

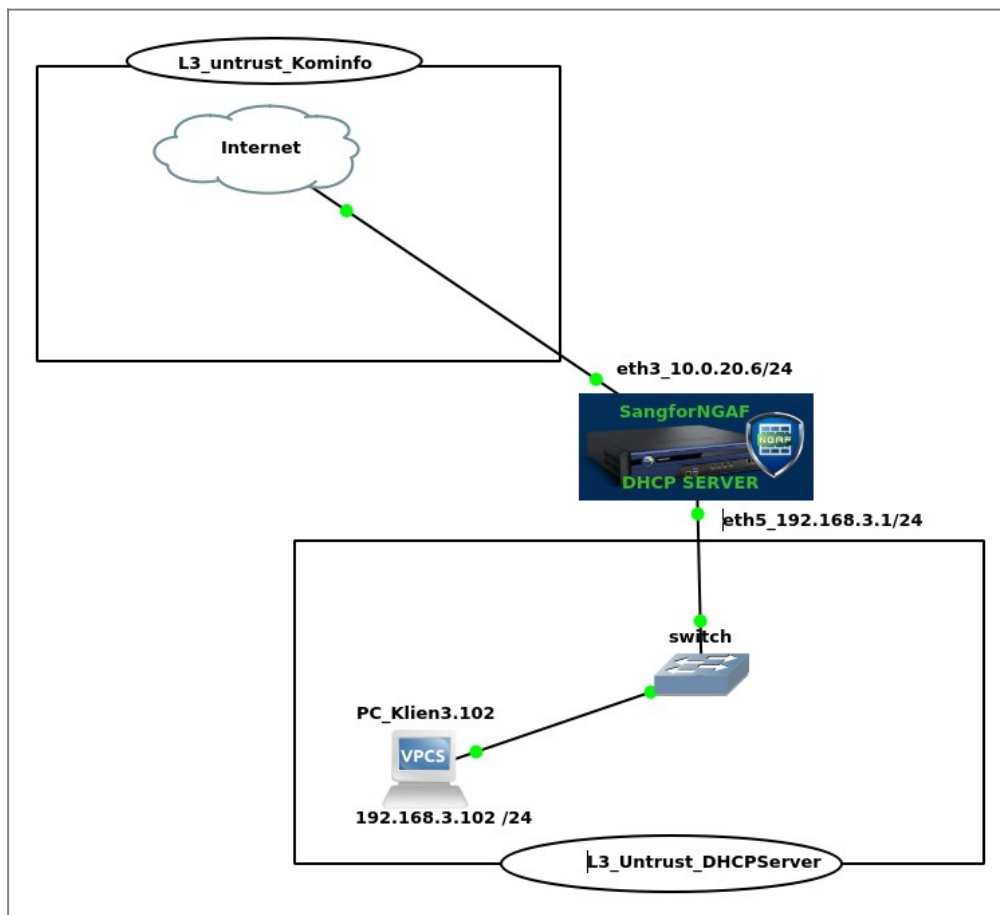
Konfigurasi Akses Internet Pada Protocol DHCP Server dalam Firewall NGAF V8.0.47

***Product:**NGAF

***Version:**8.0.47

*1. Pengantar

1.1 Skenario



Pada tulisan ini, saya membuat panduan konfigurasi akses internet klien yang menggunakan protocol DHCP Server. Dalam kasus ini, klien berhasil memperoleh IP dari DHCP Server yaitu 192.168.3.102/24. Hasil pengujian diperoleh bahwa klien dapat melakukan akses internet dengan baik. Untuk memastikan kebenarannya, dari PC Klien dapat dilakukan dengan ping dan traceroute ke website global contohnya www.google.com. Adapun tahapan-tahapannya dapat mengikuti intuksi berikut dibawah ini.

1.2 Persyaratan

- 1) Pengguna memiliki perangkat Firewall NGAF
- 2) Memiliki minimal 1 ISP (Internet Service Provider)
- 3) Pengguna memiliki 1 PC untuk uji coba

*2. Panduan Konfigurasi

Segmen jaringan lokal untuk klien dibuat class C dengan network 192.168.3.0/24. Adapun gateway kita siapkan IP 192.168.3.1/24. Sedangkan IP Klien mengikuti pool dari DHCP Server yang akan kita buat nanti.

