juga membantu meningkatkan kemanan jaringan lokal dengan menyembunyikan alamat IP lokal saat mengakses internet.

   Beberapa jenis NAT yaitu:

   a. *Static* NAT.

      Dalam jenis ini, satu alamat IP privat akan diterjemahkan ke satu alamat IP publik secara permanen. Biasanya digunakan untuk server yang perlu diakses melalui internet. Tidak digunakan dalam sebuah organisasi yang memiliki banyak perangkat yang perlu terhubung ke internet, karena butuh biaya yang besar untuk membeli banyak alamat IP publik.

   b. *Dynamic* NAT.

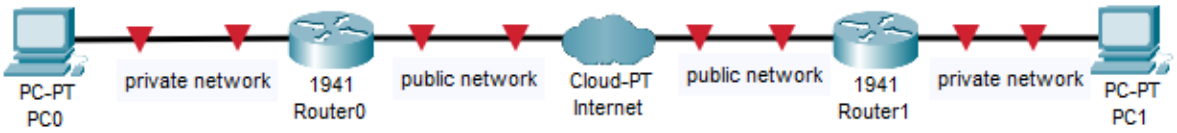
      Dalam jenis ini, alamat IP privat akan diterjemahkan ke alamat IP publik secara temporer. Biasanya digunakan untuk perangkat yang tidak perlu diakses secara permanen dari internet. Alamat IP privat akan dipetakan ke salah satu alamat IP publik yang tersedia dalam sebuah *pool*, sehingga proses ini akan bergantung pada ketersediaan alamat IP publik dalam *pool* tersebut.

   c. PAT (*Port Address Translation*).

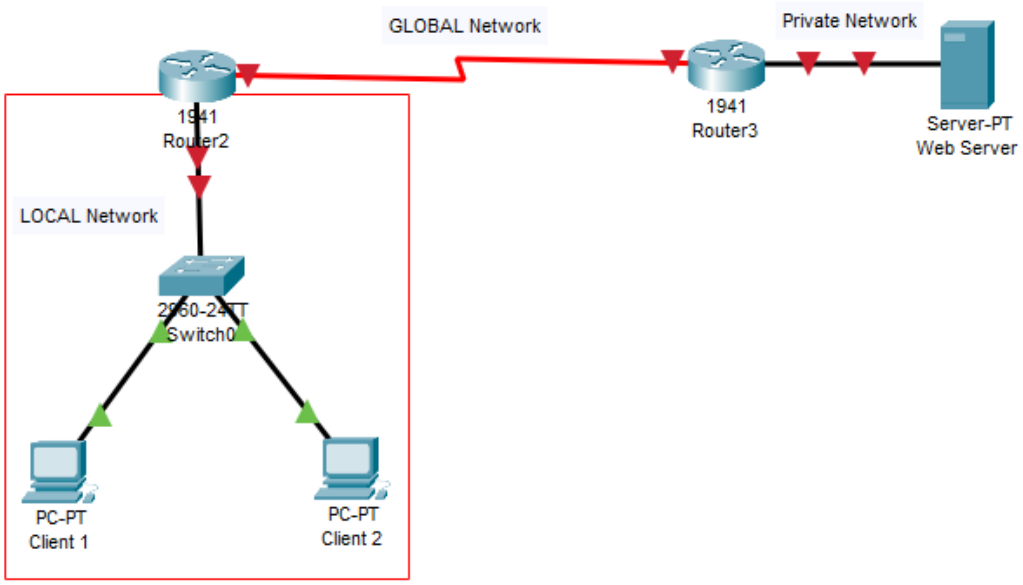
      Juga dikenal dengan istilah NAT *overload*. Dalam jenis ini, banyak alamat IP privat dapat diterjemahkan ke satu alamat IP publik. Digunakan *port number* untuk membedakan *traffic* dari setiap alamat IP privat. Menjadi jenis yang paling banyak digunakan karena dapat mengurangi biaya pembelian alamat IP publik dan dapat secara efisien menggunakan alamat IP publik yang terbatas.

   Contoh topologi NAT:

   - Dengan internet.



- Dengan web server.



Referensi:

- "Network Address Translation (NAT)" geeksforgeeks.org, Dec. 2021. [Online]. Available: https://www.geeksforgeeks.org/network-address-translation-nat/. [Accessed Mar. 03, 2024].

