IMPLEMENTASI KEAMANAN JARINGAN LAN BERBASIS VLAN STUDI KASUS STMIK WIDYA CIPTA DHARMA

Prasetyo Dwi Hidayat Paputungan[1)], Pitrasacha Adytia, S.T., M.T.[2)] dan Muhammad Fahmi, S.Kom., M.Kom[3)]
Program Studi Teknik Informatika, STMIK Widya Cipta Dharma
Jalan M. Yamin No. 25, Samarinda, 75123
E-mail : prasetyodwi0209@gmail.com

ABSTRAK

Jumlah pengguna yang terus bertambah menyebabkan masalah performa jaringan dan meningkatkan risiko keamanan. Untuk mengatasi tantangan ini, penelitian ini memusatkan perhatian pada desain dan implementasi Virtual *Local Area Network* (VLAN) dengan penggunaan *Router* MikroTik dan *switch* Cisco. Implementasi VLAN bertujuan untuk memisahkan segmen jaringan yang berbeda, mengoptimalkan penggunaan bandwidth, dan meningkatkan tingkat keamanan. Penelitian juga mencakup uji coba keamanan jaringan VLAN untuk mengidentifikasi potensi serangan seperti VLAN *hopping* dan spanning tree protocol attack. Penelitian ini bertujuan untuk meningkatkan performa dan keamanan jaringan di STMIK Widya Cipta Dharma yang telah menghadapi kendala dalam hal besarnya Broadcast Domain dan rentan terhadap serangan di jaringan LAN. Hasil penelitian ini diharapkan akan memberikan kontribusi positif dalam meningkatkan performa dan keamanan jaringan di STMIK Widya Cipta Dharma.

Kata Kunci : *VLAN, Jaringan, GNS3, MikroTik*

PENDAHULUAN

1.1. Latar Belakang Masalah

Dalam dunia teknologi informasi, keamanan jaringan merupakan salah satu hal yang sangat penting. Banyak instansi yang memiliki jaringan komputer dengan jumlah pengguna yang sangat besar. Seiring dengan bertambahnya jumlah pengguna, maka resiko terjadinya gangguan keamanan pada jaringan juga semakin besar. Oleh karena itu, dibutuhkan sebuah sistem keamanan jaringan yang handal dan efektif untuk menghindari terjadinya kerugian atau bahaya pada suatu instansi. Keamanan jaringan sendiri pada saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan sistem saat ini menjadi suatu garapan yang membutuhkan biaya penanganan dan proteksi yang sedemikian besar.

Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) merupakan salah satu perguruan tinggi di Kota Samarinda, Kalimantan Timur. Sebagai institusi pendidikan yang bergerak pada bidang IT perlunya sistem jaringan yang aman dan stabil untuk mendukung layanan administrasi kampus dan pembelajaran bagi dosen maupun mahasiswa. STMIK Widya Cipta Dharma sendiri sudah menerapkan sistem model jaringan LAN (*Local Area Network*) dengan dua ISP berbeda yang tidak saling terhubung atau berdiri sendiri.

Salah satu solusi yang dapat digunakan untuk mengamankan jaringan adalah dengan menggunakan teknologi Virtual *Local Area Network* (VLAN). VLAN merupakan sebuah teknologi yang memungkinkan pengelompokan beberapa perangkat dalam sebuah jaringan lokal yang dapat berkomunikasi satu sama lain dengan cara yang aman. Dengan menggunakan VLAN, perangkat-perangkat dalam jaringan dapat diisolasi dan hanya dapat berkomunikasi dengan perangkat lain yang berada pada VLAN yang sama. Hal ini dapat membantu mencegah serangan jaringan seperti hacking dan serangan virus.

Meskipun jaringan VLAN telah memiliki tingkat keamanan yang cukup baik namun masih perlu diuji dengan beberapa serangan dari pihak luar. Beberapa serangan yang mampu mengganggu adalah VLAN *hopping* dan *spanning tree protocol attack*. Pramawahyudi, dkk (2020), mengatakan bahwa VLAN *hopping* bertujuan untuk membuat penyerang mendapatkan akses dari satu VLAN ke VLAN lainnya, sedangkan *spanning tree protocol attack* melibatkan seorang penyerang yang akan mengambil alih hak akses *root bridge* pada sebuah topologi.

Dalam penelitian akan dilakukan implementasi jaringan VLAN dan *spanning tree protocol* menggunakan aplikasi GNS 3 serta menguji jaringan VLAN dan *spanning tree protocol* dari aspek sistem keamanannya.

Berdasarkan beberapa uraian diatas, maka diambilah judul Proposal Skripsi "Impelementasi Keamanan Jaringan LAN Berbasis VLAN Studi Kasus STMIK Wicida".

1.2. Rumusan Masalah

Berdasarkan latar belakang di atas maka terdapat rumusan masalah yang dapat di bahas adalah sebagai berikut: "Bagaimana mengimplementasikan keamanan jaringan LAN berbasis VLAN studi kasus STMIK WICIDA".

1.3. Batasan Masalah

Berdasarkan rumusan masalah di atas, terdapat beberapa Batasan masalah agar ruang lingkup penelitian tidak terlalu luas. Beberapa Batasan masalah tersebut adalah sebagai berikut:

1. Rancangan *topologi* berdasarkan *topologi* yang sudah ada sebelumnya.
2. Implementasi jaringan VLAN dan *Spanning Tree protocol* menggunakan aplikasi GNS 3 untuk menguji jaringan *VLAN Hopping* dan *Spanning Tree Protocol Attack* dari sistem keamanan.
3. Konfigurasi VLAN dilakukan secara langsung di *router* dan *switch* PUSKOM WICIDA.

1.4. Tujuan Penulisan

Tujuan dari penelitian ini adalah sebagai berikut:

1. Merancang jaringan VLAN menggunakan simulator jarigan GNS 3.
2. Meningkatkan sistem keamanan jaringan VLAN.

1.5. Manfaat Penelitian

Penelitian ini sebagai pengembangan pengetahuan suatu bidang keilmuan yang sudah ada, diharapkan memberikan manfaat bagi semua pihak yang berkaitan terutama mahasiswa, dosen, dan staff di STMIK WICIDA, berikut manfaatnya antara lain:

1. Meningkatkan keamanan jaringan di STMIK Widya Cipta Dharma.
2. Meningkatkan kestabilan koneksi jaringan di STMIK Widya Cipta Dharma.
3. Memberikan informasi dan pemahaman tentang teknologi VLAN dan mengimplementasi keamanan jaringan bebasis VLAN.
4. Meningkatkan kualitas hotpsot WICIDA.

