IMPLEMENTASI SWITCH PORT SECURITY JARINGAN LAN MENGGUNAKAN SWITCH CISCO CATALYST 2960 PADA LINGKUNGAN FAKULTAS TEKNIK UNIVERSITAS DR SOETOMO

Wahyu Nur Febrian, Edi Prihartono, Anik Vega Vitianingsih
Teknik Informatika, Universitas Dr Soetomo
Jalan Semolowaru No. 84 Surabaya, Indonesia
wahyunur.febrian10@gmail.com

ABSTRAK

Keamanan jaringan merupakan aspek penting dalam menjaga stabilitas dan integritas infrastruktur jaringan di lingkungan akademik, termasuk di Fakultas Teknik Universitas Dr. Soetomo. Berdasarkan observasi awal, diketahui bahwa laboratorium komputer di fakultas tersebut belum menerapkan konfigurasi keamanan jaringan tingkat lanjut seperti port security pada perangkat switch, khususnya Cisco Catalyst 2960. Permasalahan ini menimbulkan potensi risiko terhadap akses ilegal dari perangkat yang tidak dikenal serta kerentanan terhadap gangguan jaringan. Penelitian ini bertujuan untuk mengkaji kondisi eksisting infrastruktur jaringan serta mengevaluasi urgensi dan kesiapan penerapan port security sebagai solusi peningkatan keamanan jaringan. Metode yang digunakan adalah *Network Development Life Cycle (NDLC)* dan kualitatif dengan pendekatan studi lapangan melalui wawancara terhadap pengelola laboratorium. Hasil penelitian ini menunjukan bahwa port security berhasil menutup koneksi pengguna asing yang mencoba masuk kedalam jaringan dan hanya port yang terdaftar yang diizinkan untuk akses kedalam jaringan. Secara teknis lingkungan jaringan memiliki potensi untuk dikembangkan melalui konfigurasi port security, penerapannya belum dilakukan karena belum adanya kebijakan teknis, pemahaman operasional, serta persepsi bahwa ancaman belum mendesak. Namun, sebagian besar pihak menyatakan dukungan terhadap implementasi fitur ini demi mencegah akses tidak sah dan meningkatkan kontrol jaringan di laboratorium.

Kata kunci : *Jaringan LAN, Port Security, Switch Cisco, Keamanan Jaringan, Laboratorium Komputer, NDLC.*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah mendorong institusi pendidikan untuk terus meningkatkan kualitas infrastruktur jaringan mereka. Salah satu bagian vital dari sistem informasi yang mendukung proses akademik dan administrasi adalah jaringan *Local Area Network (LAN)*. Jaringan LAN berperan penting dalam mendukung konektivitas antar perangkat komputer dalam satu institusi, khususnya di lingkungan fakultas yang memiliki laboratorium komputer aktif seperti Fakultas Teknik Universitas Dr. Soetomo.

Dalam konteks ini, keamanan jaringan menjadi hal yang sangat krusial. Meskipun jaringan LAN di Fakultas Teknik sudah dikelola secara terstruktur dengan pembagian per laboratorium sebanyak 20 PC, masih ditemukan berbagai celah keamanan yang belum ditangani secara optimal. Berdasarkan hasil wawancara yang dilakukan dengan pihak pengelola laboratorium, saat ini jaringan masih bersifat terbuka bagi seluruh mahasiswa kecuali saat praktikum, dan belum diterapkan pengamanan tingkat port seperti *Switch Port Security*. Selain itu, perangkat switch yang digunakan saat ini bukanlah tipe Cisco Catalyst 2960, melainkan D-Link, dikarenakan perangkat Cisco sebelumnya mengalami kerusakan. Padahal, Cisco Catalyst 2960 dikenal sebagai perangkat yang mendukung berbagai fitur keamanan canggih seperti *port security*, *MAC address filtering*, dan *access control list* (ACL).

Pengamanan terhadap port switch menjadi penting karena dapat mencegah perangkat ilegal atau tidak dikenal mengakses jaringan secara langsung. Penerapan fitur port security mampu membatasi jumlah perangkat yang terhubung pada sebuah port switch serta dapat memblokir koneksi mencurigakan, sehingga meningkatkan stabilitas dan integritas jaringan. Hasil wawancara menunjukkan bahwa belum diterapkannya port security disebabkan oleh beberapa faktor seperti kebijakan jaringan yang dikelola oleh UPT, minimnya urgensi dari segi keamanan, serta keterbatasan sumber daya teknis dan administratif di laboratorium.

Selain itu, terdapat berbagai tantangan teknis lain seperti seringnya perangkat switch meminta restart karena faktor usia, gangguan jaringan dari UPT, dan belum adanya dokumentasi resmi atas perangkat yang terhubung ke jaringan. Meskipun demikian, pihak pengelola laboratorium menyambut baik upaya implementasi port security dan menyatakan kesediaannya untuk dilakukan simulasi serta penerapan konfigurasi di masa mendatang.

Melalui penelitian ini, penulis ingin menganalisis sejauh mana potensi penerapan fitur port security pada perangkat switch Cisco Catalyst 2960 dalam lingkungan laboratorium Fakultas Teknik Universitas Dr. Soetomo. Pendekatan yang digunakan adalah metode Network Development Life Cycle (NDLC) dan kualitatif deskriptif dengan pengumpulan data melalui wawancara. Hasil dari penelitian ini diharapkan dapat memberikan rekomendasi yang

aplikatif untuk peningkatan keamanan jaringan secara menyeluruh serta membangun standar pengelolaan jaringan yang lebih baik di lingkungan akademik.

