

MONITORING INTERFACES FASTETHERNET ON CISCO CATALYST 3750 TO ENSURE USE OF THE SECURITY COMPUTER NETWORK IN STTA COMPUTING LABORATORIES

Sudaryanto¹, Dwi Nurhayati²

Program Studi Informatika

Sekolah Tinggi Teknologi Adisutjipto

Jl. Janti, Blok R, Lanud Adisutjipto Yogyakarta

Email : ¹sudaryanto@stta.ac.id, ²nrhyt78@gmail.com

Abstract

Cisco is a company that concentrates on hardware and software related to computer networks. One of the hardware produced by Cisco is a switch device that can be used for management of a computer network. Many types of switches that have been produced by Cisco, one of which is the Cisco Catalyst 3750. In the configuration and monitoring of the Cisco Catalyst 3750 user / administrator must do management with command line based configuration. This is because Cisco has not facilitated its users with user interface based configurations. So the user is required to know the code syntax to execute a command on the switch. In this study, researchers will discuss how to create a user interface for monitoring web-based Fastethernet Interfaces on the Cisco Catalist 3750 and use notifications E-mail by utilizing an API to determine the up or down status of a network device. The results of the test show that the application can be monitored by the administrator remotely in real time, the user interface can run well on the personal computer browser and smartphone responsively.

Keywords: Port security, monitoring, interfaces ethernet, Cisco Catalyst 3750, API.

1. Pendahuluan

Penelitian penelitian sebelumnya banyak membahas tentang manajemen keamanan jaringan baik menggunakan port-port yang tersedia pada *switch* yaitu : *default / static port security, port security dynamic learning, sticky port security* [1], dan juga monitoring jaringan dengan menggunakan menggunakan SNMP [2][3], mikrotik [4], sms [5] dan menggunakan web [6] dimana monitoring jaringan menggunakan piranti mikrotik dengan api-mikrotik, belum ada penelitian yang memmanage dan memonitoring jaringan dengan menggunakan piranti *cisco* yang melibatkan *api-cisco*. [7][8] Dalam penelitiannya membahas tentang switch multilayer dan implementasi *port security* pada sistem keamanan jaringan untuk mengurangi pengguna yang memanfaatkan jaringan Laboratorium Komputasi untuk penggunaan *bandwidth* di luar perangkat komputer yang telah diijinkan atau didaftarkan, tetapi konfigurasinya masih secara manual yaitu menggunakan *command line*. Pada penelitian ini peneliti akan membahas tentang bagaimana membuat *user interface* untuk manajemen *Port Security* pada *Cisco Catalyst 3750* berbasis *web* sehingga konfigurasi dalam manajemen *Port Security Cisco* dapat beralih dari konfigurasi *command line* menjadi konfigurasi berbasis *User Interface* dan manajemen *Catalyst 3750* dapat dilakukan dari mana saja dan kapanpun.

Selain melakukan manajemen peneliti juga akan melakukan *monitoring* yang merupakan sebuah kegiatan yang bertujuan untuk memantau tentang perubahan status yang ada di suatu perangkat jaringan, sehingga penelitian ini mempunyai tujuan untuk *monitoring* perangkat *Cisco Catalyst 3750* secara *real time* dari tempat yang berbeda tanpa harus bersentuhan langsung dengan perangkatnya dengan menggunakan *web* dan *notifikasi E-mail*

sebagai monitoringnya. Banyak hal dalam jaringan yang bisa dimonitoring, salah satu diantaranya adalah status *up* atau *down* dari sebuah perangkat jaringan.

Adanya sistem manajemen berbasis *user interface (web)* dan monitoring dapat mempermudah administrator jaringan dalam memantau sistem jaringan yang berada di lapangan dari tempat yang berbeda tanpa harus mengecek secara berkala dan bersentuhan langsung dengan perangkat tersebut.

