MODUL 3
NETWORK AND TRANSPORT LAYER

TUJUAN PEMBELAJARAN:

1. Mahasiswa memahami konsep dasar pengalamatan di Jaringan
2. Mahasiswa mampu melakukan konfigurasi Jaringan
3. Mahasiswa mampu menganalisa koneksitas jaringan

DASAR TEORI

A. Network Layer : IP Address

A.1. Pengalamatan IP

TCP/IP merupakan protokol paling populer saat ini dipakai. Salah satu aturan yang ada pada TCP/IP pengalamatan pada setiap komputer yang ada di jaringan. Pengalamatan yang ada di jaringan biasa disebut dengan IP. Nomor IP terdiri dari bilangan biner sepanjang 32 bit yang dibagi atas 4 bagian. Tiap bagian terdiri atas 8 bit. Jadi jangkauan nomor IP yang bisa digunakan adalah dari **00000000.00000000.00000000.00000000** sampai dengan **11111111.11111111.11111111.11111111**.

Untuk memudahkan pembacaan dan penulisan, IP Address biasanya direpresentasikan dalam bilangan desimal. Jadi, range address di atas dapat diubah menjadi address **0.0.0.0** sampai address **255.255.255.255**. Nilai desimal dari IP Address inilah yang dikenal dalam pemakaian sehari-hari. Beberapa contoh IP Address adalah :

```
202.95.151.129
202.58.201.211
172.16.122.204
```

A.2. Netmask/Subnetmask

Untuk pengelompokan pengalamatan, selain nomor IP dikenal juga netmask atau subnetmask. Yang besarnya sama dengan nomor IP yaitu 32 bit. Ada tiga pengelompokan besar subnet mask yaitu dengan dikenal, yaitu **255.0.0.0 , 255.255.0.0 dan 255.0.0.0**.

Pada dunia jaringan, subnetmask tersebut dikelompokkan yang disebut class dikenal tiga class yaitu :

1. **Class A**, adalah semua nomor IP yang mempunyai subnetmask 255.0.0.0
2. **Class B**, adalah semua nomor IP yang mempunyai subnetmask 255.255.0.0
3. **Class C**, adalah semua nomor IP yang mempunyai subnetmask 255.255.255.0

Gabungan antara IP dan Netmask inilah pengalamatan komputer dipakai. Kedua hal ini tidak bisa lepas. Jadi penulisan biasanya sbb :

IP : 202.95.151.129
Netmask : 255.255.255.0

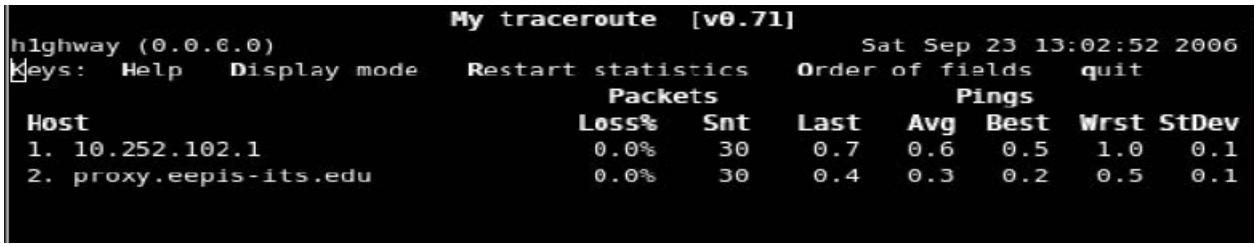
A.3. Tool network

- **traceroute**

  Untuk mengecek koneksi digunakan protokol ICMP dengan perintah ping atau traceroute.

```
h1ghway:~# traceroute proxy
traceroute to proxy.eepis-its.edu (202.154.187.7), 30 hops max, 40 byte
packets
 1  10.252.102.1 (10.252.102.1)  0.581 ms  0.527 ms  0.528 ms
 2  proxy (202.154.187.7)  0.313 ms  0.223 ms  0.288 ms
```

- **mtr**
  Gabungan antara ping dan traceroute.



