

Nama : Jonathan Natannael Zefanya
NIM : 1152200024

UAS Jarkom 2024

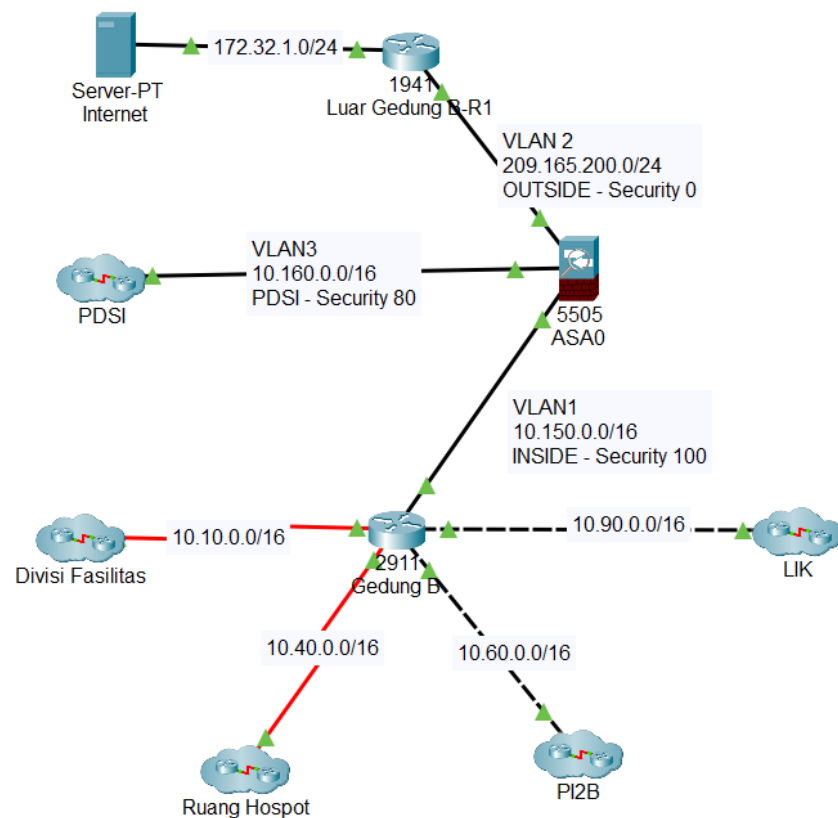
Jaringan Komputer Gedung B

STUDI KASUS

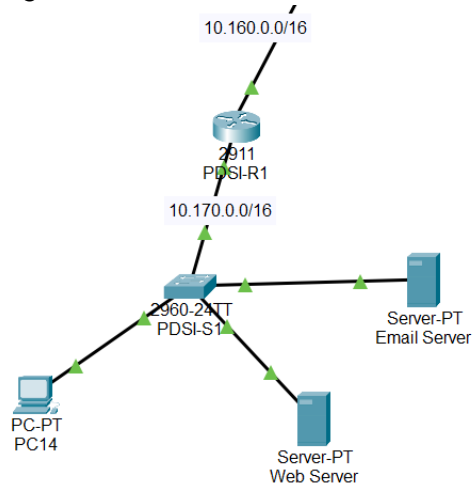
Membuat jaringan kampus ITI terutama pada gedung B agar aman mencegah penyerangan oleh jaringan luar kampus ITI dimana kita membuat zona demiliterisasi yang berada pada PDSI dan membuat jaringan dalam gedung B dapat mengakses jaringan luar tetapi jaringan luar ITI tidak bisa mengakses ITI secara langsung.

