MODUL 3
ANALISA PROTOKOL LAYER 2 DAN 3

TUJUAN PEMBELAJARAN:

1. Mahasiswa memahami konsep PDU layer 2 dan 3
2. Mahasiswa mampu mengoperasikan arp, wireshark dan tcpdump
3. Mahasiswa mampu menganalisa paket layer 2 dan 3 menggunakan wireshark dan tcpdump

PERALATAN YANG DIBUTUHKAN:

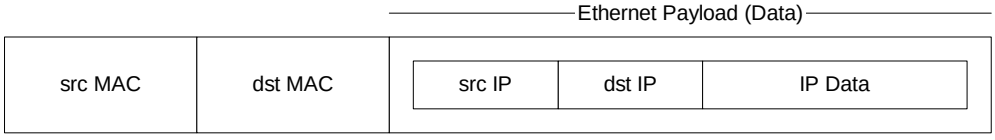
1. Beberapa PC yang akan dihubungkan dalam jaringan.
2. Hub sebagai penghubung jaringan.
3. Kabel jaringan secukupnya.

DASAR TEORI

Nomor IP diperlukan oleh perangkat lunak untuk mengidentifikasi komputer pada jaringan, namun nomor identitas yang sebenarnya diatur oleh *NIC (Network Interface Card)* atau kartu Jaringan yang juga mempunyai nomor unik. Pengalamatan di NIC biasa disebut dengan MAC Address. Pengalamatan ini merupakan bagian dari ethernet.

Alamat kartu jaringan ini terdiri atas 48 bit, 24 bit ID dari pabrik pembuat sedangkan 24 bit sisanya adalah nomor urut/*sequence number*. Oleh karena itu setiap kartu jaringan TCP/IP merupakan standar tentang mekanisme kerja jaringan, sehingga perangkat lunak dan perangkat keras dari bebagai vendor dapat saling berkomunikasi. Agar dapat bekerja maka TCP/IP membutuhkan perangkat keras jaringan dalam hal ini adalah *Ethernet*, meskipun ethernet bukan bagian dari TCP/IP, TCP/IP hanya berinteraksi untuk menggunakan fasilitasnya menggerakkan paket. Pengalamatan ethernet sudah dijelaskan di atas.

Untuk mengirim data ke komputer lain, maka software menyusun frame ethernet dalam memori sbb :



Gambar Paket Ethernet

jadi ini merupakan referensi IP ke MAC addressnya sehingga data terkirim ke komputer yang benar sesuai phisical addressnya. Berdasarkan mapping IP dengan phisical addressnya.

Bila komputer tahu nomor IP tapi tidak tahu MACnya. TCP/IP memecahkan masalah ini dengan menggunakan *ARP (Address Resolution Protocol)* .

ARP (Address Resolution Protocol)

Secara internal ARP melakukan resolusi address tersebut dan ARP berhubungan langsung dengan Data Link Layer. ARP mengolah sebuah tabel yang berisi IP-address dan Ethernet Card. Dan tabel ini diisi setelah ARP melakukan request (broadcast) ke seluruh jaringan.

Misal user host tertentu menjalankan perintah *telnet* (telnet merupakan perintah di linux yang dipakai untuk menjalankan mesin tertentu dari mesin lainnya) dengan host foghorn (`$telnet foghorn`) . Setelah user menjalankan command telnet, maka sistem akan mengecek ARP cache ada nomor phisical addres yang dimaksud. Jika informasi ini tidak ditemukan, maka host akan mengeluarkan suatu ARP khusus meminta paket. ARP Request dikapsulkan dengan semua informasi yang dibutuhkan kecuali physical addrees tujuan karena memang host tidak tahu tujuannya dimana, biasanya arp tujuan dibuat FF:FF:FF:FF secara broadcast ke jaringan, karena broadcast maka semua system pada local network akan menguji request tersebut. Paket ARP request/Reply mempunyai format yang sama. Informasi ini bisa ditangkap oleh *software sniffer tcpdump atau ethereal* (akan dijelaskan selanjutnya).

ARP Cache

Tadi sedikit disinggung, bahwa setelah menjalankan command telnet maka host akan mengecek ARP Cache. ARP cache berisi tabel IP host serta phisical adrees komputer. ARP cache akan bertambah jika ARP Request mendapat jawaban. ARP Cache ini diatur secara dinamik oleh kernel. Untuk melihat bisa pakai command `arp –a`.

