Nama : I Gusti Putu Urip Yogantara

NIM : 1504505053

Kelompok : 1

|  |
| --- |
| **MODUL I PENGALAMATAN JARINGAN** |

**Tujuan Praktikum**

1. Memahami Format IP *Addressing* versi 4 beserta pembagian kelasnya.
2. Memahami *Subnetting*.
3. Dapat mengkonfigurasi IP pada jaringan *Local Area Network*.

**Tugas Pendahuluan**

1. Jelaskan ip *addressing* version 4 dan pembagian kelasnya ! berikan contoh beserta perinciannya.
2. Jelaskan mengenai IP *subnetting* *classfull* & *classless* menggunakan CIDR & VLSM !
3. Jelaskan yang dimaksud dengan *broadcast domain* dan *default gateway*, serta berikan penjelasan jika muncul “*Destination Unreachable & Request Time Out*” pada proses *ping* !
4. Jelaskan mengenai IP *public* & IP *private*, serta metode NAT !

**Jawaban**

1. IPv4

IPv4 adalah sebuah pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IP versi 4. Panjang totalnya adalah 32-bit dan secara teori dapat mengalamati hingga 4 miliar *host* komputer atau lebih tepatnya 4.294.967.296 *host* di seluruh dunia. Jumlah *host* tersebut didapatkan dari 256 (didapatkan dari 8 bit) dipangkat 4 (karena terdapat 4 oktet) sehingga nilai maksimal dari alamt IP versi 4 tersebut adalah 255.255.255.255 dimana nilai dihitung dari nol sehingga nilai-nilai *host* yang dapat ditampung adalah 256 x 256 x 256 x 256 = 4.294.967.296 host. IPv4 dibagi menjadi 5 buah kelas, antara lain sebagai berikut.

* 1. Kelas A

Alamat kelas A diberikan ke jaringan dengan jumlah *host* yang sangat banyak. Bit orde tinggi di alamat kelas A selalu di-*set* ke nol. Tujuh bit berikutnya (yang melengkapi oktet pertama) melengkapi *network* ID. 24 bit sisanya (tiga oktet terakhir) menyatakan *host* ID. Kemungkinan ada 126 jaringan dan sekitar 17 juta *host* per jaringan. Perincian dari kelas A dapat dilihat pada Tabel 1.1.

**Tabel 1.1** Perincian Kelas A

|  |  |
| --- | --- |
| **Format** | 0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh  (n= Network ID, h= Host ID) |
| **Bit Pertama** | 0 |
| **Panjang *Network* ID** | 8 bit |
| **Panjang *Host* ID** | 24 bit |
| **Oktet Pertama** | 0-127 |
| **Range IP *Address*** | 1.xxx.xxx.xxx – 126.xxx.xxx.xxx |
| **Jumlah *Network*** | 126 |
| **Jumlah IP *Address*** | 16.777.214 |

Tabel 1.1 merupakan perincian dari kelas A. Berdasarkan perincian tersebut maka contoh dari IP *address* kelas A yaitu 123.43.5.7, dimana *network* ID adalah 123, dan *host* ID adalah 43.5.7.

* 1. Kelas B

Alamat kelas B diberikan ke jaringan berukuran sedang sampai besar. Dua bit orde tinggi di alamat kelas B selalu di-*set* ke *biner* 1 0. 14 bit berikutnya (melengkapi dua oktet pertama) melengkapi *network* ID. 16 bit sisanya (dua oktet terakhir) menyatakan *host* ID. Kemungkinan ada 16.384 jaringan dan sekitar 65.000 *host* per jaringan.

**Tabel 1.2** Perincian Kelas B

|  |  |
| --- | --- |
| **Format** | 10nnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh  (n= Network ID, h= Host ID) |
| **Bit Pertama** | 10 |
| **Panjang *Network* ID** | 16 bit |
| **Panjang *Host* ID** | 16 bit |
| **Oktet Pertama** | 128-191 |
| **Range IP *Address*** | 128.0.xxx.xxx – 192.255.xxx.xxx |
| **Jumlah *Network*** | 16.384 |
| **Jumlah IP *Address*** | 65.534 |

Tabel 1.2 merupakan perincian dari kelas B. Berdasarkan perincian tersebut maka contoh dari IP address kelas B yaitu 129.43.5.7, dimana *network* ID adalah 123.43, dan *host* ID adalah 5.7.