1. Topologi Star

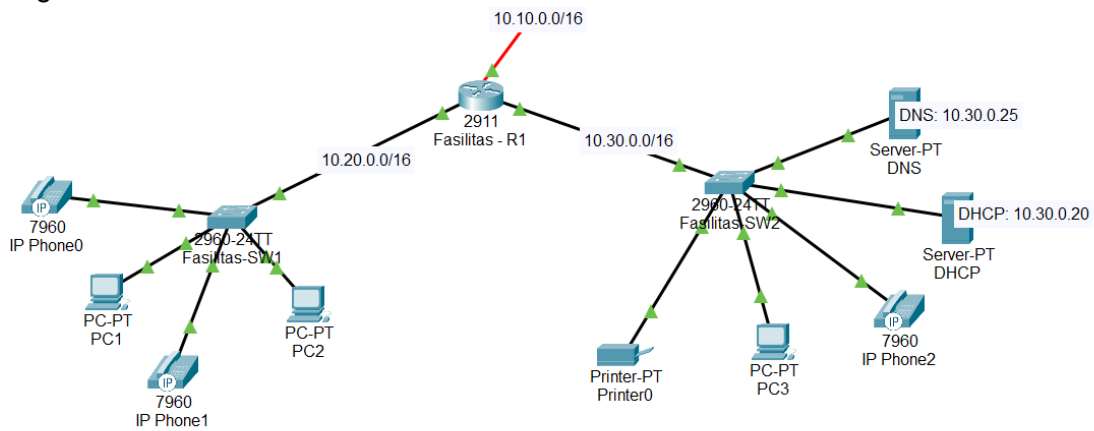
Topologi Keseluruhan



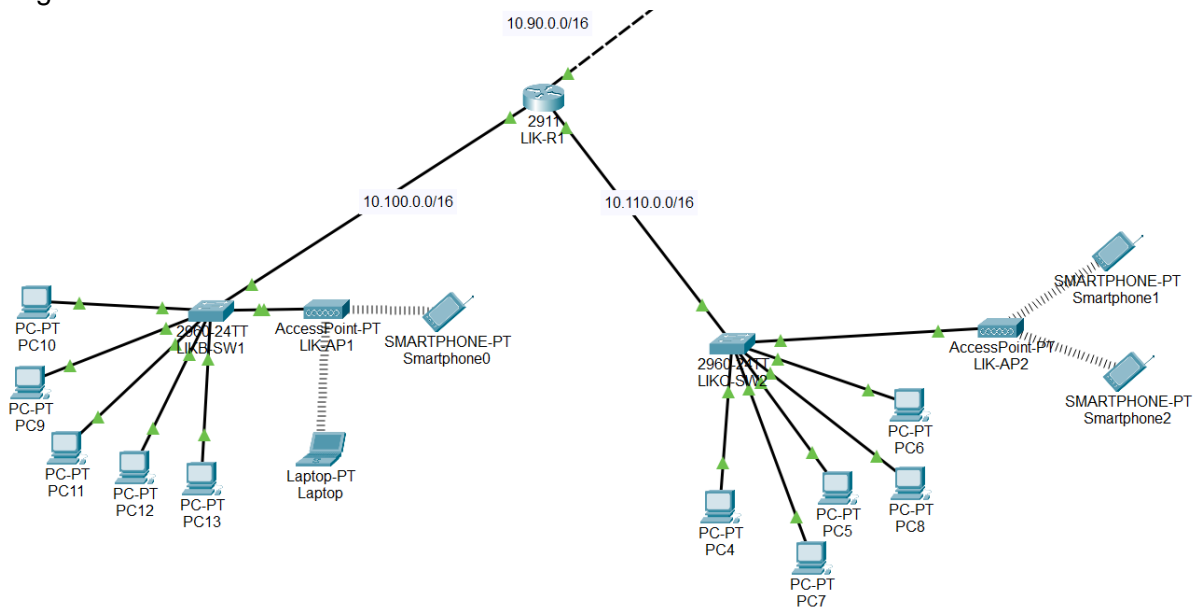
Topologi PDSI



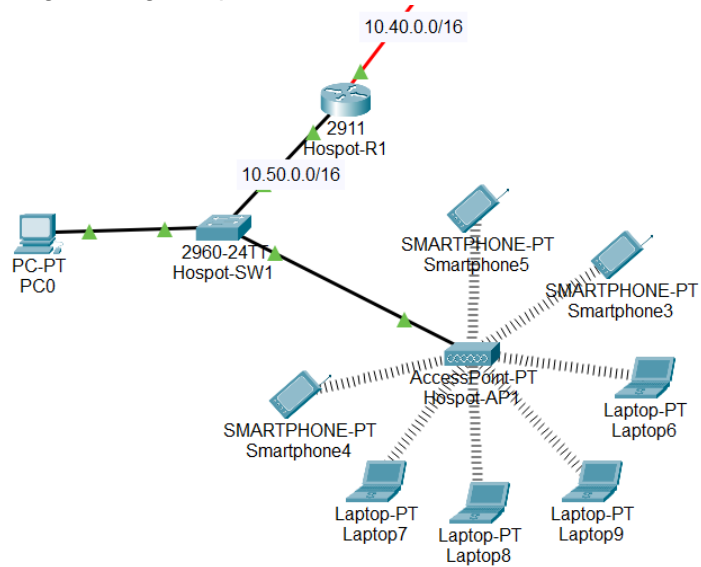
Topologi Divisi Fasilitas



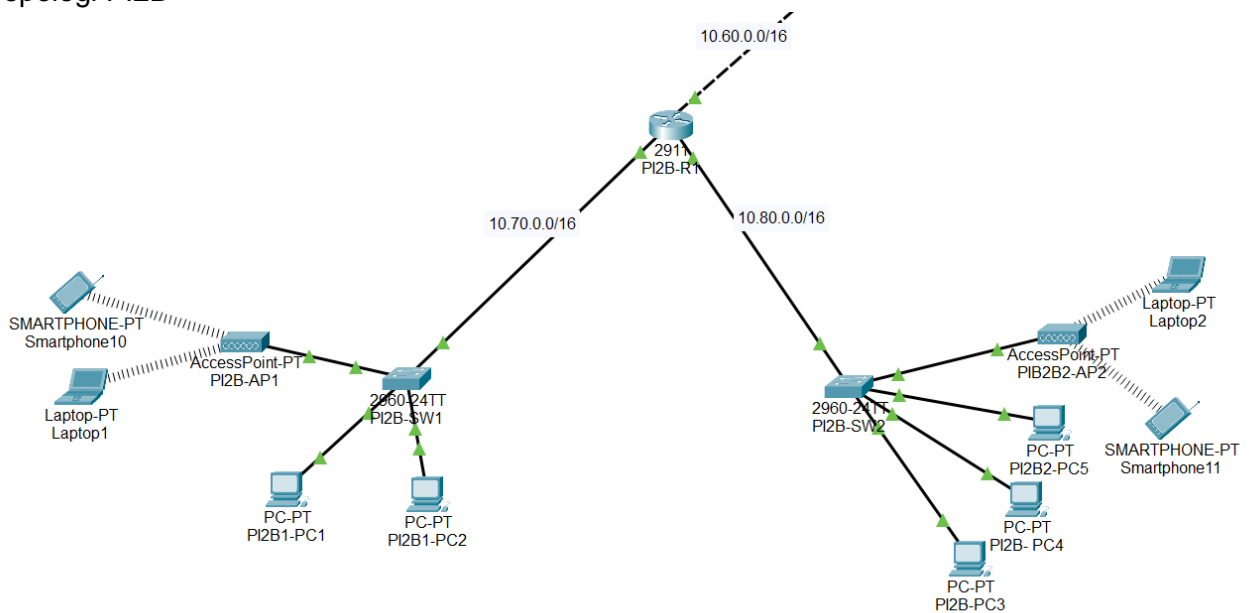
Topologi LIK



Topologi Ruang Hospot



Topologi PI2B



2. Penjelasan Tiap Area Jaringan

1. Jaringan Dalam (INSIDE)

Saya merancang jaringan dalam untuk mereplikasi sebuah kampus ITI di Gedung B dengan sejumlah ruangan yang berbeda. Sebagai contoh, saya menyertakan Divisi Fasilitas, PI2B, LIK, dan Ruang Hospot. Saya mengatur pengaturan keamanan firewall untuk jaringan internal ke 100, yang berarti jalur internal ini memiliki tingkat kepercayaan tertinggi.

Router bertindak sebagai lapisan inti dari topologi jaringan saya. Saya membuat satu router untuk setiap “ruangan” di jaringan gedung B, dengan satu router tambahan yang menghubungkan setiap ruangan. Saya sengaja menggunakan satu router dengan koneksi serial dan gigabit ke router di ruangan-ruangan untuk mempelajari lebih lanjut tentang Arsitektur Jaringan. Saya akan menjelaskannya lebih lanjut di Bagian 1 - Router.