2. Alamat IP privat merupakan alamat IP yang digunakan untuk komunikasi antar perangkat yang berada dalam satu jaringan. Setiap perangkat yang berada dalam satu jaringan memiliki alamat IP privat yang unik. Karena alamat IP privat hanya diketahui oleh perangkat lain yang berada dalam satu jaringan, maka alamat IP ini menjadi lebih aman. Selanjutnya alamat IP publik merupakan alamat IP yang digunakan untuk berkomunikasi dengan perangkat yang berada di luar jaringan. Alamat IP ini diberikan oleh ISP (*Internet Service Provider*). Alamat IP publik terbagi menjadi dua yaitu:
   - Alamat IP dinamis: yaitu alamat IP yang berubah-ubah seiiring waktu. Setiap kali sebuah perangkat terhubung ke internet, maka ISP akan memberikan alamat IP publik random ke perangkat tersebut.
   - Alamat IP statis: yaitu alamat IP yang diberikan ke sebuah perangakat secara permanen. Jenis ini banyak digunakan oleh DNS *servers*.

   Perbedaan antara alamat IP privat dan alamat IP publik adalah sebagai berikut:

Alamat IP Privat	Alamat IP Publik
Memiliki jangkauan lokal.	Memiliki jangkauan global.
Digunakan untuk berkomunikasi dalam jaringan yang sama.	Digunakan untuk berkomunikasi dengan jaringan luar.
Bekerja pada LAN.	Bekerja untuk mendapatkan layanan internet.
Didapatkan secara gratis.	Memerlukan biaya untuk mendapatkannya.
Lebih aman.	Tidak memiliki keamanan.
Dapat diketahui dengan menggunakan perintah **ipconfig** di *command prompt*.	Dapat diketahui dengan mencari "*what is my ip*" di Google.
Range alamat IP: 10.0.0.0 – 10.255.255.255 172.16.0.0 – 172.31.255.255 192.168.0.0 – 192.168.255.255	Range alamat selain milik alamat IP privat.

NAT digunakan untuk menghubungkan alamat IP privat dengan alamat IP publik. Ketika perangkat dalam jaringan lokal ingin mengakses internet, maka NAT akan berperan sebagai perantara. *Router* yang menggunakan NAT akan menerapkan pengubahan alamat IP untuk memungkinkan komunikasi antara jaringan lokal dan internet. Ketika NAT beroperasi pada *router*, maka *header* paket yang berisi alamat IP privat akan diubah menjadi alamat IP publik, hal ini juga meningkatkan keamanan, karena perangkat dari jaringan luar tidak dapat secara langsung mengetahui alamat IP privat yang digunakan oleh perangkat di dalam jaringan lokal.

Referensi:

- "Difference between Private and Public IP addresses," geeksforgeeks.org, Sep. 2023. [Online]. Available: https://www.geeksforgeeks.org/difference-between-private-and-public-ip-addresses/. [Accessed Mar. 03, 2024].

3. Kelebihan NAT:
   a. NAT menyembunyikan alamat IP privat perangkat yang berada dalam sebuah jaringan lokal, sehingga struktur jaringan lokal tersebut dapat terhindar dari akases langsung oleh perangkat luar.
   b. NAT memungkinkan beberapa perangkat dalam jaringan lokal untuk menggunakan satu alamat IP publik. Hal ini bermanfaat dalam mengatasi keterbatasan alamat IP publik.
   c. NAT mempermudah perangkat dalam jaringan lokal untuk mengakses internet.

d. NAT dapat mengelola dan memantau lalu lintas jaringan dengan efektif serta membantu administrator jaringan dengan menyederhanakan konfigurasi alamat IP di jaringan lokal.

