ULIL ALBAB : Jurnal Ilmiah Multidisiplin
Vol.2, No.1, Desember 2022

Desain Infrastruktrur Jaringan *Inter-Vlan* dengan Keamanan *Port Security* dan *Secure Shell* Berbasis *Protocol Open Short Path First*

Yoga Bayu Setiawan[1], Ibrahim Nawawi[2], Deria Pravitasari[3]
[1,2,3]Universitas Tidar
E-mail: yogabayu1902@gmail.com[1], ibrahim_nw@untidar.ac.id[2] deria.pravitasari@untidar.ac.id[3]

Article History:
Received: 16 Desember 2022
Revised: 29 Desember 2022
Accepted: 30 Desember 2022

Keywords: *InterVLAN, VLAN, Secure Shell, Open Short Path First, Spanning-tree*

Abstract: *Perencanaan infrastruktur jaringan komputer suatu instansi harus dilakukan secara efisien yang dilakukan dengan mengganti kabel menjadi wireless distribution system (WDS). Selain efisiensi transmisi data, keamanan data juga penting untuk diperhatikan terutama di lingkungan kampus. Jaringan kampus menghadapi banyak tantangan mulai dari alokasi alamat IP, kegagalan fungsi jaringan, pengguna sistem yang tidak bertanggungjawab, jaringan yang lambat, dan lain sebagainya. Penelitian ini menggunakan teknik InterVLAN untuk mengkomunikasikan antar VLAN dengan keamanan Secure Shell berbasis Open Short Path First. 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. Metode port security dan secure shell digunakan untuk mengamankan paket data, dengan cara memblock mac-address yang tidak terdaftar pada mac-address tabel, paket data yang mac-address yang tidak terdaftar pada mac-address tabel tidak akan sampai pada tujuan, sedangkan secure shell bertujuan untuk mengetahui ketersediaan layanan remote access dari perangkat jaringan pada saat akan digunakan Jika ketika menginput username dan password yang sudah didaftarkan sebelumnya pada konfigurasi salah, maka tidak dapat mengakses perangkat tersebut. Spanning-tree digunakan untuk mencegah terjadi looping atau tabrakan antar data dengan membuat jalur cadangan apabila salah satu jalur mati atau terputus. Hasil perhitungan anggaran sesuai dengan perencanaan didapat total pengeluaran biaya yang dibutuhkanvsebesar Rp 597.720.000.*

PENDAHULUAN

Perencanaan infrastruktur jaringan komputer suatu instansi harus dilakukan secara efisien. Efisiensi dapat dilakukan dengan penggantian media transmisi berupa pengkabelan dengan *wireless distribution system* (WDS)[1]. Selain efisiensi transmisi data, keamanan data juga penting untuk diperhatikan terutama di lingkungan kampus. Jaringan kampus menghadapi banyak tantangan mulai dari alokasi alamat IP, kegagalan fungsi jaringan, pengguna sistem yang tidak bertanggungjawab, jaringan yang lambat, dan lain sebagainya. Salah satu teknik yang dapat digunakan untuk mengkomunikasikan jaringan VLAN adalah teknik Inter-VLAN[2].

Permasalahan perihal keamanan jaringan dan efisiensi waktu dalam suatu insfrastruktur jaringan masih kurang diperhatikan. Beberapa penelitian sebelumnya hanya memfokuskan pada pembuatan infrastrukturnya saja, yang membuat tingkat keamanan jaringan sangat lemah dan memakan banyak waktu dalam pengiriman data. Pada penelitian ini dilakukan desain infrastruktur jaringan Inter-VLAN dengan keamanan *Secure Shell* berbasis *Open Short Path First* studi kasus di PT. ENSHU INDONESIA.

