Nama : Maisy Rahmawati

NPM : 1806147035

Kelas : Jarkomdat - A

**LOG WEEK 7**

**Materi: Network Layer DHCP**

* Network layer memiliki beberapa komponen diantaranya yaitu DHCP, NAT, ICMP, Traceroute, IPv6. Komponen tersebut ada yang berada pada application layer. Komponen tersebut membantu kita dalam untuk membantu kita dalam membantu menentukan IP address dan mengalokasikan alamat.
* Device-device dapat memperoleh IP address melalui beberapa cara yaitu diantaranya dengan menggunakan static address dan dynamic address. Ketika kita menggunakan static address maka kita perlu dan harus memasukkan IP address secara manual. Di samping itu, kita juga harus mengetahui subnettingnya. Sebaliknya, jika kita menggunakan dynamic address dengan DHCP misalkan melalui jaringan internet seperti WiFi, maka IP address kita akan ditetapkan secara otomatis atau automatic.
* Biasanya IP address yang static dikelola oleh beberapa server (pemberi jasa layanan internet) karena IP address tersebut akan bersifat permanen dan biasanya server tersebut IP addressnya bersifat public sehingga dapat diakses oleh berbagai client.
* DHCP akan menyebabkan kita memiliki IP address yang berubah-ubah (dynamic). Biasanya cara DHCP digunakan oleh pengguna jasa layanan internet (client).
* DHCP memiliki goal untuk mendapatkan IP address secara dynamic dari network server ketika client (pengguna internet) bergabung di dalam network atau jaringan internet. Kriteria dari DHCP yaitu IP address bisa diperbaharui, IP addressnya bisa digunakan kembali, dan dapat mendukung mobile users yang ingin bergabung di dalam network atau jaringan internet.
* DHCP overview:

1. Host broadcasts “DHCP discover” msg [optional]
2. DHCP server responds with “DHCP offer” msg [optional]
3. Host request IP address: “DHCP request” msg
4. DHCP server sends address: “DHCP ack” msg

* DHCP posisinya lebih dari menetapkan sebuah IP address, di mana DHCP juga dapat mengembalikan informasi lain yaitu address dari first hop router untuk client, name dan IP address dari DNS server, dan network mask (indicating network vs host portion of address).
* Router-router sederhana biasanya sudah memiliki DHCP server.
* Contoh dari DHCP yaitu:

1. Router dengan DHCP server yang ada di dalam router tersebut digunakan untuk menetapkan IP address, address dari first-hop router, dan address dari DNS server untuk laptop yang terkoneksi.
2. DHCP request dienkapsulasi di dalam UDP. Lalu dienkapsulasi di Ethernet dan di-broadcast ke dalam semua jaringan sehingga DHCP server juga terkena broadcast-an tersebut.
3. Karena DHCP server pastinya juga terkena broadcast-an tersebut, maka DHCP server mengetahui bahwa terdapat client yang membutuhkan IP address sehingga DHCP akan melakukan offering kepada client (laptop).
4. Lalu client (laptop) melakukan request IP address kepada DHCP server. Lalu masuk ke network layernya.
5. DHCP akan memberikan kembali IP address tersebut sehingga client dapat mengetahui IP address, IP address dari first-hopnya, dan name dan IP address dari DNS server. Selanjutnya client akan menulisnya di dalam network interfacenya.

* Kita dapat memperoleh IP address yaitu dengan mengalokasikan portion dari ISP provider kita. ISP provider juga memberikan IP address public kepada kita yang selanjutnya kita gunakan sehingga kita dapat berselancar di dalam internet. Akan tetapi, ketika kita masuk ke dalam jaringan router kita, maka kita hanya diberikan IP address lokal.
* Organisasi yang mengatur block dari addresses adalah ICANN (Internet Corporation for Assigned Names and Numbers). ICANN akan mengalokasikan addresses, mengelola DNS, dan menetapkan domain names serta resolves jika terjadi disputes.

Materi: Network Layer - NAT TraceRoute ICMP IPv6

* NAT (Network Address Translation) berguna untuk mentranslate IP address kita yang diberikan oleh DHCP server agar kita dapat berselancar di internet “seakan-akan” kita menggunakan IP address public.
* Semua datagram yang meninggalkan local network memiliki same single source NAT IP address (IP public).
* IP address public memiliki posisi untuk “mewakilkan” IP address local yang kita miliki untuk dapat berselancar di internet. Misalkan kita akan mengirimkan email melalui gmail maka yang akan dikenali oleh gmail adalah IP address public yang diberikan oleh ISP provider sebagai wakil dari IP address local kita. Ketika server akan mengirimkan data ke IP address local kita maka sebelumnya harus dilakukan translate terlebih dahulu oleh NAT karena server tidak dapat mengenali IP address local melainkan hanya mengenali IP address public yang diberikan oleh ISP provider yang kita gunakan.
* Range address sangat jarang atau langka dari ISP artinya satu IP address (public) bersifat untuk semua device.
* Kita dapat mengganti IP address di dalam local network kita secara dinamis sebanyak subnetting yang kita miliki.
* Kita dapat menggunakan ISP tanpa harus mengganti address dari device di dalam local network karena sudah disetting di dalam local network kita.
* Device di dalam local network secara eksplisit tidak dapat diakses dari luar sehingga perlu adanya translate menggunakan NAT.
* NAT router harus:

1. Outgoing datagram: replace
2. Remember (pada NAT translation table)
3. Incoming datagram: replace

* ICMP (Internet Control Message Protocol) sebagai suatu protokol yang digunakan agar kita dapat mengontrol atau mengetahui status dari message yang kita miliki. ICMP digunakan oleh hosts dan routers untuk saling berkomunikasi pada network level information untuk mengetahui error reporting dan echo request atau reply. ICMP message dikirim atau dibawa menggunakan IP datagram.
* Traceroute digunakan untuk mengetahui status dari tempat kita ke suatu server, jumlah hoping, dan waktu yang diperlukan untuk berpindah dari satu hop ke hop lain (dihitung dengan menggunakan TTL). Ketika ICMP message sampai maka source akan merecord RTTs.
* Stopping criteria akan terjadi jika UDP segment telah sampai ke destination host, jumlah hop-nya dibatasi atau “port unreachable”.
* ICMP juga merupakan salah satu contoh application layer sama seperti DHCP. Namun, ICMP lebih digunakan untuk mengontrol atau mengetahui status message pada network layer.
* IPv6 merupakan salah satu solusi ketika terjadi keterbatasan 32 bit address pada IPv4. IPv6 mempunyai fixed-length sebesar 40 byte header dan tidak ada fragmentasi yang diizinkan.
* Datagram format pada IPv6 terdiri dari priority, flow label, dan next header.
* IPv6 memiliki source address dan destination address sebesar 128 bits (sebagai pembeda dari IPv4).
* Beberapa hal yang berubah dari IPv4 ke IPv6 yaitu checksum yang dihapus karena dapat mengurangi waktu setiap kali berada di hop. Selain itu, ada pula versi baru ICMP yaitu ICMPv6, serta options yang diizinkan namun diluar dari header.
* Tunneling merupakan solusi agar IPv4 dapat berjalan hingga saat ini, di mana datagram IPv6 dibawa sebagai muatan dalam datagram IPv4 di antara router IPv4 karena network antara router belum semuanya dapat berganti menjadi IPv6 sehingga IPv6 dibungkus terlebih dahulu di dalam datagram IPv4.