PRAKTIKUM
DESAIN DAN MANAJEMEN JARINGAN KOMPUTER

Nama	**Aliyah Rizky Al-Afifah Polanda**	**No. Modul**	**07**
NPM	**2206024682**	**Tipe**	**Tugas Pendahuluan**

1. Syslog merupakan protokol standar yang digunakan untuk mengirimkan notifikasi kejadian dalam jaringan menuju ke perangkat yang berperan sebagai *collector*. Syslog menyediakan layanan untuk mengumpulkan informasi jaringan, memilih tipe informasi yang ingin dikumpulkan, dan menentukan perangkat tujuan yang akan menerima informasi yang telah dikumpulkan.

   NetFlow merupakan protokol yang dikembangkan oleh Cisco dan digunakan untuk mengumpulkan metadata mengenai IP traffic yang melintasi sebuah perangkat jaringan, seperti *router* atau *switch*. Perangkat jaringan yang mengaktifkan NetFlow akan menghasilkan metadata di tingkat *interface* dan mengirimkan informasi tersebut ke *flow collector*. *Flow collector* menyimpan informasi dan akan digunakan untuk melakukan analisis lalu lintas jaringan.

   SNMP (*Simple Network Management Protocol*) merupakan salah satu protokol jaringan yang bekerja pada *application layer* dan digunakan untuk memantau jaringan, mendeteksi kesalahan dalam jaringan, serta dapat digunakan dalam konfigurasi *remote devices*. SNMP menggunakan UDP *port* 161/162. Perangkat jaringan yang menerapkan SNMP dapat mengumpulkan informasi jaringan dari perangkat-perangkat dalam lingkungan LAN atau WAN dan mengirimkan informasi tersebut ke perangkat penerima.

   Referensi:

   - “Simple Network Management Protocol (SNMP),” geeksforgeeks.org, Jan.2024. [Online]. Available: https://www.geeksforgeeks.org/simple-network-management-protocol-snmp/. [Accessed Apr. 22, 2024].
   - “What is NetFlow? An Overview of the NetFlow Protocol,” kentik.com, Jul. 2023. [Online]. Available: https://www.kentik.com/kentipedia/what-is-netflow-overview/. [Accessed Apr. 22, 2024].
   - “What is Syslog server and its working ?,” geeksforgeeks.org, Aug. 2022. [Online]. Available:

https://www.geeksforgeeks.org/what-is-syslog-server-and-its-working/. [Accessed Apr. 22, 2024].

2. Syslog, SNMP, dan NetFlow digunakan dalam pemantauan dan pengelolaan jaringan. Perbedaan utama dari ketiga protokol tersebut adalah mengenai jenis informasi yang disediakan. Syslog menyediakan informasi menegenai *log* sistem, SNMP menyediakan informasi untuk manajemen perangkat jaringan, sedangkan NetFlow menyediakan informasi untuk analisis lalu lintas jaringan. Ketiganya juga dapat digunakan secara bersamaan untuk memantau dan mengelola jaringan secara lebih menyeluruh.

Aspek Perbedaan	Syslog	SNMP	NetFlow
Fungsi utama	*Monitoring* dan *troubleshooting*.	Memantau jaringan, mengidentifikasi masalah, dan mengelola konfigurasi perangkat jaringan.	Memantau lalu lintas jaringan dan mendeteksi kesalahan dalam jaringan.
Jenis informasi	Berupa pesan *log* yang memuat informasi waktu kejadian, sumber informasi, dan deskripsi.	Berupa informasi mengenai status dan kinerja perangkat jaringan.	Berupa informasi mengenai aliran data, seperti alamat IP, protokol, dan jumlah paket yang melintasi sebuah perangkat jaringan.
Keamanan	Tidak memiliki mekanisme kemanan bawaan	Keamanan diterapkan dengan menggunakan *community string* sebagai mekanisme autentikasi.	Memiliki mekanisme kemanan yang lebih tinggi.

Referensi:

- “Difference between SNMP and Syslog,” geeksforgeeks.org, Nov. 2022. [Online]. Available: https://www.geeksforgeeks.org/difference-between-snmp-and-syslog/. [Accessed Apr. 22, 2024].

3. Terdapat 3 komponen utama dalam SNMP, yaitu:

   a. SNMP *manager*.