1.6. Sistematika Penulisan

Bab ini menjelaskan latar belakang masalah mengapa perlunya Inkubator Penetas Telur Dengan Rak Otomatis Berbasis Mikrokontroler bagi para peternak perumusan masalah, batas masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

TINJAUAN PUSTAKA

2.1. Kajian Empirik

Kajian empirik dilakukan terhadap 3 penelitian terdahulu yang diuraikan sebagai berikut :

Sumber : Julandra, dkk 2022 Analisis dan Perancangan Jaringan Local Area Network Pada Lab Komputer Di SMK Negeri 5 Kota Serang.

Rokim dan Nainggolan 2021 Pemanfaatan Manajemen Jarngan Menggunakan Virtual Local Area Network (VLAN) Pada PT. Jantra Reka Saksanamas Cengkareng Timur Jakarta Barat.

Setiawan, dkk 2022 Desain Infrasttuktur Jaringan inter-Vlan Dengan Keamanan Port Security dan Secure Shell Berbasis Protocol Open Short Path First.

Perbedaan penelitian Menurut Julandra, dkk (2022), pada penelitiannya yang berjudul Analisis dan Perancangan Jaringan Local Area Network Pada Lab Komputer Di SMK Negeri 5 Kota Serang, Berdasarkan hasil pembahasan dapat diberikan yaitu analisis dan perancangan jaringan local area network pada laboratorium SMK Negeri 5 Kota Serang. Menurut Rokim dan Nainggolan (2021), pada penelitiannya yang berjudul Pemanfaatan Manajemen Jarngan Menggunakan

BAB I PENDAHULUAN

Dalam bab ini berisi tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Dalam bab ini penulis akan menjelaskan teori-teori dari rancang bangun inkubator penetas telur , alat apa saja yang akan digunakan untuk merancang penelitian.

BAB III METODE PENELITIAN

Dalam bab ini memberikan penelitian dan menjelaskan tentang metode penelitian untuk penyusunan skripsi ini yang meliputi tempat dan waktu penelitian, teknik pengumpulan data dan teknik analisa data.

BAB IV PEMBAHASAN

Dalam bab ini akan menjelaskan perancangan mulai dari perancangan inkubator hingga pemrogramman pada rak otomatis yang akan dijabarkan secara menyeluruh dan memaparkan hasil dari penelitian.

BAB V PENUTUP

Dalam bab ini akan menjelaskan kesimpulan akhir dari perancangan inkubator penetas telur dengan rak otomatis berbasis mikrokontroler serta saran untuk mengembangkan penelitian ini

.

Virtual Local Area Network (VLAN) Pada PT. Jantra Reka Saksanamas Cengkareng Timur Jakarta Barat, berdasarkan hasil penelitian yang dilakukan Router mikrotik RB941-2nd sebagai router usulan sudah dapat mengatasi kekurangan router tp-link yang sebelumnya digunakan pada perusahaan tersebut, yang mana belum bisa mengatur kecepatan. Menurut Setiawan, dkk (2022), pada penelitiannya yang berjudul Desain Infrasttuktur Jaringan inter-Vlan Dengan Keamanan Port Security dan Secure Shell Berbasis Protocol Open Short Path First, sistem hasil penelitian ini dapat menarik kesimpulan bahwa sistem hasil penelitian ini dapat digunakan Tingkat keberhasilan dalam pengiriman data dengan menggunakan InterVLAN berbasis Open Short Path First sebesar 100%, tidak ada paket data yang hilang atau packet loss, data yang dikirimkan dengan menggunakan metode tersebut dapat dikirim meskipun dengan VLAN yang berbeda, dan dengan jumlah paket data yang dikirimkan dalam skala besar.

2.2. Kajian Teoritis

2.2.1. Jaringan Komputer

Menurut Amala, dkk (2023), Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung dalam satu kesatuan. Informasi dan data bergerak melalui kabel-kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama dan bersama-sama menggunakan hardware dan software yang terhubung dengan jaringan.

2.2.2. Topologi Jaringan

Menurut Dharmalau, dkk (2022), Topologi jaringan merupakan gambaran perencanaan hubungan antar komputer dalam Local Area Network, yang meliputi komputer server, komputer client/workstation, hub/switch, pengkabelan, dan komponen jaringan yang lain.

2.2.3. Hardware Jaringan

Menurut Buana, dkk (2023), Membangun suatu jaringan, baik itu bersifat LAN (Local Area Network) maupun WAN (Wide Area Network), kita membutuhkan media baik hardware maupun software.

2.2.4. Sniffer

Menurut Rahmat, dkk (2022), Sniffer adalah orang yang melakukan proses pengendusan paket data pada sistem jaringan komputer, yang diantaranya dapat melakukan monitoring dan menangkap semua lalu lintas jaringan yang lewat tanpa peduli kepada siapa paket itu dikirimkan.

2.2.5. Keamanan Jaringan

Menurut Kusuma (2021), Keamanan Jaringan adalah konsep untuk mencegah pengguna yang tidak sah masuk ke dalam sistem jaringan komputer. Sistem tetap harus dilindungi dari segala macam serangan dan usaha penyusupan atau pemindaian oleh pihak yang tidak memiliki hak. Keamanan jaringan berfungsi untuk mengantisipasi resiko-resiko yang akan terjadi pada jaringan komputer yang dapat mengganggu aktivitas yang sedang terjadi pada sistem jaringan komputer. Ada tiga hal dalam konsep keamanan jaringan, yaitu bahaya, ancaman, dan kerapuhan sistem.

2.2.6. VLAN

Menurut Nukman, dkk (2023), VLAN merupakan suatu model jaringan yang tidak terbatas pada lokasi fisik seperti LAN, hal ini mengakibatkan suatu *network* dapat dikonfigurasi secara *virtual* tanpa harus menuruti lokasi fisik peralatan. Penggunaan *VLAN* akan membuat pengaturan jaringan menjadi sangat fleksibel dimana dapat dibuat segmen yang bergantung pada organisasi atau departemen, tanpa bergantung pada lokasi *workstation.* Perbedaan yang sangat jelas dari model jaringan *Local Area Network* adalah bahwa bentuk jaringan dengan model *Local Area Network* sangat bergantung pada letak/fisik dari *workstation,* serta penggunaan hub dan *repeater* sebagai perangkat jaringan yang memiliki beberapa kelemahan. Sedangkan yang menjadi salah satu kelebihan dari model jaringan dengan *VLAN* adalah bahwa tiap-tiap *workstation/user* yang tergabung dalam satu *VLAN* bagian (organisasi, ataupun kelompok) dapat tetap saling berhubungan walaupun terpisah secara fisik.