Divisi Fasilitas memiliki beberapa jaringan lokal yang dipisahkan ke dalam domain broadcast oleh router ruangan. Saya menambahkan perangkat yang mungkin ditemukan di LAN ruangan pada umumnya, seperti printer, telepon IP, dan komputer desktop. Saya juga menyertakan server DNS dan DHCP sehingga seluruh jaringan di dalam memiliki akses ke layanan-layanan tersebut, dan agar bisa dikelola secara terpusat dari Divisi Fasilitas.

Cluster jaringan lainnya termasuk Ruang Hospot, PI2B, dan LIK. Situs-situs ini mencakup sejumlah jenis perangkat akhir yang berbeda seperti PC, Laptop, dan smartphone. Saya menambahkan titik akses nirkabel di setiap cluster, dengan asumsi bahwa ini akan menjadi cara utama mahasiswa mengakses jaringan dalam arsitektur gedung B.

2. Jaringan PDSI (Sebagai Zona Demiliterisasi)

Saya membuat PDSI sebagai Zona Demiliterisasi sebagai cara untuk menyaring trafik dari internet OUTSIDE. Namun, trafik dari dalam jaringan masih dapat mengakses jaringan luar dan PDSI itu sendiri. Karena saya kurang percaya pada jaringan yang datang dari internet OUTSIDE yang lebih luas, saya mengatur keamanan untuk PDSI ke 80.

Saya menambahkan PDSI ke topologi Secure Byte University dengan asumsi bahwa orang-orang perlu mengakses email dan server web dari dalam dan luar jaringan. Saya berasumsi bahwa Secure Byte University juga akan memiliki banyak trafik dari luar jaringan yang mencoba mengakses ITI. Akhirnya, mahasiswa, alumni, dan staf ITI juga ingin mengakses server email ITI.

3. Jaringan Luar (OUTSIDE)

Jaringan luar dimaksudkan untuk mewakili jaringan internet yang lebih luas (bukan bagian dari ITI). Saya menambahkan router di bagian luar firewall untuk meniru router kampus yang tersambung ke Penyedia Layanan Provider Internet. Karena saya paling tidak mempercayai jalur dari jaringan internet lainnya, saya mengatur keamanan pada firewall saya ke 0, yang mewakili tingkat keamanan tertinggi.

Pengaturan firewall dikonfigurasi sehingga jalur yang datang dari jaringan internet dapat mengakses PDSI, tetapi tidak di manapun di jaringan internal. Setiap jaringan dipisahkan oleh VLAN yang terhubung ke firewall. Hal ini mencegah lalu lintas dari luar untuk mencapai jaringan di dalam, sementara memungkinkan lalu lintas untuk mengakses PDSI yang berisi email dan server web.

3. Network Architecture

Topologi jaringan Saya membagi menjadi tiga bagian berikut, dipisahkan oleh firewall:

1. Jaringan dalam kampus yang aman
2. PDSI
3. Jaringan luar yang terdiri dari internet yang lebih luas

4. Perangkat Jaringan

Dalam arsitektur jaringan saya menggunakan beberapa perangkat jaringan sebagai berikut:

1. Router (1941 & 2911)
2. Switch(2960-24TT)
3. Access Points
4. Firewall
5. Server: DNS, Web, Email, DHCP
6. End-devices: Personal computers, laptops, smartphones
7. Tambahan: Printers, IP Phones

Section 1 - Routers

Agar router dapat berkomunikasi satu sama lain, saya menggunakan dua metode terpisah untuk menghubungkannya. Pertama, saya secara statis menetapkan alamat jaringan 0.0.0.0 bersama dengan gateway default, yang merupakan alamat IP dari router penerima. Hal ini memungkinkan router untuk meneruskan IP yang tidak diketahui ke router hop berikutnya. Dalam kasus LIK dan PI2B, saya menggunakan kabel crossover yang terhubung ke port gigabit router kampus. Dalam kasus lain, saya memilih untuk menggunakan port serial router. Namun, hal ini mengharuskan saya menambahkan perangkat secara manual ke router kampus agar dapat berkomunikasi melalui port serial. Ini adalah perangkat HWIC-2T, yang menyediakan 2 port serial High-Speed WAN Interface Card Serial 2-Port Cisco. Penggunaan rute 0.0.0.0 dengan router dikenal juga dengan nama Gateway of Last Resort.