      Merupakan bagian dari *Network Management System* (NMS). Digunakan untuk memantau jaringan dengan mengumpulkan informasi dari SNMP *agent* (perangkat jaringan yang menerapkan SNMP) dengan perintah "GET". Selain itu, SNMP *manager* dapat memodifikasi konfigurasi dari SNMP *agent* dengan menggunakan perintah "SET".

   b. SNMP *agent*.

      Memiliki tugas untuk menyediakan akses bagi SNMP *manager* ke MIB dan mempertahankan informasi jaringan yang berada dalam *database* perangkat jaringan. Informasi yang disediakan oleh SNMP *agent* dapat disaring berdasarkan keperluan dari SNMP *manager*. Informasi ini berguna untuk menentukan apakah terjadi *congestion* dalam jaringan atau tidak.

   c. MIB (*Management Information Base*).

      Merupakan tempat penyimpanan informasi jaringan yang akan dikelola. Setiap SNMP *agent* memiliki isi MIB yang berbeda-beda. MIB berisi informasi mengenai 8 kategori, yaitu sistem, *interface*, *address translation*, IP, UDP, EGP, ICMP, dan TCP. Selain itu, informasi yang ada dalam MIB dapat digunakan untuk mengautentikas *remote users*.

   Referensi:

   - "Simple Network Management Protocol (SNMP)," geeksforgeeks.org, Jan.2024. [Online]. Available: https://www.geeksforgeeks.org/simple-network-management-protocol-snmp/. [Accessed Apr. 22, 2024].

4. *Community string* merupakan *string* teks yang digunakan untuk autentikasi SNMP *manager*. SNMP *manager* yang ingin mengakses MIB dalam SNMP *agent* harus memiliki *community string* yang benar. *Community string* dikirimkan bersamaan dengan pesan GET *request*. Terdapat dua tipe dari com*munity string*: *Read-Only*, yang hanya menyediakan akses ke MIB namun tidak mengizinkan perubahan terhadap MIB, dan *Read-Write*, yang memberikan izin untuk mengakses dan memodifikasi MIB.

   Fungsi utama dari *community string* adalah untuk memungkinkan SNMP *manager* dalam mengakses informasi dari SNMP *agent*. Dengan *community string* yang tepat, SNMP agent dapat memantau kinerja jaringan dan mengelola konfigurasi perangkat jaringan. Selain itu, penggunaan *community string* dapat meningkatkan keamanan dengan memberikan perizinan yang berbeda kepada setiap SNMP *manager*

dan memastikan bahwa hanya SNMP *manager* yang sah yang dapat mengakses MIB.

Referensi:

- "SNMP Community Strings Tutorial and Monitoring Tool," dnsstuff.com, May, 2020. [Online]. Available: https://www.dnsstuff.com/snmp-community-string#what-is-an-snmp-community-string. [Accessed Apr. 22, 2024].

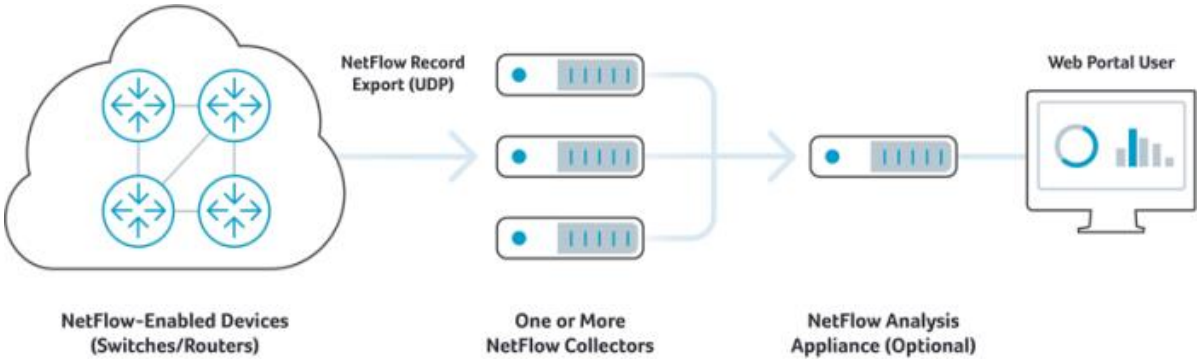
5. Tipe-tipe pesan dalam SNMP yang digunakan untuk berkomunikasi:
   a. **GetRequest**: digunakan untuk mengambil data dari SNMP *agents*.
   b. **GetNextRequest**: digunakan oleh SNMP *manager* untuk mendapatkan data selanjutnya yang diperlukan. SNMP *manager* tidak dapat mengakses data/nilai variabel yang diinginkan jika tidak mengetahui indeks dari variabel tersebut.
   c. **GetResponse**: digunakan oleh SNMP *agent* untuk merespon permintaan data dari SNMP *manager*. Berisi data-data yang diminta oleh SNMP *manager*.
   d. **SetRequest**: digunakan oleh SNMP *manager* untuk mengatur nilai dari objek MIB tertentu.
   e. **Trap**: merupakan pesan yang dikirimkan oleh SNMP *agent* tanpa adanya permintaan dari SNMP *manager*. Pesan ini akan dikirimkan saat munculnya kesalahan dalam jaringan.
   f. **InformRequest**: pesan ini mulai digunakan pada SNMPv2c dan digunakan untuk mengetahui apakah SNMP *manager* menerima pesan trap atau tidak.