2. Metodologi Penelitian

2.1 Switch

Switch merupakan perangkat keras penghubung di dalam jaringan komputer yang lebih banyak digunakan saat ini dibandingkan *hub* [9]. Hal ini disebabkan karena dengan fungsi yang serupa dengan *hub*, *Switch* memiliki dua buah kelebihan utama dibandingkan *hub*. Kelebihan-kelebihan yang dimiliki oleh *switch* yaitu:

- a. *Switch* memiliki kemampuan untuk membaca alamat fisik (*MAC Address*) dari setiap komputer yang terhubung ke dalam *switch* bersangkutan. *Switch* menyimpan alamat fisik (*MAC Address*) dari setiap komputer yang terhubung ke dalam *switch* tersebut beserta dengan nomor *port switch* yang digunakan oleh komputer bersangkutan.
- b. *Switch* memiliki kemampuan untuk melakukan filter terhadap paket data yang keluar masuk *switch*. Hal ini akan memberikan keamanan paket data (terkait dengan pengendalian paket data di dalam jaringan komputer).

Switch bekerja di dua buah layer pada jaringan komputer, yaitu *Data Link Layer* dan *Physical Layer*. Pada *Data Link Layer*, terjadi proses pengecekan terhadap alamat fisik jaringan (*MAC Address*) untuk otentikasi alamat fisik komputer yang terhubung ke *switch*, untuk kemudian disesuaikan dengan alamat jaringan pada *Network Layer (IP Address)*. Pada *Physical Layer* terjadi proses pengolahan sinyal digital.

2.2 Port Security

Port Security membatasi jumlah *MAC address* yang diizinkan terhubung dengan tiap *port* dan juga dapat membatasi *MAC address* mana saja yang diizinkan [10][11].

2.3 Perangkat yang Dipergunakan

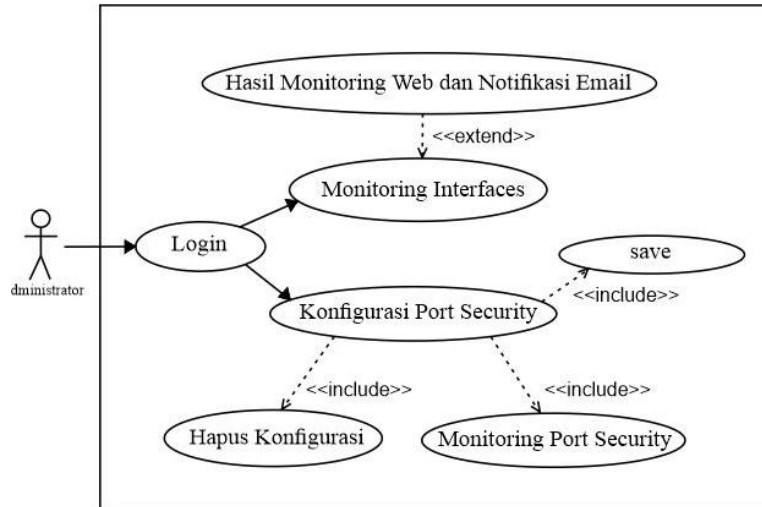
Dalam pembuatan sistem *management interfaces ethernet* diperlukan *hardware* dan *software* yang digunakan sebagai proses penunjang dalam pembuatan sistem *management interfaces ethernet*.

- a. *Hardware* (perangkat keras) merupakan komponen perangkat yang dapat dilihat secara kasat mata dan dapat disentuh secara fisik. Adapun spesifikasi *hardware* yang digunakan dalam pembuatan sistem ini, sebagai berikut:
 - 1) Cisco Catalyst 3750
 - 2) Laptop (HP Probook 4321S)
- b. *Software* (perangkat lunak) merupakan komponen yang tidak terlihat secara fisik, tetapi terdapat dalam sebuah komputer.
 - 1) Sistem Operasi Windows 10 Pro
 - 2) Bahasa Pemrograman PHP dan HTML