Saya memilih untuk menggunakan server DHCP dalam topologi jaringan saya daripada setiap router menggunakan layanan DHCP sendiri. Untuk melakukan ini, saya harus menambahkan alamat IP DHCP ke router melalui IP helper, dengan cara ini router mengetahui ke mana harus mengarahkan lalu lintas ketika perangkat ingin mendapatkan alamat IP secara dinamis. DHCP untuk semua perangkat yang terhubung ke jaringan internal kampus dari Divisi Fasilitas.

Section 2 - Switch

Saya menambahkan Switch di berbagai ruangan untuk menambahkan perangkat lapisan distribusi sehingga menghubungkan setiap perangkat di jaringan individual. Saya mengubah nama host setiap perangkat untuk mencerminkan lokasinya di topologi. Saya menghubungkannya ke perangkat akhir, titik akses, dan router dengan kabel langsung.

Section 3 - Access Points

Saya memutuskan untuk menyertakan wireless access points di LIK untuk mensimulasikan koneksi 2,4 dan 5 GHz agar dapat menangani kedua jenis perangkat tersebut. Saya mengamankan jaringan dengan mengubah SSID default, mengubah keamanan ke WPA2 Personal, dan membuat kata sandi: ***sburules!***

Section 4 - Firewall

Saya menerapkan langkah-langkah berikut untuk jalur masuk ke firewall. Pertama, saya menambahkan peta ruangan untuk mengidentifikasi jalur yang masuk, diikuti dengan peta kebijakan untuk mengidentifikasi tindakan yang harus diambil terhadap jalur yang sebenarnya. Saya kemudian menyesuaikan kebijakan layanan, yang saya gunakan untuk menerapkan langkah sebelumnya. Saya mengatur nama host, nama domain, kata sandi, mengaktifkan VLAN1 dan 2 di dalam dan di luar, dan menambahkan kata sandi "***sbu1***".

Saya mengintegrasikan mekanisme perutean IP Statis ke dalam konfigurasi firewall, memperkenalkan pendekatan strategis untuk menentukan jalur perutean untuk lalu lintas masuk. Melalui penetapan rute statis, saya memastikan bahwa lalu lintas masuk dapat diarahkan kembali ke IP sumber secara efisien, sehingga memfasilitasi komunikasi dua arah yang optimal.

NAT Dinamis dikonfigurasi untuk lalu lintas keluar yang berasal dari jaringan internal, memungkinkan pemetaan alamat IP pribadi internal ke kumpulan alamat IP publik saat mengakses jaringan eksternal. Selain itu, NAT Statis diterapkan untuk sumber daya internal dan firewall tertentu, memfasilitasi jalur masuk dari internet dengan mempertahankan pemetaan yang konsisten.

Untuk menyelaraskan dengan kebijakan keamanan dan kontrol akses, saya menerapkan NAT pada jalur masuk yang ditujukan ke PDSI dari lapisan luar. Hal ini melibatkan penerjemahan alamat IP sumber secara strategis untuk memastikan bahwa lalu lintas dapat mencapai PDSI dengan lancar, sehingga menciptakan keseimbangan antara aksesibilitas dan langkah-langkah keamanan yang ketat.

Sepanjang proyek ini, saya berhasil mengatasi sejumlah tantangan dengan firewall saya, seperti membangun saluran komunikasi dua arah yang efisien, memastikan bahwa lalu lintas masuk, setelah menjalani perutean NAT dan IP statis, dapat melintasi kembali ke IP sumber.

Selain itu, saya menavigasi kompleksitas kontrol akses PDSI, secara strategis menerapkan NAT untuk lalu lintas PDSI yang masuk guna menegakkan kebijakan keamanan.

Section 5 - Servers

Jaringan saya mencakup server web, server email dalam PDSI, dan server DNS, dan server DHCP di Divisi Fasilitas.