METODE PENELITIAN

Penelitian ini berfokus pada perancangan infrastruktur jaringan dengan teknik Inter-VLAN yang memiliki efisiensi dan keamanan tinggi, dengan menerapkan *Secure Shell* berbasis *Open Short Path First*. Peneliti menentukan lokasi penelitian berdasarkan wawancara yang sebelumnya dilakukan oleh salah satu pekerja di perusahaan tersebut yang menanganani masalah jaringan di perusahaan tersebut. Lokasi penelitian ini berlokasi di PT. ENSHU INDONESIA Jl. Boulevard Grand Wisata, Lambangsari, Kec. Tambun Sel., Kabupaten Bekasi, Jawa Barat 17510.

Dalam menyelesaikan penelitian ini, dilakukan beberapa tahapan yang harus dilakukan. Adapun tahapan-tahapan yang dilakukan yaitu:

1. Studi literatur

   Pada tahap ini dilakukan studi literatur dengan mengumpulkan dan mempelajari materi-materi yang relevan dengan tema. Materi-materi tersebut dapat diperoleh dari buku, jurnal, internet maupun diskusi.
2. Pengumpulan data

   Pengumpulan data dilakukan dengan datang secara langsung ke lokasi penelitian. Data yang yang dikumpulkan berupa data primer dan data sekunder. Data primer adalah data yang diperoleh secara langsung di lapangan atau lokasi penelitian. Data sekunder adalah data yang diperoleh dengan melakukan studi literatur mengenai penelitian yang diambil. Adapun data primer yang didapatkan yaitu dengan melihat, denah penempatan perangkat yang akan digunakan dalam perancangan infrastruktur jaringan, denah wiring jaringan untuk mengetahui perangkat akan tersambung ke perangkat mana saja, kemudian jumlah pengguna atau client yang berguna untuk menentukan jumlah perangkat yang akan digunakan. Data sekunder didapatkan dari penelitian sebelumnya untuk dijadikan acuan melakukan penelitian.
3. Perencanaan

   Penelitian ini dilakukan dengan perancangan topologi jaringan dengan menggunakan software cisco packet tracer dan juga ms.visio yang nantinya akan dikonfigurasi dan akan mendapatkan hasil dari konfigurasi tersebut.
4. Pengujian

   Pada tahap ini dilakukan dengan pengujian terhadap konektifitas jaringan, kemudian keamanan jaringan dengan menerapkan keamanan port security dan Secure Shell. Pengujian dilakukan dengan menggunakan software cisco packet tracer.

5. Analisis hasil

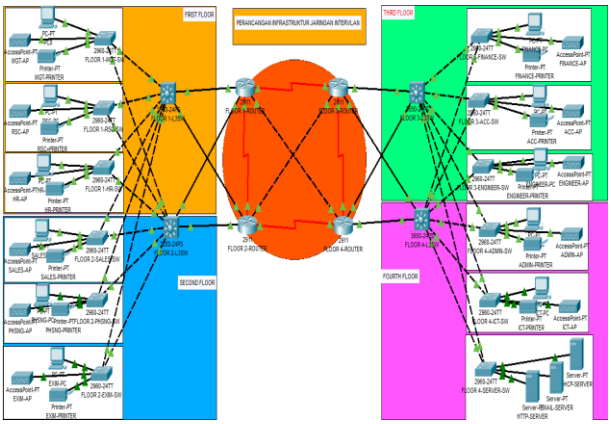
Pada tahap ini dilakukan analisis dari hasil pengujian yang sudah diujikan. Dari pengujian tersebut apa ada kendala atau tidak

HASIL DAN PEMBAHASAN

Hasil

1. Gambar Topologi

Perancangan topologi jaringan didapat dari hasil dari observasi dan wawancara pada lokasi penelitian, dimana perancangan topologi dimaksudkan untuk membuat jaringan *Inter-Vlan* dengan menggunakan sistem keamanan *port security* dan *secure shell* dengan menggunakan *routing protocol open short path first* yang ditunjukkan pada gambar 1.



