

# **Mini Project With Gemini Cisco Packet Tracer**

**Week 2**

**Cristhian Abimayu Wibowo**

**Daftar Isi**

<b>Pendahuluan .....</b>	3
<b>Soal Praktik .....</b>	4
<b>Soal Essai .....</b>	5
<b>Jawaban Essai .....</b>	6
<b>Hasil Praktik .....</b>	7
1. <b>Topologi.....</b>	7
1. <b>VLSM.....</b>	7
2. <b>Konfigurasi Router .....</b>	8
3. <b>Konfigurasi Switch.....</b>	12
4. <b>Konfigurasi PC.....</b>	14
5. <b>Hasil Konfigurasi .....</b>	18
<b>Penutup .....</b>	20

## Pendahuluan

Ini merupakan mini project yang saya buat untuk mengisi waktu luang saya, dimana saya memanfaat gemini untuk membuatkan saya soal dengan cara menjadikan gemini peran sebagai senior network engineer yang memberikan tugas kepada junior network engineer (peran saya), dengan prompt sebagai berikut.

“saya ingin membuat mini project jaringan menggunakan cisco packet tracer disini saya ingin meminta bantuan anda. Anda berperan sebagai Senior Network Engineer yang memberikan tugas kepada Junior Network Engineer untuk mengerjakan tugas menggunakan packet tracer dimana anda memberikan soal dengan tingkat kesulitan yang sesuai dengan kebutuhan perusahaan serta anda juga memberikan 3 soal essay yang berhubungan dengan jaringan jadi nanti ada 2 soal dimana ada soal essay dan soal praktik menggunakan packet tracer soal praktik sudah sama tugas VLSM. Hasil akhir nanti saya berikan kepada anda untuk di koreksi serta diberikan saran jika memang ada.”

AI ada bukan untuk menggantikan proses berpikir kita tapi untuk mempertajamnya hehe. Semoga bermanfaat dan semoga dengan adanya dokumentasi ini bisa membantu seseorang dalam belajar mengenai jaringan khususnya konfigurasi pada cisco packet tracer.

## Soal Praktik

Tugas Proyek Jaringan Skala Lanjut (Enterprise WAN & Security)

Skenario Perusahaan: Konektivitas Kantor Pusat (HQ) dan Kantor Cabang (Branch)

TechGlobal Corp (Perusahaan Anda) perlu menghubungkan Kantor Cabang (Branch) baru ke Kantor Pusat (HQ). Kantor Pusat memiliki beberapa departemen (VLAN) dan koneksi Internet utama. Kantor Cabang adalah situs yang lebih kecil dan hanya memiliki satu LAN.

Tugas Anda adalah membangun topologi ini, memastikan konektivitas penuh, menerapkan keamanan dasar dengan ACL, dan mengizinkan seluruh jaringan internal mengakses Internet melalui satu alamat IP Public.

Topologi Dasar:

- Router 1 (R-HQ): Terhubung ke LAN (dengan VLAN) dan ke Router ISP.
- Router 2 (R-Branch): Terhubung ke LAN-nya sendiri dan ke R-HQ melalui link WAN.
- Router 3 (R-ISP): Mensimulasikan Internet (cukup berikan satu Loopback Interface).

Alokasi IP Awal: Anda dialokasikan Network Address tunggal: 192.168.100.0/24

Kebutuhan Host (VLSM):

Lokasi Segmen Jaringan Kebutuhan Host Minimum

HQ VLAN 10 – Sales 50 Host

HQ VLAN 20 – Technical 25 Host

Branch VLAN 30 – Admin 10 Host

WAN Link HQ ke Branch 2 Host (Point-to-Point)

WAN Link HQ ke ISP 2 Host (Point-to-Point)

**Tugas Utama (Implementasi di Packet Tracer):**

### Perhitungan VLSM

Menggunakan Network Address 192.168.100.0/24, hitung alokasi subnet untuk semua 5 segmen di atas (Sales, Technical, Admin, HQ-Branch, HQ-ISP).

Ingat, urutkan dari kebutuhan terbesar ke terkecil.

Buat tabel hasil perhitungan VLSM Anda.

Konfigurasi R-HQ (Kantor Pusat)

### Inter-VLAN Routing (ROAS):

- Buat VLAN 10 (Sales) dan VLAN 20 (Technical) pada Switch HQ.
- Konfigurasikan interface fisik router (misalnya G0/0) dengan Sub-interface (.10 dan .20) menggunakan enkapsulasi dot1Q.
- Pastikan link dari Switch ke R-HQ adalah Trunk.
- Konfigurasikan PC di setiap VLAN.

### Koneksi WAN (Static Routing):

- Konfigurasikan interface Serial (atau Ethernet) yang terhubung ke R-Branch dengan IP dari alokasi VLSM Anda.
- Konfigurasikan interface Serial (atau Ethernet) yang terhubung ke R-ISP dengan IP dari alokasi VLSM Anda.

**NAT Overload (PAT):**

- Konfigurasikan PAT pada R-HQ sehingga semua jaringan internal (VLAN 10, VLAN 20, dan VLAN 30 dari Branch) dapat mengakses "Internet" (R-ISP).
- Definisikan interface inside dan outside dengan benar.

**Routing:**

- Buat Static Route di R-HQ agar dapat menjangkau LAN R-Branch (VLAN 30).
- Buat Default Route (0.0.0.0 0.0.0.0) yang mengarah ke R-ISP.

**1. Konfigurasi R-Branch (Kantor Cabang)**

## Konfigurasi LAN:

- Konfigurasikan interface G0/0 (LAN) dengan Default Gateway untuk VLAN 30 (Admin).
- Konfigurasikan PC di VLAN 30.

## Routing :

- Buat Default Route (0.0.0.0 0.0.0.0) yang mengarah ke R-HQ. (Mengapa ini cara yang efisien untuk Branch? Pikirkan tentang itu).

**2. Konfigurasi R-ISP (Simulasi Internet)**

Konfigurasi Interface: Konfigurasikan interface yang terhubung ke R-HQ.

Simulasi Layanan: Buat Loopback Interface 0 dengan alamat IP 8.8.8.8/32. Ini mewakili server Google.

**3. Konfigurasi Keamanan (ACL)**

Tujuan: Departemen Sales (VLAN 10) sedang mengalami masalah dan tidak boleh diizinkan mengakses jaringan Admin di Kantor Cabang (VLAN 30).