Kita dapat mengetikkan nama domain yang sepenuhnya memenuhi syarat atau sebagian domain, termasuk www.sbu.edu, sbu.edu atau bahkan hanya "sbu" dan tetap menjangkau situs web Secure Byte University, yang mencerminkan bagaimana situs web dalam kehidupan nyata menggunakan Sistem Nama Domain. Namun, ketika situs dimuat, nama domain yang sepenuhnya memenuhi syarat tidak ditampilkan pada toolbar URL seperti di dunia nyata karena keterbatasan server DNS Packet Tracer.

Section 6 - End-devices & Tambahan

Saya mengenable DHCP pada perangkat akhir untuk terhubung ke gateway default masing-masing di setiap "ruangan", secara otomatis menetapkan alamat IP, subnet mask, dan IP server DNS yang saya temukan di Divisi Fasilitas.

Saya menambahkan alamat IP statis di server dan perangkat lain seperti printer karena alamat tersebut tidak perlu diubah atau tidak boleh memperbarui alamat IP secara otomatis.

Tambahan di jaringan saya, hanya terdiri dari printer dan telepon IP. Saya menetapkan IP statis ke printer karena ini dianggap sebagai 'praktik terbaik' karena printer adalah perangkat yang dimaksudkan untuk selalu terhubung ke jaringan.









	Device	Interface	IP Address	Subnet Mask	Default Gateway
Main Map	Firewall Inside	VLAN 1	10.150.0.1	255.255.0.0	
	Firewall Outside	VLAN 2	209.165.200.1	255.255.255.0	
	Firewall PDSI	VLAN3	10.160.0.1	255.255.0.0	
	Luar Gedung-R1	G0/0	172.32.1.1	255.255.255.0	
		G0/1	209.165.200.2	255.255.255.0	
	Internet Server	Fe0/0	172.32.1.2	255.255.255.0	
	Gedung B	G0/0	10.150.0.2	255.255.0.0	
		G0/1	10.90.0.1	255.255.0.0	
		G0/2	10.60.0.1	255.255.0.0	
		Se0/0/0	10.10.0.1	255.255.0.0	
		Se0/0/1	10.40.0.1	255.255.0.0	
Divisi Fasilitas	Router Fasilitas-R1	Serial 0/0/1	10.10.0.2	255.255.0.0	
		G0/1	10.20.0.1	255.255.0.0	
		G0/2	10.30.0.1	255.255.0.0	

	Device	Interface	IP Address	Subnet Mask	Default Gateway
Divisi Fasilitas	Switch Fasilitas-SW1	Fe0/1			10.20.0.1
	Switch Fasilitas-SW2	Fe0/1			10.30.0.1
	DNS Server		10.30.0.25	255.255.0.0	
	DHCP Server		10.30.0.20	255.255.0.0	
Ruang Hospot	Router Hospot-R1	Se0/0/0	10.40.0.2	255.255.0.0	
		G0/1	10.50.0.1	255.255.0.0	
	Switch Hospot-SW1				10.50.0.1
LIK	Router LIK-R1	G0/0	10.90.0.2	255.255.0.0	
		G0/1	10.100.0.1	255.255.0.0	
		G0/2	10.110.0.1	255.255.0.0	
	Switch LIK-SW1	Fe0/1			10.100.0.1
	Switch LIK-SW2	Fe0/1			10.110.0.1
PI2B	Router PI2B-R1	G0/0	10.60.0.2	255.255.0.0	
		G0/1	10.70.0.1	255.255.0.0	

	Device	Interface	IP Address	Subnet Mask	Default Gateway
PI2B		G0/2	10.80.0.1	255.255.0.0	
	Switch PI2B-SW1				10.70.0.1
	Switch PI2B-SW2				10.80.0.1
PDSI	Router PDSI-R1	0/0	10.160.0.2	255.255.0.0	
		0/1	10.170.0.1	255.255.0.0	
	Switch PDSI-S1				10.170.0.1
	Web Server	Fe0/0	10.170.0.20	255.255.0.0	
	Email Server	Fe0/0	10.170.0.30	255.255.0.0	

