Gavin Benjiro Ramadhan
103012300452
IF-47-GAB.06

TP MODUL 10

Bagian A
No 1
Protokol IP bekerja sebagai protokol lapisan jaringan yang bertugas melakukan pengalamatan serta rute dalam paket data di jaringan. Sementara TCP dan UDP bekerja pada lapisan transport yang ebrtugas menyediakan layanan pengiriman data ke aplikasi. Hubungan antara IP dengan TCP/UDP adalah TCP/UDP membungkus data kemudian mengirim ke IP lalu IP mengirimkan paket ke tujuan menggunakan alamat IP. Namun IP mirip dengan UDP yaitu tidak menjamin keandalam pengiriman, sementara TCP menjamin keandalan pengiriman data.

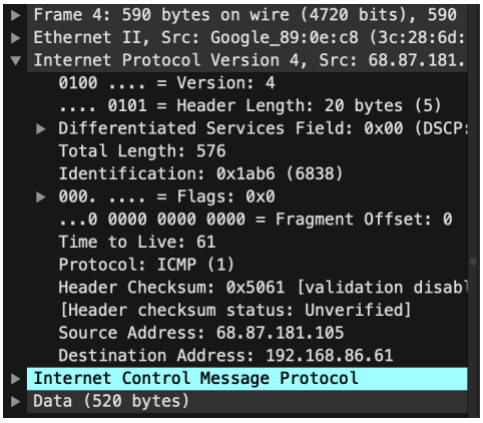
Keterkaitan dengan OSI Model
IP berada pada layer 3 (network layer) yang berfungsi sebagai pengalamatan dan routing paket TCP/UDP berada pada layer 4 (transport layer) yang berfungsi sebagai segmentasi data port, realibility (TCP) dan fast delivery (UDP).

Keterkaitan dengan TCP/IP model
IP berada pada internet layer sedangkan TCP/UDP berada pada transport layer. Jadi transport layer membuat segmen kemudian internet layer memberi alamat IP dan melakukan routing

No 2
192.0.2.33 adalah alamat IPv4 dari blok dokumentasi TEST-NET. Kemudian 2001:db8::192.0.2.33 adalah alamat IPv6 pada dokumentasi prefix dengan bagian akhir berupa IPv4 embedded. Keduanya digunakan untuk contoh, demonstrasi, dan berfungsi sebagai alamat sumber/tujuan pada datagram IPv4/IPv6 sesuai versi protokolnya.

Bagian B

No 1

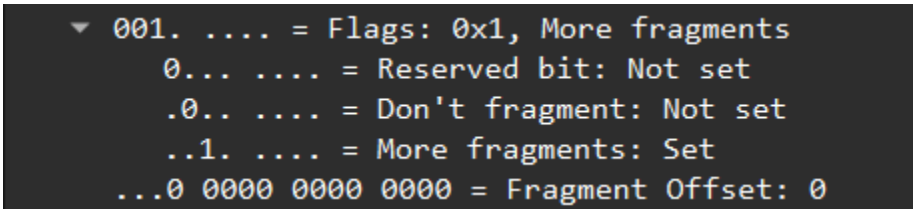


Berdasarkan hasil analisis pada header IPv4 di frame nomor 4, diperoleh informasi bahwa nilai TTL = 61 dan Protocol = 1 (ICMP). Kedua nilai ini menunjukkan dengan jelas bagaimana proses kerja router dan bagaimana jaringan memberikan respons terhadap paket yang TTL-nya habis. Nilai TTL = 61 mengindikasikan bahwa paket ICMP tersebut dikirim oleh sebuah router yang sedang memberi respons “Time-to-Live Exceeded”. Nilai TTL (Time To Live) selalu ditetapkan ulang oleh router ketika menghasilkan paket ICMP baru. Router biasanya menggunakan TTL awal seperti 64, dan nilai 61 menunjukkan bahwa paket ICMP ini telah melewati beberapa hop sebelum tiba pada host penangkap. Hal ini menggambarkan mekanisme kerja router: setiap router akan mengurangi TTL paket yang melintas, dan ketika TTL mencapai 0, router akan mengembalikan pesan ICMP untuk memberi tahu bahwa paket tidak dapat diteruskan lagi. Nilai Protocol = 1 menunjukkan bahwa paket tersebut adalah paket ICMP (Internet Control Message Protocol). ICMP merupakan protokol yang digunakan router untuk mengirim pesan kesalahan dan informasi diagnostik. Dalam konteks file ini, ICMP “Time-to-Live Exceeded” merupakan respons langsung dari router untuk memberitahukan bahwa paket asal sebelumnya sudah mencapai batas TTL. Dengan demikian, nilai TTL dan Protocol pada header IPv4 ini menggambarkan:

Kerja router dalam memproses TTL, yaitu mengurangi TTL setiap hop dan mengirimkan pesan ICMP saat TTL mencapai 0.

Respons jaringan melalui protokol ICMP, yang digunakan untuk melaporkan error dan kondisi jaringan.

No 2



Berdasrkan informasi tersebut, bisa dilihat nilai 1 pada more fragments itu artinya masih ada paket selanjutnya. More fragment bernilai 0 jika paket itu di reassembled atau disatukan kembali.