2. TINJAUAN PUSTAKA

2.1. Keamanan Jaringan Komputer

Keamanan jaringan komputer merupakan aspek penting dalam menjaga stabilitas dan kerahasiaan informasi yang ditransmisikan dalam sistem jaringan. Ancaman terhadap jaringan dapat berasal dari luar maupun dalam, seperti penyusupan ilegal, penyadapan data, hingga sabotase perangkat keras. Oleh karena itu, penerapan sistem keamanan jaringan menjadi bagian integral dari manajemen infrastruktur teknologi informasi. Penelitian terdahulu [1] menyatakan bahwa manajemen keamanan jaringan perlu melibatkan strategi yang menyeluruh, mencakup identifikasi risiko, pengendalian akses, serta penerapan sistem pengawasan terhadap aktivitas jaringan. Sistem keamanan jaringan yang terencana dan terimplementasi dengan baik akan mampu mengurangi risiko serta memastikan ketersediaan jaringan bagi pengguna yang sah.

2.2. Switch Cisco dan Port Security

Switch Cisco Catalyst, khususnya seri 2960, merupakan perangkat jaringan yang mendukung berbagai fitur keamanan seperti *VLAN, Access Control List (ACL),* dan *port security*. Salah satu fitur andalannya adalah *port security*, yang memungkinkan administrator jaringan untuk membatasi akses ke port berdasarkan alamat MAC yang terdaftar. Menurut penelitian terdahulu [2], penggunaan port security pada Switch Cisco dapat mencegah perangkat ilegal terhubung ke jaringan, serta memberikan perlindungan tambahan terhadap ancaman seperti spoofing dan sniffing. Implementasi port security juga memungkinkan sistem untuk secara otomatis menonaktifkan port ketika terdeteksi aktivitas mencurigakan, sehingga mencegah penyebaran serangan lebih lanjut.

Penelitian lain oleh [3] menunjukkan bahwa simulasi penerapan port security menggunakan Cisco Packet Tracer dapat memberikan pemahaman praktis dalam mengatur batasan akses dan merespons pelanggaran secara real time. Hasilnya memperlihatkan bahwa penggunaan port security mampu meningkatkan kontrol terhadap lalu lintas jaringan, terutama dalam lingkungan yang memiliki tingkat aktivitas dan pergantian perangkat tinggi, seperti laboratorium komputer di institusi pendidikan.

2.3. Implementasi Sistem Keamanan Jaringan

Implementasi sistem keamanan jaringan tidak hanya melibatkan perangkat keras, tetapi juga membutuhkan perencanaan dan kebijakan yang terintegrasi. Penelitian [4] menggabungkan metode *DHCP Snooping* dan port security dalam menjaga integritas jaringan, dengan hasil yang menunjukkan bahwa kombinasi tersebut efektif dalam mengidentifikasi dan memblokir perangkat yang tidak dikenal. Hal ini penting terutama dalam jaringan dengan lalu lintas padat dan terbuka untuk publik, seperti kampus atau laboratorium mahasiswa.

Selain itu, pada penelitian [5] menekankan pentingnya pengaturan firewall dan port security pada jaringan perusahaan untuk meminimalkan potensi akses tidak sah. Firewall bertindak sebagai penjaga lalu lintas antar jaringan, sedangkan port security berfungsi di tingkat perangkat switch. Kolaborasi antara keduanya menghasilkan sistem keamanan berlapis yang dapat diandalkan.

2.4. Studi Implementasi Cisco Catalyst 2960

Dalam studi mengenai implementasi perangkat jaringan Cisco Catalyst 2960 menegaskan bahwa perangkat ini sangat cocok digunakan untuk jaringan skala menengah hingga besar. Fitur manajemen dan keamanan yang terintegrasi di dalam switch seri ini memungkinkan fleksibilitas pengaturan serta efisiensi dalam distribusi jaringan [6]. Di sisi lain, menunjukkan bahwa penggunaan switch Cisco pada jaringan perusahaan mampu meningkatkan kecepatan transfer data serta kemudahan dalam pengaturan topologi jaringan yang kompleks [1].

Penelitian lain juga menekankan pentingnya pengaturan VLAN dalam mendukung keamanan jaringan. Meski tidak secara langsung membahas port security, penggunaan VLAN dapat mendukung implementasi segmentasi jaringan, sehingga bila digabungkan dengan port security, akan menghasilkan sistem keamanan yang lebih kokoh [7]

2.5. Perancangan Sistem Keamanan Jaringan

Perancangan sistem keamanan jaringan harus memperhatikan kebutuhan spesifik dari lingkungan jaringan yang digunakan. [2] menyusun perancangan sistem keamanan menggunakan Switch Cisco dengan pendekatan port security di perusahaan swasta. Hasilnya menunjukkan bahwa sistem ini tidak hanya mampu membatasi akses berdasarkan MAC address, tetapi juga meningkatkan efisiensi pengelolaan jaringan karena administrator dapat mengawasi dan mengatur setiap port secara individual. Dengan demikian, pendekatan serupa dapat diterapkan di lingkungan akademik, seperti laboratorium komputer, yang memiliki pola akses jaringan yang dinamis.