Implementasi: Buat Extended Access Control List (ACL) di R-HQ.

## Logika ACL:

- Deny traffic dari subnet VLAN 10 ke subnet VLAN 30.
- Permit semua traffic IP lainnya (agar VLAN 20 dan Internet tetap berfungsi).

Terapkan ACL ini pada interface (atau sub-interface) yang paling efisien.

**4. Verifikasi dan Pengujian**

- Test 1 (Inter-VLAN): Ping dari PC Sales (VLAN 10) ke PC Technical (VLAN 20). Harus Berhasil.
- Test 2 (PAT): Ping dari PC Technical (VLAN 20) ke 8.8.8.8 (R-ISP Loopback). Harus Berhasil.
- Test 3 (ACL Deny): Ping dari PC Sales (VLAN 10) ke PC Admin (VLAN 30). Harus GAGAL (Destination host unreachable).
- Test 4 (ACL Permit): Ping dari PC Technical (VLAN 20) ke PC Admin (VLAN 30). Harus Berhasil.

**Soal Essai****Jawablah pertanyaan-pertanyaan berikut dengan jelas dan ringkas.****1. Soal Esai 1 (Analisis Routing Protocol)**

Anda sudah pernah menggunakan OSPF (di tugas pertama Anda) dan saya minta Anda menggunakan *Static Route* di tugas ini. Jelaskan perbedaan fundamental antara **(a)**

**Static Routing, (b) OSPF (Link-State), dan (c) EIGRP (Advanced Distance-Vector).** Fokus pada:

- a) Bagaimana *router* "belajar" (*learn*) tentang *route* baru?
- b) Apa itu *Administrative Distance (AD)* dan mengapa itu penting?
- c) Kapan Anda sebagai *Network Engineer* akan memilih Static Route daripada *dynamic protocol*?

## 2. Soal Esai 2 (Analisis Access Control List - ACL)

Dalam tugas ini, saya meminta Anda menggunakan **Extended ACL**. Jelaskan perbedaan utama antara **Standard ACL** dan **Extended ACL**. Mengapa Anda tidak bisa menggunakan Standard ACL untuk menyelesaikan tugas keamanan (Test 3) di atas?

## 3. Soal Esai 3 (Konsep DHCP Relay)

Di semua skenario kita sejauh ini, DHCP Server (jika digunakan) berada di *subnet* yang sama dengan *client* (atau DHCP Server dikonfigurasi langsung di router/L3 Switch). Jelaskan apa itu **DHCP Relay (IP Helper-Address)**. Dalam skenario apa seorang *Network Engineer* mutlak harus menggunakan fitur ini?

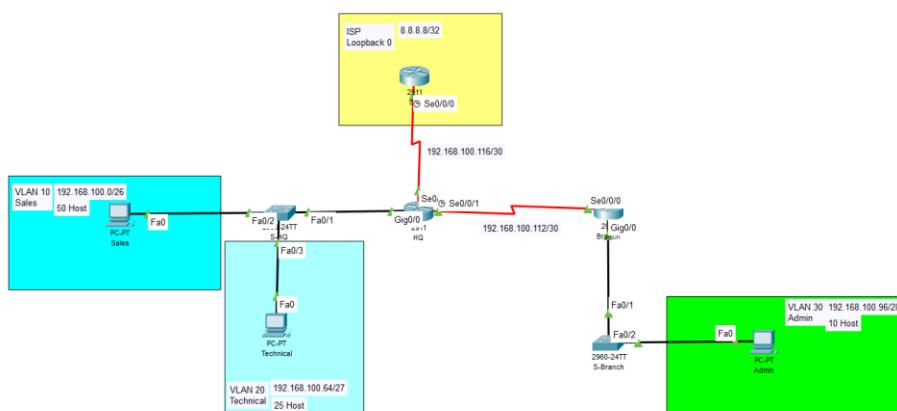
# Jawaban Essai

1. Perbedaan fundamental antara static routing, OSPF, dan EIGRP terletak pada pemakaiannya, konfigurasinya, serta cara routing mengenali topologi jaringannya
  - a) Pada static routing router tidak belajar karena konfigurasi yang digunakan merupakan konfigurasi secara langsung untuk mengenali jaringan di sekitarnya. OSPF mengandalkan LSA (Link state advertisement) dimana setiap router membuat table routing berdasarkan LSA yang dikirimkan oleh setiap router kemudian algoritma yang digunakan pada OSPF merupakan algoritma SPF (Shortest Path First) dimana jarak terdekatlah yang akan digunakan. Jika OSPF mengandalkan semua router EIGRP hanya belajar dari router di jaringan terdekatnya kemudian algoritma yang digunakan yaitu DUAL (Diffusing Update Algorithm) dimana algoritma ini digunakan untuk menghitung rute terdekat serta memastikan rute bebas loop.
  - b) AD pada routing merupakan angka yang digunakan untuk memilih rute atau penggunaan routing terbaik berdasarkan angka terkecil. AD sangat penting dalam routing jika dalam penggunaan topologi kita terdapat dua routing, disini peran AD akan berguna dimana nantinya router akan menentukan jalur berdasarkan AD terkecil.
  - c) Penggunaan static routing lebih cocok pada jaringan yang memiliki skala kecil jika jaringan yang dibangun besar lebih baik menggunakan dynamic routing

2. Standar ACL dan Extended ACL merupakan konsep yang digunakan untuk membuat ACL dalam sebuah ruter untuk menentukan sesuatu penggunaan standar ACL digunakan Ketika membuat rule tanpa perlu tahu spesifik apa yang ingin diijinkan atau diblokir sementara Extended ACL digunakan untuk membuat rule yang spesifik seperti pemberian protocol serta port. Jadi pada test 3 menggunakan extended ACL dikarenakan perlunya sesuatu yang spesifik terhadap tindakan antara VLAN 10 dan VLAN 30.
3. DHCP Relay digunakan Ketika router tidak memberikan dhcp secara langsung namun terdapat server khusus untuk dhcp, disinilah peran DHCP Relay yaitu untuk menghubungkan antara client dengan server dhcp pada jaringan vln yang berbeda misalnya. Penggunaan DHCP Relay digunakan Ketika router tidak memberikan ip dhcp secara langsung dan peran tersebut digantikan oleh server dhcp.