2.2.7. VLAN *Hopping*

Menurut Hariadi (2021), VLAN Hopping adalah jenis serangan jaringan dimana penyerang mencoba untuk mendapatkan akses ke jaringan VLAN dengan mengirimkan paket ke jaringan VLAN lain yang terhubung dengan penyerang. Dalam jenis serangan ini, penyerang dengan jahat mencoba untuk mendapatkan akses ke lalu lintas yang datang dari VLAN lain dalam jaringan atau dapat mengirim lalu lintas ke VLAN lain di jaringan itu, yang tidak memiliki akses legal. Dalam kebanyakan kasus, penyerang hanya mengeksploitasi 2 lapisan yang membagi berbagai host. Serangan ini memungkinkan penyerang jahat mendapatkan akses ke jaringan secara ilegal. Penyerang kemudian dapat mengambil kata sandi, informasi pribadi, atau data lain yang dilindungi. Demikian pula, mereka juga dapat memasang malware dan spyware, menyebarkan trojan horse, worm, dan virus, atau mengubah dan bahkan menghapus informasi penting.

2.2.8. *Spanning Tree Protocol*

Menurut Subli, dkk (2022), Spanning Tree Protocol adalah sebuah protokol yang digunakan untuk mencegah terjadinya network loop, dengan cara menemukan redundant link, lalu mengebloknya hingga redundant link tersebut benar-benar dibutuhkan.

2.2.9. *Spanning Tree Protocol Attack*

Menurut Renwarin dan Radiyah (2021), Serangan spanning tree protocol merupakan jenis serangan cyber yang mengeksploitasi kerentanan di STP untuk mengganggu atau merusak topologi jaringan. Proses serangan spanning tree protocol dimulai dengan penyerang mengirimkan BPDU (bridge protocol data unit) palsu ke dalam jaringan. BPDU ini berisi informasi palsu tentang nilai Bridge ID, Root Bridge, atau designated port. Dengan menggunakan BPDU manipulatif, penyerang dapat menciptakan situasi dimana switch lain dalam jaringan memilih jalur yang sebenarnya tidak optimal atau bahkan membentuk loop.

2.2.10. *Network Development Life Cycle* (NDLC)

Menurut Mutaqin (2017), NDLC adalah salah satu metode yang dilakukan dalam pengembangan metode dalam jaringan. Metode pengembangan sistem yang digunakan adalah metode Network Development Life Cycle (NDLC), dimana NDLC memiliki enam (6) tahapan, tahapan-tahapan yang dimaksud adalah sebagai berikut:

1. Analisa, pada langkah pertama yang dilakukan yaitu menganalisis kebutuhan, menganalisa kebutuhan pengguna, serta menganalisa bentuk topologi jaringan yang sedang digunakan.
2. Desain, informasi yang sudah dikumupulkan dalam desain ini akan dibuat rancangan desain topologi, diharapkan dari rancangan ini dapat mendukung rancangan seluruhnya dari apa yang dibutuhkan.
3. Simulasi prototype, rencana ini ditujukan untuk memantau cara kerja awal suatu jaringan yang akan dirancang juga untuk materi presentasi dan sharing dengan setiap teamwork.
4. Implementasi, pada titik ini tentu menghabiskan banyak waktu daripada langkah sebelumnya, saat implememtasi para ahli tentu saja mengimplementasikan seluruh rencana yang sudah dibangun sebelumnya. Implementasi adalah langkah yang begitu menentukan sukses atau tidaknya suatu proyek yang tengah dibuat, juga pada tahap inilah

menguji di lapangan dengan tujuan agar berbagai isu teknis dan non-teknis selesai.

5. Monitoring, setelah implementasi tahapan monitoring merupakan tahapan yang penting agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginanan dan tujuan awal dari user pada tahap awal analisis, maka perlu dilakukan kegiatan monitoring.
6. Management, di manajemen ketentuan harus diterapkan supaya sistem yang sudah dibuat dan dijalankan dengan lancar bisa berguna dalam waktu lama dan unsur reliabilitas tetap aman.

2.2.11. GNS3

Menurut Widodo, dkk (2023), GNS3 adalah sebuah program Graphical Network Simulator (GUI) yang dapat mensimulasikan topologi jaringan yang lebih kompleks dibandingkan dengan simulator lainnya. Program ini dapat dijalankan di berbagai sistem operasi, seperti Windows, Linux, atau MacOS X.

2.2.12. Hotspot

Menurut Syahputra dan Wijaya (2022), Hotpsot adalah sebuah metode autentikasi yang di terapkan pada akses point, dan dengan diterapkannya metode hotpsot dapat dengan mudah mengautentikasi user yang terhubung ke dalam suatu jaringan. Kelebihan yang diperoleh dari metode hotpsot sangatlah banyak, diantaranya dengan metode hotpsot kita dapat mengetahui jumlah data yang di download/upload, dan juga dapat melakukan limitasi bandwidth dan waktu pemakaian user berdasarkan data rate. Selain itu, metode hotpsot umumnya banyak digunakan untuk user atau pelanggan yang ingin tetap terkoneksi internet dimanapun mereka berada selama tempat tersebut terdeapat akses point.

METODE PENELITIAN

3.1. Tempat dan Waktu Penelitian

Kegiatan penelitian ini dilakukan di Kampus STMIK Widya Cipta Dharma berada di Jl. M. Yamin No. 25 Samarinda.

3.2. Teknik Pengumpulan Data

3.2.1 Observasi (Pengamatan Langsung)

Adapun observasi atau pengamatan langsung dilakukan di Puskom Widya Cipta Dharma terhadap sistem jaringan yang ada.

3.2.2 Studi Pustaka

Studi pustaka salah satu teknik pengumpulan data yang digunakan dalam penelitian dilakukan dengan cara mengumpulkan data yang relevan atau sesuai yang dibutuhkan untuk penelitian dari buku, artikel ilimiah, berita, maupun sumber kredibel lainnya yang reliabel dan juga sesuai dengan topik penelitian yang dilakukan.

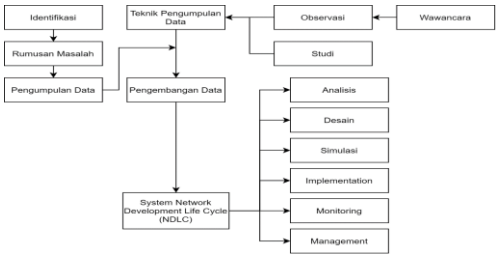
3.2.3 Wawancara

Wawancara adalah teknik pengumpulan data yang dilakukan untuk menentukan permasalahan yang harus diteliti atau apabila peneliti ingin mengetahui hal-hal dari responden yang sifatnya lebih mendalam. Wawancara dapat dilakukan dengan cara terstruktur maupun tidak terstruktur, dan dapat dilakukan melalui tatap muka.