Kita bisa melakukan penghapusan sebuah entry ARP dengan `arp –d hostname`

Untuk mengecek di layer 2 lapisan OSI dapat digunakan perintah **arp**
(AddressResolution Protocol).
Contoh :

```
hlghway:~# arp
Address          HWtype    HWaddress           Flags  Mask     Iface
10.252.102.1     ether     00:09:E8:8E:0F:80   C                eth0
```

Perintah diatas dapat diartikan bahwa kita baru terkoneksi dengan 10.252.102.1 saja belum ada lainnya.

TCPDump

Jaringan TCP/IP terdiri atas keseluruhan paket dan cara terbaik untuk mendebug jaringan adalah dengan cara melacak paket. Dengan demikian kita dapat menentukan informasi yang tepat dari sumber yang benar. Untuk melacak paket kita dapat menggunakan TCPDump, yang tersedia gratis. Dengan memakai ini seumpama kita berada di web maka kita bisa memakainya untuk mencari penyebab sesuatu tidak beres/gagal sumber penyebabnya dimana dengan tracing tersebut.

Dengan menjalankan TCPDump, kita bisa melihat semua traffic yang masuk atau meninggalkan NIC dan bisa melihat aktifitas jaringan.

Dengan TCPDump bisa juga dipakai untuk menganalisa seumpama terjadi kelambatan aplikasi, kita bisa menganalisanya mulai dari ini.

Kemampaun TCPDump akan berkurang jika kita menggunakan switch, jadi untuk mempelajari paket jaringan secara detail dengan memakai TCPDump sebaiknya memakai

hub sebab jika memakai switch yang dapat diketahui dari TCPDump hanya traffic ke dan dari komputer.

TCPDump akan berjalan dengan menjalankan command tcpdump [-n|-t|-e] dst.

Dengan TCPDump kita bisa : memilih paket yang diminati, memilih paket berdasarkan alamat host, memilih paket berdasarkan tipe traffic.

Wireshark

Wireshark merupakan software sniffer gratis yang sudah berbentuk Graphical User Interface(GUI). Software ini berjalan baik di linux. Dengan grafiknya mempermudah melihat setiap detail sebuah paket dan frame ethernet.

TUGAS PENDAHULUAN

1. Apa kegunaan ARP
2. Gambarkan dan jelaskan format datagram ARP Request/Reply
3. Cari option – option pada command arp (misal arp –a, arp -??), dan jelaskan maksud dan kegunaannya.
4. Apa perbedaan antara tcpdump dan wireshark ?

PERCOBAAN

1. Buka terminal dan jalankan command `arp –a` pada host anda masing-masing (komputer sumber dan target), catat dan amati hasilnya. Apa maksud output yang dihasilkan command `arp –a`. Catat juga no ip dari masing-masing komputer tersebut. Gunakan `dhclient` untuk mendapatkan ip dari server.
2. Jalankan software wireshark pada komputer target untuk mengamati paket data yang lewat
   ```
   # wireshark
   ```
   Jika belum terinstall, instalasi terlebih dahulu paket tersebut :
   ```
   # apt-get install wireshark
   ```
3. Lakukan command `ping no_ip` ke komputer target.
4. Jalankan perintah `arp –a` atau `arp –n` sekali lagi. Amati pada perbedaan output dibanding waktu percobaan no 1. Stop wireshark dan amati proses yang terjadi pada wireshark
5. Jalankan wireshark lagi pada komputer target, dan lakukan ping sekali lagi dari komputer sumber ke komputer target.
   Amati proses yang terjadi pada wireshark.
6. Jawab pertanyaan berikut ini : Kenapa bisa terjadi perbedaan hasil percobaan meskipun kita memakai command yang sama, jelaskan secara singkat.
   Tabel arp tersimpan di /proc/net/arp, bisa dicek dengan :
   ```
   # cat /proc/net/arp
   ```
7. Kita bisa melakukan pengurangan ARP Cache atau disable ARP Cache, lakukan percobaan di bawah ini :
   a. Jalankan command `arp –d hostname` (pakai salah satu hostname / no_ip yang terdaftar pada arp cache). Amati hasilnya dengan menjalankan command arp –a.
   b. Jalankan command berikut : `ifconfig eth0 –arp down`, amati hasilnya dengan menjalankan `arp –a`.

c. Jalankan perintah ping ke komputer sebelah apa yang terjadi ?