   Referensi:

- "Simple Network Management Protocol (SNMP)," geeksforgeeks.org, Jan.2024. [Online]. Available: https://www.geeksforgeeks.org/simple-network-management-protocol-snmp/. [Accessed Apr. 22, 2024].

6. Terdapat tiga komponen dalam NetFlow, yaitu:
   a. **Flow exporter**: perangkat yang mengaktifkan NetFlow. Memiliki tugas untuk menghasilkan *flow records* dan mengirimkannya ke *flow collector* secara periodik.
   b. **Flow collector**: program yang bekerja pada sebuah *server*. Memiliki tugas untuk menerima dan menyimpan *flow records* yang dikirimkan oleh *flow exporter*.

c. **Flow analyzer**: aplikasi yang digunakan untuk menganalisis *flow records* dan mengubahnya ke bentuk laporan atau pesan peringatan.



Flow record berisi informasi mengenai aliran lalu lintas tertentu. Jika terdapat aliran lalu lintas baru yang melewati *flow exporter*, maka *flow record* akan dibuat dalam perangkat tersebut. *Flow records* akan dienkapsulasi dalam *datagram* UDP, untuk selanjutnya dikirimkan ke *flow collector*. *Flow records* yang diterima akan disimpan oleh *flow collector* dan dianalisis oleh *flow analyzer*.

Referensi:

- "What is NetFlow? An Overview of the NetFlow Protocol," kentik.com, Jul. 2023. [Online]. Available: https://www.kentik.com/kentipedia/what-is-netflow-overview/. [Accessed Apr. 22, 2024].

7. *Command* yang digunakan untuk mengetahui *host* yang melakukan *traffic* tertinggi dalam jaringan:

   Router# show ip flow top-talkers

   Referensi:

- "NetFlow Commands: cache through top," cisco.com. [Online]. Available: http://www.cisco.com/en/US/docs/ios/12_3t/netflow/command/reference/nfl_a1gt_ps5207_TSD_Products_Command_Reference_Chapter.html. [Accessed Apr. 22, 2024].

8. Sebuah *flow* siap dikirimkan ke *flow collector* jika memenuhi satu dari keberapa kondisi berikut:

   - *Flow* tidak aktif. Jika tidak ada paket baru yang diterima untuk *flow* tertentu selama periode waktu yang telah ditentukan oleh *flow exporter*, maka *flow* tersebut dianggap tidak aktif. Setelah *flow* tidak aktif, *flow records* dapat dikirimkan ke *flow collector*.

- *Flow* aktif, namun melebihi batas waktu yang ditetapkan dalam *active timer*. Hal ini dilakukan agar informasi mengenai aliran yang telah tersimpan untuk waktu yang cukup lama tidak hilang dan tetap dapat dianalisis.
- TCP *flag* mengindikasikan bahwa aliran telah berakhir atau dihentikan. Hal ini terjadi karena *flow* telah selesai dan informasi mengenai *flow* tersebut tidak lagi diperlukan untuk pengaturan koneksi.

Referensi:

- "What is NetFlow? An Overview of the NetFlow Protocol," kentik.com, Jul. 2023. [Online]. Available: https://www.kentik.com/kentipedia/what-is-netflow-overview/. [Accessed Apr. 22, 2024].