3.2.4 Tahap Metode Penelitian

Tahap metode penelitian adalah level atau tingkatan bisa disebut juga jenjang dalam sebuah aktivitas penelitian. Dimana tahapan tersebut terdapat memiliki proses yang dilakukan secara terstruktur, runtut, baku, logis dan sistematis. Tahapan metode peneliti adalah metode Network Development Life Cycle (NDLC), dengan tahapannya seperti Analysis, Design, Simulation Prototype, Implementation, Monitoring, dan Management.

3.2.5 Alur Penelitian



3.2.6 Analisis

Pada tahap ini merupakan metode pengumpulan data yang mana sudah dijelaskan sebelumnya, ada tiga pengumpulan data yang peneliti ambil yaitu observasi, studi pustaka, wawancara.

3.2.7 Design

Pada tahap ini peneliti mendesain rancangan berdasarkan peta jaringan yang sudah ada di Puskom Kampus STMIK Widya Cipta Dharma. Diharapkan dengan gambar ini akan memberikan gambaran sesuai kebutuhan sistem jaringan di STMIK Widya Cipta Dharma.

3.2.8 Simulation Prototype

Pada tahap ini peneliti mensimulasikan hasil rancangannya menggunakan aplikasi GNS 3 untuk selanjutnya diimplementasikan secara langsung.

3.2.9 Implemetation

Pada tahap ini peneliti mengeimplementasikan secara langsung hasil rancangan simulasi sebelumnya. Sesuai dengan langkah-langkah yang dibuat oleh peneliti.

3.2.10 Monitoring

Pada tahap ini setelah diiplementasikan peneliti melakukan monitoring hasil dari rancangannya agar jaringan dapat berjalan dengan baik.

3.2.11 Management

Pada tahapan ini disebut tahap kontrol yang merupakan tahapan akhir yang mana hasil implementasi harus berjalan dengan baik dan sesuai dengan tujuan awal dalam jangka waktu yang lama.

PEMBAHASAN

4.1. Hasil Penelitian

Pada penelitian yang dilakukan dan ingin dicapai ialah untuk menerapkan VLAN pada jaringan internet di STMIK WICIDA

4.2. Pembahasan

4.2.1. Analisis

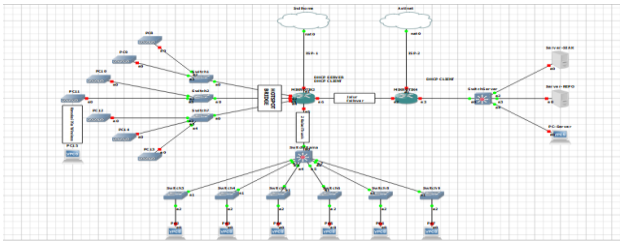
Dalam analisis peneliti melakukan wawancara kepada staff Puskom Wicida dan melihat topologi dan manajemen jaringan yang diterapkan oleh Kampus STMIK Widya Cipta Dharma. Masalah yang terjadi adalah belum adanya pengaturan VLAN yang lebih aman dan penanganan yang tepat dalam konfigurasi jaringan dari VLAN Hopping dan spanning tree protocol attack. VLAN hopping adalah sebuah serangan yang bertujuan untuk memungkinkan penyerang untuk mendapatkan akses dari satu VLAN ke VLAN lainnya. Hal ini merupakan ancaman keamanan yang mungkin terjadi ketika pengaturan VLAN tidak dilakukan dengan benar. VLAN hopping dapat digunakan oleh penyerang untuk mengakses data yang seharusnya tidak dapat diakses dari VLAN mereka. Untuk mengatasi masalah ini, perlu ada pengaturan VLAN yang lebih aman dan penanganan yang tepat dalam konfigurasi jaringan.

Sebagai contoh adalah, pada serangan Switched Spoofing VLAN Hopping, penyerang mencoba mengecoh switch yang sah untuk membentuk tautan trunking antara perangkat penyerang dan switch. Tautan trunking membawa lalu lintas antara switch yang terhubung atau switch yang terhubung dan router, mempertahankan data VLAN. Setelah tautan trunking terbentuk, penyerang dapat mengakses lalu lintas dari semua VLAN dalam jaringan.

Untuk pencegahan dari VLAN Hopping, langkah-langkah mitigasi dapat diimplementasikan. Pada serangan Switched Spoofing VLAN Hopping, penting untuk menonaktifkan Dynamic Trunking Protocol (DTP) pada port switch yang tidak memerlukan trunking. Konfigurasi port akses dan trunk harus diatur secara manual dengan menghingari mode "dynamic desirable," "dynamic auto," atau "trunk". Selain itu, semua antarmuka yang tidak digunakan sebaiknya dimasukkan ke dalam VLAN dan dinonaktifkan. Dengan menerapkan langkah-langkah ini, potensi risiko serangan VLAN Hopping dapat dikurangi.

4.2.2. Design

Desain topologi menggunakan aplikasi GNS3, berikut merupakan desain topologi yang telah di buat. Dapat dilihat pada gambar 4.1 dibawah merupakan rancangan dari topologi yang telah dibuat.



Dalam hal ini peneliti membagi segmen ke dalam 6 VLAN yaitu VLAN 10 untuk BAUK, VLAN 20 untuk UPM, VLAN 30 untuk BKK, VLAN 40 untuk Balai Bahasa, VLAN 50 untuk LAB, dan VLAN 99 untuk lainnya. Berikut adalah topologi yang di buat dan pembagian VLAN. Dapat dilihat pada gambar - Pembagian VLAN.