* 1. Kelas C

Alamat kelas C diberikan kepada jaringan lokal (LAN) yang kecil. Tiga bit orde tinggi di alamat kelas C selalu di-*set* ke biner 1110. 21 bit sisanya (melengkapi tiga oktet pertama) melengkapi *network* ID. Nilai 8 bit sisanya (oktet terakhir) menyatakan *host* ID. Kemungkinan terdapat sekitar 2 juta jaringan dan 254 *host* per jaringan.

**Tabel 1.3** Perincian Kelas C

|  |  |
| --- | --- |
| **Format** | 110nnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh  (n= Network ID, h= Host ID) |
| **Bit Pertama** | 110 |
| **Panjang *Network* ID** | 24 bit |
| **Panjang *Host* ID** | 8 bit |
| **Oktet Pertama** | 192-223 |
| **Range IP *Address*** | 192.0.0.xxx – 255.255.255.xxx |
| **Jumlah *Network*** | 2.097.152 |
| **Jumlah IP *Address*** | 254 |

Tabel 1.3 merupakan perincian dari kelas C. Berdasarkan perincian tersebut maka contoh dari IP *address* kelas C yaitu 195.43.5.7, dimana *network* ID adalah 195.43.5, dan *host* ID adalah 7.

* 1. Kelas D

Alamat kelas D digunakan untuk *group multicast*. *Group* *multicast* dapat terdiri atas satu atau lebih *host*, atau tidak sama sekali. Empat bit orde tinggi di alamat kelas D selalu di-*set* ke *biner* 1110. Bit sisanya menyatakan *grup multicast* tertentu. Tidak ada bit *network* dan *host* dalam operasi *multicast*. Paket diberikan ke *subnet host* tertentu di jaringan. Hanya *host-host* yang terdaftar ke alamat *multicast* yang menerima paket. Microsoft mendukung alamat kelas D bagi aplikasi untuk *multicast* data ke *host* di jaringan, termasuk WINS dan Microsoft NetShow.

**Tabel 1.4** Perincian Kelas D

|  |  |
| --- | --- |
| **Format** | 1110mmmm.mmmmmmmm.mmmmmmmm.mmmmmmmm |
| **4 Bit Pertama** | 110 |
| **Bit *Multicast*** | 28 bit |
| ***Byte* Inisial** | 224-247 |

Tabel 1.4 merupakan perincian dari kelas D. Kelas ini digunakan untuk keperluan *multicasting*/ 4 bit pertama 110, bit*-*bit berikutnya diatur sesuai keperluan *multicast group* yang menggunakan IP *address* ini. *Multicasting* tidak mengenal *network* bit dan *host* bit.

* 1. Kelas E

Kelas E adalah alamat eksperimental yang tidak tersedia untuk penggunaan biasa. Kelas ini dicadangkan untuk penggunaan di masa depan. Bit orde tinggi di kelas E di-*set* 1111.

**Tabel 1.5** Perincian Kelas E

|  |  |
| --- | --- |
| Format | 1111rrrr.rrrrrrrr.rrrrrrrr.rrrrrrrr |
| 4 Bit Pertama | 1111 |
| Bit Cadangan | 28 bit |
| *Byte* Inisial | 248-255 |

Tabel 1.5 merupakan perincian dari kelas E. Kelas E merupakan ruang alamat yang dicadangkan untuk keperluan eksperimental.

1. Metode *Subnetting*

*Subnetting* adalah proses memecah suatu IP jaringan ke sub jaringan yang lebih kecil yang disebut "*subnet*". Setiap *subnet* deskripsi non-fisik (atau ID) untuk jaringan-sub fisik (biasanya jaringan beralih dari host yang mengandung satu router -router dalam jaringan multi). *Subnetting* memiliki beberapa metode yaitu sebagai berikut.