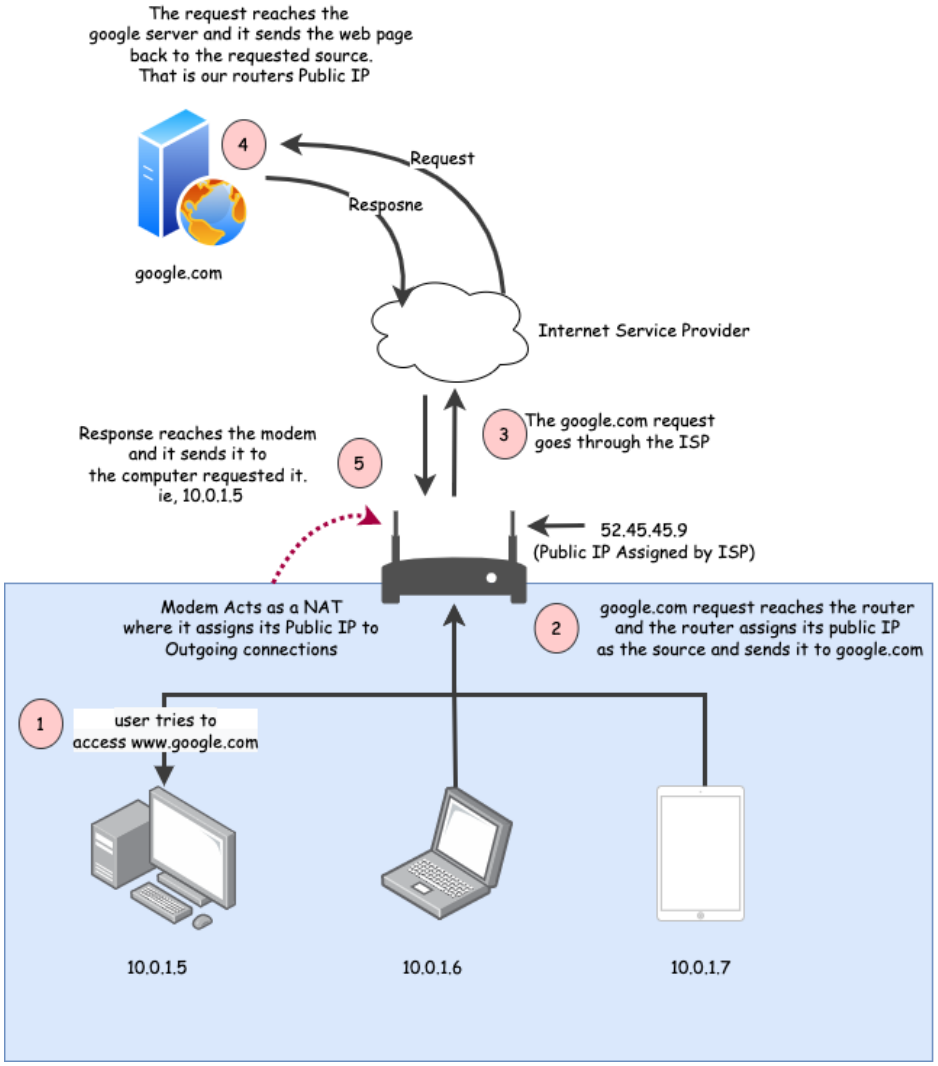
Kekurangan NAT:

a. Beberapa aplikasi dapat mengalami kesulitan beroperasi melalui NAT, terutama dengan yang memiliki masalah dengan pembatasan alamat IP.
b. NAT bekerja pada *router*, sehingga dapat menambah *overhead* pada *router* dan berakibat buruk pada kinerja jaringan.
c. NAT dapat memiliki konfigurasi yang kompleks jika terdapat skenario yang melibatkan banyak perangkat.

Referensi:

- "Network Address Translation (NAT)" geeksforgeeks.org, Dec. 2021. [Online]. Available: https://www.geeksforgeeks.org/network-address-translation-nat/. [Accessed Mar. 03, 2024].
- A. Kapoor. "What Is NAT? Significance of Network Address Translation in Network Model," simplilearn.com, Apr. 2023. [Online]. Available: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-nat-in-networking. [Accessed Mar. 03, 2024].

4. Cara kerja NAT:
   a. Permintaan akses/koneksi oleh *end devices* yang berada di jaringan lokal. Permintaan ini berisi alamat IP tujuan di internet dan akan dikirimkan ke *router*/*gateway* lain.
   b. *Router* menerima permintaan tersebut dan menerjemahkan alamat IP privat perangkat sumber ke alamat IP publik. Informasi mengenai terjemahan ini akan disimpan di tabel NAT.
   c. Selanjutnya *router* mengirimkan permintaan tersebut ke tujuannya melalui internet (ISP). Alamat IP privat perangkat tidak diketahui oleh internet.
   d. Setelah sampai ke tujuan, maka perangkat tujuan akan mengirimkan respon terhadap permintaan yang diterimanya. Respon tersebut akan dikirimkan kembali melalui internet.
   e. Respon sampai di *router* dan alamat IP publik akan diterjemahkan kembali ke alamat IP privat dengan mengandalkan informasi dalam tabel NAT.
   f. Proses NAT selesai, *router* akan mengirimkan respon tersebut ke perangkat yang sesuai di jaringan lokal.



Referensi:

- "What is NAT? How Does NAT Work?" devopscube.com, Jul. 2022. [Online]. Available: https://devopscube.com/what-is-nat-how-does-nat-work/. [Accessed Mar. 03, 2024].