No	VLAN ID	*NETWORK*
1.	VLAN 10	192.168.10.0/24
2.	VLAN 20	192.168.20.0/24
3.	VLAN 30	192.168.30.0/24
4.	VLAN 40	192.168.40.0/24
5.	VLAN 50	192.168.60.0/24
6.	VLAN 99	192.168.99.0/24
7.	*Bridge*	192.168.170.0/24

4.2.3. Simulasi

Setelah melakukan desain topologi, selanjutnya dilakukan simulasi jaringan dengan mambuat user virtual yang terhubung ke jaringan melalui aturan yang telah disesuaikan dalam topologi. Contoh adalah PC1 terkoneksi melalui VLAN10 dengan IP Address yang ditentukan adalah 192.168.10.1/24 yang dapat dilihat pada gambar dibawah ini.

```
VPCS> dhcp
DORA IP 192.168.10.253/24 GW 192.168.10.1
```

Kemudian, dilakukan ‘ping’ yang mencakup beberapa respons ICMP dari alamat IP 192.168.188.254 menunjukkan proses pengujian konektivitas. Proses ini dilakukan untuk memeriksa apakah VPCS (user virtual) dapat berkomunikasi dengan perangkat yang memiliki alamat IP 192.168.188.254 melalui jaringan. Ketika VPCS mengirim permintaan ‘ping’ ke alamat tersebut, perangkat dengan alamat IP 192.168.188.254 akan merespon dengan balasan yang menandakan bahwa konektivitas jaringan antara keduanya berfungsi dengan baik. Dengan kata lain, proses ini bertujuan untuk memeriksa apakah dua perangkat dapat berkomunikasi satu sama lain di dalam jaringan. Tampilan dari proses ping dapat dilihat pada gambar dibawah.

```
VPCS> ping 192.168.188.254

84 bytes from 192.168.188.254 icmp_seq=1 ttl=62 time=19.813 ms
84 bytes from 192.168.188.254 icmp_seq=2 ttl=62 time=14.452 ms
84 bytes from 192.168.188.254 icmp_seq=3 ttl=62 time=13.466 ms
84 bytes from 192.168.188.254 icmp_seq=4 ttl=62 time=13.643 ms
84 bytes from 192.168.188.254 icmp_seq=5 ttl=62 time=14.992 ms
```

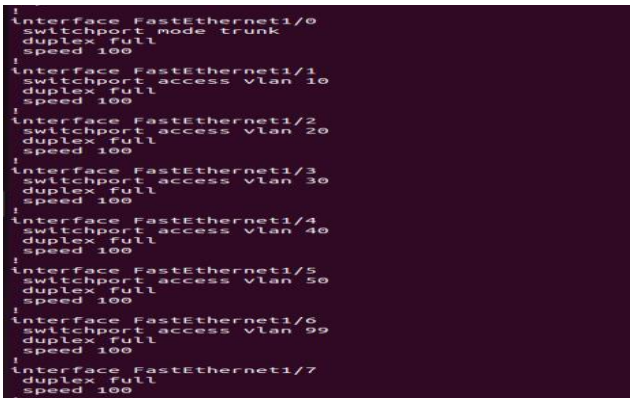
4.2.4. Implementasi

Implementasi merupakan tahapan untuk mengkonfigurasi switch dan router. Tahap pertama adalah melakukan konfigurasi pada VLAN dengan membagi

VLAN ke dalam 6 segmen yang dapat dilakukan sebagai berikut.

```
ESW(config)#vlan 10

ESW(config-vlan)#name VLAN0010

Switch(config)#vlan 20

Switch(config-vlan)#name 0020

Switch(config)#vlan 30

Switch(config-vlan)#name 0030

Switch(config)#vlan 40

Switch(config-vlan)#name 0040

Switch(config)#vlan 50

Switch(config-vlan)#name 0050

Switch(config)#vlan 99

Switch(config-vlan)#name 0099
```

Selanjutnya adalah konfigurasi port access dan trunk. Port access berfungsi melewatkan data yang berada di VLAN yang sama, sedangkan port trunk berfungsi untuk melewatkan data dari beberapa VLAN yang berbeda agar sampai ke router. Berikut adalah konfigurasi port access dan port trunk pada switch. Berikut merupakan hasil konfigurasi Port access dan Trunk yang dapat dilihat pada gambar dibawah**.**



Selanjutnya adalah melakukan konfigurasi terhadap alamat IP pada CHR. Pada tahap ini, kita memberikan alamat IP ke masing-masing perangkat MikroTik CHR, yaitu CHR 1 dan CHR 2. Alamat IP yang diberikan harus sesuai dengan jaringan lokal yang digunakan di lingkungan tersebut. Dalam konteks ini, kita mengatur alamat IP 10.10.1.1/24 pada CHR 2 dan alamat IP 10.10.1.2/24 pada CHR 1, dan ini dilakukan pada antarmuka Ether3 pada masing-masing perangkat. Dengan mengatur alamat IP ini, koneksi antara CHR 1 dan CHR 2 melalui Ether3 dijembatani, memungkinkan failover untuk berfungsi sehingga perangkat dapat beralih antara rute utama dan rute cadangan tanpa adanya gangguan atau interupsi dalam koneksi internet saat terjadi masalah.

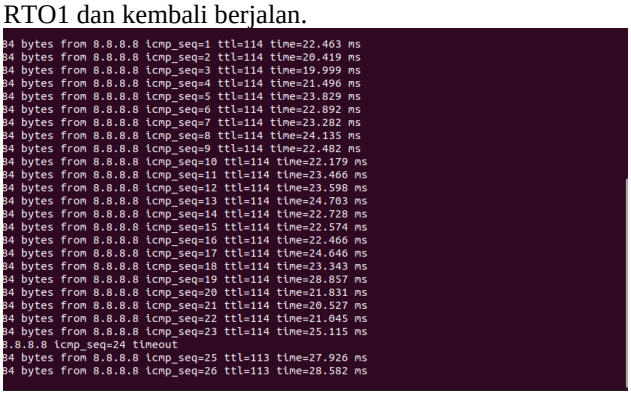
Selanjutya adalah menghubungkan LAN melalui Ether3. Menggunakan Ether3 sebagai antarmuka yang menghubungkan LAN dari CHR1 ke CHR2 memungkinkan jaringan lokal di CHR1 terhubung ke jaringan lokal di CHR2 melalui Ether3. Dengan pengaturan ini, koneksi lintas CHR1 dan CHR2 dijembatani, memungkinkan aliran data yang lancar antara kedua perangkat sehingga failover dapat berfungsi dengan baik, dan jaringan tetap stabil bahkan jika terjadi masalah dengan salah satu rute jaringan.

4.2.5. Monitoring

Pada tahap ini, dilakukan monitoring untuk memastikan user mendapat alamat IP yang sesuai dengan VLAN masing-masing. Berikut merupakan Host VLAN yang terhubung.

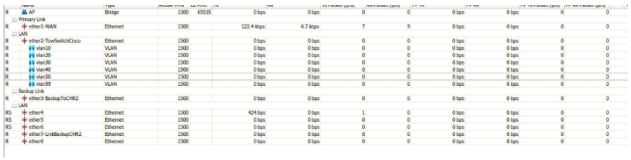
	Address	MAC Address	Client ID	Server	Active Addre...	Active MAC Addr...	Active Ho...
D	192.168.10.253	00:50:79:66:68:0A	1:0:50:79:66:68:a	dhcp2	192.168.10.253	00:50:79:66:68:0A	VPCS
D	192.168.20.253	00:50:79:66:68:10	1:0:50:79:66:68:10	dhcp3	192.168.20.253	00:50:79:66:68:10	PC1

Apabila ISP utama mengalami gangguan jalur internet maka akan terjadi RTO1 saat melakukan ping dan jaringan akan berpindah ke ISP cadangan dan akan kembali berjalan. Berikut merupakan tampilan saat terjadi RTO1 dan kembali berjalan.