## Hasil Praktik

### 1. Topologi



Topologi yang saya buat menggunakan 3 router dimana setiap router memiliki perannya masing-masing seperti router ISP yang digunakan untuk menghubungkan ke internet kemudian ada router HQ dimana router HQ memiliki peran yang penting untuk menghubungkan internet ke jaringan branch. Router HQ merupakan router yang berada di Perusahaan utama kemudian ada router branch yang ditempatkan di Perusahaan cabang. Konsep topologi yang saya gunakan yaitu WAN multi cabang.

### 1. VLSM

- HQ VLAN 10 – Sales 50 Host
- HQ VLAN 20 – Technical 25 Host
- Branch VLAN 30 – Admin 10 Host
- WAN Link HQ ke Branch 2 Host (Point-to-Point)
- WAN Link HQ ke ISP 2 Host (Point-to-Point)
- IP Address awal **192.168.100.0/24**

Nama	Host	Prefix	Network	Range IP	Broadcast	Subnet
VLAN 10 - Sales	50	/26	192.168.100.0	192.168.100.1 - 192.168.100.62	192.168.100.63	255.255.255.192
VLAN 20 - Technical	25	/27	192.168.100.64	192.168.100.65 - 192.168.100.94	192.168.100.95	255.255.255.224
VLAN 30 - Admin	10	/28	192.168.100.96	192.168.100.97 - 192.168.100.110	192.168.100.111	255.255.255.240
HQ - Branch	2	/30	192.168.100.112	192.168.100.113 - 192.168.100.114	192.168.100.115	255.255.255.252
HQ - ISP	2	/30	192.168.100.116	192.168.100.117 - 192.168.100.118	192.168.100.119	255.255.255.252

## 2. Konfigurasi Router

### a. Konfigurasi Router HQ (Perusahaan Utama)

- Konfigurasi dasar

```

Router>ena
Router#conf t
Router(config)#hostname R-HQ
R-HQ(config)#no ip domain-lookup
R-HQ(config)#banner motd #
Enter TEXT message. End with the character '#'.
Router HQ, Unauthorized user can't login #
R-HQ(config)#enable secret admin123
R-HQ(config)#line con 0
R-HQ(config-line)#password admin123
R-HQ(config-line)#login
R-HQ(config-line)#exit
R-HQ(config)#ip domain name HQ.local
R-HQ(config)#username admin privilege 15 password admin123
R-HQ(config)#crypto key generate rsa
The name for the keys will be: R-HQ.HQ.local
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

```

```

R-Branch(config)#ip ssh version 2
R-HQ(config)#line vty 0 4
R-HQ(config-line)#transport input ssh
R-HQ(config-line)#login local
R-HQ(config-line)#exit

```

- Konfigurasi IP Address

```

Router>ena
Router#conf t

```

```
R-HQ(config)#int gig0/0
R-HQ(config-if)#no sh
R-HQ(config-if)#ex
R-HQ(config)#int gig0/0.10
R-HQ(config-subif)#encapsulation dot1Q 10
R-HQ(config-subif)#ip add 192.168.100.1 255.255.255.192
R-HQ(config-subif)#ex
R-HQ(config)#int gig0/0.20
R-HQ(config-subif)#encapsulation dot1Q 20
R-HQ(config-subif)#ip add 192.168.100.65 255.255.255.224
R-HQ(config-subif)#ex
R-HQ(config)#int se0/0/0
R-HQ(config-if)#ip add 192.168.100.117 255.255.255.252
R-HQ(config-if)#no sh
R-HQ(config-if)#ex
R-HQ(config)#int se0/0/1
R-HQ(config-if)#ip add 192.168.100.113 255.255.255.252
R-HQ(config-if)#no sh
R-HQ(config-if)#ex
```

- **Konfigurasi DHCP**

```
Router>ena
Router#conf t
R-HQ(config)#ip dhcp pool Sales
R-HQ(dhcp-config)#network 192.168.100.0 255.255.255.192
R-HQ(dhcp-config)#default
R-HQ(dhcp-config)#default-router 192.168.100.1
R-HQ(dhcp-config)#dns 8.8.8.8
R-HQ(dhcp-config)#ex
R-HQ(config)#ip dhcp pool Technical
R-HQ(dhcp-config)#network 192.168.100.64 255.255.255.224
R-HQ(dhcp-config)#default-router 192.168.100.65
R-HQ(dhcp-config)#dns 8.8.8.8
R-HQ(dhcp-config)#ex
```

- **Konfigurasi Static Routing**

```
Router>ena
Router#conf t
R-HQ(config)#ip route 192.168.100.96 255.255.255.240 192.168.100.114
R-HQ(config)#ip route 0.0.0.0 0.0.0.0 192.168.100.118
```

- **Konfigurasi NAT**

```
Router>ena
Router#conf t
R-HQ(config)#access-list 1 permit 192.168.100.0 0.0.0.63
R-HQ(config)#access-list 1 permit 192.168.100.64 0.0.0.31
R-HQ(config)#access-list 1 permit 192.168.100.112 0.0.0.3
R-HQ(config)#access-list 1 permit 192.168.100.96 0.0.0.15
R-HQ(config)#access-list 1 deny any
R-HQ(config)#ip nat pool HQ 198.100.100.1 198.100.100.1 netmask
255.255.255.0
R-HQ(config)#ip nat inside source list 1 pool HQ overload
R-HQ(config)#int gig0/0.10
```

```
R-HQ(config-subif)#ip nat inside
R-HQ(config-subif)#ex
R-HQ(config)#int gig0/0.20
R-HQ(config-subif)#ip nat inside
R-HQ(config-subif)#ex
R-HQ(config)#int se0/0/1
R-HQ(config-if)#ip nat inside
R-HQ(config-if)#ex
R-HQ(config)#int se0/0/0
R-HQ(config-if)#ip nat outside
R-HQ(config-if)#ex
```