Kemudian nilai DF 0 artinya router diizinkan memecah paket menjadi beberapa fragmen dan paket akan di fragment jika ukuran paket lebih besar daripada MTU. Namun jika nilai DF 1 artinya router dilarang memecah paket dan jika ukuran paket lebih besar daripada MTU maka paket akan dibuang dan router mengirim ICMP

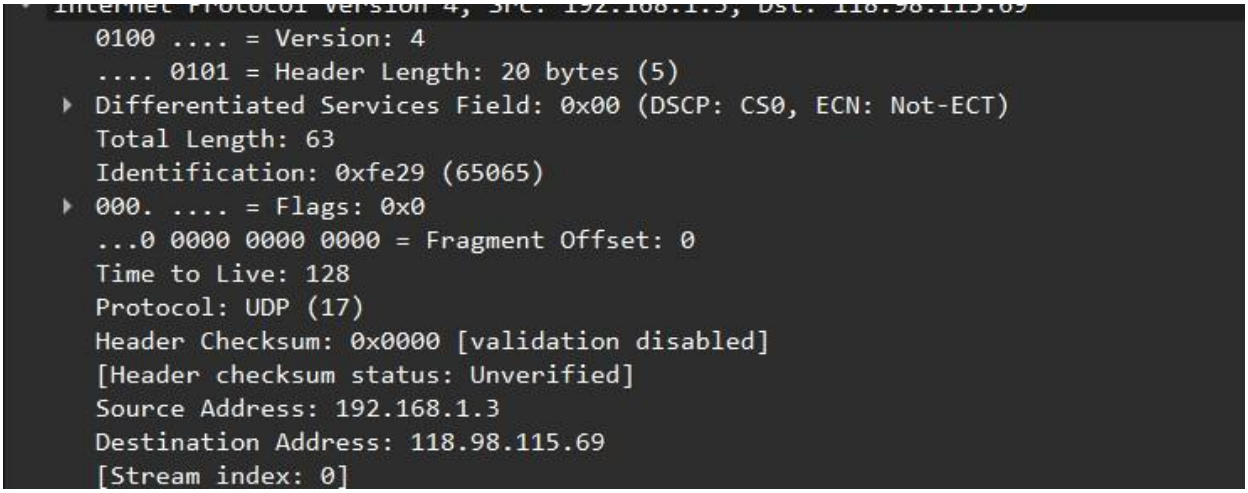
Fragment Offset menunjukkan posisi mulai fragmen dalam paket asli, dihitung dalam satuan 8-byte. Field ini digunakan untuk menentukan urutan fragmen dan membantu proses reassembly oleh host tujuan.

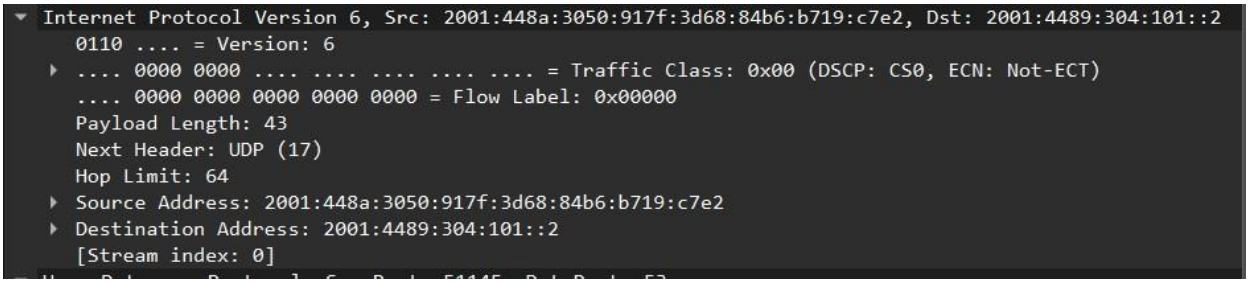
No 3

Nilai DSCP 0 menunjukkan bahwa pajet menggunakan layanan best effort tanpa prioritas QoS. Time To Live bernilai 61 menunjukkan paket kemungkinan berasal dari perangkat dengan TTL awal 64 dan telah melewati sekitar 3 hop, sehingga sumbernya dekat. Kemudian Ipv4 Header Checksum valid berarti tidak terdapat kerusakan pada header Ipv4 dan integritas paket terjamin saat ditangkap.

Bagian C

No 1





Perbedaan antara paket permintaan dan jawaban pada DNS dapat dilihat dari informasi yang dibawa. Jika jenisnya adalah *query*, maka paket tersebut merupakan permintaan. Jika berisi *response*, maka itu merupakan jawaban. Pada paket DNS untuk IPv4, contoh yang terlihat adalah *Record A* yang berisi alamat IPv4. Paket tersebut memiliki IP sumber 192.168.1.3 dan dikirim menuju alamat tujuan 118.98.115.69 dengan versi protokol 4, nilai *Traffic Class* berupa DSCP = 0 dan ECN = 0, serta nilai TTL sebesar 128. Sementara itu, pada paket DNS untuk IPv6, contoh yang digunakan adalah *Record AAAA* yang berisi alamat IPv6. Paket memiliki sumber 2001:448a…c7e2 dan tujuan 2001:4489:304:101::2, menggunakan versi protokol 6, *Traffic Class* bernilai 0, *Flow Label* bernilai 0, dan *Hop Limit* sebesar 64

No 2

Host pada awalnya menggunakan IPv4 untuk melakukan query DNS jenis A dan AAAA. Pola ini merupakan perilaku umum di banyak sistem operasi sebagai mekanisme *fallback* atau pengaturan bawaan sebelum mencoba koneksi melalui IPv6. Setelah itu, host juga terlihat mengirim query melalui IPv6, yang menunjukkan bahwa perangkat tersebut beroperasi dalam mode *dual-stack*. DNS server kemudian memberikan jawaban menggunakan protokol yang sama dengan protokol yang digunakan pada query. Pola pemilihan protokol ini mengikuti pendekatan *Dual-stack* dan *Happy Eyeballs*, yaitu mencoba IPv4 terlebih dahulu untuk memastikan konektivitas yang lebih cepat dan stabil, kemudian mencoba IPv6 jika tersedia, dan pada akhirnya menggunakan jalur yang paling responsif