2.6. Analisis dan Evaluasi Sistem Keamanan

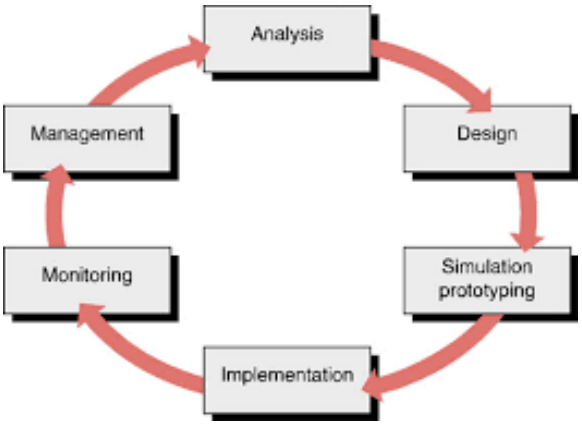
Analisis dan evaluasi terhadap sistem keamanan jaringan diperlukan untuk memastikan bahwa kebijakan yang diterapkan benar-benar efektif dalam mengantisipasi ancaman. [8] mengemukakan bahwa evaluasi keamanan jaringan sebaiknya dilakukan secara berkala melalui pemantauan lalu lintas data, identifikasi perangkat terhubung, serta pengujian terhadap kebijakan keamanan yang diterapkan. Dalam lingkungan laboratorium, pengawasan aktif sangat diperlukan mengingat akses jaringan yang cenderung terbuka, baik bagi mahasiswa maupun staf. Oleh

karena itu, sistem keamanan berbasis port security dapat dijadikan salah satu solusi utama yang dapat diimplementasikan secara bertahap.

3. METODE PENELITIAN

Metode yang dipakai dalam penelitian ini adalah metode *Network Development Life Cycle (NDLC)* yang dikombinasikan dengan pendekatan penelitian kualitatif deskriptif. *Network Development Life Cycle (NDLC)* merupakan metodologi pengembangan jaringan yang sistematis dan terstruktur, yang dirancang khusus untuk menganalisis, merancang, mengimplementasikan, dan mengevaluasi sistem jaringan komputer secara komprehensif [9].

Dalam konteks penelitian implementasi switch port security jaringan LAN menggunakan Switch Cisco Catalyst 2960 pada lingkungan Fakultas Teknik Universitas Dr Soetomo, metode NDLC menyediakan kerangka kerja yang ideal untuk memahami kompleksitas infrastruktur jaringan yang ada, mengidentifikasi kebutuhan keamanan yang spesifik, serta merancang solusi yang tepat sasaran dan dapat diimplementasikan secara efektif.



Gambar 1. NDLC

Pada gambar 1, dapat dilihat :

a. Analysis, Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul di Fakultas Teknik Universitas Dr Soetomo, analisa kebutuhan pengguna, dan analisa topologi jaringan yang sudah ada. Metode pada tahap ini diantaranya yaitu wawancara, survei langsung, membaca blueprint.
b. Design, Tahap perancangan (design) adalah membuat spesifikasi kebutuhan sistem dari hasil analisis sebagai masukan dan spesifikasi rancangan atau desain sebagai masukan dan spesifikasi rancangan atau desain sebagai solusi dari permasalahan. Spesifikasi desain sistem yang akan dibuat, dibentukan dengan merancang topologi sistem jaringan.
c. Simulation, Pada tahap ini penulis akan menganalisa dengan cara membuat dalam bentuk simulasi dengan bantuan tools khusus dibidang jaringannya, yaitu Cisco Packet Tracer
d. Implementation, Konfigurasi dan analisis yang meliputi proses instalasi dan konfigurasi terhadap rancangan topologi jaringan dan komponen jaringan yang perlu dilakukan konfigurasi diantaranya yaitu Switch dan Laptop. Proses instalasi dan konfigurasi dilakukan untuk menjamin konektifitas keseluruhan komponen jaringan agar dapat bekerja secara efektif.
e. Monitoring, yaitu melakukan pemantauan terhadap jaringan yang sudah di implementasikan pada tahapan sebelumnya. Mengecek terhadap penggunaaan konfigurasi Switch Port Security apakah ada permasalahan atau tidak. Serta permasalahan yang berpotensi menganggu jaringan tersebut
f. Management, dibuat untuk mengatur dan membuat sistem yang telah di buat dapat terjaga dengan baik sehingga diperlukan backup konfigurasi seperti log monitoring.

Dalam metode NDLC ini, dibuat model konseptual yang merupakan sebuah konsep yang terkait dengan studi literatur serta membantu peneliti untuk melihat permasalahan dengan sudut pandang yang berbeda. Model konseptual ini berfungsi sebagai representasi abstrak dari sistem jaringan yang akan dikembangkan, mencakup komponen-komponen utama seperti infrastruktur fisik, kebijakan keamanan, prosedur operasional, dan interaksi antar elemen sistem. Model konseptual juga menolong peneliti dalam menentukan inti permasalahan yang ada dan memberikan referensi untuk menyederhanakan permasalahan yang ada agar lebih mudah dipahami, terutama dalam konteks implementasi port security yang melibatkan aspek teknis, administratif, dan kebijakan institusional yang saling berinteraksi.[9]

Pemilihan metode NDLC dalam penelitian ini didasarkan pada karakteristik penelitian yang memerlukan pendekatan sistematis dan bertahap dalam menganalisis kondisi eksisting jaringan, merancang solusi keamanan, dan mengevaluasi efektivitas implementasi. NDLC memberikan struktur yang jelas untuk mengorganisir seluruh proses penelitian, mulai dari tahap analisis kebutuhan hingga evaluasi hasil implementasi, sehingga memungkinkan peneliti untuk melakukan kajian yang mendalam dan komprehensif terhadap setiap aspek yang terkait dengan implementasi port security di lingkungan akademik.