- **Konfigurasi Extended ACL**

```
Router>ena
Router#conf t
R-HQ(config)#ip access-list extended dilarang
R-HQ(config-ext-nacl)#deny icmp 192.168.100.0 0.0.0.63 192.168.100.96
0.0.0.15
R-HQ(config-ext-nacl)#deny tcp 192.168.100.0 0.0.0.63 192.168.100.96
0.0.0.15 eq 21
R-HQ(config-ext-nacl)#permit ip any any
R-HQ(config-ext-nacl)#ex
R-HQ(config)#int se0/0/1
R-HQ(config-if)#ip access-group dilarang out
R-HQ(config-if)#ex
R-HQ(config)#int gig0/0.20
R-HQ(config-subif)#ip access-group dilarang in
R-HQ(config-subif)#ex
R-HQ(config)#int gig0/0.10
R-HQ(config-subif)#ip access-group dilarang in
R-HQ(config-subif)#ex
```

**b. Konfigurasi Router Branch (Perusahaan Cabang)**

- **Konfigurasi dasar**

```
Router>ena
Router#conf t
Router(config)#hostname R-Branch
R-Branch(config)#no ip domain-lookup
R-Branch(config)#banner motd #
Enter TEXT message. End with the character '#'.
Router Branch, Unauthorized user can't login #
R-Branch(config)#enable secret admin123
R-Branch(config)#line con 0
R-Branch(config-line)#password admin123
R-Branch(config-line)#login
R-Branch(config-line)#exit
R-Branch(config)#ip domain name Branch.local
R-Branch(config)#username admin privilege 15 password admin123
R-Branch(config)#crypto key generate rsa
The name for the keys will be: R-Branch.Branch.local
Choose the size of the key modulus in the range of 360 to 4096 for your
```

General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R-Branch(config)#ip ssh version 2

R-Branch(config)#line vty 0 4

R-Branch(config-line)#transport input ssh

R-Branch(config-line)#login local

R-Branch(config-line)#exit

- **Konfigurasi IP Address**

Router>ena

Router#conf t

R-Branch(config)#int gig0/0

R-Branch(config-if)#no sh

R-Branch(config-if)#ex

R-Branch(config)#int gig0/0.30

R-Branch(config-subif)#

R-Branch(config-subif)#encapsulation dot1Q 30

R-Branch(config-subif)#ip add 192.168.100.97 255.255.255.240

R-Branch(config-subif)#ex

R-Branch(config)#int se0/0/0

R-Branch(config-if)#ip add 192.168.100.114 255.255.255.252

R-Branch(config-if)#no sh

R-Branch(config-if)#ex

- **Konfigurasi Static routing**

Penggunaan default route pada router branch efisien karena tidak perlu mengenali semua jaringan yang ada di kantor pusat serta pada kantor cabang hanya ada satu jaringan. Serta penggunaan default route secara penggunaanya itu Ketika paket masuk ke router dan router tidak tahu akan kemana paket dikirimkan maka router akan memilih hop yang di konfigurasi pada default route.

Router>ena

Router#conf t

R-Branch(config)#ip route 0.0.0.0 0.0.0.0 192.168.100.113

### c. Konfigurasi Router ISP

- **Konfigurasi dasar**

Router>ena

Router#conf t

Router(config)#hostname ISP

ISP(config)#no ip domain-lookup

ISP(config)#enable secret admin123

ISP(config)#banner motd #

Enter TEXT message. End with the character '#'.  
ISP, Unauthorized user can't login #

ISP(config)#ip domain name ISP.local

ISP(config)#username admin privilege 15 password admin123

ISP(config)#crypto key generate rsa

The name for the keys will be: ISP.ISP.local

Choose the size of the key modulus in the range of 360 to 4096 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

ISP(config)#ip ssh version 2

ISP(config)#line vty 0 4

ISP(config-line)#transport input ssh

ISP(config-line)#login local

ISP(config-line)#exit

- **Konfigurasi IP Address**

Router>ena

Router#conf t

ISP(config)#int se0/0/0

ISP(config-if)#ip add 192.168.100.118 255.255.255.252

ISP(config-if)#no sh

ISP(config-if)#ex

ISP(config)#int lo 0

ISP(config-if)#ip add 8.8.8.8 255.255.255.255

ISP(config-if)#no sh

ISP(config-if)#ex

- **Konfigurasi Static Routing**

Router>ena

Router#conf t

ISP(config)#ip route 0.0.0.0 0.0.0.0 192.168.100.117

### 3. Konfigurasi Switch

Switch disini diberikan konfigurasi dasar untuk diberikan akses SSH serta mengamankan switch dari pengguna yang tidak sah serta memberikan VLAN.

- **Switch HQ**

Switch>ena

Switch#conf t

Switch(config)#hostname S-HQ

S-HQ(config)#no ip domain-lookup

S-HQ(config)#banner motd #

Enter TEXT message. End with the character '#'.  
Switch HQ, Unauthorized user can't login #

S-HQ(config)#enable secret admin123

S-HQ(config)#line con 0

S-HQ(config-line)#password admin123

S-HQ(config-line)#login

S-HQ(config-line)#exit

S-HQ(config)#ip domain name HQ.local

S-HQ(config)#username admin privilege 15 password admin123

S-HQ(config)#crypto key generate rsa

The name for the keys will be: S-HQ.HQ.local

Choose the size of the key modulus in the range of 360 to 4096 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024

```
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
S-HQ(config)#ip ssh version 2
S-HQ(config)#line vty 0 4
S-HQ(config-line)#transport input ssh
S-HQ(config-line)#login local
S-HQ(config-line)#exit
S-HQ(config)#vlan 10
S-HQ(config-vlan)#name Sales
S-HQ(config-vlan)#vlan 20
S-HQ(config-vlan)#name Technical
S-HQ(config-vlan)#exit
S-HQ(config)#int fa0/1
S-HQ(config-if)#switchport mode trunk
S-HQ(config-if)#exit
S-HQ(config)#int fa0/2
S-HQ(config-if)#switchport mode access
S-HQ(config-if)#switchport access vlan 10
S-HQ(config-if)#exit
S-HQ(config)#int fa0/3
S-HQ(config-if)#switchport mode access
S-HQ(config-if)#switchport access vlan 20
S-HQ(config-if)#exit
S-HQ(config)#

