JURNAL TEKNIK KOMPUTER AMIK BSI

WILDCARD MASK SEBAGAI *FILTERING IP ADDRESS* MENGGUNAKAN METODE *ACCESS LIST CONTROL* PADA *ROUTER CISCO*

Aziz Setyawan. H

Abstract*—Implementation of a firewall in the computer network is important. In national newspapers proclaiming dated May 12, 2015 that Indonesia's second largest order of Origin Cyber Crime in the World. Furthermore, a report issued in 2014 the period of January to Desmber by Indonesia Security Incident Response Team on Internet Infrastructure / Coordination Center (id-SIRTII) that there was an attack ± 350,000 times in May in the form of an exploit. Exploit code is a computer security attack specifically. Exploit widely used for penentrasi either legally or illegally to find the weaknesses (Vulnerability) on the destination computer. Web attacks and attack-misc at its peak in August as much as ± 41,000 times. The first step to anticipate the occurrence of such attacks is a firewall application. Implementation firewall one of them by utilizing the Cisco Router. Cisco Router in the device that applies the concept of Access Control List (ACL) and included some content, such as: Application wildcard mask, specify the source IP address, destination IP address and define the final data package.

Keyword*—Firewall, Access Control List, the Destination IP Address, Wildcard Mask.

Intisari*—Implementasi sebuah firewall didalam jaringan komputer sangatlah penting. Dalam surat kabar nasional memberitakan tanggal 12 Mei 2015 bahwa Indonesia Urutan kedua terbesar Negara Asal Cyber Crime di Dunia. Selanjutnya laporan yang dikeluarkan tahun 2014 periode Bulan Januari sampai dengan Desmber oleh Indonesia *Security Incident Response Team on Internet Infrastructure/Coordination Center* (id-SIRTII) bahwa terjadi serangan ± 350.000 kali pada bulan Mei berupa exploit. Exploit adalah sebuah kode yang menyerang keamanan komputer secara spesifik. Exploit banyak digunakan untuk penentrasi baik secara legal ataupun ilegal untuk mencari kelemahan (*Vulnerability*) pada komputer tujuan. Dan terjadi serangan serangan web-misc pada puncaknya bulan Agustus sebanyak ± 41.000 kali. Langkah awal untuk mengantisipasi terjadinya serangan tersebut adalah penerapan Firewall. Implementasi firewall salah satunya dengan memanfaatkan perangkat Router Cisco. Di dalam perangkat Router Cisco tersebut menerapkan konsep *Access Control List* (ACL) dan di dalamnya terdapat beberapa konten, seperti : Penerapan wildcard mask, menentukan alamat IP sumber, mendefinisikan alamat IP tujuan dan terakhir paket datanya.

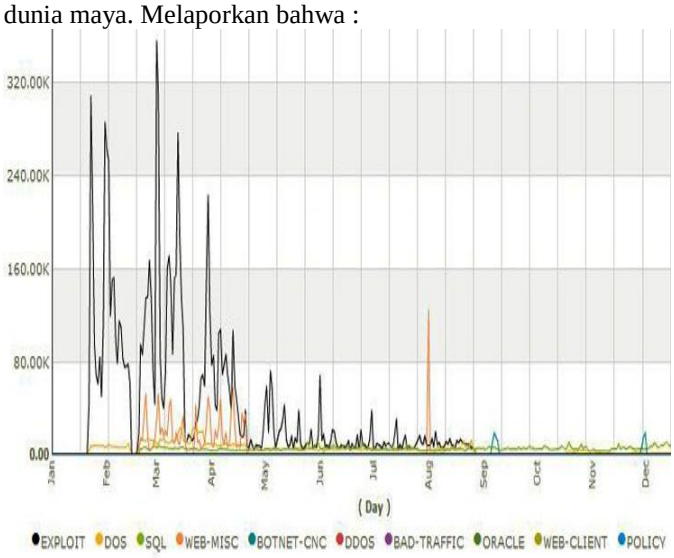
Kata Kunci—Firewall, Access Control List, Alamat IP Tujuan, Wildcard Mask.