Gambar 1. Topologi Jaringan Penelitian

Topologi tersebut menggunakan topologi jaringan hierarki dimana pada topologi tersebut terdapat 3 lapisan, yaitu lapisan inti, lapisan distribusi dan lapisan akses. Setelah melakukan perancangan topologi langkah selanjutnya adalah menentukan pengalamatan internet protocol (IP) yang akan diterapkan pada masing – masing perangkat jaringan dan host yang tersambung. Dalam pengalamatan jaringan ini menggunakan parent network 192.168.10.0/26 yang nanti akan dilakukan konfigurasi variable length subnet mask (VLSM) untuk meningkatkan keamanan jaringan serta menghemat penggunaan IPv4 pada jaringan yang akan dibangun. Jaringan ini akan menggunakan metode virtual local area network (VLAN) yang berfungsi untuk membagi jaringan LAN yang ada menjadi lebih kecil yang berfungsi untuk manajemen jaringan serta meningkatkan keamanan jaringan.

2. Pengujian Konektifitas

Pengujian konektifitas berkaitan dengan desain dan implementasi yang dilakukan dalam tahap perencanaan awal. Apabila pada tahap ini masih terdapat kesalahan seperti kesalahan dalam pembuatan topologi, kesalahan dalam pengalamatan IP, bahkan kesalahan pada konfigurasi baik intermediary device maupun host akan dapat diketahui. Pengujian konektifitas dilakukan dengan cara melakukan perintah pada command-line yaitu “ping -n 50” *<ip address target>* pada komputer server pada setiap IP address perangkat yang tersambung dengan jaringan. Perintah CLI tadi akan melakukan looping untuk perintah ping sebanyak 50 kali. Dalam pengujian ini yang menjadi parameter pengujian adalah jumlah paket data yang dikirim, jumlah paket data yang diterima kembali, waktu tempuh paket rata – rata, dan tingkat kegagalan

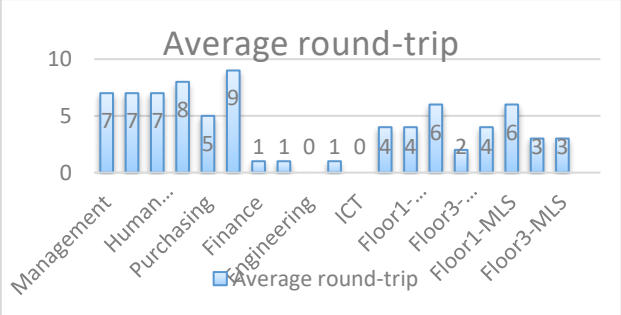
paket data untuk dikirim atau packet loss. Pada pengujian konektifitas ini dilakukan di *DHCP Server*. Untuk hasil dari pengujian konektifitas dapat dilihat pada Tabel 1.

Tabel 1. Hasil Uji Konektifitas

No	Destination	Package Sent	Package Received	Average Round-Trip	Packet Loss Precentage
1	Management	50	50	7 ms	0 %
2	Research	50	50	7 ms	0 %
3	Human Resource	50	50	7 ms	0 %
4	Sales	50	50	8 ms	0 %
5	Purchasing	50	50	5 ms	0 %
6	Exim	50	50	9 ms	0 %
7	Finance	50	50	1 ms	0 %
8	Accounting	50	50	1 ms	0 %
9	Engineering	50	50	0 ms	0 %
10	Administrator	50	50	1 ms	0 %
11	ICT	50	50	0 ms	0 %
12	Server Room	50	50	4 ms	0 %
13	Floor1-Router	50	50	4 ms	0 %
14	Floor2-Router	50	50	6 ms	0 %
15	Floor3-Router	50	50	2 ms	0 %
16	Floor4-Router	50	50	4 ms	0 %
17	Floor1-MLS	50	50	6 ms	0 %
18	Floor2-MLS	50	50	3 ms	0 %
19	Floor3-MLS	50	50	3 ms	0 %
20	Floor4-MLS	50	50	0 ms	0 %