```

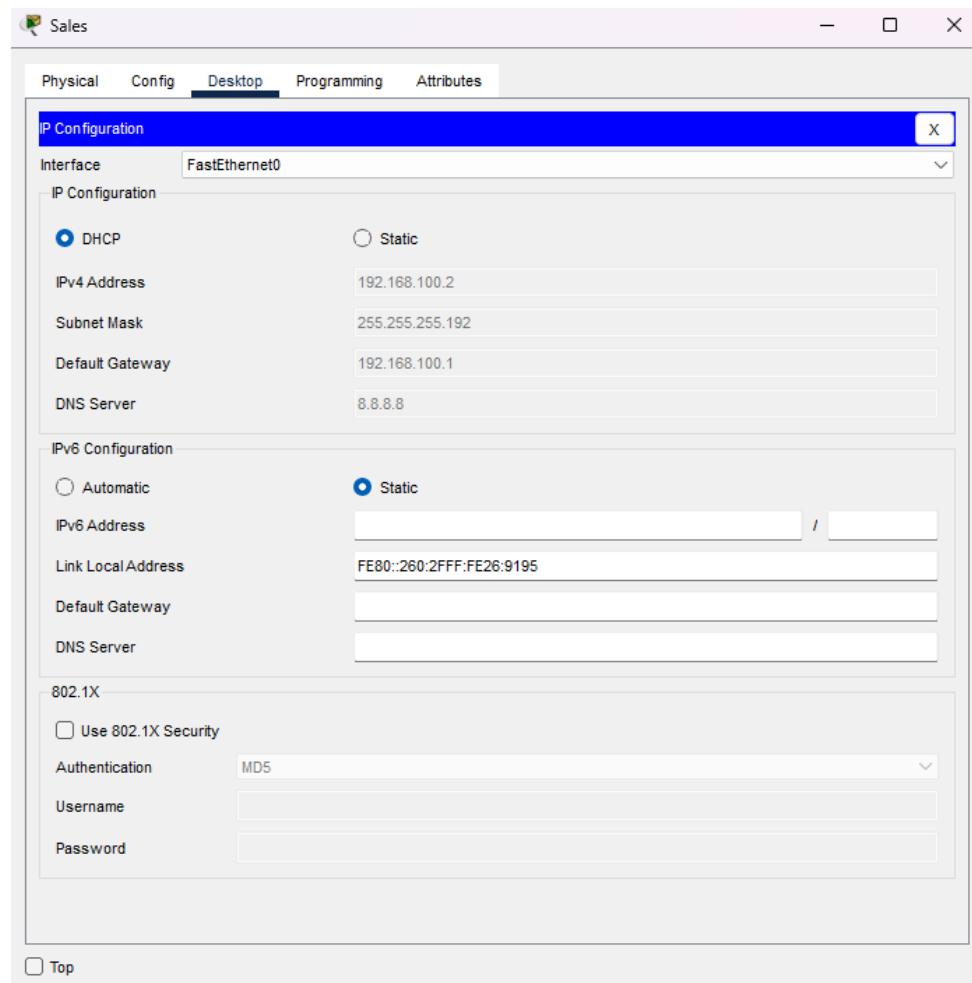
- **Switch Branch**

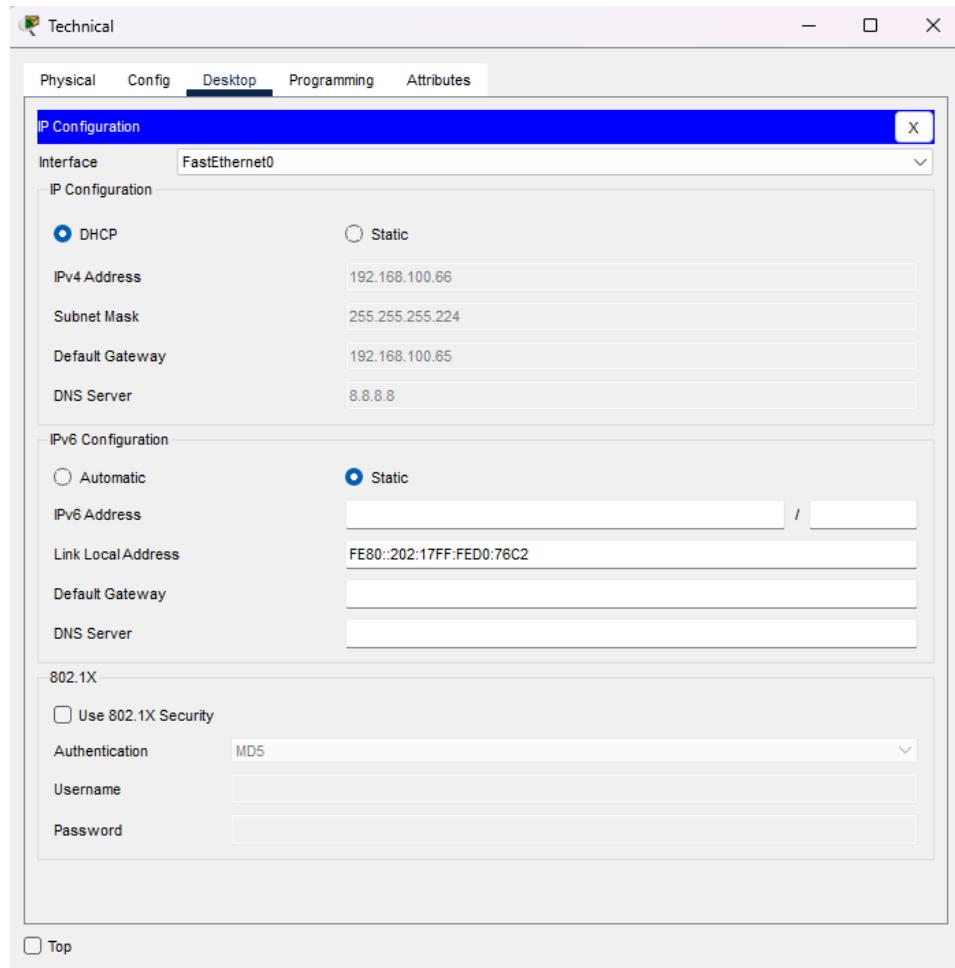
```
Switch>ena
Switch#conf t
Switch(config)#hostname S-Branch
S-Branch(config)#no ip domain-lookup
S-Branch(config)#banner motd #
Enter TEXT message. End with the character '#'.
Switch Branch, Unauthorized user can't login #
S-Branch(config)#enable secret admin123
S-Branch(config)#line con 0
S-Branch(config-line)#password admin123
S-Branch(config-line)#login
S-Branch(config-line)#exit
S-Branch(config)#username admin privilege 15 password admin123
S-Branch(config)#ip domain name Branch.local
S-Branch(config)#crypto key generate rsa
The name for the keys will be: S-Branch.Branch.local
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
S-Branch(config)#ip ssh version 2
*Mar 1 0:38:34.345: %SSH-5-ENABLED: SSH 1.99 has been enabled
S-Branch(config)#line vty 0 4
S-Branch(config-line)#transport input ssh
S-Branch(config-line)#login local
```