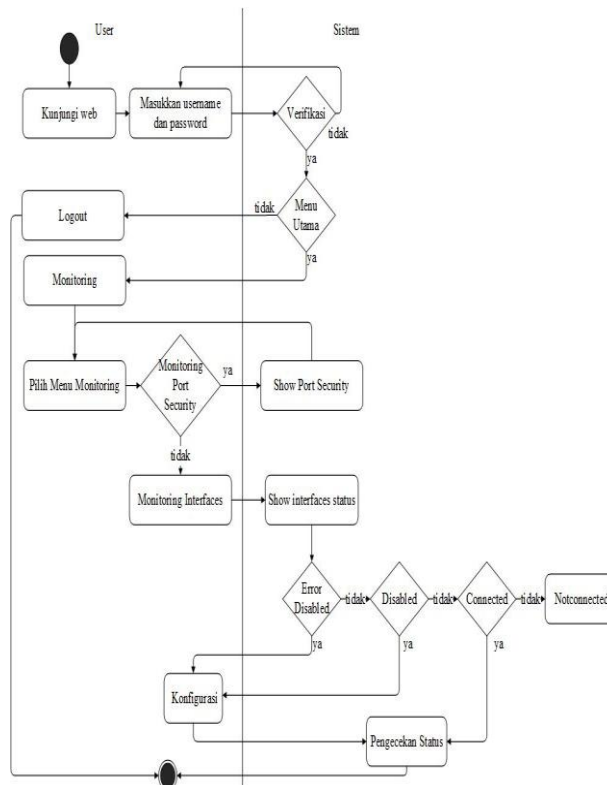
2.4 Metode Penelitian

Pada Gambar 1 dan 2 dijelaskan bahwa administrator bisa melakukan *monitoring* untuk mengetahui status *up* atau *down* dari sebuah perangkat jaringan melalui web dan notifikasi

email selain itu administrator juga bisa melakukan konfigurasi untuk melakukan perubahan status pada perangkat jaringan dari status *up* ke *down* ataupun sebaliknya.



Gambar 1. Use Case Diagram Sistem Management Interfaces Ethernet



Gambar 2. Activity Diagram Monitoring pada Sistem Management Interfaces Ethernet

3. Hasil dan Pembahasan

3.1 Pengujian interface fasethernet dengan Port Security

Pengujian dilakukan dengan cara tes ping pada setiap komputer untuk mengetahui balasan dari setiap kondisi. Pengujian dilakukan di laboratorium Komputasi Sekolah Tinggi Teknologi Adisutjipto seperti yang terlihat pada Gambar 3 dan Gambar 4.



Gambar 3. Laboratorium Komputasi STTA



Gambar 4. Switch Cisco Catalyst 3750

Pada pengujian ini, kondisi semua personal komputer belum terkonfigurasi *port security* dan diulang dengan kondisi semua personal komputer terkonfigurasi *port security*. Oleh karena itu, jika personal komputer melakukan *request* atau ping pada semua personal komputer dengan *network* yang sama maka akan mendapat balasan *reply*. Proses pengujian (ping) yang terlihat pada Gambar 5 dari personal komputer dengan IP address 10.10.10.1 dan diulang untuk 14 personal komputer yang IP address dan hasilnya dapat dilihat pada Tabel 1.

Tabel 1. Ping antar Komputer Tanpa dan Dengan Konfigurasi *Port Security*

```
C:\>ping 10.10.10.1
Pinging 10.10.10.1 with 32 bytes of data:
Reply from 10.10.10.1: bytes=32 time<2ms TTL=128
Reply from 10.10.10.1: bytes=32 time<1ms TTL=128
Reply from 10.10.10.1: bytes=32 time<1ms TTL=128
Reply from 10.10.10.1: bytes=32 time<1ms TTL=128
Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms
C:\>ping 10.10.10.2
Pinging 10.10.10.2 with 32 bytes of data:
Reply from 10.10.10.2: bytes=32 time<1ms TTL=128
Reply from 10.10.10.2: bytes=32 time<1ms TTL=128
Reply from 10.10.10.2: bytes=32 time<1ms TTL=128
Reply from 10.10.10.2: bytes=32 time<1ms TTL=128
Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 10.10.10.3
Pinging 10.10.10.3 with 32 bytes of data:
Reply from 10.10.10.3: bytes=32 time<2ms TTL=128
Reply from 10.10.10.3: bytes=32 time<1ms TTL=128
Reply from 10.10.10.3: bytes=32 time<1ms TTL=128
Reply from 10.10.10.3: bytes=32 time<1ms TTL=128
Ping statistics for 10.10.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms
C:\>ping 10.10.10.4
Pinging 10.10.10.4 with 32 bytes of data:
Reply from 10.10.10.4: bytes=32 time<1ms TTL=128
```