Dari hasil pengujian pada Tabel 1 dapat diketahui bahwa untuk hasil uji konektifitas dengan cara mengirimkan paket ping sebanyak 50 kali memiliki tingkat keberhasilan sebesar 100%, hal ini diketahui dengan membandingkan antara parameter *package sent* dan *package received*, yang berarti dari 50 buah sinyal ping yang dikirimkan, komputer server mendapatkan kembali sinyal sebanyak 50 kali. Dari hasil tersebut dapat menjelaskan parameter *packet loss* yang memiliki nilai 0%, atau tidak ada paket yang hilang selama komunikasi berlangsung. Sedangkan yang menjadi perbedaan pada pengujian konektifitas ini adalah waktu tempuh paket tersebut (*round-trip*) dari hasil pada tabel diketahui pengiriman menuju tujuan atau *destination* memiliki waktu tempuh yang berbeda-beda. Hal ini dapat terjadi karena ada faktor jumlah loncatan (*hop*) yang dilakukan sebuah paket dari sumber ke destinasinya. Untuk visualisasi data *average round-trip* terdapat pada Gambar 1

.



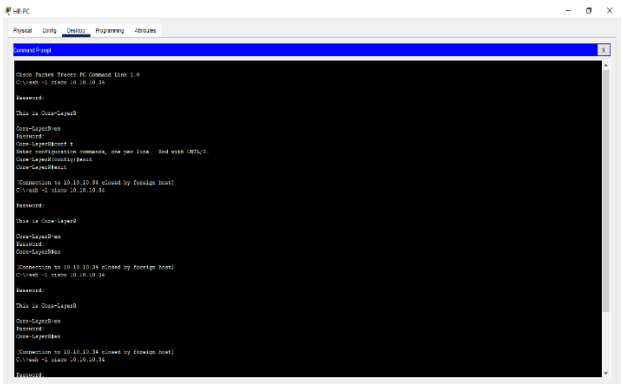
Gambar 2. Grafik Average Round-Trip

3. Pengujian Koneksi Secure Shell

Pengujian koneksi SSH ini dilakukan untuk mengetahui ketersediaan layanan *remote access* dari perangkat jaringan pada saat akan digunakan. Pengujian dilakukan dengan menggunakan fitur command-line yang terdapat pada server. Untuk perintah yang diberikan adalah ssh-l <username> <ip address>. Parameter yang digunakan untuk menentukan ketersediaan SSH adalah dari berapa kali perangkat tersebut dapat diakses dalam lima kali percobaan. SSH dianggap dapat diakses ketika banner <sesuai dengan perangkat> muncul pada laman SSH. Berikut hasil pengujian SSH pada Tabel 2.

Tabel 2. Pengujian SSH

Perangkat	Jumlah Percobaan Akses SSH	Jumlah Akses SSH Didapatkan	Persentase
Floor 1-Router	5	5	100%
Floor 2-Router	5	5	100%
Floor 3-Router	5	5	100%
Floor 4-Router	5	5	100%
Floor 1-MLS	5	5	100%
Floor 2-MLS	5	5	100%
Floor 3-MLS	5	5	100%
Floor 4-MLS	5	5	100%



Gambar 3. Pengujian SSH

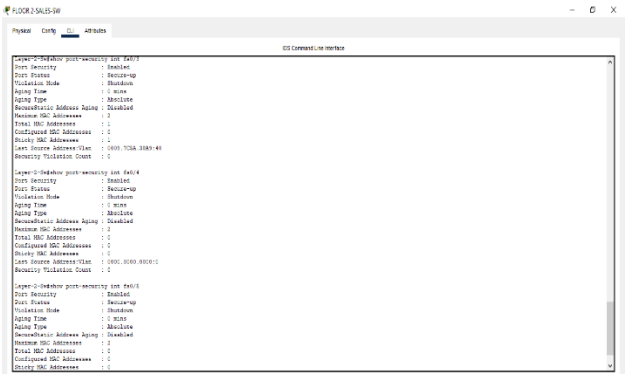
Dari pengujian akses SSH yang telah dilakukan, tingkat keberhasilan yang didapatkan pada setiap perangkat jaringan adalah 100%. Hal ini mungkin terjadi karena percobaan akses SSH ini dilakukan dalam sebuah software simulasi. Namun, apabila percobaan dilakukan dalam keadaan nyata, pasti akan terdapat kegagalan akses yang biasa diakibatkan oleh koneksi yang tidak stabil.