I. PENDAHULUAN

Implementasi sebuah firewall didalam jaringan komputer pada sebuah instansi amatlah sangat diperlukan saat ini. Mengingat banyak sekali serangan maupun ancaman yang menunggu di dalam dunia maya. Mereka akan mencari celah atau ruang untuk dapat melakukan aksinya.

Dalam berita yang ditulis [10] bahwa Indonesia mengungkapkan bahwa sejak 2012 sampai dengan April 2015, ada 36,6 juta serangan terjadi *cyber crime* terjadi di Indonesia. Dan dalam kurun waktu tersebut Subdit IT*Cyber Crime* telah menangkap 497 orang tersangka kasus kejahatan di dunia maya.

Begitu pula hasil laporan yang dikeluarkan oleh Indonesia *Security Incident Response Team on Internet Infrastructure* (id-SIRTII), sebuah tim yang dibentuk oleh Kementerian Komunikasi dan Informasi (KOMINFO) berfungsi sebagai benteng pertahanan pertama dalam menghadapi serangan dunia maya. Melaporkan bahwa :



Sumber : id-SIRTII Laporan Tahun 2014

Gambar 1
Grafik Serangan Dunia Maya di Indonesia

Program Studi Teknik Komputer AMIK BSI Tegal, JL Sipelem, No. 8, Kemandungan, Tegal Barat Tegal Jawa-Tengah 52112 Telp +62 283 325114; e-mail: aziz.aiz@bsi.ac.id

Bahwa terjadi serangan ± 350.000 kali pada bulan Mei berupa exploit. ***Exploit*** adalah sebuah kode yang menyerang keamanan komputer secara spesifik. Exploit banyak digunakan untuk penentrasi baik secara legal ataupun ilegal untuk mencari kelemahan (*Vulnerability*) pada komputer tujuan. Dan terjadi serangan serangan web-misc pada puncaknya bulan Agustus sebanyak ± 41.000 kali.

Maka dapat dipastikan mengamankan sebuah jaringan saat ini adalah amatlah sangat penting. Karena keamanan jaringan di dalam sebuah instansi bukan hanya tugas negara saja tetapi elemen-elemen masyarakat harus dapat mendukung untuk terciptanya perlindungan dalam pengaksesan di dunia maya.

Langkah awal untuk mengantisipasi terjadinya serangan tersebut adalah penerapan *Firewall* pada jaringan komputer. Implementasi firewall di dalamnya terdapat beberapa konten yang harus dipahami agar firewall ini dapat berjalan dengan baik sesuai dengan harapan. Maka diperlukan sebuah pengetahuan yang baik oleh administrator jaringan.

Dengan mengacu pada latar belakang masalah tersebut di atas pada paragraph-paragraf sebelumnya, maka penulisan ini mencoba menganalisa peggunaan *Wildcard mask* pada aplikasi firewall yaitu *Access List Control* (ACL) sebagai filtering IP Address. Sebagai optimaslisasi dari sebuah sistem firewall yang digunakan pada perangkat Router Cisco.

Sedangkan batasan-batasan agar masalah yang dibahas di dalam penulisan menjadi lebih terarah, Antara lain :

1. Penerapan Wildcard mask pada Access List Control.
2. Penerapan Access List Control pada IOS Router Cisco.
3. Penerapan implementasi pada Program Simulasi Packet Tracer.

II. KAJIAN LITERATUR

A. *Internetwork Operation System* (IOS)

IOS merupakan sistem operasi yang terdapat di dalam perangkat router dan switch hasil pabrikan dari cisco company. Sistem operasi ini yang berfungsi sebagai dokumentasi dari sebuah perintah dan command yang telah di konfigurasi oleh admin jaringan agar dapat berjalan sesuai dengan keinginan dari admin jaringan tersebut.