Gambar 5. Tes Ping antar komputer

| No | IP Tujuan | Interface | Hasil |
|-----|-------------|---------------------|-------|
| 1. | 10.10.10.1 | FastEthernet 5/0/1 | √ |
| 2. | 10.10.10.2 | FastEthernet 5/0/2 | √ |
| 3. | 10.10.10.3 | FastEthernet 5/0/3 | √ |
| 4. | 10.10.10.4 | FastEthernet 5/0/4 | √ |
| 5. | 10.10.10.5 | FastEthernet 5/0/5 | √ |
| 6. | 10.10.10.6 | FastEthernet 5/0/6 | √ |
| 7. | 10.10.10.7 | FastEthernet 5/0/7 | √ |
| 8. | 10.10.10.8 | FastEthernet 5/0/8 | √ |
| 9. | 10.10.10.9 | FastEthernet 5/0/9 | √ |
| 10. | 10.10.10.10 | FastEthernet 5/0/10 | √ |
| 11. | 10.10.10.11 | FastEthernet 5/0/11 | √ |
| 12. | 10.10.10.12 | FastEthernet 5/0/12 | √ |
| 13. | 10.10.10.13 | FastEthernet 5/0/13 | √ |
| 14. | 10.10.10.14 | FastEthernet 5/0/14 | √ |

3.2 Pengujian hubungan antara komputer setelah ditukar interfacenya

Pada pengujian ini, komputer yang seharusnya berada di *interface* FastEthernet 5/0/1 dipindah ke *interface* FastEthernet 5/0/20 dan begitu juga dengan *interface* yang lain. Oleh karena itu, jika personal komputer melakukan *request* atau ping pada semua personal komputer dengan *network* yang sama maka akan mendapat balasan *destination host unreachable* sekaligus *interface*-nya akan otomatis mati (*shutdown*). Hal ini dikarenakan MAC address yang baru masuk dibandingkan dengan MAC address yang

ada di *switching table* pada *interface* tersebut, jika *MAC address*-nya berbeda maka *action*-nya akan dijalankan. Proses pengujian (ping) yang terlihat pada Gambar 6 dari personal komputer(*server*) dengan *IP address* 10.10.10.63 dan diulang untuk 14 personal komputer yang *IP address* dan hasilnya dapat dilihat pada Tabel 2.