* 1. *Classfull*

*Classful* secara sederhana dapat diartikan "dengan kelas" atau "menggunakan kelas". Metode *classful* dapat diartikan menjadi "pengalamatan IP berdasarkan kelas". Pengalamatan dengan metode ini ada pada pengalamatan IPv4 yang dibagi menjadi kelas A, B, C, D, dan E. Pengalokasian *host* pada jaringan dengan menggunakan sebuah *subnet mask* yang sama, biasanya menggunakan protokol RIPv1 dan IGRP, dimana protokol ini tidak mempunyai *field* untuk menyimpan informasi *subnet* sehingga informasi-informasi *subnet* tidak dikirimkan.

*Classfull* juga merupakan metode pembagian IP *address* berdasarkan kelas dimana IP *address* (yang berjumlah sekitar 4 milyar) dibagi kedalam lima kelas. Kelas tersebut dapat dilihat pada Tabel 2.1.

**Tabel 2.1** Pembagian Kelas Metode *Classfull*

|  |  |
| --- | --- |
| **IP *Address*** | **Bit Pertama** |
| Kelas A | 0 |
| Kelas B | 10 |
| Kelas C | 110 |
| Kelas D | 1111 |

*Classfull* memiliki suatu kelemahan. Kelemahan dari *classfull routing protocols* ialah tak dapat men-*suport* VLSM.

* 1. *Classless*

*Classless* secara sederhana dapat diartikan "tanpa kelas" atau "tidak menggunakan kelas". Metode *classless* dapat diartikan menjadi "pengalamatan IP tanpa mengenal kelas" dengan cara menggunakan *Classless-Inter Domain Rouing* (CIDR) atau juga dapat dikenal dengan istilah panjang prefiks. Format pengalamatannya adalah dengan memberi tanda *slash* (/) di belakang alamat IP kemudian diikuti dengan variabel panjang prefiks. Pengalokasian *host*/IP yang dapat menggunakan *subnet mask* yang berbeda, yang didukung oleh *routing* *protocol* (RIPv2, OSPF, dan EIGRP) yang dapat memberikan informasi *subnet*, sehingga dapat menghemat sejumlah alamat *host*/IP.

1. *Broadcast Domain* dan *Default Gateway*, serta “ *Destination unreachable & Request Time Ou”t* pada Proses *Ping*

*Subnetting* terdapat istilah *broadcast domain* dan *default gateway*, serta “*Destination unreachable & Request Time Out”* pada proses *ping.* Istilah-istilah tersebut dapat dijelaskan sebagai berikut.

* 1. *Broadcast Domain*

*Broadcast domain* secara umum dapat didefinisikan sebagai semua *device* atau perangkat yang dapat mengetahui sinyal yang berasal dari perangkat *network* tertentu yang berada dalam satu segmen.

*Broadcast domain* adalah sebuah divisi logis dari sebuah jaringan komputer, di mana semua *node* dapat mencapai atau terhubung satu sama lain dengan *broadcast* pada lapisan data *link.domain broadcast* dapat berada dalam segmen LAN yang sama atau dapat dijembatani untuk segmen LAN lain.

* 1. *Default Gateway*

*Default gateway* merupakan sebuah *device* atau perangkat yang merutekan trafik dari *local network* menuju *device* atau perangkat yang berada pada *remote network*. *Default gateway* biasanya digunakan untuk menghubungkan *local network* (komputer-komputer yang ada pada satu LAN) ke internet.

Apabila suatu *host* mengirim suatu paket menuju *device* yang berada pada IP *network* yang berbeda, *host* pengirim tadi harus mem-*forward* atau meneruskan paket tersebut melalui perantara *device* menuju *default gateway*. Hal ini dikarenakan *device host* tidak menyediakan *routing information* di luar *area local network* menuju *remote destination* atau tujuan di luar LAN. *Default gateway* biasanya diimplementasikan di *router* dan bekerja dengan *routing table*. *Routing table* sendiri merupakan sebuah *file* data yang tersimpan di dalam RAM yang digunakan untuk menyimpan informasi rute yang secara langsung terhubung ke jaringan, juga digunakan untuk menyimpan entri atau data pada *remote network* yang telah diketahui oleh *device*. *Router* menggunakan informasi yang terdapat pada *routing table* untuk menentukan jalan terbaik agar data bisa sampai pada tujuan.