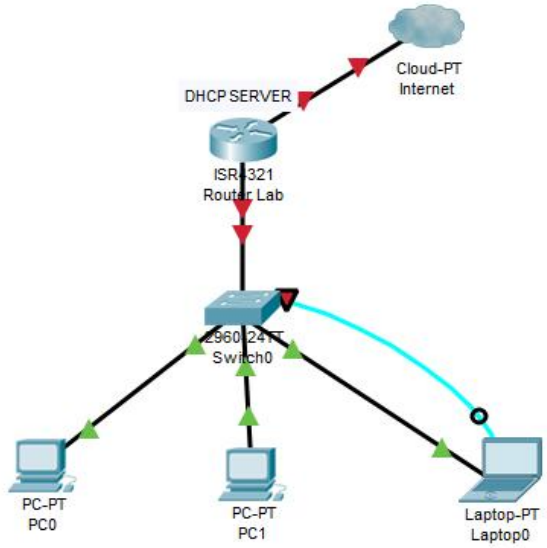
4. HASIL DAN PEMBAHASAN

4.1. Analisis Kebutuhan

Hasil wawancara dengan Kepala Laboratorium menunjukkan bahwa laboratorium komputer di Fakultas Teknik belum mengimplementasikan konfigurasi keamanan jaringan tingkat lanjut, salah satunya adalah fitur *port security* pada perangkat switch Cisco Catalyst 2960. Ketiadaan pengamanan ini membuka celah terhadap berbagai potensi ancaman, seperti akses ilegal dari perangkat yang tidak

dikenal, penyalahgunaan jaringan oleh pihak yang tidak berwenang, serta meningkatnya kerentanan terhadap gangguan internal maupun eksternal. Selain itu, kurangnya penerapan sistem keamanan berdampak pada lemahnya kontrol terhadap lalu lintas data dalam jaringan, sehingga berisiko mengganggu stabilitas dan kinerja sistem. Hal ini mengindikasikan perlunya peningkatan kebijakan keamanan, pembaruan konfigurasi perangkat jaringan, serta edukasi bagi pengelola laboratorium mengenai pentingnya perlindungan terhadap aset digital.

4.2. Desain



Gambar 2. Topologi

Pada gambar 2 dapat dilihat topologi atau desain ini menggambarkan sebuah sistem yang terdiri dari tiga komponen utama: router yang berfungsi sebagai DHCP server, switch model Cisco Catalyst 2960, dan perangkat end-user seperti laptop dan PC yang terhubung secara langsung dengan switch tersebut. Rangkaian ini dirancang untuk memberikan konektivitas yang efisien sekaligus fleksibel dalam pengelolaan jaringan, sejalan dengan kebutuhan pendidikan ataupun lab komputer yang dinamis.

Pada bagian pertama, router berperan sebagai DHCP server, yang bertugas untuk secara otomatis memberikan alamat IP kepada perangkat-perangkat end-user yang terhubung ke jaringan. Fungsi utama router ini adalah memanajemen alokasi IP secara dinamis kepada perangkat di jaringan tersebut, sehingga mengurangi beban kerja administrator dalam mengatur alamat IP secara manual. Selain itu, sebagai perangkat jaringan utama dalam topology ini, router juga bertanggung jawab untuk mengatur rute antar jaringan, sehingga memastikan data dapat mengalir secara lancar dari dan ke perangkat lain di luar jaringan lokal jika diperlukan, serta mengelola pengaturan jaringan secara umum agar tetap berjalan stabil dan aman.

Selanjutnya, switch Cisco Catalyst 2960 menjadi pusat penghubung bagi perangkat-perangkat end-user yang terdiri dari laptop dan PC, yang diwakilkan oleh L1, L2, dan PC1. Switch ini menghubungkan perangkat tersebut dalam satu LAN, memastikan komunikasi data yang cepat dan efisien antarmuka perangkat. Switch ini juga dilengkapi dengan fitur-fitur keamanan dan pengaturan VLAN yang memungkinkan segmentasi jaringan, sehingga jaringan dapat dibagi menjadi beberapa bagian sesuai kebutuhan, memberikan keamanan dan pengendalian akses yang lebih baik. Koneksi dari switch ke perangkat end-user dilakukan melalui port-ports tertentu, seperti port FastEthernet0/1 - 3, yang memudahkan pembatasan dan pengaturan trafik serta perangkat yang terhubung.

Penggunaan kabel FastEthernet yang menghubungkan perangkat end-user ke switch menunjukkan bahwa jaringan ini dirancang untuk kecepatan transfer data yang cukup tinggi dan kompatibel dengan perangkat modern. Sistem ini mengintegrasikan komunikasi dua arah yang efisien, memungkinkan pengguna seperti mahasiswa dan staf untuk berinteraksi secara simultan tanpa hambatan berarti. Keberadaan port-port tersebut juga mempermudah administrasi, termasuk pengaturan keamanan seperti port security, yang dapat membatasi jumlah perangkat yang terhubung maupun memblokir perangkat yang mencurigakan, sehingga menambah tingkat keamanan jaringan di lingkungan tersebut.