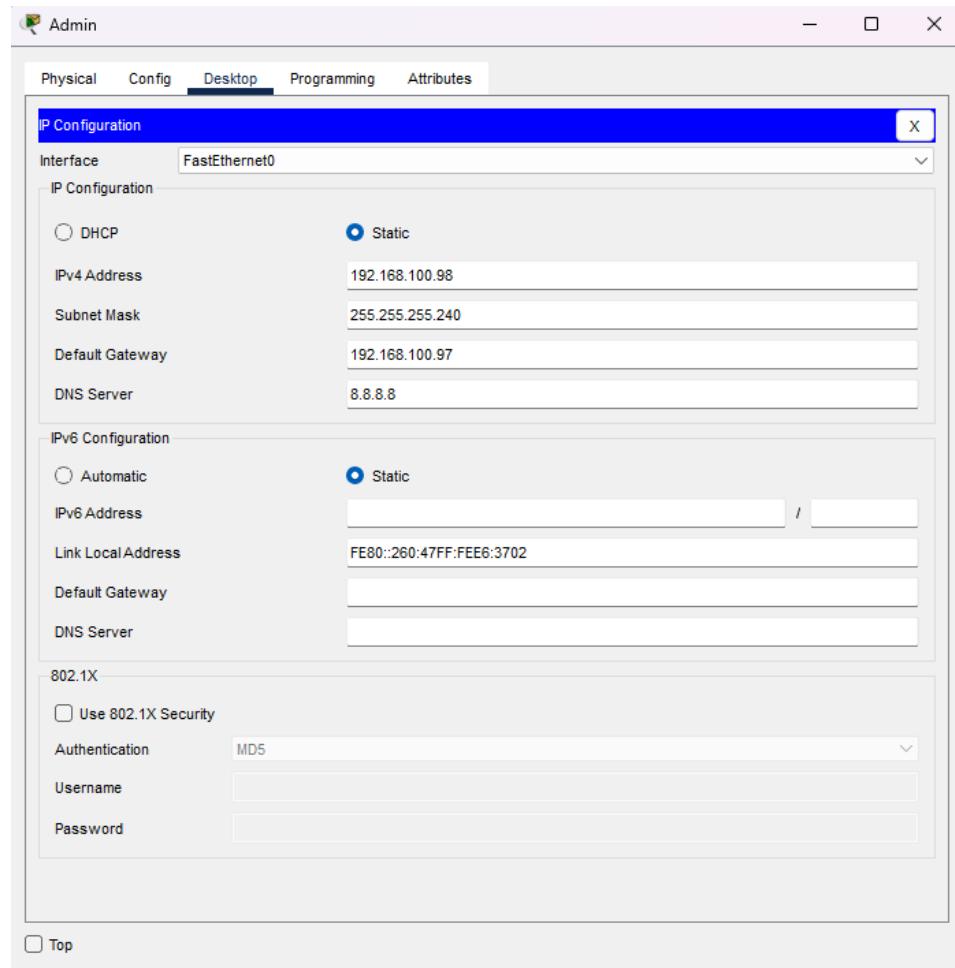
```
S-Branch(config-line)#exit
S-Branch(config)#vlan 30
S-Branch(config-vlan)#name Admin
S-Branch(config-vlan)#exit
S-Branch(config)#int fa0/1
S-Branch(config-if)#switchport mode trunk
S-Branch(config-if)#exit
S-Branch(config)#int fa0/2
S-Branch(config-if)#switchport mode access
S-Branch(config-if)#switchport access vlan 30
S-Branch(config-if)#exit
```

#### 4. Konfigurasi PC

Pada PC disini khusus untuk bagian Admin diberikan IP Address secara statis kemudian setiap PC pada Perusahaan utama atau PC dalam jaringan HQ diberikan IP secara dinamis pemilihan ini didasari dari banyaknya jumlah pemakai statis untuk admin dikarenakan pengguna admin hanya beberapa namun pemberian IP dinamis pada jaringan HQ dikarena jaringan tersebut digunakan untuk produktifitas perusahaan.