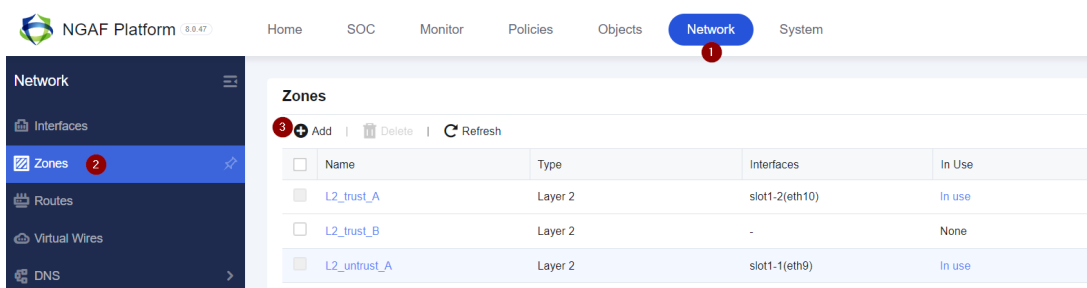
2.1. Membuat Zone

a) Zone Untrust DHCP Server

Zona Untrust DHCP Server merupakan zona yang dibuat sebagai zona dimana klient mendapatkan ip secara otomatis.

Langkah-langkahnya sebagai berikut:

1. Klik **Network→Zones→Add**



2. Masukkan nama: **L3_trust_DHCPServer**

Type: Layer3

Interface: eth5

Secara detail tampak seperti gambar berikut ini:

Edit Zone

×

Name:

4

L3_Untrust_DHCPServer

Type:

Layer 2

5

Layer 3

Virtual wire

Interfaces

Available (18)

Search

Q

☐ veth.90

☐ veth.97

☐ veth.5

☐ veth.99

☐ veth.101

☐ vpntun

☒ eth5

6

Selected (1)

Clear

Search

Q

eth5

7

Save

Cancel

3. Simpan

Jika berhasil maka akan muncul seperti gambar dibawah ini:

Zones

+

Add

🗑

Delete

↻

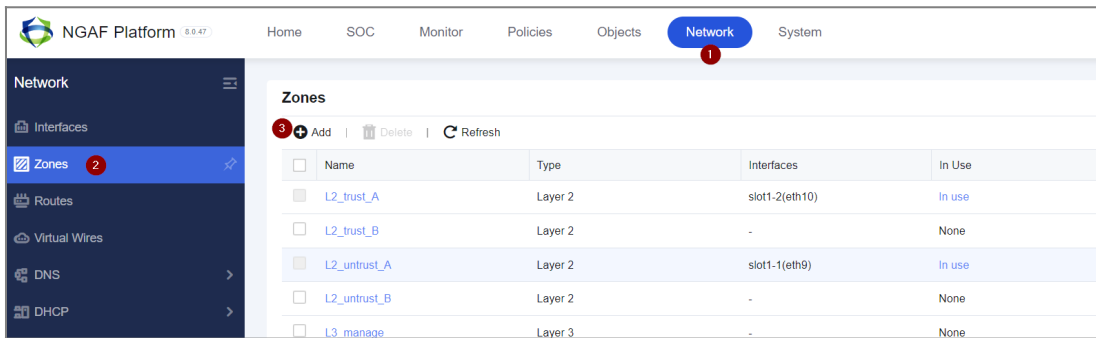
Refresh

<input type="checkbox"/>	Name	Type	Interfaces
<input type="checkbox"/>	L3_untrust_B	Layer 3	-
<input type="checkbox"/>	L3_untrust_C	Layer 3	-
<input type="checkbox"/>	Virtual_trust_A	Virtual wire	-
<input type="checkbox"/>	Virtual_trust_B	Virtual wire	-
<input type="checkbox"/>	Virtual_untrust_A	Virtual wire	-
<input type="checkbox"/>	Virtual_untrust_B	Virtual wire	-
<input checked="" type="checkbox"/>	L3_Untrust_DHCPServer	Layer 3	eth5

b) Zone Untrust Kominfo

Selanjutnya kita buat Zone Untrust Kominfo (ISP). Langkah-langkah nya sama seperti diatas,

1. Klik **Network** → **Zones** → **Add**



2. Masukkan nama : L3_Untrust_Kominfo

Type: Layer3

Interface: eth3

Name: 4 L3_Untrust_Kominfo

Type: ☐ Layer 2 ☒ 5 Layer 3 ☐ Virtual wire

Interfaces

Available (17)