4.2.6. Management

Tahap management dilakukan untuk mengatur sistem yang telah dibuat dapat terjaga dengan baik. Berikut merupakan konfigurasi yang telah dibuat untuk dapat terus dimonitor agar tidak terjadi kendala kedepannya, dan apabila terjadi kendala dapat segera dilakukan penanganan agar cepat teratasi.



4.2.7. Pengujian Vlan Hopping

Serangan VLAN hopping dimulai dengan memanfaatkan Dynamic Trunking Protocol (DTP), sebuah protokol pada perangkat jaringan seperti switch untuk mengonfigurasi port sebagai trunk atau access. Kelemahan dalam DTP dieksploitasi oleh penyerang untuk membobol switch dan mengizinkan lalu lintas VLAN melewati batasannya. Melalui manipulasi proses otomatis antar-switch yang terjadi melalui DTP, penyerang dapat menipu switch target agar membuka jalur trunk yang seharusnya terisolasi. Berikut tampilan dynamic trunk protocol, dapat dilihat pada Gambar.

Langkah berikutnya dalam serangan VLAN hopping melibatkan pelaksanaan trunking pada switch yang sebelumnya telah diatur. Jika protokol Dynamic Trunking Protocol (DTP) dapat dijalankan dari sistem operasi Kali Linux, maka penyerang dapat mengeksploitasi situasi tersebut dengan menambahkan konfigurasi atau tindakan tertentu.

Pada langkah ketiga, ketika paket DTP dikirim dengan aktivasi trunking melalui Kali Linux, menunjukkan bahwa serangan VLAN hopping telah berhasil diimplementasikan di sistem operasi tersebut. Tindakan ini memanfaatkan kerentanannya dalam Dynamic Trunking Protocol (DTP) untuk membuka jalur trunk yang seharusnya terisolasi, memungkinkan Kali Linux memanipulasi switch dan mengakses lalu lintas VLAN yang seharusnya terbatas. Ini membawa potensi risiko keamanan dan memberikan kontrol kepada penyerang atas informasi dalam jaringan.

Pada langkah ke empat, penyerang mencatat bahwa konfigurasi trunk tidak mengalami perubahan, dan tetap pada port yang memiliki mode trunk seperti sebelumnya. Hal ini mengindikasikan bahwa, meskipun serangan VLAN Hopping telah dilakukan melalui Kali Linux , konfigurasi trunk pada port tertentu tidak mengalami perubahan. Meskipun serangan tersebut berjalan, switch tidak merespon dengan perubahan konfigurasi yang diinginkan oleh penyerang. Fakta bahwa mode trunk pada port tetap tidak berubah dapat menjadi faktor penting dalam mengevaluasi efektivitas atau keberhasilan serangan tersebut.

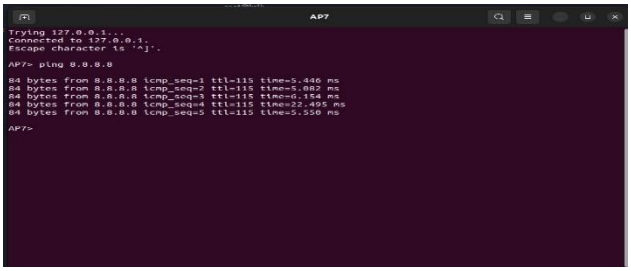
Kemudian, perangkat komputer yang terkoneksi dengan Ethernet Switch (ESW) 1 mengalami dampak serangan VLAN hopping. Hal ini mengindikasikan bahwa tingkat keamanan jaringan di ESW 1 telah terganggu, dan penyerang berhasil memanfaatkan kerentanannya untuk meretas atau mengubah akses ke lalu lintas VLAN yang seharusnya terisolasi. Sebagai akibatnya, perangkat komputer yang terhubung ke switch tersebut menjadi rentan, memungkinkan penyerang untuk potensial mengakses informasi atau sumber daya yang seharusnya terlindungi oleh pembatasan VLAN.

4.2.8. Pengujian Spanning Tree Protocol Attack

Pengujian STP Attack adalah usaha untuk mengidentifikasi dan menguji kerentanan dalam protokol penyebaran pohon jaringan, yang digunakan untuk mencegah loop dalam topologi mesh. Dalam pengujian ini, serangan melibatkan manipulasi pesan BPDU untuk memicu perubahan dalam struktur pohon, potensial menciptakan loop atau mengganggu kinerja jaringan. Berikut pengujian Spanning Tree Protocol Acttack antara lain:

Langkah pertama dalam pengujian STP Attack melibatkan pendeteksian serangan STP oleh Kali Linux. Setelah terdeteksi, langkah berikutnya adalah mengeksekusi serangan dengan mengklaim status Root pada switch terdampak. Tujuannya adalah untuk memanipulasi proses pengaturan pohon jaringan (STP), berpotensi menciptakan loop atau gangguan dalam kinerja jaringan. Tindakan ini dirancang untuk menguji keamanan jaringan dan memberikan wawasan yang diperlukan untuk memperkuat perlindungan dan kestabilan sistem.

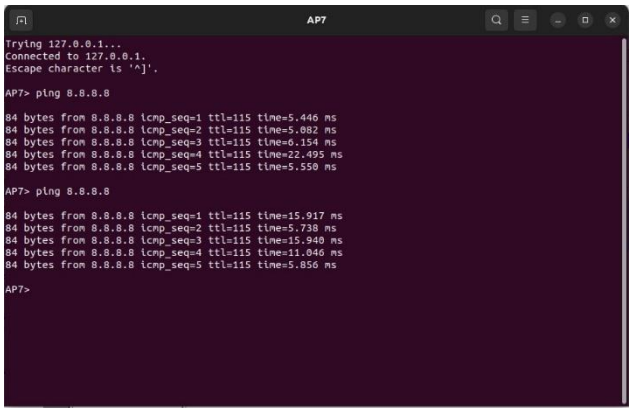
Kemudian, pada langkah kedua, Access Point (AP7) yang terhubung ke switch yang sama mengalami perubahan. Sebelum serangan dilakukan, AP7 dapat menjalankan ping dengan normal. Namun, setelah serangan berhasil dieksekusi, AP7 tidak lagi dapat menjalankan ping, dan terdapat Resend Time-Out (RTO). Hal ini disebabkan oleh penyerangan yang berhasil mengklaim jalur utama, menyebabkan gangguan pada jalur komunikasi dan mempengaruhi kemampuan AP7 untuk berkomunikasi secara efektif.



