

**PRAKTIKUM
DESAIN DAN MANAJEMEN JARINGAN KOMPUTER**

Nama	Aliyah Rizky Al-Afifah Polanda	No. Modul	08
NPM	2206024682	Tipe	Tugas Pendahuluan

1. *Network virtualization* merupakan metode yang mengelompokkan infrastruktur jaringan fisik menjadi satu atau beberapa jaringan *virtual*. Dengan metode ini, suatu perusahaan/organisasi tidak perlu menambah infrastruktur fisik baru setiap kali ingin menambah jaringan, karena infrastruktur yang sudah ada dapat disimulasikan ke dalam jaringan *virtual*. Infrastruktur fisik yang dimaksud mencakup perangkat keras, perangkat lunak, dan sumber daya jaringan lainnya. Untuk menerapkan *network virtualization*, dapat digunakan teknologi seperti *hypervisor* atau *Software Defined Network (SDN)*.

Cara kerja dari *network virtualization* adalah dengan melakukan abstraksi terhadap infrastruktur jaringan fisik. Teknologi virtualisasi akan menciptakan sumber daya *virtual*. Setiap jaringan *virtual* saling terisolasi satu sama lain dan memiliki kebijakannya masing-masing. Dengan hal ini, *network virtualization* memberikan fleksibilitas, efisiensi, dan keamanan yang lebih tinggi dibandingkan dengan jaringan fisik tradisional.

Referensi:

- “Network Virtualization in Cloud Computing,” geeksforgeeks.org, Mar.2021. [Online]. Available: <https://www.geeksforgeeks.org/network-virtualization-in-cloud-computing/>. [Accessed May 05, 2024].
- J. English, “What is network virtualization? Everything you need to know,” techtarget.com. [Online]. Available: <https://www.techtargget.com/searchnetworking/What-is-network-virtualization-Everything-you-need-to-know>. [Accessed May 05, 2024].

2. Penggunaan *network virtualization* dapat memberikan beberapa manfaat dibandingkan penggunaan jaringan biasa, diantaranya adalah sebagai berikut:
 - a. Skalabilitas. Dengan menggunakan *network virtualization*, perusahaan/organisasi dapat menambahkan atau mengurangi jumlah jaringan *virtual* tanpa perlu mengubah infrastruktur fisik

yang sudah ada. Hal ini juga mempercepat proses perubahan jaringan sesuai dengan kebutuhan perusahaan/organisasi.

- b. Keamanan. Meskipun beberapa jaringan *virtual* berbagi jaringan fisik yang sama, keamanan diantara jaringan-jaringan *virtual* tersebut tetap dapat dipertahankan dengan menerapkan isolasi antar jaringan. Sehingga saat suatu jaringan *virtual* mengalami masalah atau serangan, hal ini tidak akan mempengaruhi jaringan *virtual* lainnya.
- c. Manajemen jaringan terpusat. Hanya terdapat satu infrastruktur fisik yang digunakan untuk beberapa jaringan *virtual*, sehingga pengaturan dan pemantauan jaringan akan terpusat pada infrastruktur fisik tersebut.
- d. Efisiensi biaya. *Network virtualization* memungkinkan perusahaan/organisasi untuk menghindari biaya tambahan untuk pembelian, instalasi, dan pemeliharaan infrastruktur baru. Selain itu, karena jaringan *virtual* menggunakan sumber daya yang sama, maka dapat menghemat biaya operasional jangka panjang.
- e. Uji coba yang terisolasi. Dengan jaringan *virtual*, dapat dilakukan percobaan terhadap jaringan tanpa perlu mengganggu jaringan utama yang berjalan.

Referensi:

- “Network Virtualization in Cloud Computing,” geeksforgeeks.org, Mar.2021. [Online]. Available: <https://www.geeksforgeeks.org/network-virtualization-in-cloud-computing/>. [Accessed May 05, 2024].