Search

☐ veth.90
☐ veth.97
☐ veth.5
☐ veth.99
☐ veth.101
☐ vpntun
☒ 6 eth3

Selected (1) Clear

Search

eth3

7 Save Cancel

3. Simpan, jika berhasil maka seperti gambar dibawah ini

Zones			
+ Add Delete Refresh			
<input type="checkbox"/>	Name	Type	Interfaces
<input type="checkbox"/>	Virtual_trust_B	Virtual wire	-
<input type="checkbox"/>	Virtual_untrust_A	Virtual wire	-
<input type="checkbox"/>	Virtual_untrust_B	Virtual wire	-
<input type="checkbox"/>	L3_Untrust_Kominfo	Layer 3	eth3
<input type="checkbox"/>	L3_Trust_Server	Layer 3	eth1

2.2. Setting interface

Langkah selanjutnya setelah membuat zona adalah melakukan konfigurasi pada interface tempat kita akan memasukkan zona yang telah dibuat diatas. Interface **eth5** untuk Zona L3_Untrust_DHCP Server, dan **eth3** untuk Zona L3_Untrust_Kominfo.

a) Konfigurasi eth5 (L3_Untrust_DHCP Server)

1. Masuk ke menu **Network→Interface→Pilih Eth5**

NGAF Platform 5.0.47					
Home SOC Monitor Policies Objects Network System					
Network <ul style="list-style-type: none"> Interfaces (2) Zones Routes Virtual Wires DNS 					
Physical Interfaces Subinterfaces VLAN Interfaces Aggregate Interfaces					
<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable Refresh					
<input type="checkbox"/>	Name	Interface Status	WAN Attribute	Type	Zone
<input type="checkbox"/>	eth4		Yes	Layer 3	L3_Untrust_Biznet2
<input type="checkbox"/>	eth5		No	Layer 3	L3_Untrust_DHCP Server

2. Pilih status: enabled

Description: dhcp Server

Type: layer 3

Zone: L3_Untrust_DHCP Server

Ip static: 192.168.3.1/24

Kemudian simpan, seperti gambar dibawah ini.

Basics

Name: 4 eth5

Status: 5 ☒ Enabled ☐ Disabled

Description: DHCP Server

Type: 6 Layer 3

Zone: 7 L3_Untrust_DHCPServer

Basic Attributes: ☐ WAN attribute

System Upgrade: ☐ Temporarily use this interface for system upgrade ⓘ

IPv4 IPv6 Link State Detection Advanced

IP Assignment: 8 ☒ Static ☐ DHCP ☐ PPPoE

Static IP: 9 192.168.3.1/24 ⓘ

Next-Hop IP: ⓘ

Link Bandwidth: Outbound 1000 Mbps Inbound 1000 Mbps

Management Service

Allow: ☒ WEBUI ☒ PING ☐ SNMP ☐ SSH

10 Save Cancel

b) Konfigurasi eth3 (L3_Untrust_Kominfo)

1. Masuk ke menu **Network→Interface→Pilih Eth3**

NGAF Platform (8.0.47) Home SOC Monitor Policies Objects **Network** System

Network

- Interfaces** 2
- Zones
- Routes
- Virtual Wires
- DNS
- DHCP
- ARP

Physical Interfaces Subinterfaces VLAN Interfaces Aggregate Interfaces

✓ Enable ⏻ Disable | Refresh

	Name	Interface Status	WAN Attribute	Type	Zone
<input type="checkbox"/>	eth0		No	Layer 3	L3_trust_A
<input type="checkbox"/>	eth1		No	Layer 3	L3_Trust_Server
<input type="checkbox"/>	eth2		Yes	Layer 3	L3_Untrust_Biznet
3 <input checked="" type="checkbox"/>	eth3		Yes	Layer 3	L3_Untrust_Kominfo

2. Pilih status : enabled

Description : WAN(Diskominfo)

Type : layer 3

Zone : L3_Untrust_Kominfo

Basic Attribute : WAN attribute (centang)

IP static : 10.0.20.6/24

Next Hop : 10.0.20.1 (ini adalah gateway dari ISP kominfo)

Kemudian simpan, seperti gambar dibawah ini.