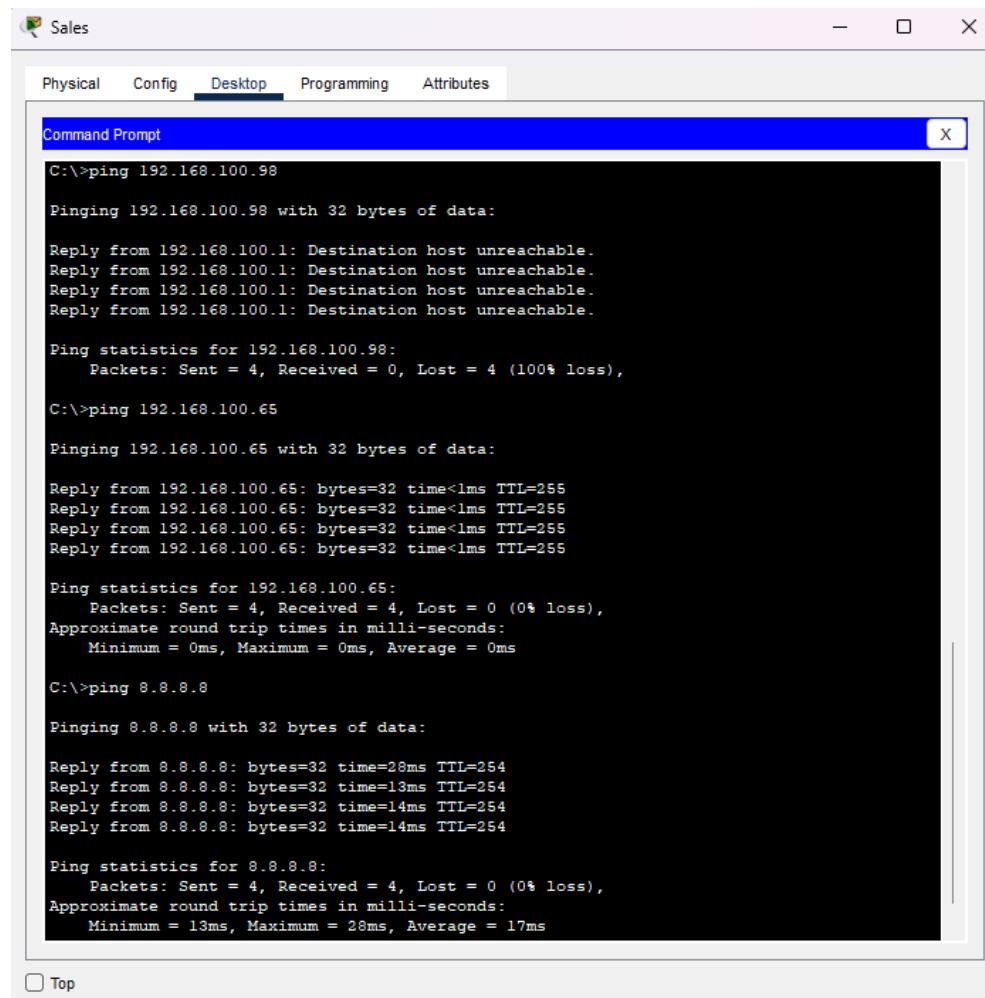






## 5. Hasil Konfigurasi

Hasil konfigurasi disini menunjukan hasil dari ACL yang diberikan pada jaringan khusus VLAN 10 Sales berhasil diterapkan hal tersebut dapat dilihat dari hasil ping dari pc sales menuju pc admin. Pada pc admin Ketika ping ke pc sales juga tidak berhasil hal tersebut dikarenakan Ketika paket diterima pc sales kemudian pc sales mengirimkan paket Kembali paket tersebut di drop oleh ACL di router HQ.



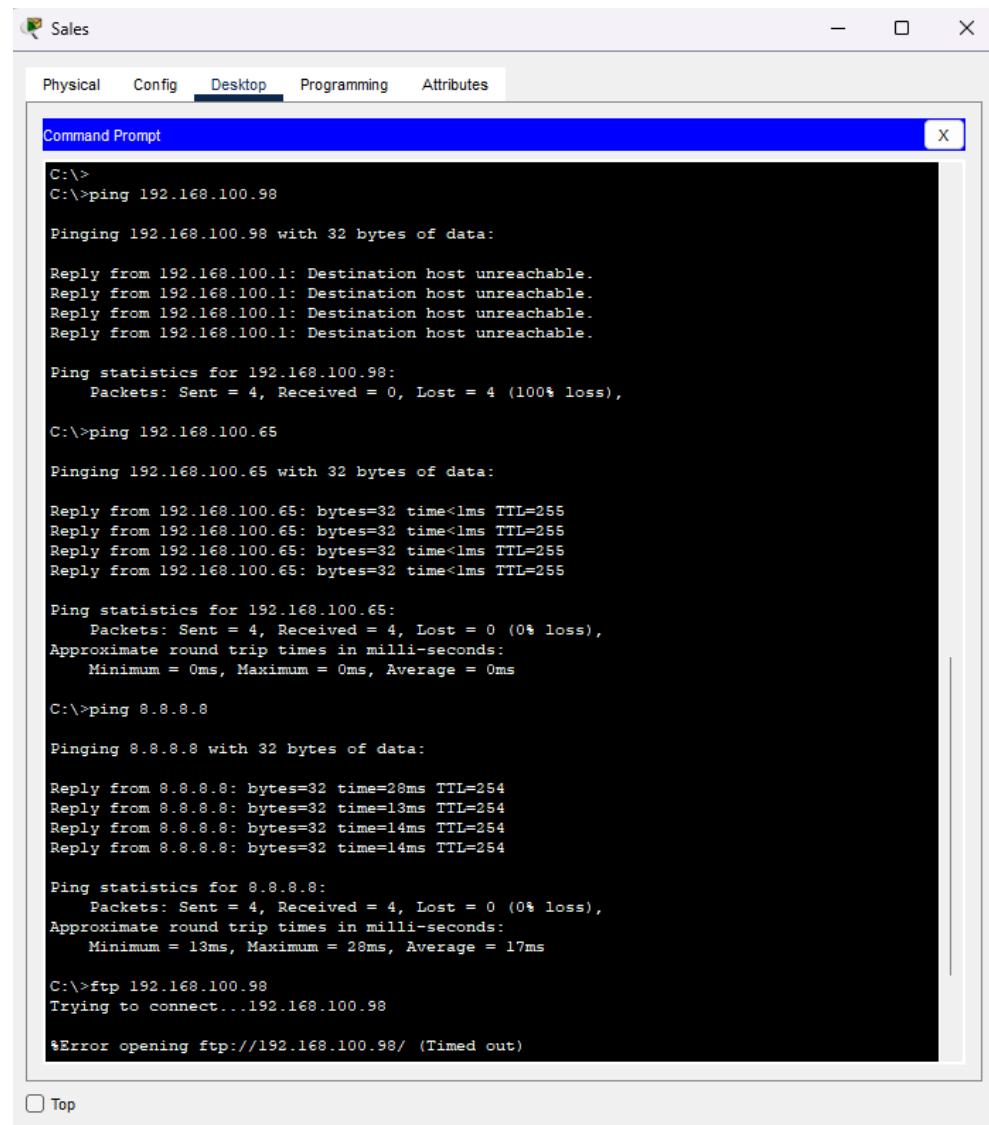
The screenshot shows a Windows Command Prompt window titled "Sales". The window has tabs at the top: Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is selected. The main area of the window displays command-line output:

```
C:\>ping 192.168.100.98
Pinging 192.168.100.98 with 32 bytes of data:
Reply from 192.168.100.1: Destination host unreachable.

Ping statistics for 192.168.100.98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.100.65
Pinging 192.168.100.65 with 32 bytes of data:
Reply from 192.168.100.65: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.100.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=28ms TTL=254
Reply from 8.8.8.8: bytes=32 time=13ms TTL=254
Reply from 8.8.8.8: bytes=32 time=14ms TTL=254
Reply from 8.8.8.8: bytes=32 time=14ms TTL=254

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 28ms, Average = 17ms
```