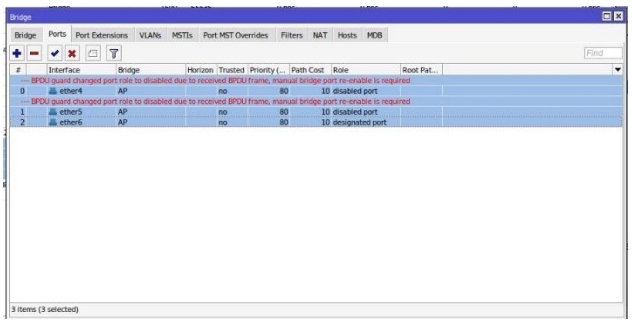
Pada langkah ketiga, setelah Kali Linux diaktifkan, perangkat ini akan mengambil peran sebagai root dalam protokol Spanning Tree (STP). Dalam konteks ini, Kali Linux mengirimkan informasi perannya sebagai root ke switch. Hal ini menunjukkan bahwa Kali Linux berusaha mengendalikan peran root dalam konfigurasi pohon jaringan (STP), yang pada gilirannya dapat memengaruhi struktur dan jalur koneksi dalam jaringan.

Namun, pada tahap ini, ketika AP7 diuji kembali, masih memungkinkan untuk melakukan ping. Hal ini menunjukkan bahwa BPDU guard, suatu mekanisme keamanan yang melibatkan deteksi dan

pemblokiran pesan BPDU (Bridge Protocol Data Unit) yang tidak sah, berhasil diimplementasikan. Dengan demikian, BPDU guard berhasil mencegah perangkat.



Pada langkah kelima, saat terjadi serangan, perangkat Mikrotik mendeteksi adanya serangan yang melibatkan pesan BPDU (Bridge Protocol Data Unit). Dalam respons terhadap deteksi ini, perangkat Mikrotik mengambil langkah-langkah tindakan dengan meng-handle dan menjatuhkan (drop) port yang terlibat dalam serangan tersebut. Tindakan ini dilakukan untuk mengisolasi atau menghentikan akses perangkat yang mencoba melakukan serangan BPDU, sehingga melindungi kestabilan dan keamanan jaringan secara keseluruhan.



PENUTUP

5.1 Kesimpulan

Berdasarkan dari hasil penelitian yang telah dilakukan pada penelitian ini, dapat disimpulkan bahwa:

1. Penelitian berhasil mengimplementasikan keamanan jaringan LAN berbasis VLAN di STMIK WICIDA, menggunakan simulasi topologi jaringan dengan GNS3 dan membagi domain menjadi enam dengan VLAN.
2. Penerapan Bridge pada WICIDA memastikan kelangsungan koneksi pengguna saat berpindah dari satu area ke area lain dengan IP yang sama, tanpa terputus.
3. Failover berhasil diterapkan dengan menambahkan kabel antara Mikrotik jaringan utama dan cadangan, berfungsi sebagai backup saat terjadi gangguan pada jaringan utama.
4. Konfigurasi keamanan untuk mencegah VLAN hopping sangat penting untuk menjaga integritas jaringan. Dengan mengatur setiap port switch dalam mode access dan mengisolasi ke dalam VLAN yang sesuai, serangan VLAN hopping dapat dicegah efektif. Tindakan ini meningkatkan perlindungan jaringan dari upaya penyerangan yang berusaha memanfaatkan kerentanan dalam struktur VLAN.
5. Penerapan BPDU Guard sangat penting untuk melindungi jaringan dari serangan Spanning Tree Protocol (SPT). Dengan memonitor dan menonaktifkan port yang diterima BPDU tidak sah, BPDU Guard akan mencegah loop layer-2 dan mengganggu lalu lintas jaringan, sehingga mampu meningkatkan keamanan dan stabilitas jaringan secara keseluruhan.

5.2 Saran

Saran yang dapat diberikan adalah untuk terus memantau dan memelihara sistem yang telah diimplementasikan guna memastikan kinerja jaringan yang optimal serta melakukan uji coba failover secara berkala untuk memastikan kesiapan dalam menghadapi gangguan jaringan. Selain itu, pengelolaan dan pemantauan VLAN perlu ditingkatkan untuk memastikan isolasi segmen jaringan berjalan dengan baik dan aman. Untuk mencegah VLAN hopping dan melindungi dari serangan Spanning Tree Protocol (STP), administrator jaringan harus mengatur seluruh port switch dalam mode Access sehingga setiap port hanya terhubung dengan satu VLAN. Penggunaan ACL, DHCP snooping, dan ARP inspection dapat membatasi akses dan mencegah manipulasi alamat MAC. Selain itu, penerapan BPDU Guard penting untuk memonitor dan menonaktifkan port yang menerima BPDU tidak sah, mencegah loop layer-2 yang dapat mengganggu jaringan.

DAFTAR PUSTAKA

Altarik, M. F., & Putra, A. D. (2023). Perancangan Keamanan Jaringan Metode Authentication Login Hotspot Menggunakan Router Mikrotik di PT. Nusindo Rekatama Semesta. *Jurnal Nasional Ilmu Komputer*, 103-120.

Amala, R., Mewengkang, A., & Djamen, A. C. (2023). ANALISIS DAN PERANCANGAN JARINGAN KOMPUTER DI SMK NEGERI 2 BITUNG. *EduTIK: Jurnal Pendidikan Teknologi Informasi dan Komunikasi*, 1-10.

Aprillianto, B., & Pamungkas, D. (2023). Analisis Pengembangan Model Laboratorium Jaringan Virtual Menggunakan GNS3. *Jaringan: Jurnal Hasil Kegiatan Pengabdian Kepada Masyarakat*, 31-38.

Ardhiansyah, M., Noris, S., & Andrianto, R. (2020). *Jaringan Komputer*. Tangerang Selatan, Banten: Unpam Press.

Azad, U. (2021). *VLAN Hopping Attack and Mitigation*. Retrieved from linuxhint:

https://linuxhint.com/vlan-hopping-attack-mitigation/

Buana, W., Hariyandi, A., & S, F. R. (2023). PENGEMBANGAN JARINGAN LOCAL AREA NETWORK (LAN) DAN WIDE AREA NETWORK (WAN) PADA SMKN 4 PADANG DENGAN METODE RESEARCH DAN DEVELOPMENT. *JOISIE Journal Of Information System And Informatics Engineering*, 120-134.