B. Transport Layer

Aplikasi yang digunakan untuk mengetahui penggunaan layer transport adalah perintah netstat. Untuk mengetahui port berapa saja yang terbuka untuk koneksi pada PC kita dapat diketahui dengan perintah :

```
# netstat -nlptu
```

```
debianGUI:~# netstat -nlptu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:34699           0.0.0.0:*               LISTEN      2669/rpc.statd
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      2164/portmap
tcp        0      0 0.0.0.0:113             0.0.0.0:*               LISTEN      2624/inetd
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      2624/inetd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      2495/cupsd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      2612/exim4
udp        0      0 0.0.0.0:52750           0.0.0.0:*                           2669/rpc.statd
udp        0      0 0.0.0.0:68              0.0.0.0:*                           2760/dhclient3
udp        0      0 0.0.0.0:725             0.0.0.0:*                           2669/rpc.statd
udp        0      0 0.0.0.0:111             0.0.0.0:*                           2164/portmap
udp        0      0 0.0.0.0:631             0.0.0.0:*                           2495/cupsd
```

Untuk mengetahui koneksi yang sedang terjadi antar PC kita dengan PC lain dapat diketahui dengan perintah :

-netstat -nat Dilihat dari State yang bernilai “ESTABLISHED”

```
debianGUI:~# netstat -nat -4
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:34699           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:113             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
tcp        0      0 192.168.1.5:50793       192.168.1.4:23          ESTABLISHED
```

TUGAS PENDAHULUAN

1. Jelaskan pembagian kelas address di dalam TCP/IP
2. Apa yang dimaksud dengan Network Address, Broadcast Address dan Netmask, jelaskan secara singkat.
3. Jelaskan proses yang terjadi pada lapisan transport di system komunikasi data.

PERCOBAAN

1. Nomor IP Percobaan yang dipakai adalah : 192.168.x.yy (x adalah no kelompok anda, dgn range 10-20; yy adalah no client dgn range 1-254) dengan netmask 255.255.255.0. Atur dengan kelompok lain supaya nomor IP tidak bertabrakan, tidak ada yang memakai nomor IP yang sama.
   ```
   # ifconfig eth0 no_ip netmask no_netmask
   Contoh untuk kelompok 1 :
   # ifconfig eth0 192.168.10.2 netmask 255.255.255.0
   ```

   NB : Gunakan 2 komputer, satu sebagai komputer sumber dan satunya komputer target. Jalankan wireshark pada komputer target untuk menganalisa paket data.
   ```
   # wireshark
   ```
2. Setelah melakukan konfigurasi untuk melihat hasilnya ketikkan perintah ifconfig
3. Selanjutnya lakukan tes konektifitas dengan menggunakan perintah *ping no_address* dari komputer sumber ke komputer target.
   Catat hasilnya di komputer sumber dan catat pula proses yang terjadi (proses ping) pada wireshark di komputer target.
4. Lakukan lagi cek konektifitas tetapi kali ini lakukan dengan komputer lain yang berbeda subnet (beda kelompok). Catat hasilnya seperti langkah 3 dan bandingkan hasilnya.
5. Jalankan wireshark pada komputer sumber, setelah itu jalankan perintah
   ```
   # dhclient
   ```
   Untuk mendapatkan ip secara otomatis dari server.
   Setelah mendapatkan ip dari server, stop wireshark, catat proses yang terjadi selama proses DHCP.
6. Pastikan PC menggunakan IP DHCP, kemudian catat hasil dari ping, traceroute dan mtr pada target berikut
   a. 10.252.42.1
   b. 202.154.187.7
   c. www.eepis-its.edu
   d. www.yahoo.com

7. Jalankan perintah berikut dan catat hasilnya :
   ```
   # netstat -nlptu
   ```

   Bandingkan hasilnya jika dijalankan perintah :
   ```
   # netstat –nat
   # netstat –natu
   ```

8. Dengan web browser, buka halaman
   http://www.eepis-its.edu
   ftp://fileserver.eepis-its.edu

   kemudian catat hasil koneksi dengan perintah
   ```
   # netstat –nat
   ```

   Tutup kembali web browser anda, dan jalankan perintah diatas, amati apa yang terjadi.

LAPORAN RESMI

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Di dunia dikenal dengan IP public dan privat apa maksudnya jelaskan secara singkat !
3. Dikenal juga IP statis dan IP dinamis apa yang dimaksud dengan kedua hal diatas ?
4. Apa yang dimaksud dengan DHCP Server ?

LEMBAR ANALISA

Praktikum Jaringan Komputer -1 (Network dan Transport Layer)
Tanggal Praktikum :
Kelas :
Nama dan NRP :

A. Gambar topologi jaringan beserta informasi IP Addressnya.

B. Tes koneksi pada satu jaringan dengan perintah ping (poin 3)

C. Tes koneksi pada jaringan yang berbeda dgn perintah ping (poin 4)

D. Catat dan amati proses terjadinya DHCP pada wireshark (poin 5)

E. Catat hasil ping, traceroute dan mtr pada poin 6.

F. Catat dan amati proses pada lapisan transport (poin 7)

G. Cek hasil koneksi dgn protokol http dan ftp pada lapisan transport (poin 8)