5. ACL (Access Control *List*) merupakan seperangkat aturan yang digunakan untuk mengatur lalu lintas jaringan dengan tujuan untuk mengurangi serangan terhadap jaringan. ACL bekerja dengan membatasi akses ke sumber daya jaringan atau ke sebuah layanan. Pembatasan ini dilakukan dengan menyaring paket data yang masuk dan keluar suatu jaringan berdasarkan alamat IP serta protokol dan *port* yang digunakan. Jika informasi dalam *header* paket data cocok dengan salah satu aturan yang telah dikonfigurasi, maka ACL akan mengambil tindakan yang sesuai dengan aturan tersebut, seperti mengizinkan atau menolak paket tersebut.

Penerapan ACL dapat dilakukan pada *router*, *switch*, atau *firewall*. Pemilihan perangkat yang akan diterapkan ACL bergantung pada tujuan penerapannya.

a. Pada *router*.

Router menghubungkan jaringan lokal dengan internet. Jika ACL diterapkan pada *router* maka, lalu lintas yang masuk dan keluar dapat diawasi sehingga dapat melindungi seluruh jaringan lokal dari serangan yang tidak diinginkan.

b. Pada *switch*.

Switch menghubungkan perangkat-perangkat yang berada dalam satu jaringan lokal. Jika ACL diterapkan pada *switch*, lalu lintas antar perangkat dapat diawasi sehingga dapat dilakukan pembatasan akses ke perangkat tertentu.

c. Pada *firewall*.

Firewall digunakan untuk melindungi jaringan. Hampir sama seperti *router*, penerapan ACL pada *firewall* juga dapat mengawasi lalu lintas yang masuk dan keluar jaringan. Namun aturan yang diterapkan pada firewall dapat lebih spesifik.

Selain pada perangkat-perangkat diatas, ACL juga dapat diterapkan pada suatu mekanisme, seperti pada jaringan nirkabel dan pada inter-VLAN.

Referensi:

- "Access-Lists (ACL)" geeksforgeeks.org, Jun. 2022. [Online]. Available: https://www.geeksforgeeks.org/access-lists-acl/. [Accessed Mar. 03, 2024].
- B. Lutkevich. "access control list (ACL)" techtarget.com. [Online]. Available: https://www.techtarget.com/searchnetworking/definition/access-control-list-ACL. [Accessed Mar. 03, 2024].

6. Perbedaan antara:

a. *Standard* dan *Extended* ACL.

- *Standard* ACL hanya mempertimbangkan alamat IP sumber, sedangkan *extended* ACL mempertimbangkan beberapa kriteria, seperti alamat IP, nomor *port*, dan protokol yang digunakan.
- Nomor yang digunakan oleh *standard* ACL adalah 1-99 dan 1300-1999, sedangkan untuk *extended* ACL memiliki nomor 100-199 dan 2000-2699.
- *Standard* ACL lebih mudah dikonfigurasi daripada *extended* ACL.

- *Standard* ACL cocok untuk diterapkan pada jaringan sederhana yang hanya membutuhkan keamanan dasar. *Extended* ACL sesuai untuk diterapkan pada jaringan kompleks yang membutuhkan keamanan lengkap.

b. *Numbered* dan *Named* ACL.
   - *Numbered* ACL diidentifikasi oleh nomor, sedangkan *named* ACL diidentifikasi oleh nama.
   - *Numbered* ACL lebih mudah dikonfigurasi daripada *named* ACL.
   - Pada konteks jaringan yang kompleks, *numbered* ACL lebih sulit untuk diingat dan diidentifikasi daripada *named* ACL.
   - Suatu aturan tidak dapat dihapus begitu saja dari *numbered* ACL (penghapusan harus dilakukan untuk seluruh ACL). Namun penghapusan suatu aturan dapat dilakukan pada *named* ACL.
   - *Numbered* ACL cenderung digunakan pada *router* dan *firewall*, sedangkan named ACL banyak digunakan pada jaringan yang kompleks dengan banyak aturan ACL.

c. ACL *in* dan *out*.
   - ACL *in* (*inbound* ACL) digunakan untuk menyaring paket data yang masuk ke sebuah *interface*. Sedangkan ACL *out* (*outbound* ACL) digunakan untuk menyaring paket data yang keluar dari sebuah *interface*.
   - ACL *in* berfungsi untuk melindungi jaringan dari serangan pihak luar, sedangkan ACL *out* berfungsi untuk mengatur lalu lintas paket yang keluar dari suatu jaringan.