3. *Physical machine* merupakan perangkat keras dengan *motherboard*, CPU, memori, dan *controllers*. Jenis ini hanya dapat menjalankan satu sistem operasi dalam satu perangkat. *Virtual machine* merupakan representasi dari *physical machine*. Perangkat-perangkat fisik akan diabstraksi oleh sebuah fungsi yang disebut sebagai *hypervisor*. Perbedaan dari *physical machine* dan *virtual machine* adalah sebagai berikut:

- a. *Physical machine* merupakan *server* yang berjalan diatas perangkat keras yang sesungguhnya. Sedangkan *virtual machine* merupakan *server*/lingkungan komputasi yang berjalan diatas perangkat keras yang sesungguhnya. Namun satu perangkat keras dapat menjalankan beberapa *virtual machine*.
- b. *Data/workload* dari sebuah *physical machine* lebih sulit untuk dipindahkan dari satu perangkat ke perangkat lain. Hal ini karena konfigurasi dari satu perangkat dapat berbeda dengan perangkat

lainnya. Sedangkan untuk *virtual machine*, *workload* lebih mudah dipindahkan karena tidak bergantung pada konfigurasi dari suatu perangkat. *Virtual machine* bergantung pada kompatibilitas *hypervisor* yang sama dan memiliki format penyimpanan data yang *portable*.

- c. Satu *physical machine* hanya dapat menggunakan satu sistem operasi, sedangkan satu *virtual machine* dapat menggunakan lebih dari satu sistem operasi.
- d. Pengelolaan *physical machine* tidak membutuhkan keahlian khusus karena sering kali pengaturan telah dilakukan oleh sistem operasi yang digunakan. Pada *virtual virtualization* dibutuhkan keahlian khusus untuk mengelola semua sistem yang berjalan didalamnya. Dalam lingkungan *virtual*, *administrator* harus memahami konfigurasi, manajemen *hypervisor*, serta pengaturan dan pemantauan setiap *virtual machine* yang berjalan di dalamnya.
- e. Lebih mudah untuk mengimplementasikan keamanan yang terpusat pada *virtual machine* daripada *physical machine*.
- f. *Virtual machine* menyediakan lebih banyak opsi untuk memulihkan sistem seperti replikasi data. Sehingga pemulihan sistem lebih fleksibel daripada pemulihan di *physical machine* yang mungkin membutuhkan penggantian perangkat keras baru.

Referensi:

- R. Bastiaansen, "Virtual servers vs. physical servers: What are the differences?" techtarget.com, Feb. 2021. [Online]. Available: <https://www.techtargget.com/searchitoperations/tip/Virtual-servers-vs-physical-servers-What-are-the-differences>. [Accessed May 05, 2024].

4. *Hypervisor* merupakan *software* yang menyediakan pengoperasian beberapa *virtual machine* pada suatu perangkat keras. *Hypervisor* memungkinkan beberapa sistem operasi atau aplikasi berjalan secara bersamaan pada satu *physical machine*. Beberapa *virtual machine* yang berjalan akan berbagi sumber daya sistem (siklus prosesor, ruang memori, dan *bandwidth*) yang sama. Terdapat dua jenis *hypervisor* utama, yaitu:

a. **Hypervisor tipe 1 (*bare-metal*).**

Jenis ini diterapkan langsung diatas perangkat keras tanpa adanya sistem operasi atau *software* lain yang mendasarinya. *Hypervisor* tipe 1 memiliki akses langsung ke sumber daya sistem. Selain itu, penggunaannya dapat meningkatkan keamanan karena tidak terdapat lapisan tambahan antara *hypervisor* dan perangkat keras. Contoh dari *hypervisor* jenis ini adalah vSphere dan Hyper-V, serta

sering digunakan pada pusat data dari sebuah perusahaan.

b. Hypervisor tipe 2 (hosted).

Jenis ini berjalan diatas sistem operasi host yang sudah ada pada perangkat keras yang digunakan. Terdapat lapisan tambahan antara hypervisor dan perangkat keras, sehingga dapat mempengaruhi kinerja dan keamanan. Contohnya adalah *VMware Workstation Player* dan sering digunakan pada komputer pribadi.

Cara kerja dari *hypervisor* dimulai dengan inisialisasi yang dilakukan saat *booting* sistem (*hypervisor* akan dimuat). Selanjutnya, *hypervisor* akan membagi sumber daya fisik dari perangkat keras ke dalam beberapa bagian yang akan dialokasikan untuk setiap *virtual machine*. *Hypervisor* juga menyediakan *virtual interface* yang digunakan untuk komunikasi antara *physical machine* dan *virtual machine*. Pengelolaan *virtual machine* juga menjadi tanggung jawab dari *hypervisor*.