Name: eth3

Status: 4 ☒ Enabled ☐ Disabled

Description: 5 WAN (Diskominfo)

Type: 6 Layer 3

Zone: 7 L3_Untrust_Kominfo

Basic Attributes: ☒ WAN attribute 8

System Upgrade: ☐ Temporarily use this interface for system upgrade ⓘ

IPv4 IPv6 Link State Detection Advanced

IP Assignment: ☒ Static ☐ DHCP ☐ PPPoE

Static IP: 9 10.0.20.6/24 ⓘ

Next-Hop IP: 10 10.0.20.1 ⓘ

Link Bandwidth: Outbound 1000 Mbps Inbound 1000 Mbps

Management Service

Allow: ☒ WEBUI ☒ PING ☒ SNMP ☒ SSH

11 Save Cancel

2.3. Buat Network Objects

Langkah selanjutnya membuat network object untuk menampung blok ip yang terdaftar dalam DHCP Server. Adapun langkah-langkahnya sebagai berikut:

1. Klik menu **Objects** → **Network Objects** → **Add**

NGAF Platform 8.0.47 Home SOC Monitor Policies 1 Objects

Objects

2 Network Objects

Services

Security Policy Template

Threat Signature Database

Content Identification Database

IP Location Database

3 Add | Delete | Import | Export | Refresh

No.	Name	Type	Critical
1	All	IP Address	-
2	point to point 34	IP Address	-
3	SIMDA	IP Address	-

2. Masukkan type: IP Address

Name : Segmen DHCP Server

Protocol: IPV4

IP: 192.168.3.0/24

Kemudian simpan seperti pada gambar dibawah ini.

3. Jika berhasil seperti gambar berikut ini

No.	Name	Type	Criticality	Address	Description
1	Segmen DHCP Server	IP Address	-	192.168.3.0-192.168.3.255	-

2.4. Membuat Service DHCP Server

Langkah selanjutnya membuat service DHCP Server, tujuannya adalah sebagai server yang melayani pengaturan IP klien secara otomatis. Adapun langkah-langkahnya sebagai berikut:

1. Klik menu **Network → DHCP → DHCP Option → Add**

No.	Name	Interface	Service Type	IP Address	Lease (day/hr/min)	Status	Operation
1	Pool DHCP Server	eth5	DHCP Server	192.168.3.100-192.168.3...	0/2/0	✓	Edit Delete

2. Masukkan,

Service Type : Pilih DHCP Server

Name : Pool DHCP Server

Status : pilih enabled

Network : Interface →eth5

Ip range →192.168.3.100-192.168.3.254

Netmask→ 255.255.255.0

DHCP Gateway : 192.168.3.1

DNS Server : Pilih specified

Preferred DNS : 8.8.8.8

Alternate DNS : 8.8.4.4

Kemudian simpan seperti pada gambar dibawah ini.

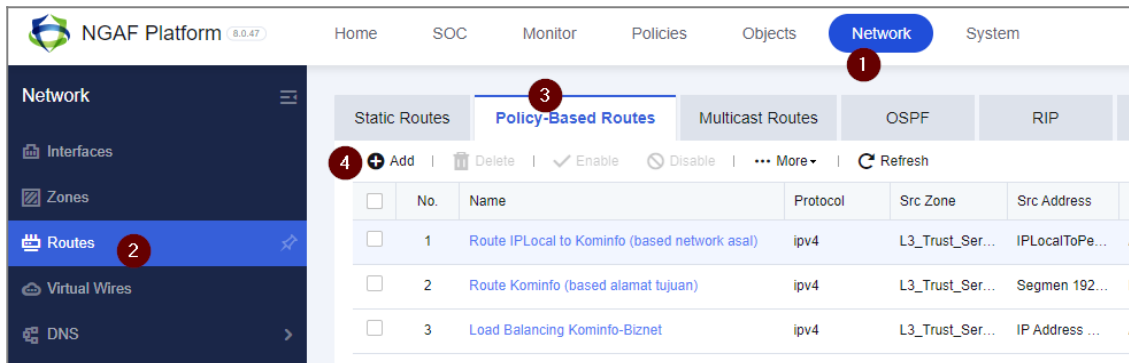
3. Jika benar

DHCP Options							
+ Add Delete Enable Disable Refresh							
	No.	Name	Interface	Service Type	IP Address	Lease (day/hr/min)	Status
<input checked="" type="checkbox"/>	1	Pool DHCP Server	eth5	DHCP Server	192.168.3.100-192.168.3.254	0/2/0	✓

2.5. Menambahkan Konfigurasi di Policy Based Routes

Setelah tahapan diatas telah dilakukan, maka langkah selanjutnya adalah menambahkan **policy based routes**. Dalam firewall Sangfor NGAF dapat dilakukan sebagai berikut:

1. Buka menu **Network→Routes→Policy →Based Routes→Add**



2. Masukkan

Route Type : Pilih source-based-route

Protocol : IPV4

Name : Akses Internet Ke Kominfo

Status : enabled

Move to : Top

Src Zone : L3_Untrust_DHCPServer

Src Address : Segmen DHCP Server

Destination : ISP → Pilih All

Services : Any

Outbound Interface: Pilih Interface → Eth3

Secara detil seperti gambar berikut dibawah ini,

Add Policy-Based Route ✕

Route Type: 5 ☒ Source-based route ☐ Link load-balancing

Protocol: 6 ☒ IPv4 ☐ IPv6

Basics

Name: 7

Status: 8 ☒ Enabled ☐ Disabled

Description:

Move To: 9

Schedule: 10

Data Packet

Src Zone: 11

Src Address: 12

Destination: ☐ Network Object ☒ ISP 13 ☐ Country/Region

14

Services: 15

Others

Outbound Interface: ☒ Interface 16 ☐ Next-Hop IP

17

Link State Detection:

18

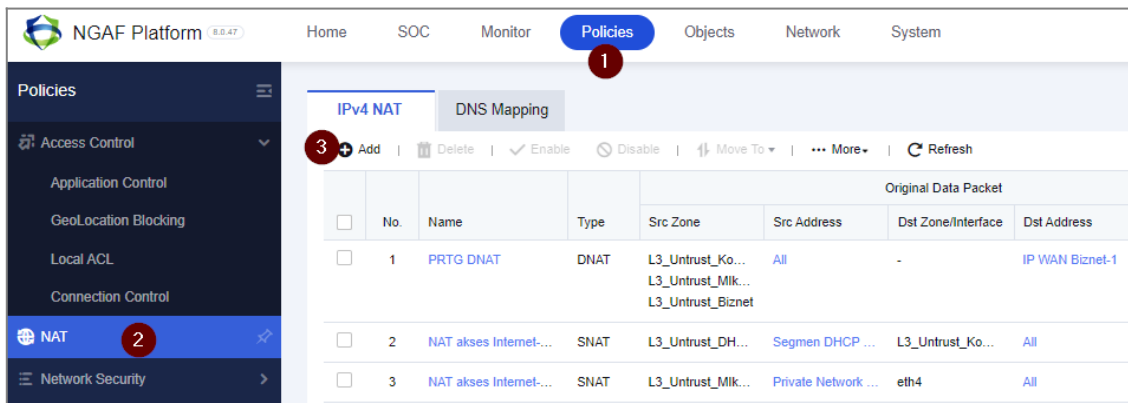
3. Kemudian simpan, dan jika berhasil akan muncul seperti gambar berikut ini:

Static Routes									
Policy-Based Routes									
Multicast Routes									
OSPF									
RIP									
BGP									
All Routes									
Route Testing									
<div> + Add ✕ Delete ✓ Enable ⏻ Disable ⋮ More ↻ Refresh </div>									
No.	Name	Protocol	Src Zone	Src Address	Dst Address/Region	Services	Applications	Interface-Next Hop IP	
<input checked="" type="checkbox"/>	1	Akses Internet Kominfo	ipv4	L3_Untrust_DHCPServer	Segmen DHCP Server	All	any	-	eth3-10.0.20.1

2.6. Menambahkan SNAT

Langkah selanjutnya adalah membuat NAT untuk akses ke internet.