Secara keseluruhan, topologi jaringan ini menampilkan sebuah sistem yang sederhana namun sangat efektif untuk kebutuhan laboratorium komputer atau pengembangan jaringan di lingkungan pendidikan. Dengan konfigurasi seperti ini, administrator dapat dengan mudah mengelola IP, mengontrol akses perangkat, serta memastikan komunikasi yang lancar dan aman di antara perangkat-perangkat user yang terhubung. Keberadaannya juga memungkinkan pengembangan jaringan yang lebih luas dan kompleks di masa depan, dengan penambahan perangkat baru maupun segmentasi jaringan, tanpa perlu merombak struktur utama dari sistem yang sudah diimplementasikan. Pendekatan ini mendukung efisiensi, keamanan, dan fleksibilitas dalam mengelola infrastruktur jaringan di lingkungan edukasi maupun institusi lain yang sejenis.

4.3. Simulasi

Penggunaan switch port security didalam jaringan laboratorium dilakukan simulasi terlebih dahulu dengan menggunakan tools yang bernama cisco packet tracer, dengan menggunakan tools tersebut terlebih dahulu bertujuan agar penelitian mendapatkan Gambaran tentang penerapan switch port security tersebut

4.4. Implementasi

Gambar 3. Skenario

Pada gambar 3 dapat dilihat scenario implementasi pada penelitian ini menggunakan switch Cisco Catalyst 2960, 3 device end user 2 laptop + 1 PC, 1 router (berfungsi sebagai DHCP Server)

Konfigurasi router sebagai DHCP server yaitu yang pertama, administrator harus mengakses mode privileged dengan perintah enable, kemudian masuk ke mode konfigurasi global menggunakan configure terminal. Langkah ini merupakan langkah awal yang umum dilakukan untuk mengatur berbagai parameter penting pada router agar dapat berfungsi sesuai kebutuhan jaringan yang diinginkan. Untuk menerapkan konfigurasi tersebut menggunakan Syntax sebagai berikut :

```
Router> enable
Router# configure terminal
```

Selanjutnya, konfigurasi dilakukan pada interface FastEthernet0/0, yang menjadi penghubung utama antara router dan switch maupun perangkat lain dalam jaringan LAN. Di sini, alamat IP 192.168.1.1 beserta subnet mask 255.255.255.0 diberikan sebagai alamat IP dari interface tersebut. Perintah no shutdown digunakan untuk mengaktifkan interface agar dapat memulai proses komunikasi. Dengan konfigurasi ini, router dapat menjadi titik pusat pengendali jaringan dan sebagai gateway bagi perangkat-perangkat di jaringan tersebut. Untuk menerapkan konfigurasi tersebut menggunakan Syntax sebagai berikut :

```
! IP address di interface ke switch
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 no shutdown
```

Selanjutnya, konfigurasi DHCP dilakukan melalui pembuatan sebuah pool yang diberi nama LAN. Dalam pool ini, diatur bahwa alamat jaringan yang akan didistribusikan kepada perangkat-perangkat klient adalah 192.168.1.0 dengan subnet mask 255.255.255.0. Selain itu, dibuat pengaturan default gateway dengan memberikan alamat IP 192.168.1.1, yang merupakan alamat IP dari interface router, sehingga perangkat lain dapat mengarahkan lalu lintas mereka keluar jaringan lokal. Pengaturan DNS server juga disertakan dengan menggunakan server Google DNS 8.8.8.8, memastikan perangkat dapat melakukan pencarian domain dan pemetaan nama secara efisien.

Konfigurasi DHCP Server. Untuk menerapkan konfigurasi tersebut menggunakan Syntax sebagai berikut :

```
ip dhcp pool LAN
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 8.8.8.8
```

Terakhir, bagian konfigurasi mengatur pengecualian alamat IP tertentu dari distribusi DHCP, yaitu alamat IP 192.168.1.1 yang digunakan oleh router itu sendiri. Dengan perintah ip dhcp excluded-address 192.168.1.1, router tidak akan memberikan alamat IP tersebut kepada perangkat client ketika mereka meminta alamat secara otomatis. Ini adalah langkah penting untuk memastikan bahwa alamat IP yang vital untuk fungsi jaringan, seperti alamat gateway router, tidak akan dialokasikan kepada klien, sehingga menjaga kestabilan dan keamanannya. Secara keseluruhan, konfigurasi ini menyediakan fondasi yang lengkap bagi pengelolaan jaringan dinamis yang efisien dan aman, dengan pengaturan otomatis alamat IP dan pengelolaan trafik jaringan secara terintegrasi. Untuk menerapkan konfigurasi tersebut menggunakan Syntax sebagai berikut :

```
! Exclude address untuk router
ip dhcp excluded-address 192.168.1.1
exit
```

Setelah itu pengujian DHCP penting dilakukan untuk memastikan bahwa sistem jaringan berjalan secara otomatis dan efisien dalam memberikan alamat IP kepada perangkat yang terkoneksi. Pada proses ini, semua laptop dan PC yang terhubung ke jaringan laboratorium harus diatur agar memperoleh alamat IP secara otomatis melalui mode DHCP. Konfigurasi ini memastikan bahwa perangkat mendapatkan alamat IP dari router DHCP yang berada di jaringan, dalam hal ini 192.168.1.x, dimana 'x' adalah angka yang berbeda untuk setiap perangkat secara unik. Jika perangkat berhasil mengatur dan memperoleh IP secara otomatis dari DHCP, berarti sistem DHCP berjalan dengan baik dan mampu mendistribusikan alamat IP secara otomatis tanpa perlu pengaturan manual pada setiap perangkat. Hal ini menyederhanakan proses pengelolaan jaringan dan meminimalisasi kemungkinan kesalahan konfigurasi yang bisa terjadi bila pengaturan dilakukan secara manual.