* 1. *Destination Unreachable*

*Destination unreachable* terjadi jika *host*, jaringan, *port* atau protokol tertentu tidak dapat dijangkau atau masih mencari. Komunikasi di jaringan tergantung dari beberapa kondisi yang ditemui.

Pertama, protokol TCP/IP harus dikonfigurasi untuk *device* yang mengirim dan menerima data. Termasuk pemasangan protokol TCP/IP dan konfigurasi alamat IP dan *subnet mask*. *Default gateway* juga harus dikonfigurasi jika *datagram* keluar jaringan lokal. Kedua, *device* harus ditempatkan untuk melewatkan *datagram* dari *device* asal dan jaringannya ke *device* tujuan. *Router* juga harus mempunyai protokol TCP/IP yang dikonfigurasi di *interface*-nya dan harus menggunakan protokol *routing* tertentu.

Komunikasi jaringan tidak dapat dilakukan, jika kondisi tidak ditemukan. *Device* pengirim mengalamatkan *datagram* ke IP *address* yang tidak ada atau ke *device* tujuan yang tidak terhubung ke jaringan. *Router* dapat juga sebagai titik kesalahan jika koneksi *interface* putus atau jika *router* tidak memiliki informasi yang berguna untuk menemukan jaringan tujuan. Jaringan tujuan tidak dapat diakses seperti ini disebut dengan *unreachable destination*.

* 1. *Request Time Out*

*Request time out* atau RTO pada jaringan adalah suatu kejadian dimana server tidak menjawab / merespon permintaan dari komputer *client* setelah beberapa waktu berlalu. *Request time out* juga menandakan bahwa tidak ada koneksi yang antara komputer satu dengan komputer yang dituju. RTO memiliki berbagai macam penyebab antara lain.

1. *Utilisasi*/pemakaian *bandwidth* sudah penuh. solusi harus *upgrade* kecepatan.
2. Kualitas akses jaringan (*wireless*/*wireline*) kurang bagus.
3. *Website* yang dituju memiliki *delay* yang tinggi, sehingga *ping timeout*.
4. Koneksi ke IP tersebut putus.
5. *Port* di komputer tersebut ditutup.

*Request time out* pada sebuah jaringan dapat diatasi. Cara mengatasinya antara lain sebagai berikut.

1. Cek kembali penulisan IP tujuan pada sintaks *ping*.
2. Cek kembali apakah pemasangan kabel sudah tepat di komputer tujuan
3. Cek kembali NetID pada computer tujuan
4. Matikan *firewall* di kedua komputer.
5. IP *Public* dan IP *Private*, serta Metode NAT

*Subnetting* mengenal istilah IP *public*, IP *private*, dan metode NAT. Penjelasan mengenai istilah tersebut antara lain sebagai berikut.

* 1. IP *Public*

IP *public* adalah suatu IP *address* yang digunakan pada jaringan lokal oleh suatu organisasi dan organisasi lain dari luar organisasi tersebut dapat melakukan komunikasi langsung dengan jaringan lokal tersebut.

Sebuah alamat IP *public* yang ditugaskan untuk setiap komputer yang terhubung pada internet dimana setiap IP adalah unik. Maka akan tidak bisa ada dua komputer dengan alamat IP *public* yang sama dalam seluruh internet. Skema pengalamatan memungkinkan komputer untuk “menemukan satu sama lain” dan melakukan pertukaran informasi. Pengguna tidak memiliki kontrol atas alamat IP (*public*) yang diberikan ke komputer. Alamat IP *public* ditugaskan untuk komputer oleh *internet service provider* secara langsung setelah komputer terhubung ke *gateway* internet.