Referensi:

- P. Kirvan, B. Posey, and A. S. Gillis, “hypervisor,” techtarget.com. [Online]. Available: <https://www.techtarget.com/searchitoperations/definition/hypervisor>. [Accessed May 05, 2024].

5. *Software Defined Network* (SDN) termasuk salah satu pendekatan arsitektur jaringan yang memungkinkan pengelolaan jaringan menggunakan *software application*. SDN memisahkan lapisan kontrol dan lapisan data dengan menerapkan kontrol jaringan yang tersentraslisasi dengan bantuan SDN *controller*. Melalui SDN, jaringan dapat diprogram secara terpusat dengan menggunakan *open APIs*. SDN banyak digunakan oleh perusahaan karena dapat menerapkan aplikasi dengan lebih cepat dan mengurangi biaya pengoperasi secara keseluruhan. Selain itu, SDN juga digunakaan pada jaringan *cloud*.

Beberapa manfaat dari penerapan SDN adalah sebagai berikut:

- a. SDN memungkinkan manajemen jaringan secara terpusat dengan bantuan SDN *controller*.
- b. SDN menyediakan konektivitas jaringan yang lebih baik dan memungkinkan berbagi data dengan lebih cepat.
- c. Meningkatkan kualitas kemananan dengan menerapkan tingkat keamana yang berbeda pada setiap perangkat. Selain itu, SDN juga membeikan kontrol yang lebih leluasa kepada *administrator* jaringan.

- d. Penambahan, pengurangan, dan konfigurasi jaringan dapat dilakukan secara dinamis sesuai kebutuhan.

Meskipun memiliki banyak manfaat, SDN masih memiliki beberapa kekurangan seperti ketergantungan pada pusat jaringan. karena SDN dikonfigurasi di satu lokasi, maka jika SDN *controller* mengalami kegagalan, maka seluruh jaringan akan terpengaruh. Penggunaan SDN dalam skala yang besar juga belum didefinisikan secara tepat.

Referensi:

- “Software defined Networking(SDN)” [geeksforgeeks.org](https://www.geeksforgeeks.org/software-defined-networking/), May 2023. [Online]. Available: <https://www.geeksforgeeks.org/software-defined-networking/>. [Accessed May 05, 2024].

6. Dalam SDN, terdapat dua lapisan utama yang menjalankan fungsi yang berbeda, yaitu *control plane* dan *data plane*.

a. Control plane (lapisan kontrol).

Merupakan lapisan yang bertugas untuk mengatur dan mengelola lalu lintas jaringan. lapisan ini dikelola secara terpusat oleh SDN *controller*. SDN *controller* mendapatkan informasi mengenai keadaan jaringan dan menggunakan informasi tersebut untuk mengarahkan lalu lintas. Aktivitas yang terjadi pada lapisan kontrol adalah pembuatan *routing table* dan menetapkan kebijakan penanganan paket.

b. Data plane (lapisan data).

Merupakan lapisan yang bertugas untuk meneruskan lalu lintas jaringan berdasarkan instruksi yang diterima dari lapisan kontrol. Lapisan ini merupakan representasi dari perangkat keras seperti *router* dan *switch*. Dalam SDN, lapisan data diimplementasikan di perangkat keras yang disebut sebagai *software defined switch*. Aktivitas yang terjadi pada lapisan ini adalah penerusan paket, segmentasi dan penyusunan kembali data, serta replikasi paket.