The screenshot shows a software application window titled "Sales". The main menu bar includes "Physical", "Config", "Desktop", "Programming", and "Attributes". A tab labeled "Desktop" is currently selected. Below the menu is a "Command Prompt" window with a blue header bar containing the title and a close button ("X"). The command prompt displays the following terminal session:

```
C:\>
C:\>ping 192.168.100.98

Pinging 192.168.100.98 with 32 bytes of data:

Reply from 192.168.100.1: Destination host unreachable.

Ping statistics for 192.168.100.98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.100.65

Pinging 192.168.100.65 with 32 bytes of data:

Reply from 192.168.100.65: bytes=32 time<1ms TTL=255

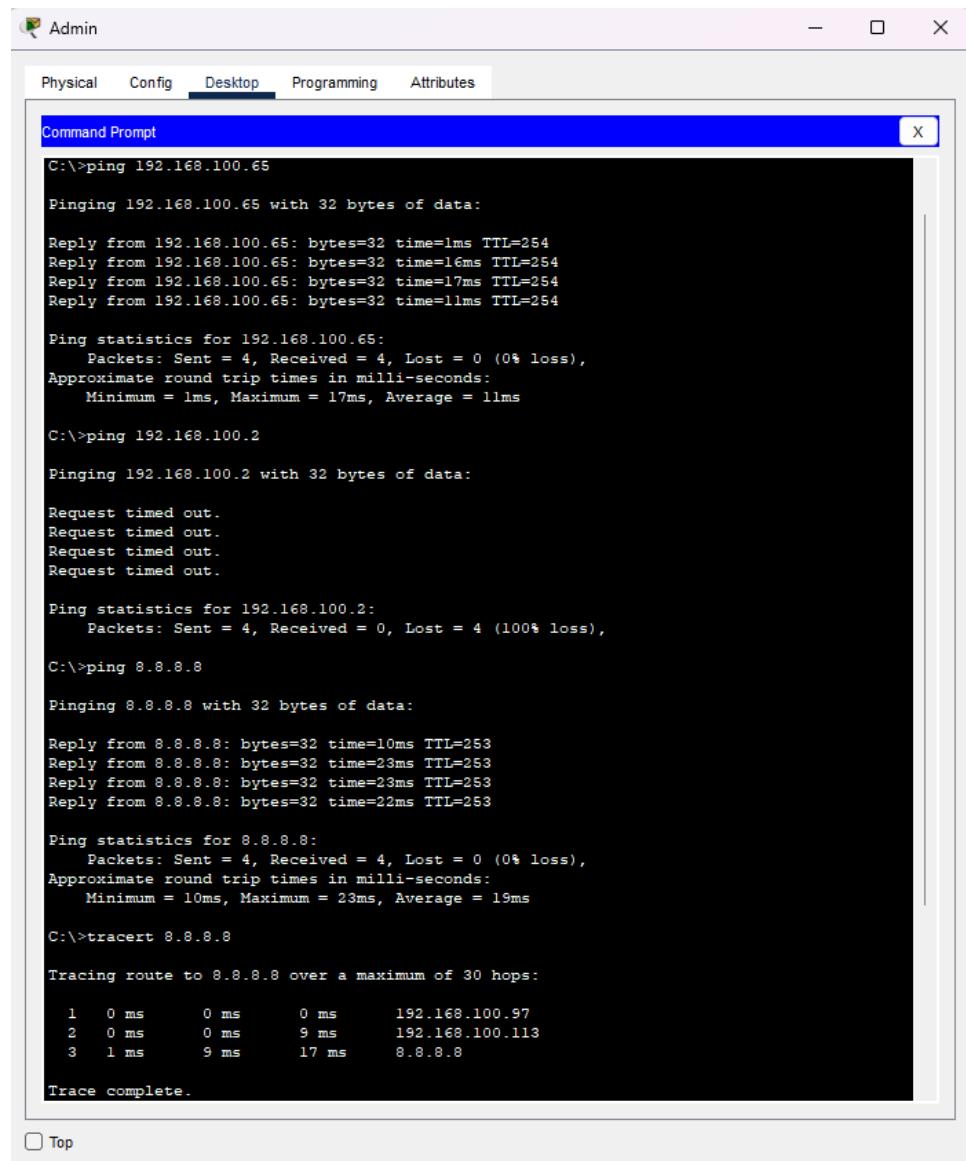
Ping statistics for 192.168.100.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time=28ms TTL=254
Reply from 8.8.8.8: bytes=32 time=13ms TTL=254
Reply from 8.8.8.8: bytes=32 time=14ms TTL=254
Reply from 8.8.8.8: bytes=32 time=14ms TTL=254

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 28ms, Average = 17ms
C:\>ftp 192.168.100.98
Trying to connect...192.168.100.98
*Error opening ftp://192.168.100.98/ (Timed out)
```

At the bottom left of the command prompt window, there is a small checkbox labeled "Top".



The screenshot shows a Cisco Packet Tracer interface with a Command Prompt window open. The window title is "Command Prompt". The user has run several commands:

- `C:\>ping 192.168.100.65`: Pings 192.168.100.65 with 32 bytes of data. Returns 4 replies from 192.168.100.65 with TTL=254 and times ranging from 1ms to 17ms.
- `C:\>ping 192.168.100.2`: Pings 192.168.100.2 with 32 bytes of data. Returns 4 request timed out messages.
- `C:\>ping 8.8.8.8`: Pings 8.8.8.8 with 32 bytes of data. Returns 4 replies from 8.8.8.8 with TTL=253 and times ranging from 10ms to 23ms.
- `C:\>tracert 8.8.8.8`: Traces route to 8.8.8.8 over a maximum of 30 hops. Shows three hops: 192.168.100.97, 192.168.100.113, and 8.8.8.8.

At the bottom of the Command Prompt window, there is a checkbox labeled "Top".

## Penutup

Terima kasih atas perhatiannya, mohon maaf jika dokumentasi ini masih terdapat kekurangan. Saya harap dengan adanya dokumentasi ini bisa membantu siapapun dalam belajar konfigurasi cisco packet tracer.