4. Pengujian Port-Security

Port-security merupakan suatu keamanan yang dikonfigurasi pada lapisan akses pada perangkat switch yang dimana *port-security* digunakan untuk memblok atau tidak mengizinkan perangkat yang tidak terdaftar *mac-address* pada *mac-address table*. Dengan mendaftarkan mac-address mana saja yang diizinkan dapat mengirimkan data pada *switch*, keamanan baik pada jaringan dan perangkat lainnya dapat terjamin. Berikut hasil pengujian *port-security* ditunjukkan Gambar 4 dan Gambar 5.

```
Layer-2-Sw>en
Password:
Layer-2-Sw#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                 (Count)       (Count)         (Count)
------------------------------------------------------------------------
          Fa0/3          2           1                0          Shutdown
          Fa0/4          2           0                0          Shutdown
          Fa0/5          2           0                0          Shutdown
          Fa0/6          2           0                0          Shutdown
          Fa0/7          2           0                0          Shutdown
          Fa0/8          2           0                0          Shutdown
          Fa0/9          2           0                0          Shutdown
         Fa0/10          2           0                0          Shutdown
         Fa0/11          2           0                0          Shutdown
         Fa0/12          2           0                0          Shutdown
         Fa0/13          2           0                0          Shutdown
         Fa0/14          2           0                0          Shutdown
         Fa0/15          2           0                0          Shutdown
         Fa0/16          2           0                0          Shutdown
         Fa0/17          2           0                0          Shutdown
         Fa0/18          2           0                0          Shutdown
         Fa0/19          2           0                0          Shutdown
         Fa0/20          2           0                0          Shutdown
         Fa0/21          2           0                0          Shutdown
         Fa0/22          2           0                0          Shutdown
         Fa0/23          2           0                0          Shutdown
         Fa0/24          2           0                0          Shutdown
------------------------------------------------------------------------
Layer-2-Sw#
```

Gambar 4. Interface yang Tidak Terdaftar di Mac-Address Table



Gambar 5. Pengujian *Port-Security*

Pada gambar diatas dapat dilihat *interface* dari *range* 3-24 tidak terdaftar pada *mac-address tabel*, otomatis jalur pengiriman data dari interface 3-24 tidak diizinkan. Pada pengujian *port-security* ini hanya *2 mac-address* yang didaftarkan pada *mac-address* tabel yaitu, *interface fast ethernet* 1 dan *interface fast ethernet* 2.

5. Penerapan Spanning Tree Protocol

Tujuan utama STP adalah untuk menghentikan perulangan tautan dan radiasi siaran yang ditimbulkannya. Tanpa risiko *loop* jaringan atau persyaratan untuk mengaktifkan/ menonaktifkan *backup* link ini secara manual, *spanning tree* juga memungkinkan arsitektur jaringan untuk menggabungkan backup link (redundan) untuk menyediakan jalur backup otomatis jika link aktif gagal. Setiap switch hanya mempunyai jalur tunggal namun itu menyebabkan tidak adanya *fault tolerancy* atau toleransi kesalahan yang mengakibatkan jika koneksi terputus maka *frame* yang dikirim tidak akan sampe ke alamat tujuan. Berikut merupakan contoh STP pada sebuah perangkat dapat dilihat pada Gambar 6.

```
Fl-l3sw#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0002.165A.E524
             Cost        19
             Port        5(GigabitEthernet1/0/5)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00D0.BA8A.E2D9
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/7          Desg FWD 19        128.7    P2p
Gi1/0/8          Desg FWD 19        128.8    P2p
Gi1/0/3          Desg FWD 19        128.3    P2p
Gi1/0/4          Desg FWD 19        128.4    P2p
Gi1/0/5          Root FWD 19        128.5    P2p
Gi1/0/6          Desg FWD 19        128.6    P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     00D0.BA2B.622A
             Cost        19
             Port        3(GigabitEthernet1/0/3)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     00D0.BA8A.E2D9
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
```

Gambar 6. Spanning Tree pada MLS 1

a. Pemilihan Root Bridge
   1) Setiap switch akan membandingkan Bridge ID masing-masing, yang terkecil akan dipilih menjadi Root Bridge
   2) Bridge ID = Switch priority + MAC Address
   3) Switch priority by default 32768 (angkanya 0 – 65535, kelipatan 4096)
   4) Untuk bisa mengetahui Root Bridge dari 5 switch di topologi diatas bisa menggunakan perintah " show spanning-tree".