Pada langkah selanjutnya, konfigurasi dilakukan untuk sekelompok port yang akan diamankan, misalnya port FastEthernet0/1 sampai 0/3. Dengan menggunakan perintah interface range FastEthernet0/1 - 3, administrator dapat mengatur beberapa port sekaligus, yang memudahkan proses

konfigurasi secara efisien. Setiap port tersebut kemudian diatur ke mode akses *(switchport mode access)* dan dikonfigurasikan ke VLAN tertentu, dalam hal ini VLAN 10, yang sesuai dengan kebutuhan jaringan di lingkungan tersebut. Konfigurasi ini memastikan bahwa port-port tersebut hanya mengizinkan lalu lintas dari perangkat yang terhubung sesuai dengan pengaturan VLAN dan keamanan yang diterapkan. Untuk menerapkan konfigurasi tersebut menggunakan Syntax sebagai berikut :

```
! Konfigurasi port Fa0/1 untuk laptop/PC
interface range FastEthernet0/1 - 3
 switchport mode access
 switchport access vlan 10
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 spanning-tree portfast
exit
```

Selain pengaturan dasar tersebut, fitur port security diaktifkan dengan perintah *switchport port-security*. Ini merupakan langkah utama dalam membatasi akses ke port secara spesifik berdasarkan MAC address, sebuah elemen penting dalam mencegah perangkat tidak sah mengakses jaringan. Pengaturan *maximum 1* merupakan batas maksimal jumlah MAC address yang diizinkan pada setiap port, sehingga hanya satu perangkat yang dapat terhubung dan berkomunikasi melalui port tersebut. Pengaturan ini sangat berguna di laboratorium atau lingkungan kantor yang menginginkan kontrol ketat terhadap perangkat yang terhubung ke jaringan.

Pengaturan *violation restrict* adalah salah satu cara untuk mengendalikan pelanggaran keamanan. Saat terjadi pelanggaran, misalnya perangkat yang terhubung memiliki MAC address yang berbeda dari yang terdaftar, port tidak akan langsung dimatikan, melainkan hanya dibatasi aksinya. Hal ini memungkinkan administrator untuk tetap memantau kejadian pelanggaran dan mengambil tindakan lebih lanjut jika diperlukan, tanpa mengganggu keseluruhan koneksi jaringan secara langsung. Pendekatan ini sangat berguna untuk menghindari gangguan besar yang bisa timbul akibat pelanggaran keamanan yang tidak terduga.

Fitur *mac-address sticky* menambah lapisan keamanan otomatis, di mana MAC address perangkat pertama yang terhubung ke port tersebut akan secara otomatis disimpan dan dikonfigurasi sebagai MAC address yang diizinkan oleh port security. Jadi, ketika perangkat baru terhubung, switch akan mengenali dan menyimpan MAC address perangkat tersebut secara otomatis tanpa perlu konfigurasi manual. Pengaturan ini sangat membantu dalam memudahkan administrasi dan memastikan bahwa hanya perangkat yang dikenal dan terdaftar yang dapat mengakses jaringan melalui port tertentu. Secara keseluruhan, konfigurasi port security ini menciptakan sistem keamanan dinamis dan otomatis yang mampu melindungi jaringan dari akses yang tidak diinginkan dengan efisiensi tinggi.

4.5. Pengujian

Pengujian port security dilakukan untuk memastikan bahwa mekanisme keamanan berfungsi sebagaimana mestinya. Skenario untuk memastikan port security berjalan, coba tukar laptop atau cabut dan ganti dengan laptop lain. Jika MAC-nya tidak cocok, port akan dibatasi (restrict). Tujuannya adalah untuk memverifikasi apakah port security mampu mendeteksi adanya perangkat baru yang mencoba terhubung melalui MAC address yang berbeda dari yang sebelumnya terdaftar atau sticky. Jika perangkat baru tersebut terdeteksi, maka sistem harus menanggapi sesuai dengan pengaturan violation yang telah dikonfigurasi, misalnya restrict atau shutdown.

Dengan cara ini, administrator dapat memastikan bahwa pengaturan port security dapat membatasi perangkat yang tidak dikenal dan mencegah akses tidak sah ke jaringan. Untuk mengecek status port security menggunakan perintah berikut :

```
Switch# show port-security interface fastEthernet 0/1
Untuk melihat semua port security:
Switch# show port-security
Switch# show port-security address
```

Verifikasi port security adalah langkah penting dalam memastikan bahwa konfigurasi keamanan yang telah diterapkan pada switch Cisco Catalyst 2960 berjalan dengan baik dan sesuai dengan yang diharapkan. Setelah melakukan konfigurasi pengamanan port, administrator perlu melakukan pengecekan secara konkret terhadap status port tertentu, misalnya port FastEthernet0/1.

Gambar 4. Perintah show port security

Pada gambar 4 dapat dilihat dengan menggunakan perintah show port-security interface fastEthernet 0/1, administrator dapat menampilkan detail terkait pengaturan port security yang aktif pada port tersebut, termasuk status keamanan, MAC address yang terdaftar, jumlah perangkat yang diizinkan, serta pelanggaran yang mungkin terjadi. Perintah ini sangat membantu dalam mengetahui apakah port tersebut sudah dikonfigurasi dengan benar dan berfungsi sesuai kebijakan keamanan yang diinginkan.