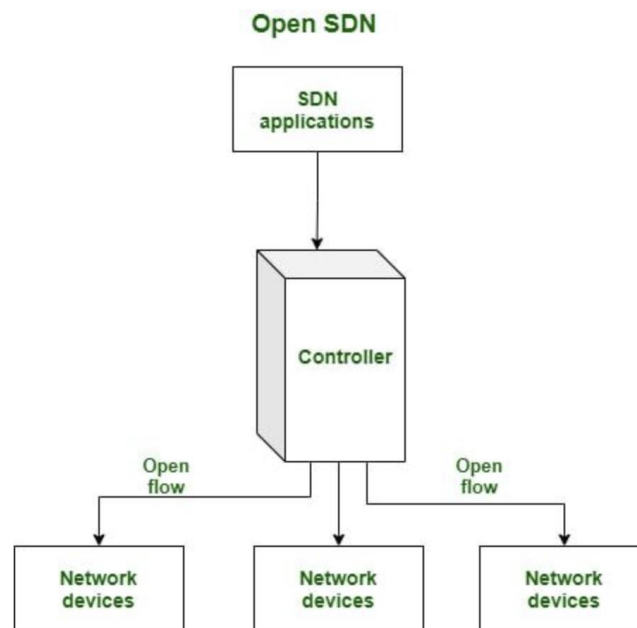
Referensi:

- “Software defined Networking(SDN)” [geeksforgeeks.org](https://www.geeksforgeeks.org/software-defined-networking/), May 2023. [Online]. Available: <https://www.geeksforgeeks.org/software-defined-networking/>. [Accessed May 05, 2024].

7. Tipe-tipe SDN:

a. Open SDN.

Merupakan jenis SDN yang menggunakan protokol terbuka, seperti OpenFlow. OpenFlow merupakan protokol komunikasi standar yang digunakan antara SDN *controller* dengan *software defined switch*. Dengan menggunakan protokol tersebut, SDN *controller* dapat memberikan instruksi ke *switch* untuk mengarahkan lalu lintas berdasarkan kebijakan yang telah ditetapkan. Menggunakan *open SDN*, perusahaan dapat membangun jaringan yang lebih terbuka dan fleksibel. Jenis ini memungkinkan adaptasi yang lebih cepat terhadap kebutuhan perusahaan yang terus berubah.



b. SDN via API.

Merupakan jenis SDN yang menggunakan API (*Application Programming Interface*) untuk memungkinkan komunikasi antara SDN *controller* dengan perangkat jaringan. beberapa protokol yang dapat digunakan adalah SNMP (*Simple Network Management Protocol*), CLI (*Command Line Interface*), dan REST (*Representational State Transfer*) API. Dalam jenis ini, setiap perangkat jaringan memiliki titik kontrol yang memungkinkan mereka untuk menerima instruksi dari SDN *controller* melalui API. Penerapan SDN melalui API memiliki kelebihan, yaitu memungkinkan SDN *controller* untuk memanipulasi perangkat dari jarak jauh (*remote*), sehingga pengaturan jaringan dapat dilakukan dengan lebih fleksibel.

c. Hybrid SDN.

Merupakan jenis SDN yang mengintegrasikan konsep jaringan tradisional dengan SDN dalam satu infrastruktur jaringan. misalnya suatu arus lalu lintas akan dikendalikan oleh SDN, sedangkan arus lalu lintas lainnya akan dikendalikan oleh protokol jaringan tradisional. Tujuan dari penggabungan

ini adalah untuk mendukung kebutuhan jaringan dalam skala yang lebih besar. Beberapa lokasi dapat saling terhubung dengan menggunakan jenis jaringan seperti VPN, *ethernet*, dan MPLS (*Multi-Protocol Label Switching*).

Tantangan dalam menggunakan *hybrid* SDN adalah pendekatan yang digunakan dapat menciptakan jaringan yang kompleks, sehingga *administrator* jaringan harus membiasakan diri dengan berbagai sistem yang akan digunakan. Selain itu, biaya yang diperlukan untuk menerapkan *hybrid* SDN juga lebih besar. Jenis ini sesuai untuk digunakan oleh perusahaan skala menengah hingga besar.

Referensi:

- “Software defined Networking(SDN)” [geeksforgeeks.org](https://www.geeksforgeeks.org/software-defined-networking/), May 2023. [Online]. Available: <https://www.geeksforgeeks.org/software-defined-networking/>. [Accessed May 05, 2024].
- Howard, “What Is Software-Defined Networking (SDN)?” [community.fs.com](https://community.fs.com/article/what-is-software-defined-networking-sdn.html), Jun. 2022. [Online]. Available: <https://community.fs.com/article/what-is-software-defined-networking-sdn.html>. [Accessed May 05, 2024].