   Dan setelah melakukan langkah – langkah diatas MLS 1 menjadi *Root Bridge* untuk menjadi memilih rute dan rekonfigurasi fungsi-fungsi dari *bridge-bridge* lainnya bila perlu. Setelah *Root Bridge* sudah ditentukan yaitu di MLS 1, ketika melakukan konfigurasi pada MLS 1 yang lain tidak akan menjadi *Root Bridge*, tapi menjadi *cost* yang berarti sebuah jalur total yang diakumulasi berdasarkan pada *bandwith* yang tersedia pada tiap link lakukan pada MLS 3. Konfigurasi hanya dilakukan pada dua perangkat karena, masing masing perangkat terdapat beberapa VLAN didalam. Pada MLS 1 terdapat VLAN 10 hingga 60 sedangkan untuk MLS 3 terdapat VLAN 70 -120.

b. Tentukan *Root Port* (RP) di tiap *switch* lain selain *Root Bridge*

   Cari cost dari setiap interface switch menuju Root Bridge. Yang terkecil costnya yang akan dipilih menjadi Root Port. Cost:
   1) 10 Mbps = 100
   2) 100 Mbps = 19
   3) 1 Gbps = 4
   4) 10 Gbps = 2
   5) Kalau sama, bandingkan Port ID yang terkecil akan dipilih menjadi Root Port
   6) Port ID = Port Priority + Port Number
   7) Port Priority by default 128 (angkanya 0 – 255)

```
VLAN0060
  Spanning tree enabled protocol ieee
  Root ID    Priority    32828
             Address     0006.2AB9.BAC5
             Cost        19
             Port        8(GigabitEthernet1/0/8)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32828  (priority 32768 sys-id-ext 60)
             Address     00D0.BA8A.E2D9
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/7          Desg FWD 19        128.7    P2p
Gi1/0/3          Desg FWD 19        128.3    P2p
Gi1/0/6          Desg FWD 19        128.6    P2p
Gi1/0/8          Root FWD 19        128.8    P2p
Gi1/0/4          Desg FWD 19        128.4    P2p
Gi1/0/5          Desg FWD 19        128.5    P2p
```

Gambar 7. *Root Por* pada MLS 1

Gambar diatas dapat dilihat bahwasanya setiap vlan sudah mempunyai *root* masing – masing dan mengarah kepada *cost* 19. Dapat disimpulkan setiap VLAN mempunyai kecepatan sebesar 19 Mbps sebagai *root port* atau *port* untuk pengiriman data.

6. Rencana Anggaran Biaya

Berdasarkan perhitungan sesuai dengan perencanaan didapat total pengeluaran biaya sebesar Rp 625.320.000.

Pembahasan

Berdasarkan hasil dari pengujian yang telah dilakukan dngan menerapkan beberapa metode yang direncanakan didapat hasil sesuai dengan yang diharapkan. Pengiriman paket data dengan menerapkan *Inter-VLAN Routing* berbasis *open short path first* dapat melakukan pengiriman data meskipun dengan VLAN yang berbeda, dengan melakukan pengujian konektifitas sebanyak 50 kali, data yang dikirimkan 100% sampe ke tujuan dengan tidak ada data yang hilang atau *packet loss*, kemudian untuk membuat pengiriman data tetap dalam kondisi aman dan terjaga autentikasi dari data tersebut metode *port security* dan *secure shell* menjadi solusi supaya pihak yang tidak bertanggung jawab tidak dapat mengakses data selama dikirimkan. Port security melakukan *blocking* terhadap *mac-address* yang tidak terdaftar pada *mac-address* tabel, yang membuat data tersebut tidak dapat masuk kedalam server atau jaringan. *Secure shell*. Pengujian ini dilakukan pada salah satu PC atau *Client*, yang bertujuan untuk mengetahui ketersediaan layanan remote access dari perangkat jaringan pada saat akan digunakan Jika ketika menginput *username* dan *password* yang sudah didaftarkan sebelumnya pada konfigurasi salah, maka tidak dapat mengakses perangkat tersebut. Tingkat keamanan pada sistem *Secure Shell* sangat tinggi, jika tidak sesuai akan muncul tulisan "*login invalid*". Dapat dipastikan pengguna tidak akan bisa mengakses atau menggunakan perangkat tersebut. Spanning-tree diaktifkan untuk menghindari tabrakan antar data saat pengiriman paket data, dengan terdapat *spanning-tree* tersedia jalur *back-up* atau *redundancy* yang membuat pengiriman paket data tetap dapat terkirim meskipun salah satu jalur mati atau terputus