5. Result

a. Sesama di gedung B

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC5	PI2B- PC4	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC7	PC0	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC5	PC2	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC5	PC7	ICMP		0.000	N	3	(edit)	(delete)

Test ping PC 5 (LIK) ke PC PI2B-PC4 (PI2B)

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.80.0.6

Pinging 10.80.0.6 with 32 bytes of data:

Request timed out.
Reply from 10.80.0.6: bytes=32 time<1ms TTL=125
Reply from 10.80.0.6: bytes=32 time=9ms TTL=125
Reply from 10.80.0.6: bytes=32 time<1ms TTL=125

Ping statistics for 10.80.0.6:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 9ms, Average = 3ms

C:\>ping 10.80.0.6

Pinging 10.80.0.6 with 32 bytes of data:

Reply from 10.80.0.6: bytes=32 time<1ms TTL=125
Reply from 10.80.0.6: bytes=32 time<1ms TTL=125
Reply from 10.80.0.6: bytes=32 time<1ms TTL=125
Reply from 10.80.0.6: bytes=32 time<1ms TTL=125

Ping statistics for 10.80.0.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
  
```

b. PC 5 (LIK) ke PC 14 (PDSI) dan PC 5 LIK ke Server Internet (Luar Gedung B)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC5	PC14	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC5	Internet	ICMP		0.000	N	1	(edit)	(delete)

Test Ping PC 5 (LIK) ke PC 14 (PDSI)

```

C:\>ping 10.170.0.10

Pinging 10.170.0.10 with 32 bytes of data:

Reply from 10.170.0.10: bytes=32 time=14ms TTL=124
Reply from 10.170.0.10: bytes=32 time=1ms TTL=124
Reply from 10.170.0.10: bytes=32 time=2ms TTL=124
Reply from 10.170.0.10: bytes=32 time<1ms TTL=124

Ping statistics for 10.170.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 4ms
  
```

Test Ping PC 5 (LIK) ke Server Internet (Luar Gedung B)

```





C:\>ping 172.32.1.2

Pinging 172.32.1.2 with 32 bytes of data:

Reply from 172.32.1.2: bytes=32 time=1ms TTL=124
Reply from 172.32.1.2: bytes=32 time<1ms TTL=124
Reply from 172.32.1.2: bytes=32 time=2ms TTL=124
Reply from 172.32.1.2: bytes=32 time=1ms TTL=124

Ping statistics for 172.32.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms
  
```

c. PC 14 (PDSI) ke PC 5 (LIK) dan Server Internet (Luar Gedung B)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC14	PC5	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC14	Internet	ICMP		0.000	N	1	(edit)	(delete)

Test Ping PC 14 (PDSI) ke PC 5 (LIK)

```
C:\>ping 10.110.0.5

Pinging 10.110.0.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.110.0.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Test Ping PC 14(PDSI) ke Server Internet (Luar Gedung B)





```
C:\>ping 172.32.1.2

Pinging 172.32.1.2 with 32 bytes of data:

Reply from 172.32.1.2: bytes=32 time=2ms TTL=125
Reply from 172.32.1.2: bytes=32 time<1ms TTL=125
Reply from 172.32.1.2: bytes=32 time<1ms TTL=125
Reply from 172.32.1.2: bytes=32 time=2ms TTL=125

Ping statistics for 172.32.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

d. Server Internet (Luar Gedung B) ke PC 14 (PDSI) dan PC 5 (LIK)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Internet	PC14	ICMP		0.000	N	0	(edit)	(delete)
	Failed	Internet	PC5	ICMP		0.000	N	1	(edit)	(delete)

Test Ping Server Internet (Luar Gedung B) ke PC 14 (PDSI)

```
C:\>ping 10.170.0.10

Pinging 10.170.0.10 with 32 bytes of data:

Reply from 10.170.0.10: bytes=32 time=1ms TTL=125
Reply from 10.170.0.10: bytes=32 time=1ms TTL=125
Reply from 10.170.0.10: bytes=32 time<1ms TTL=125
Reply from 10.170.0.10: bytes=32 time=1ms TTL=125