NB : Dengan perintah pada b, maka jika dicek dengan ifconfig akan muncul NOARP

8. Setelah selesai melakukan percobaan 6, untuk menormalkan koneksi jaringan, jalankan perintah berikut :
   a. `ifdown eth0`
   b. `ifup eth0`
   c. `ifconfig eth0 arp up` -> jika dicek dgn ifconfig, NOARP akan hilang
   d. `arp –a`
   e. `dhclient` -> untuk mendapatkan ip dari server
   f. ping ke komputer sebelah
   g. Catat semua hasilnya.
9. Selain melakukan pengurangan juga bisa melakukan penambahan Arp Cache, lakukan command berikut :

   ```
   arp –s hostname physical_address
   ```

   Hostname bisa digantikan dengan no IP.
   Misal :
   ```
   # arp –s 192.168.10.5 00-01-4A-FJ-FD-CF
   ```

   Sebelum anda mengetik no phisical_address cari dulu di komputer teman anda dengan command `ifconfig`.

   ```
   selanjutnya jalankan command arp -a
   ```
   Amati hasil percobaan, berikan kesimpulan anda.

10. Untuk melakukan pengintaian kita bisa juga memakai tcpdump. Bukalah terminal baru dan jalankan tcpdump, biarkan tcpdump berjalan. Cobalah beberapa variasi command-command tambahan di tcpdump untuk mengintai paket yang lewat, misal tcpdump –n, tcpdump –n –t, tcpdump –n –t –e, tcpdump –i eth0, tcpdump –X –i eth0

11. Buka kembali terminal baru, lakukan langkah berikut pada terminal baru dan tulis hasil percobaannya:
    a. Jalankan perintah ping ke komputer satu jaringan. Amati hasil tcpdump.
    b. Jalankan perintah arp –a, catat hasilnya
    c. Jalankan perintah ping ke komputer diluar jaringan kita, amati hasilnya di tcpdump.
    d. Jalankan arp –a, analisa hasilnya. Amati pada tabel arp ketika kita berhubungan dengan komputer diluar jaringan, apa yang tertera pada tabel arp ?
    e. jalankan browser dan masuklah ke www yang anda suka. Amati traffic yang ada pada tcpdump. Analisa hasil percobaan anda apa maksud output yang dihasilkan.

12. Dengan menggunakan langkah yang sama seperti pada percobaan 10, gunakan paket wireshark
    a. Pastikan wireshark sudah terinstal pada komputer anda
    b. Buka terminal baru dan jalankan wireshark pada terminal tersebut

c. Mulailah mencapture data menggunakan wireshark dan filter hanya paket arp dan icmp (ping merupakan paket icmp)
d. Jalankan percobaan 11.a – e amati hasilnya di wireshark
e. Amati juga pada bagian data di wireshark, bandingkan dengan isi paket pada tcpdump.
f. Catatlah paket wireshark (src mac, dst mac, src ip, dst ip) jika kita berhubungan dengan komputer diluar kita, amati dan buat analisa yang terjadi.

LAPORAN RESMI

Daftar Pertanyaan

1. Bagaimana kesimpulan yang anda dapatkan jika komputer berhubungan dengan komputer di luar jaringan apa yang tercatat pada tabel arp ?.
2. Bagaimana kesimpulan yang anda dapatkan jika komputer berhubungan dengan komputer di luar jaringan dengan melihat paket data dari ethereal, rincilah src mac, dst mac, dst ip dan src ip yang terjadi jika kita berhubungan dengan jaringan luar.
3. Buat shell programming dengan ketentuan :
    a. jika kabel tersambung akan ditampilkan komentar “plug”
    b. jika tidak tersambung akan ditampilkan komentar “unplug”

LEMBAR ANALISA

Praktikum Jaringan Komputer -1 (Analisa Paket Layer)
Tanggal Praktikum :
Kelas :
Nama dan NRP :

A. Catat no ip komputer sumber dan target, dan catat juga hasil perintah : arp -a (poin 1)

B. Catat hasil perintah arp –a setelah dilakukan ping, catat juga proses yang terjadi di Wireshark (poin 4)

C. Catat proses di wireshark setelah dilakukan ping (poin 5)

D. Catat tabel arp cache yang tersimpan di /proc/net/arp

E. Percobaan dengan pengurangan atau disable ARP cache (poin 7-8)

F. Catat hasilnya dari poin 8

G. Percobaan dengan penambahan ARP cache (poin 9)

H. Catat hasil pada poin 10

I. Catat hasil pada poin 11 (tcpdump)

J. Catat hasil pada poin 12 (wireshark)