KESIMPULAN

Dari penelitian tentang Perancangan Infrastruktur Jaringan *InterVLAN* dengan keamanan *port security* dan *Secure Shell* berbasis *Open Short Path First* pada PT. ENSHU INDONESIA, dapat terlihat 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. Kemudian metode *port security* dan *secure shell* merupakan metode yang digunakan untuk mengamankan paket data, dengan cara memblock *mac-address* yang tidak terdaftar pada mac-address tabel, paket data yang *mac-address* yang tidak terdaftar pada *mac-address* tabel tidak akan sampai pada tujuan, sedangkan *secure shell* bertujuan untuk mengetahui ketersediaan layanan *remote access* dari perangkat jaringan pada saat akan digunakan Jika ketika menginput *username* dan *password* yang sudah didaftarkan sebelumnya pada konfigurasi salah, maka tidak dapat mengakses perangkat tersebut. *Spanning-tree* digunakan untuk mencegah terjadi *looping* atau tabrakan antar data dengan membuat jalur cadangan apabila salah satu jalur mati atau terputus.

DAFTAR REFERENSI

A. Hendri Ardiansyah, H. Y., 2021. *Perancangan Jaringan Intervlan Routing Dan Penerapan Acls Pada Pt.Sinar Alam Permai Dengan Simulasi Menggunakan Packet Tracer*. Seminar Hasil Penelitian Vokasi (Semhavok).

Adi Sopian, K. K. I. D. P. G., 2022. *Perancangan Jaringan Virtual Lan Menggunakan Metode Protokol Peer-Vlan Spanning Tree*. Jurnal Elektro & Informatika Swadharma (Jeis).

Adia Pratama Nugraha Permana, R. F., 2018. *Distribusi Jaringan Menggunakan Routing Ospf Dengan Metode Redistribution*. Simetris.

Ahmad, A. N., 2020. *Design And Implementation Of Network Security Using Inter- Vlan-Routing And Dhcp*. Asian Journal Of Applied Science And Technology, Volume 4, Pp. 37-44.

Ahmad, S. P., 2021. *Perancangan Infrastruktur Jaringan Komputer Menggunakan Fiber Optic Dengan Metode Network Develpoment Life Cycle (Ndlc)*. E-Proceeding Of Engineering, Volume 8, Pp. 12066 - 12079.

Badia Raja, L. S., 2017. *Kualitas Jaringan Pada Jaringan Virtual Local Area Network (Vlan) Yang Menerapkan Linux Terminal Server Project (Ltsp).* Pinter.

Givy Devira Ramady, R. H. A. A. G. M. W. H., 2019. *Optimizing Wireless Distribution System Network Infrastructure in Hybrid Topology using PCQ Method*. Journal of Physics: Conference Series.

S.Somasundaram, M., 2018. *A Simulation based study on Network Architecture Using Inter-VLAN Routing and Secure Campus Area Network (CAN)*. International Journal of Computer Sciences and Engineering.

Sutanto, P. H., 2018. *Perancangan Virtual Local Area Network Berbasis VTP Dan Inter-Vlan Routing*. Jurnal Teknik Komputer