DHARMA SAMARINDA, S. W. (2017). *Google Drive*. Retrieved from https://drive.google.com/file/d/19NWPN64gGyqUt2TxwWz2MMurr_shka83/view

Dharmalau, A., Ar-Rasyid, H., & Iskandarsyah, M. A. (2022). IMPLEMENTASI METODE SWOT PADA ANALISIS JARINGAN AREA LOKAL SEKOLAH. *JURNAL ELEKTRO & INFORMATIKA*, 1-8.

Fauzan, M. A., & Purwanto, T. D. (2021). PERANCANGAN FIREWALL ROUTER MENGGUNAKAN OPNSENSE UNTUK MENINGKATKAN KEAMANAN JARINGAN PT. PERTAMINA ASSET 2 PRABUMULIH. *Seminar Hasil Penelitian Vokasi (SEMHAVOK)*, 1-10.

Firmansyah, Sandi, T. A., Anwar, R. S., & Fauzi, A. (2023). Analisis Performa Redundancy Link Menggunakan Metode Spanning Tree Protocol dan Per VLAN Spanning Tree. *Jurnal Infortech*, 47-52.

Fitriani, P., Dani, U., & Prayogi, A. (2021). Implementasi Jaringan Internet dan Konfigurasi Mikrotik dengan Simulasi GNS3 Pada Perusahaan Intelligent Komputer. *Jurnal Informasi Komputer Logika*, 1-5.

Hariadi, F. (2021). Manual Load Balancing pada Redundancy LinkMenggunakan Multi-Group Hot Standby Router Protocol. *Jurnal Teknik Informatika dan Sistem Informasi*, 1-12.

Hasibuan, F. A., & Subhiyanto. (2021). Jaringan Komputer Berbasis Radius Server untuk Meningkatkan Pemanfaatan Internet di Madrasah Aliyah Al-Azhaar Ummu Suwanah. *JURNAL TEKNIK INFORMATIKA*, 1-10.

Irfan, Satra, R., & Fattah, F. (2021). Keamanan Jaringan VLAN dan VoIP Menggunakan Firewall. *Buletin Sistem Informasi dan Teknologi Islam*, 27-35.

Julandra, B. P., Putri, & Mabruri, A. (2022). ANALISIS DAN PERANCANGAN JARINGAN LOCAL AREA NETWORK PADA LAB KOMPUTER DI SMK NEGERI 5 KOTA SERANG. *Engineering And Technology International Journal* , 1-14.

Kusuma, G. H. (2021). Perancangan Skema Sistem Keamanan Jaringan Web Server menggunakan Web Application Firewall dan Fortigate untuk Mencegah Kebocoran Data di Masa Pandemi Covid-19. *Journal of Informatics and Advanced Computing* , 1-4.

Nukman, Khulaimi, M., & Taqiudin, M. (2023). Pelatihan Jaringan VLAN Menggunakan Mikrotik Di SMK Darussholihin NW Kalijaga. *JOMPA ABDI: Jurnal Pengabdian Masyarakat* , 1-7.

Ofrianky. (2022). Rancang Bangun Daftar Nomor Urut Kepangkatan Pada SMA Negeri 1 Batui Berbasis Jaringan Internet. *Jurnal Teknologi Informasi Indonesia*, 1-8.

Rahmat, Wahyuningrum, R. W., Haerullah, E., & Sodikin. (2022). ANALISIS MONITORING SISTEM JARINGAN KOMPUTER MENGGUNAKAN APLIKASI SPICEWORKS. *Jurnal PROSISKO*, 1-9.

Renwarin, V. M., & Radiyah, U. (2021). IMPLEMENTASI SPANNING TREE PROTOCOL (STP) PADA PERANCANGAN VIRTUAL LOCAL AREA NETWORK (VLAN) PADA PT. REGALINDO SAKTI JAKARTA. *JI-Tech: Jurnal Ilmiah Sekolah Tinggi Teknologi Informasi NIIT*, 1-6.

Rokim, M. N., & Nainggolan, E. R. (2021). PEMANFAATAN MANAJEMEN JARINGAN MENGGUNAKAN VIRTUAL LOCAL AREA NETWORK (VLAN) PADA PT. JANTRA REKA SAKSANAMAS CENGKARENG TIMUR JAKARTA BARAT. *Reputasi: Jurnal Rekayasa Perangkat Lunak*, 1-7.

Setiawan, Y. B., I. N., & Pravitasari, D. (2022). Desain Infrastruktrur Jaringan Inter-Vlan dengan Keamanan Port Security dan Secure Shell Berbasis Protocol Open Short Path First. *ULIL ALBAB : Jurnal Ilmiah Multidisiplin*, 1-9.

Sipayung, P. I., Purba, V., & Agussalim. (2024). Analisis, Perancangan, dan Simulasi Jaringan VLAN Menggunakan Metode PPDIOO (Studi Kasus: SMAS Santo Yusup Surabaya). *Jurnal Ilmiah Teknologi-Informasi&Sains*, 110-118.

Subli, M., Hoiriyah, & Wahyudi, E. (2022). Penerapan Spanning Tree Protocol Untuk Mencegah Terjadinya Looping Pada Frame Ethernet. *Explore*, 7-13.

Sujadi, H., & Mutaqin, A. (2017). Rancang Bangun Arsitektur Jaringan Komputer Teknologi Metropolitan Area Network (MAN) Dengan

Menggunakan Metode Network Development Life Cycle (NDLC) (Studi Kasus: Universitas Majalengka). *Jurnal J-Ensitec*, 142-146.

Syahputra, H., & Wijaya, R. (2022). Pembangunan Jaringan Hotspot Berbasis Mikrotik pada Kampung Tematik di Kecamatan Padang Utara. *Majalah Ilmiah UPI YPTK*, 60-66.

Widodo, B., Aziezah, N., & Wicaksono, A. (2023). Pengembangan Model Laboratorium Jaringan Virtual Menggunakan GNS3 di SMKS Bhinneka Karya 5 Boyolali. *NUSANTARA: Jurnal Pengabdian Kepada Masyarakat*, 72-80.

Yulianto, R., & Aprilyani, F. (2020). Sistem Keamanan Jaringan Komputer Menggunakan Metode NDLC Dengan Linux Zentyal Pada Instansi KEMENKO Maritim. *JURNAL TEKNIK INFORMATIKA*, 1-8.

Zaen, M. T., & Tantoni, A. (2022). Topologi Redundansi Link Untuk Keamanan Serta Mitigasi Ketersediaan Jaringan Komputer Menggunakan Rapid Spanning Tree Protocol. *Journal of Computer System and Informatics (JoSYC)*, 88-100.