Tabel 2. Tes Ping antar Komputer setelah Ditukar *Interface*-nya

```
C:\>ping 10.10.10.1
Pinging 10.10.10.1 with 32 bytes of data:
Reply from 10.10.10.63: Destination host unreachable.
Reply from 10.10.10.63: Destination host unreachable.
Reply from 10.10.10.63: Destination host unreachable.
Reply from 10.10.10.63: Destination host unreachable.

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\>ping 10.10.10.2
Pinging 10.10.10.2 with 32 bytes of data:
Reply from 10.10.10.63: Destination host unreachable.
Reply from 10.10.10.63: Destination host unreachable.
Reply from 10.10.10.63: Destination host unreachable.
Reply from 10.10.10.63: Destination host unreachable.

Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\>ping 10.10.10.3
Pinging 10.10.10.3 with 32 bytes of data:
Reply from 10.10.10.63: Destination host unreachable.
Reply from 10.10.10.63: Destination host unreachable.
Reply from 10.10.10.63: Destination host unreachable.
Reply from 10.10.10.63: Destination host unreachable.

Ping statistics for 10.10.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\>ping 10.10.10.4
Pinging 10.10.10.4 with 32 bytes of data:
Reply from 10.10.10.63: Destination host unreachable.
Reply from 10.10.10.63: Destination host unreachable.
Reply from 10.10.10.63: Destination host unreachable.
Reply from 10.10.10.63: Destination host unreachable.

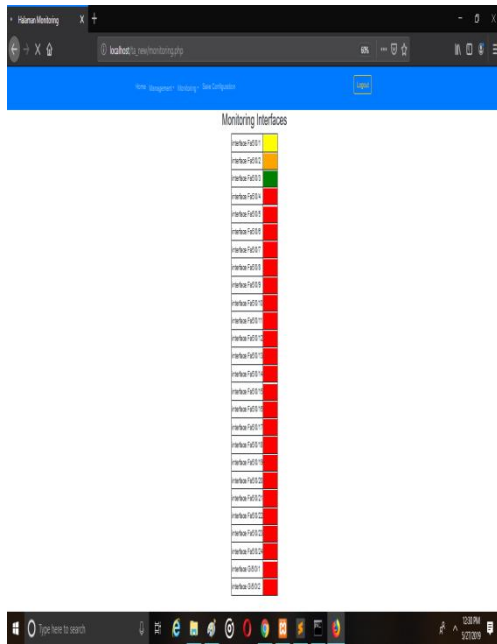
Ping statistics for 10.10.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Gambar 6. Tes Ping antar komputer

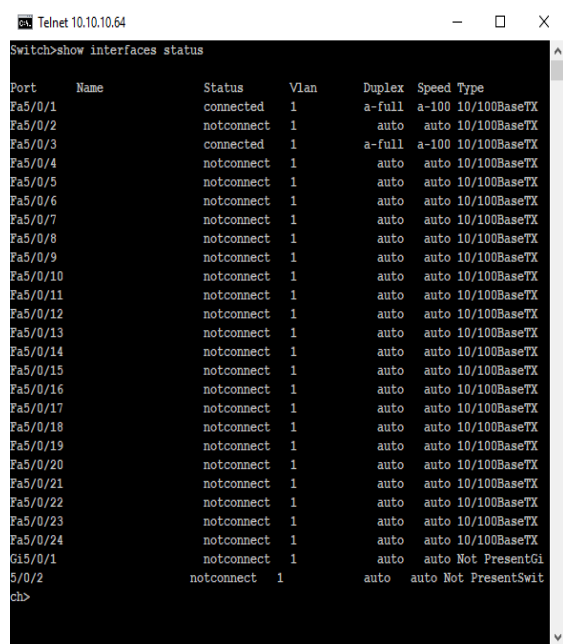
| No | IP Tujuan | Interface | Hasil |
|-----|-------------|---------------------|-------|
| 1. | 10.10.10.1 | FastEthernet 5/0/20 | x |
| 2. | 10.10.10.2 | FastEthernet 5/0/19 | x |
| 3. | 10.10.10.3 | FastEthernet 5/0/18 | x |
| 4. | 10.10.10.4 | FastEthernet 5/0/17 | x |
| 5. | 10.10.10.5 | FastEthernet 5/0/16 | x |
| 6. | 10.10.10.6 | FastEthernet 5/0/15 | x |
| 7. | 10.10.10.7 | FastEthernet 5/0/14 | x |
| 8. | 10.10.10.8 | FastEthernet 5/0/13 | x |
| 9. | 10.10.10.9 | FastEthernet 5/0/12 | x |
| 10. | 10.10.10.10 | FastEthernet 5/0/11 | x |
| 11. | 10.10.10.11 | FastEthernet 5/0/10 | x |
| 12. | 10.10.10.12 | FastEthernet 5/0/9 | x |
| 13. | 10.10.10.13 | FastEthernet 5/0/8 | x |
| 14. | 10.10.10.14 | FastEthernet 5/0/7 | x |

3.3 Tampilan *Monitoring Interfaces* di *Sistem Management Interface Ethernet* dan di *Command Line*