Selain meninjau port tertentu, administrator juga dapat melakukan pemeriksaan terhadap seluruh port yang diatur dengan port security di switch menggunakan perintah *show port-security*. Dengan menjalankan perintah ini, semua port yang memiliki pengaturan port security akan ditampilkan lengkap dengan status keamanan mereka, seperti apakah keamanan aktif, jumlah MAC address yang terdeteksi, dan bila ada pelanggaran yang terjadi. Data ini memberi gambaran lengkap tentang situasi port security di seluruh perangkat, sehingga memudahkan pengawasan dan identifikasi potensi masalah yang harus segera ditindaklanjuti. Informasi dari perintah ini sangat penting untuk memastikan bahwa tidak ada port yang tidak diinginkan atau berpotensi menjadi celah keamanan.

Selain itu, administrator juga dapat mengecek daftar MAC address yang saat ini terhubung dan diizinkan melalui port security dengan perintah *show port-security address*. Perintah ini menampilkan semua MAC address yang tercatat dan diizinkan pada port-port yang diamankan, termasuk MAC address yang disimpan secara otomatis melalui fitur sticky. Data ini sangat berguna untuk memverifikasi apakah perangkat yang terhubung sesuai dengan daftar yang diharapkan dan untuk mendeteksi keberadaan perangkat ilegal yang mungkin terhubung ke jaringan. Melalui informasi ini, administrator dapat melakukan audit berkala dan memastikan sistem port security berfungsi optimal.

Pentingnya verifikasi ini tidak hanya sebatas memastikan konfigurasi telah dilakukan, tetapi juga sebagai langkah pengawasan aktif yang memungkinkan deteksi dini terhadap pelanggaran keamanan. Jika terjadi pelanggaran, seperti MAC address yang tidak dikenali atau tidak terdaftar, administrator dapat segera mengambil tindakan untuk mengatasi masalah tersebut, baik dengan mencabut koneksi perangkat yang tidak dikenal maupun dengan melakukan penyesuaian konfigurasi apabila diperlukan. Dengan pemeriksaan rutin, keamanan jaringan dapat dipertahankan secara konsisten dan potensi ancaman dari perangkat yang tidak diotorisasi dapat diminimalkan, sehingga jaringan tetap terlindungi dan stabil.

Proses verifikasi port security sangat penting untuk menjaga integritas dan keamanan jaringan. Dengan menggunakan perintah-perintah yang tepat), administrator dapat memastikan bahwa pengaturan yang telah dilakukan berjalan sesuai harapan, dan menemukan serta menanggapi pelanggaran secara cepat dan efektif. Langkah ini merupakan bagian dari manajemen keamanan yang komprehensif, di mana pemantauan rutin dan pemeriksaan terhadap konfigurasi serta status port security membantu menjaga keandalan dan kerahasiaan jaringan di lingkungan laboratorium maupun perusahaan. Pendekatan ini mendorong implementasi kebijakan keamanan yang proaktif dan terukur, sehingga jaringan tetap aman dari ancaman internal maupun eksternal.

Pengujian lebih lanjut dilakukan dengan mengganti perangkat yang terhubung agar memastikan bahwa mekanisme violation berjalan sesuai pengaturan. Jika violation security dikonfigurasi sebagai 'restrict', maka port akan membatasi atau membatasi aktivitas perangkat baru tersebut tanpa menonaktifkan port secara permanen. Dengan demikian, perangkat yang tidak dikenal tidak dapat mengakses jaringan secara lengkap, tetapi port tetap aktif dan dapat dipantau. Sebaliknya, jika pengaturan violation adalah 'shutdown', maka port akan secara otomatis dinonaktifkan begitu perangkat yang tidak dikenal terdeteksi. Dalam kondisi ini, keamanan jaringan lebih ketat karena port akan benar-benar menonaktifkan akses perangkat asing dan memerlukan tindakan manual, seperti menggunakan perintah *shutdown* di CLI untuk menonaktifkan port secara permanen, dan kemudian perintah no *shutdown* untuk mengaktifkannya kembali setelah perangkat yang diizinkan terhubung.

Pengujian ini sangat penting untuk memastikan bahwa pengaturan port security bekerja secara efektif dalam mencegah koneksi perangkat yang tidak terotorisasi. Dengan menggunakan praktik seperti mengganti perangkat dan memantau respons sistem, administrator dapat menilai apakah konfigurasi yang diterapkan sudah mampu mengidentifikasi dan membatasi perangkat asing secara akurat. Hal ini juga membantu dalam mengidentifikasi potensi kelemahan sistem keamanan terkait konfigurasi violation yang digunakan, serta memastikan bahwa prosedur manual yang diperlukan untuk mengaktifkan kembali port berjalan dengan lancar jika terjadi pelanggaran. Ketika pengujian ini berhasil, maka sistem keamanan port security dapat diandalkan sebagai bagian dari strategi keamanan jaringan, melindungi jaringan dari ancaman dari perangkat tidak sah yang mencoba mengakses sumber daya jaringan secara ilegal.