1. Klik **Policies → NAT → Ipv4 NAT → add**



2. Kemudian isikan,

Type : Pilih Source NAT

Name : NAT Akses Internet DHCP Client

status : Pilih enabled

Move To : Top

Src Zone : L3_Untrust_DHCPServer

Src Address : Segmen DHCP Server

Dst Zone/Interface: Pilih Zone → L3_Untrust_Kominfo

Dst Address : All

Services : Any

Translate Src IP To: Outbound Interface

Secara detil seperti gambar dibawah ini,

Add NAT Policy

Type: **4** ☒ Source NAT ☐ Destination NAT ☐ Bidirectional NAT

Basics

Name: **5** NAT akses Internet-DhcpClient

Status: **6** ☒ Enabled ☐ Disabled

Description: Optional

Move To: **7** Top

Schedule: All week

Original Data Packet

Src Zone: **8** L3_Untrust_DHCPServer

Src Address: **9** Segmen DHCP Server

Dst Zone/Interface: **10** ☒ Zone ☐ Interface

11 L3_Untrust_Kominfo

Dst Address: **12** All

Services: **13** any

Translated Data Packet

Translate Src IP To: **14** Outbound Interface

Translate Dst IP To: Untranslated

Translate Dst Port To: Untranslated

15 Save and Copy Save Cancel

3. Kemudian simpan, jika benar akan tampak seperti gambar berikut dibawah ini

IPv4 NAT		DNS Mapping							
		Add Delete Enable Disable Move To More Refresh							
		Original Data Packet							
No.	Name	Type	Src Zone	Src Address	Dst Zone/Interface	Dst Address	Services	Src Address	
1	NAT akses Internet-DhcpClient	SNAT	L3_Untrust_DH...	Segmen DHCP Server	L3_Untrust_Kominfo	All	any	Outbound Interf...	

2.7. Melakukan Ujicoba

Tahap terakhir yang bisa dilakukan adalah dengan melakukan ujicoba di sisi klien. Dalam hal ini **PC Klien (ip dhcp 192.168.3.103/24)**. Pertama kita mengecek dhcp server yang telah berjalan. Kedua melakukan ping ke situs internet contoh www.google.com dan ketiga, kita lakukan traceroute ke situs global tersebut untuk memastikan jalur yang dilewati sudah benar.

Dari hasil pengecekan diperoleh sebagai berikut:

a. Cek IP DHCP

Komputer berhasil mendapatkan IP dari DHCP Server yang telah kita setting diatas.

```

Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : WIN-8023IPQF8DU
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-09-27-C8
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::d883:c0cc:7db6:f672:12<Preferred>
IPv4 Address. . . . . : 192.168.3.102<Preferred>
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, March 25, 2024 3:49:51 PM
Lease Expires . . . . . : Monday, March 25, 2024 5:49:50 PM
Default Gateway . . . . . : 192.168.3.1
DHCP Server . . . . . : 192.168.3.1
DHCPv6 Client DUID. . . . . : 00-01-00-01-25-C0-C5-F7-08-00-27-09-27-C8

DNS Servers . . . . . : 8.8.8.8
                        8.8.4.4
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.{896CBEED-754F-4096-9D5A-5177A55D97AF}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

C:\Users\Administrator>

```

b. Ping google.com

Komputer dapat melakukan PING dengan baik terhadap situs global www.google.com

```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>ping google.com

Pinging google.com [74.125.130.138] with 32 bytes of data:
Reply from 74.125.130.138: bytes=32 time=23ms TTL=103
Reply from 74.125.130.138: bytes=32 time=23ms TTL=103
Reply from 74.125.130.138: bytes=32 time=22ms TTL=103
Reply from 74.125.130.138: bytes=32 time=23ms TTL=103

Ping statistics for 74.125.130.138:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 23ms, Average = 22ms

C:\Users\Administrator>_
```

c. Traceroute google.com

Komputer dapat melakukan traceroute ke situs global www.google.com dengan jalur yang dilalui yaitu gateway ISP Kominfo.

```
Administrator: C:\Windows\system32\cmd.exe - tracert google.com

C:\Users\Administrator>tracert google.com

Tracing route to google.com [74.125.130.138]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    192.168.3.1
  1  <1 ms    <1 ms    <1 ms    10.0.20.1
  2  <1 ms    <1 ms    <1 ms    192.168.253.1
  3  <1 ms    <1 ms    <1 ms    10.127.252.1
  4  <1 ms    <1 ms    <1 ms    10.127.252.1
  5  8 ms     8 ms     9 ms     ip-74.184.hsp.net [103.134.184.74]
  6  9 ms     9 ms     9 ms     ip-66.162.hsp.net [103.139.162.66]
  7  21 ms    22 ms    22 ms    ip-247.30.hsp.net.id [103.115.30.247]
  8  23 ms    23 ms    24 ms    72.14.205.170
  9  22 ms    22 ms    22 ms    209.85.253.241
 10  22 ms    21 ms    21 ms    142.250.60.240
 11  *


```

*3. Pencegahan

- 1) Jika DHCP Server tidak berjalan, bisa dicek lagi settingan diatas pastikan sudah sesuai, jika masih belum berjalan, silahkan restart.
- 2) Beberapa kasus DHCP tidak berjalan karena interface klien harus di disable dan enable ulang
- 3) Jika sudah dapat IP DHCP tetapi tidak bisa akses internet, silahkan diperiksa setting DNS nya, kemudian gateway yang digunakan, pastikan sudah sesuai.