Ping statistics for 10.170.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Test Ping Server Internet (Luar Gedung B) ke PC 5 (LIK)

```
C:\>ping 10.110.0.5

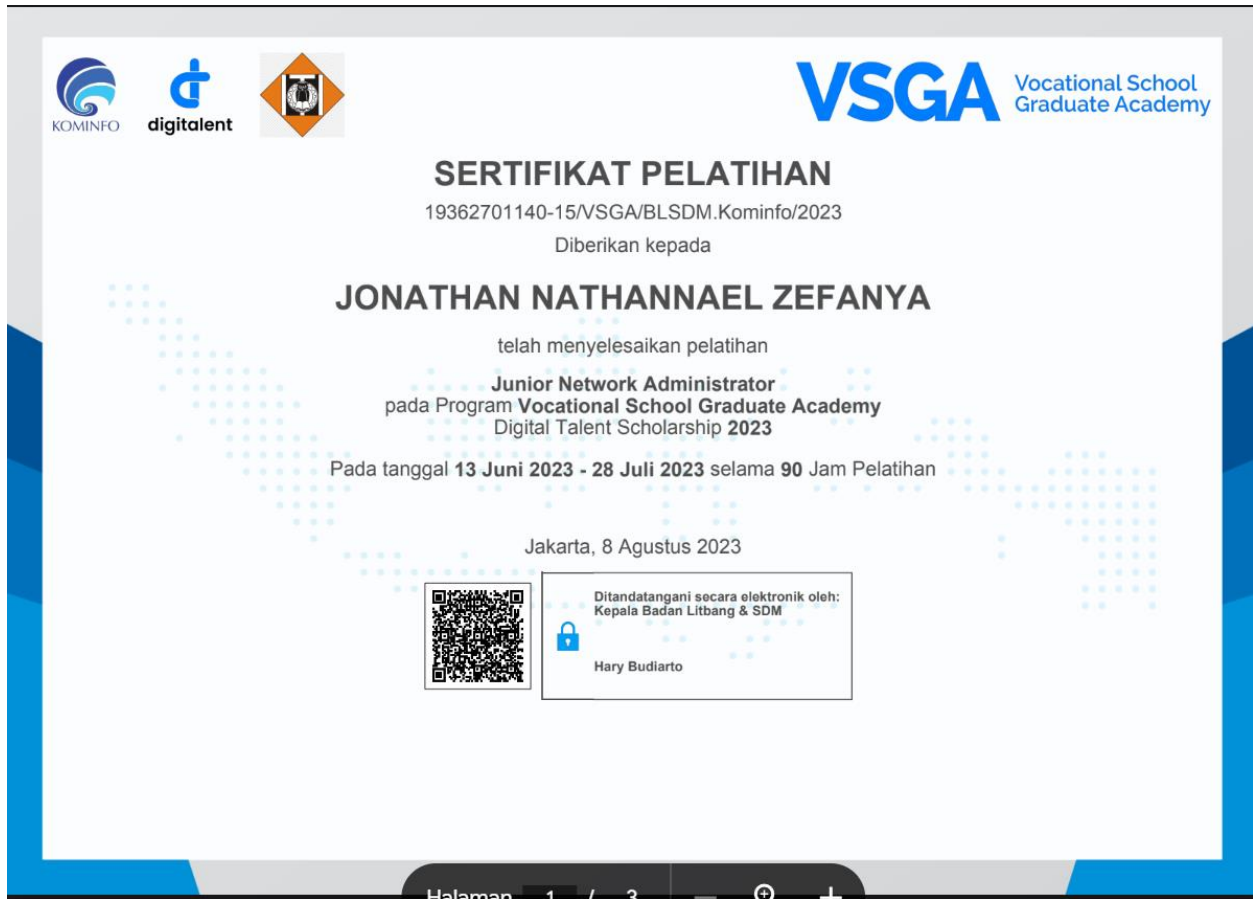
Pinging 10.110.0.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.110.0.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

LAMPIRAN SERTIFIKAT SEBAGAI NILAI TAMBAHAN:

Foto Sertifikat:



Link sertifikat:

<https://drive.google.com/file/d/1CbxNC9-8YdUWJCbRxtfK4sszAOEzhqjn/view>