Referensi:

- "Access-Lists (ACL)" geeksforgeeks.org, Jun. 2022. [Online]. Available: https://www.geeksforgeeks.org/access-lists-acl/. [Accessed Mar. 03, 2024].
- "ACL Types: Standard and Extended," study-ccna.com. [Online]. Available" https://study-ccna.com/types-of-acls/. [Accessed Mar. 03, 2024].

7. *Blacklist* dan *whitelist* merupakan fitur yang tersedia pada ACL. Keduanya digunakan untuk mengatur akses ke dalam sebuah ACL.

   a. *Blacklist*.

   Merupakan daftar kriteria, seperti alamat IP, protokol, atau *port*, yang ditolak aksesnya ke suatu jaringan atau layanan/sumber daya. Lebih sesuai digunakan untuk menolak akses dari banyak sumber yang tidak diinginkan, misalnya memblokir alamat IP yang dikenal sebagai

sumber spam. *Blacklist* dapat diimplementasikan dengan membuat ACL yang secara eksplisit menolak akses dari kriteria yang telah ditentukan.

Keuntungan penggunaan *blacklist*:

- Mudah untuk memblokir banyak sumber yang tidak diinginkan.
- Mencegah serangan dari akses yang tidak sah.

Kekurangan penggunaan *blacklist*:

- Jika terdapat daftar yang panjang, maka konfigurasi yang dilakukan akan rumit.
- Dapat secara tidak sengaja memblokir sumber yang sah.

b. *Whitelist*.

Merupakan daftar kriteria, seperti alamat IP, protokol atau *port*, yang diizinkan untuk mengakses suatu jaringan atau layanan/sumber daya. Biasanya diterapkan untuk membatasi akses ke sumber daya sensitif dari suatu perusahaan, jadi hanya alamat IP yang diizinkan saja yang dapat mengakses sumber daya tersebut. *Whitelist* dapat diimplementasikan dengan membuat ACL yang secara eksplisit mengizinkan akses dari kriteria yang telah ditentukan.

Keuntungan penggunaan *whitelist*:

- Dapat memberikan kontrol terhadap akses dengan lebih spesifik.
- Meminimalkan risiko masuknya akses yang tidak sah.

Kekurangan penggunaan *whitelist*:

- Jika terdapat daftar yang panjang, maka konfigurasi yang dilakukan akan rumit.
- Membutuhkan konfigurasi manual untuk setiap sumber yang sah.

Referensi:

- "Access Control Lists," support.kemptechnologies.com, Jan. 2024. [Online]. Available: https://support.kemptechnologies.com/hc/en-us/articles/202029385-Access-Control-Lists. [Accessed Mar. 03, 2024].

8. Dalam suatu *interface router* dapat diterapkan lebih dari satu ACL, dengan syarat bahwa ACL yang diterapkan berbeda arah, yaitu menerapkan ACL *in* dan ACL *out*. Lebih jelasnya, hanya satu ACL yang dapat diterapkan untuk setiap *interface*, setiap protokol, dan setiap arah paket. Penerapan *multiple* ACL dapat memberikan aturan yang lebih spesifik untuk mengontrol lalu lintas jaringan. Selain itu, urutan penerapan ACL pada suatu *interface* sangat penting. Hal ini karena paket yang masuk dan keluar *interface* akan dievaluasi secara berurutan terhadap setiap ACL. Setelah aturan yang sesuai ditemukan, maka proses evaluasi ACL akan berhenti meskipun masih terdapat ACL yang berlum diperiksa.

Referensi:

- "Access Control List (ACL) Cisco in networking," manageengine.com. Available: https://www.manageengine.com/network-configuration-manager/access-control-list-cisco.html#:~:text=Only%20one%20ACL%20per%20interface,is%20either%20permitted%20or%20denied. [Accessed Mar. 03, 2024].

9. Membuat perintah untuk *number standard* ACL.

   X = 2; Y = 2;

   Router(config)# access-list 22 permit 192.168.2.0 0.0.0.255

   Referensi:

   - "Standard Access-List," geeksforgeeks.org, Aug. 2022. [Online]. Available: https://www.geeksforgeeks.org/standard-access-list/. [Accessed Mar. 03, 2024].

10. Membuat perintah untuk *number extended* ACL.

    X = 2; Y = 2;

    Router(config)# ip access-list extended 222

    Router(config-ext-nacl)# deny tcp 172.168.2.0 0.0.255.255 10.10.10.10 0.0.0.0 eq 443

    Router(config-ext-nacl)# permit ip any

    Referensi:

    - "Extended Access-List," geeksforgeeks.org, Jul. 2022. [Online]. Available: https://www.geeksforgeeks.org/extended-access-list/. [Accessed Mar. 03, 2024].