Pengujian port security memastikan bahwa perangkat yang tidak sah dapat dibatasi atau bahkan secara otomatis dinonaktifkan agar tidak menimbulkan risiko keamanan. Melalui kedua proses pengujian ini, pihak pengelola jaringan dapat memastikan bahwa penerapan kebijakan keamanan dan konfigurasi jaringan berjalan efektif, serta mampu menghadapi berbagai situasi nyata yang mungkin terjadi. Jaringan ini dianggap penting dan tentunya juga diperlukan oleh berbagai jenis instansi termasuk pada sektor pendidikan. [10]

4.6. Monitoring

Melakukan pemantauan terhadap jaringan yang sudah di implementasikan pada tahapan sebelumnya. Mengecek terhadap penggunaaan konfigurasi Switch Port Security apakah ada permasalahan atau tidak. Serta permasalahan yang berpotensi menganggu jaringan tersebut.

4.7. Management

Menyusun kebijakan keamanan jaringan yang terintegrasi, melakukan pelatihan teknis bagi pengelola laboratorium, serta melakukan evaluasi berkala terhadap efektivitas sistem keamanan yang diterapkan untuk menjamin stabilitas dan integritas jaringan dalam mendukung aktivitas akademik dan penelitian di lingkungan Fakultas Teknik Universitas Dr Soetomo.

5. KESIMPULAN DAN SARAN

Berdasarkan wawancara dengan Kepala Laboratorium Fakultas Teknik Universitas Dr. Soetomo, diketahui bahwa laboratorium belum menerapkan keamanan jaringan tingkat lanjut, sehingga rentan terhadap perangkat tidak dikenal dan gangguan jaringan. Implementasi *switch port security* pada Cisco Catalyst 2960 berhasil membatasi akses hanya untuk perangkat yang terdaftar, dengan konfigurasi *MAC Address Sticky*, *Violation Restrict*, dan pembatasan satu perangkat per port. Sistem ini efektif mencegah akses ilegal dan meningkatkan kontrol jaringan. Namun, penerapannya masih belum optimal karena keterbatasan kebijakan teknis, pemahaman operasional, dan rendahnya kesadaran akan pentingnya keamanan jaringan. Penelitian selanjutnya disarankan untuk menggunakan teknologi lain sebagai cara untuk menambah kualitas jaringan agar lebih sesuai dengan kebutuhan dan karakteristik jaringan yang dimiliki.

DAFTAR PUSTAKA

[1] A. Pranata and R. R. Harahap, "PERANCANGAN SISTEM JARINGAN MENGGUNAKAN SWITCH CISCO PADA PT . PRIMA INDONESIA LOGISTIK," *J. Sci. Soc. Res.*, vol. VII, no. 3, pp. 855–860, 2024.

[2] L. Azharuddin, Jenih, T. Sugiarso, and T. Nurhastuti, "Perancangan dan Implementasi Sistem Keamanan Jaringan dengan Port Security Menggunakan Switch CISCO di PT. Citra Solusi Pratama," *J. Teknol. Inf.*, vol. 9, no. 1, pp. 56–68, 2024, doi: 10.52643/jti.v9i1.3175.

[3] A. Satria and F. Ramadhani, "Analisis Keamanan Jaringan Komputer dengan Menggunakan Switch Port Security di Cisco Packet Tracer," *J. Tek. Inform.*, vol. 2, no. 2, pp. 52–60, 2023, doi: 10.56211/sudo.v2i2.260.

[4] Y. C. Dara, F. Hariadi, and P. A. R. Lede, "Analisis Penerapan Sistem Keamanan Jaringan Menggunakan Metode DHCP Snooping dan Switch Port Security," *J. Inov. Wira Wacana*, vol. 01, no. 03, pp. 187–196, 2022, [Online]. Available: https://ojs.unkriswina.ac.id/index.php/inovatif/article/view/337

[5] S. Sutiman and A. Gunawan, "Firewall Port Security Switch Untuk Keamanan Jaringan Komputer Menggunakan Cisco Router 1600S Pada Pt. Tirta Kencana Tata Warna Sukabumi," *CONTEN Comput. Netw. Technol.*, vol. 1, no. 1, pp. 13–22, 2021, doi: 10.31294/conten.v1i1.402.

[6] M. Efendy dan M. M. Achlaq, "Implementasi Sistem Monitoring dan Backup Konfigurasi Perangkat Jaringan Menggunakan Librenms di PT. Data Utama Dinamika," *Smart Comp*, vol. 11, no. 4, pp. 668–673, Okt. 2022, p-ISSN: 2089-676X, e-ISSN: 2549-0796.

[7] Novinaldi, R. Nurbahri, and Ikhsan, "Perancangan dan Implementasi Virtual Local Area Network (Vlan) untuk," *J. LITEK J. List. Telekomun. Elektron.*, vol. 21, no. 1, pp. 26–31, 2024.

[8] Y. C. Dara, F. Hariadi, dan P. A. R. L. Lede, "Analisis Penerapan Sistem Keamanan Jaringan Menggunakan Metode DHCP-Snooping dan Switch-Port-Security," *JTIF | Jurnal Inovatif Wira Wacana*, vol. 1, no. 3, pp. 187–196, Des. 2022, p-ISSN: 2961-7316, e-ISSN: 2962-5998.

[9] Rosano, A., & Sudaradjat, D. (2024). Rancangan Power Management dengan Metode NDLC Berdasarkan Standar TIA-942 Tier 1 pada Unit Pusat Data PT. BPR Artha Sejahtera. REMIK: Riset dan E-Jurnal Manajemen Informatika Komputer, 8(2), 452-463

[10] Najib, Warsun. Panduan Praktikum Jaringan Komputer: Laboratorium Jaringan Komputer dan Aplikasi Terdistribusi. UGM PRESS, 2020.