IP *public* memiliki suaru kelebihan. Kelebihan IP *public* tersebut yaitu dapat dikenali dalam internet dengan mudah, sebab langsung terhubung dengan internet tanpa perlu membutuhkan *proxy* tertentu, server khusus, atau ditranslasikan lewat NAT.

Selain memiliki kelebihan IP *public* juga memiliki beberapa kekurangan. Kekurangan tersebut antara lain sebagai berikut.

1. Tingkat *security* yang lemah dan rentan diserang *hacker*, sebab IP ini akan diberikan sebagai alamat umum dan langsung terhubung ke internet.
2. Biaya registrasi yang mahal, sebab merupakan alamat IP eksternal dan seperti kita tahu bahwa IP eksternal atau *public* sangat terbatas ketersediannya.
   1. IP *Private*

IP *private* adalah IP yang biasanya digunakan dalam jaringan yang tidak terhubung ke internet atau bisa juga terhubung ke internet tapi melalui NAT. IP *private* digunakan pada jaringan lokal oleh suatu organisasi dan organisasi lain dari luar organisasi tersebut dapat melakukan komunikasi langsung dengan jaringan lokal tersebut. IP *private* memiliki beberapa kelebihan antara lain sebagai berikut.

1. Aman dari gangguan orang yang tidak bertanggung jawab karena IP *private* tidak langsung terhubung pada internet.
2. Biaya registrasi IP *private* ini cukup rendah
3. Bebas menetukan IP dengan sendiri karena mempunyai rentang IP yang banyak.

Selain memiliki kelebihan IP *private* juga memiliki beberapa kekurangan. Kekurangan tersebut antara lain sebagai berikut.

1. Tidak langsung terhubung ke internet tanpa adanya *proxy server* dan NAT (*Network Address Translator*).
2. Tidak dapat di akses dari mana saja kita berada karena tidak langsung terhubung ke internet.
   1. Metode NAT

NAT (*Network Address Translation*) adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP. Banyaknya penggunaan metode ini disebabkan karena ketersediaan alamat IP yang terbatas, kebutuhan akan keamanan (*security*), dan kemudahan serta fleksibilitas dalam administrasi jaringan; Jaringan yang didisain untuk menyederhanakan IP *address* dan berperan juga untuk melindungi jaringan. NAT merupakan teknologi yang memungkinkan jaringan IP *private*, *software* yang melakukan NAT yang memungkinkan seluruh koneksi rumahan berbagi koneksi internet melalui satu IP *address*. NAT berlaku sebagai penerjemah antara dua jaringan. Beberapa kasus pada jaringan rumahan, posisi NAT diantara jaringan internet dan jaringan lokal. Internet sebagai sisi *public* dan jaringan lokal sebagai sisi *private*. Perangkat NAT akan membuka sedikit saluran antara komputer dan komputer tujuan, ketika komputer pada jaringan *private* menginginkan data dari jaringan *public* (internet). Ketika komputer pada jaringan internet membalikkan hasil dari permintaan, yang dilewati melalui perangkat NAT kepada komputer peminta, sehingga paket tersebut dapat diteruskan melewati jaringan *public*. NAT dapat membagi koneksi akses internet. Penggunaan metode NAT memberikan banyak keuntungan. Keuntungan tersebut antara lain sebagai berikut.

1. Menghemat alamat IP legal yang ditetapkan oleh NIC atau *service provider*.
2. Mengurangi terjadinya duplikat alamat jaringan.
3. Meningkatkan fleksibilitas untuk koneksi ke internet.
4. Menghindarkan proses pengalamatan kembali (*readdressing*) pada saat jaringan berubah.
5. Meningkatkan keamanan sebuah jaringan.
6. Memberikan keluwesan dan performa dibandingkan aplikasi alternatif setingkat *proxy*.

Selain memiliki kelebihan metode NAT juga memiliki beberapa kekurangan. Kekurangan tersebut antara lain sebagai berikut.

1. Translasi menimbulkan *delay switching*.
2. Menghilangkan kemampuan *trace* (*traceability*) *end to end* IP.
3. Aplikasi tertentu tidak dapat berjalan jika menggunakan NAT, khususnya NAT yang menggunakan *software*.