Weekly Log
Week 7

Jonathan Filbert
JARKOMDAT - A
1806191692

Topic: DHCP, NAT, ICMP, IPv6

1. DHCP (Dynamic Host Configuration Protocol)

Tidak semua host (laptop, HP, server, dll) memiliki IP sendiri-sendiri, pada saat mereka baru diinstall, atau baru terkoneksi kepada sebuah *router,* maka mereka akan membutuhkan sebuah IP. Ada 2 cara pembagian IP, yaitu menggunakan IP static dan menggunakan DHCP.

Static IP yaitu setiap host akan di *hard code* IP nya pada sistem.
Keuntungan dari metode ini adalah biasanya digunakan kepada host yang IP nya tidak boleh berubah, misalnya server yang akan menerima request dari client, dll.

DHCP adalah metode yang dimana host akan di assign IP nya secara otomatis oleh sebuah server DHCP.
Keuntungan dari metode ini adalah *maintainer* atau admin tidak perlu melakukan hard code untuk setiap host yang ada, jadi konsep **plug-and-play** akan membuat pengguna sangat diuntungkan, tinggal *connect* sebuah host baru, dan tanpa konfigurasi akan langsung mendapatkan IP address.

Sistem DHCP:
1. Host akan membroadcast "**DHCP Discover**", dimana host akan membroadcast sebuah sinyal yang berasal dari IP kosong (0.0.0.0) ke seluruh device yang ada di network tersebut.
2. Karena server DHCP merupakan salah satu host juga yang ada di network, maka dia akan menerima broadcast signal dan akan menangkap broadcast tersebut. Setelah ditangkap maka DHCP akan mengirimkan "**DHCP Offer**" dimana DHCP akan mengirimkan sebuah address yang ditawarkan kepada host tersebut.
3. Setelah menerima offer, maka host dapat mengajukan apakah dia mau atau tidak, bila mau, maka host dapat mengirimkan "**DHCP Request**" dimana akan berisi IP address yang diinginkan kepada server DHCP.
4. Setelah menerima DHCP Request, maka server DHCP akan mengirimkan **"DHCP ACK"** yang merupakan pesan *acknowledgement* bahwa host sudah diberikan IP address tersebut.

2. NAT (Network Address Transslation)
Setelah mendapatkan sebuah IP, maka kita dapat berselancar di internet sekarang, tetapi apakah kita akan menggunakan IP yang baru saja kita dapatkan dari DHCP untuk berselancar? Ternyata tidak! Yang diberikan dari DHCP adalah sebuah IP private, sedangkan, untuk berselancar kita membutuhkan IP public, bagaimana cara mengubah IP private menjadi IP public? Jawabannya adalah IP address tersebut harus di translate dengan menggunakan NAT.

NAT adalah sebuah operasi yang akan dilakukan pada router ISP, dimana semua request yang akan meninggalkan sebuah ISP dan menuju ke internet sana, akan diubah menjadi menggunakan IP public dari ISP.

Skema NAT:
1. Sebuah PC dengan private IP address **10.0.0.1** akan mengunjungi google.com, maka request tersebut akan pergi ke router ISP.
2. Router ISP akan menerima request tersebut dan mengubah IP address tersebut menjadi sebuah IP address public yang dimiliki oleh ISP tersebut, contohnya **138.21.21.1:5000**
3. Request dari 138.21.21.1 akan sampai ke server google.com dan kemudian server google.com akan mengirimkan response ke 138.21.21.1:5000.
4. Response akan ditangkap oleh router ISP, dan kemudian akan diubah menjadi IP address private pengirim, yaitu **10.0.0.1**
5. Response akan diterusskan router ISP ke 10.0.01

Proses pengubahan private ke public IP dan sebaliknya menggunakan **translation table,** sebuah tabel key-value yang melakukan alokasi *mapping* public-private IP, sehingga router dapat dengan mudah melakukan perubahan antara public dan private IP.

Jonathan Filbert
JARKOMDAT - A
1806191692

3. ICMP (Internet Control Message Protocol)
ICMP adalah protokol pesan internet untuk mengirimkan dan memberitahu berbagai status dari request.

Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

Protocol ini sudah standar dan digunakan dalam program contohnya traceroute, sebuah program untuk melihat jejak dari request internet kita melalui berbagai router.

Contohnya pada saat kita mengunjungi google.com, maka host kita (laptop atau handphone) akan mengirimkan sebuah request ke router rumah, lalu router rumah akan mengirimkan request ke router ISP, lalu ke router ISP regional, dll dll. Apa yang terjadi bila pada saat kita mengirimkan request, lalu server yang dituju tidak merespon? Maka ICMP "**time-exceeded**" akan dikirimkan kepada host kita, sehingga host kita bisa tahu bahwa server yang sedang kita hop, tidak memberikan respons.

Untuk informasi mengenai bagaimana traceroute bekerja dapat membaca thread saya di SCELE,\

4. IPV6
Seiring dengan berkembangnya internet dan dunia server, maka kebutuhan akan public IP sangat meningkat, tentunya IPv4 yang hanya memiliki 32 bit address akan penuh, maka dari itu diciptakan lah IPv6 yang akan menjawab kebutuhan tersebut.

Perubahan IPv6:
- 40 byte header
- address dan destination sekarang 128 bit (dulu 32 bit)
- remove checksum
- options dikeluarkan dari header
- ICMPv6 (banyak kode message baru)

Tidak semua router sayangnya mensupport IPv6, karena biasanya hanya router high-end yang baru mensupport IPv6, untuk itu datagram yang dikirim dengan menggunakan IPv6 bila melalui router yang hanya mensupport IPv4 akan dibungkus dengan sebuah datagram IPv4 dimana datagram IPv6 akan dimasukan dalam payload, sehingga pada saat sampai ke router IPv6 lainnya, datagram tersebut akan dibuka dan payload nya dapat diteruskan lagi. Metode enkapsulasi dalam IPv6 ini disebut **tunneling.**