Tampilan *monitoring interfaces* digunakan untuk melihat status dari setiap *interface*. Status yang dimaksud dalam sistem ini adalah *connected*, *notconnected*, *disabled*, *error disabled*. Tampilan *monitoring interfaces* yang ada di sistem *management interfaces ethernet* seperti yang terlihat pada Gambar 7 menunjukkan bahwa status *connected* (warna hijau), *notconnected* (warna merah), *disabled* (warna orange), dan *error disabled* (warna kuning). Sedangkan tampilan yang terlihat pada Gambar 8 merupakan tampilan *monitoring interfaces* yang ada di *command line*, jika ingin melihat status dari *interfaces* maka harus mengetikkan perintahnya terlebih dahulu.



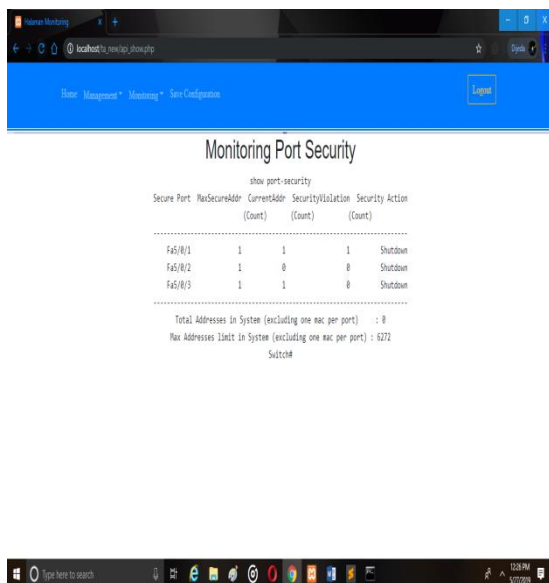
Gambar 7. Tampilan *Monitoring Interfaces* di *System Management Interface Ethernet*



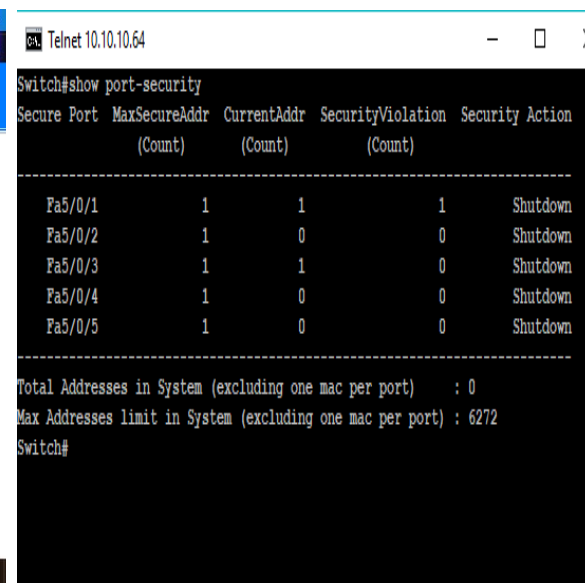
Gambar 8. Tampilan *Monitoring Interfaces* di *Command Line*

3.4 Tampilan *Monitoring Port Security* di *System Management Interface Ethernet* dan di *Command Line*

Tampilan *monitoring port security* digunakan untuk melihat status dari *interfaces* mana saja yang sudah ada konfigurasi *port security*-nya. Tampilan yang terlihat pada Gambar 9 merupakan tampilan *monitoring port security* di *system management interface ethernet*. Sedangkan pada Gambar 10 merupakan tampilan *monitoring port security* di *Command Line*.



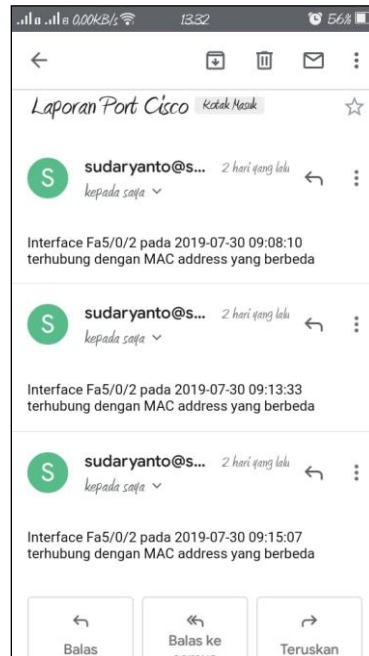
Gambar 9. Tampilan *Monitoring Port Security* di *System Management Interface Ethernet*



Gambar 10. Tampilan *Monitoring Port Security* di *Command Line*

3.5. Tampilan *Notification* pada E-mail

Notifikasi digunakan untuk memudahkan administrator dalam mengetahui perubahan yang terdapat di dalam perangkat Cisco Catalyst 3750, tampilan *notification* di Email dapat dilihat pada Gambar 7.



Gambar 7 Tampilan *Notification* pada Email

Dengan menggunakan *monitoring* berbasis *notifikasi E-mail* administrator tidak perlu selalu mengecek secara berkala untuk mengetahui terjadi perubahan aktifitas (status *up* dan *down*) ataupun penggunaan *port* yang tidak diijinkan pada sebuah perangkat jaringan (terhubungnya perangkat komputer dengan perangkat Cisco Catalyst 3750 dimana *MAC Address* yang ada di perangkat komputer tidak dikenali oleh perangkat Cisco Catalyst 3750) karena apabila terdapat perubahan tersebut maka sistem akan langsung mengirim *notifikasi* ke *E-mail* administrator yang sudah diatur dalam program. Selain itu administrator juga tidak perlu datang ke peralatan jaringan untuk memastikan bahwa kondisi peralatan sudah berjalan dengan baik atau tidak karena sudah bisa dilakukan dari jarak jauh secara *real time* baik konfigurasi *port* maupun *monitoring port interface Fastethernet*.

4 Kesimpulan

Berdasarkan hasil dari penelitian dengan judul “*Monitoring Interfaces Fastethernet On Cisco Catalyst 3750 To Ensure Use Of The Security Computer Network In Stta Computing*” maka dapat diambil beberapa kesimpulan sebagai berikut:

- a. Berdasarkan uji coba program yang telah dilakukan, didapatkan untuk melakukan konfigurasi dan *monitoring* administrator tidak perlu bersentuhan langsung dengan perangkat jaringan.
- b. Berdasarkan uji coba program yang telah dilakukan, didapatkan bahwa jika terjadi perubahan data di *table mac address* pada *switch port interface Fastethernet* maka port akan *shutdown*.

- c. Berdasarkan uji coba yang telah dilakukan, jika ada perubahan data di *table mac address* pada *switch* yang menyebabkan status *port Up* ataupun *Down*, sistem akan mengirimkan informasi perubahan ke *E-mail* yang sudah ditentukan.

Daftar Pustaka

- [1] Sulaiman, K. (2016). Analisis Sistem Keamanan Jaringan Dengan Menggunakan *Switch Port Security*. *CESS (Journal Of Computer Engineering, System And Science)* (Vol. 1, ISSN :2502-7131)
- [2] Pradikta, R., Affandi, A., & Setijadi, E. (2013). Rancang Bangun Aplikasi Monitoring Jaringan Dengan Menggunakan *Simple Network Management Protocol*. *Jurnal Teknik Pomits*, 2(1), 154-159.
- [3] Taftazanie, S., Prasetijo, A. B., & Widiyanto, E. D. (2017). Aplikasi Pemantau Perangkat Jaringan Berbasis *Web* Menggunakan Protokol Snmp Dan Notifikasi SMS. *Jurnal Teknologi dan Sistem Komputer*, 5(2), 62-68.
- [4] Rinaldo, R. (2016). Implementasi Sistem Monitoring Jaringan Menggunakan Microtik Router Os Di Universitas Islam Batik Surakarta. *Jurnal Emitor*, 16(2), 5-12.
- [5] Gobel. M. A. A., Sumarsono. S., & Indrianingsih. Y. (2012). *Notification Of Security Threats On The Internet Proxy Server Is A Server-Based Short Message Service (SMS)*. In *Compiler STT Adisutjipto Yogyakarta*, 1(1), 77-90.
- [6] Herliana, A., Rasyid, P.M. (2016). Sistem Informasi Monitoring Pengembangan *Software* Pada Tahap Development Berbasis *Web*. *Jurnal Informatika*, 3(1), 41-50.
- [7] Sudaryanto, S. (2018). *Implementation Port Security For Security System Network At The Computing Laboratory Of Adisutjipto Technology College*. In *Conference SENATIK STT Adisutjipto Yogyakarta*, 4, 257-265.
- [8] Sudaryanto, S. (2018). *The Effect Of Multi Layer Switch For Data Transfer Speeds On Computer Network*. In *Compiler STT Adisutjipto Yogyakarta*, 7(2), 85-90.
- [9] Pratama, I. P. A. E. (2014). *Handbook Jaringan Komputer Teori dan Praktik Berbasis Open Source*. Informatika. Bandung.
- [10] Sofana, I. (2015). *Membangun Jaringan Komputer Mudah Membuat Jaringan Komputer (Wire & Wireless) untuk Pengguna Windows dan Linux*. Cetakan Pertama. Informatika. Bandung
- [11] Sofana, I. (2012). *CISCO CCNP dan Jaringan Komputer (Materi Router, Switch, & Troubleshooting)*. Informatika. Bandung.
- [12] Sulaiman, O. K. (2016). Analisis Sistem Keamanan Jaringan Dengan Menggunakan *Switch Port Security*. *CESS (Journal Of Computer Engineering, System And Science)*, 1(1), 9-14.