Menurut [3] "Cisco IOS (*Internetwork Operating System),* yaitu suatu sistem operasi yang berfungsi untuk mengatur dan mengkonfigurasi Cisco Router. Seperti sistem operasi DOS untuk komputer, Cisco IOS menggunakan perintah baris (*command line*) untuk menjalankan suatu perintah".

Di dalam sistem operasi IOS seorang admin jaringan atau pengguna agar dapat mengakses IOS ini memelukan sebuah aplikasi yang di kenal dengan *Command Line Interface* (CLI), CLI ini berfungsi sebagai percabangan dalam berbagai macam mode yang ada di dalam IOS. Di dalam prompt CLI admin jaringan mendapatkan daftar perintah-perintah *command* yang berjalan pada setiap *command mode*.

Tabel I
Perintah dalam IOS

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in	Router >	Menggunakan perintah **Logout** *command*
Previleged EXEC	Berpindah dari User EXEC mode, menggunakan perintah **enable**	Router #	Untuk kembali ke User EXEC mode, menggunakan perintah **disable** *command*
Konfigurasi Global	Dari Priveledge mode, mengggunakan perintah **configure terminal** *command*	Router (config) #	Untuk kembali ke Priviledge mode, menggunakan perintah **exit** atau **end** *command*, atau bisa juga **Ctrl-z**
Konfigurasi Interface	Dari konfigurasi global mode, spesifik interface menggunakan perintah **interface** *command*	Router (config-if)#	Untuk kembali ke konfigurasi global mode, menggunakan perintah **exit** *command*. Untuk kembali ke Priveledge EXEC mode, menggunakan perintah **end** atau **exit** *command*, atau tekan **Ctrl-z.**
ROM Monitor	Dari Priveledge EXEC mode, menggunakan peritah **reload**		Untuk keluar ROM monitor mode, menggunakan perintah **continue** *command*

Log in awal pada sebuah router dengan menggunakan CLI awal pertama kali pengguna masuk ke dalam *user exec mode*. Di dalam *user exec mode* pengguna hanya dapat melihat-lihat atau menampilkan isi konfigurasi yang ada didalam IOS tidak dapat melakukan konfigurasi di dalam IOS. Pengguna untuk dapat mengakses atau menggunakan perintah-perintah konfigurasi didalam IOS, pengguna harus masuk ke dalam *Priviledge Exec Mode.*

B. Firewall

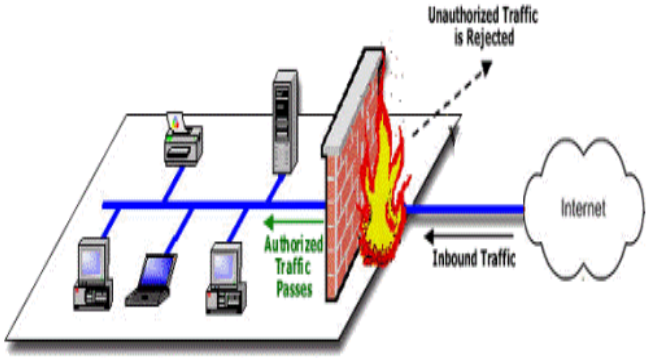
Menurut [9] mengatakan bahwa "Tujuan keamanan jaringan biasanya melibatkan tiga konsep dasar:

1. *Confidentiallity;* Ada dua jenis data: data yang bergerak di seluruh jaringan; dan data diam, ketika data yang diam di media penyimpanan (server, workstation lokal, dan sebagainya). Kerahasiaan hanya individu yang berwenang/sistem dapat melihat informasi rahasia. Hal ini juga berarti bahwa individu yang tidak sah tidak boleh memiliki jenis akses ke data tersebut. Mengenai data yang bergerak, cara utama untuk melindungi data adalah mengenkripsi sebelum mengirimnya melalui jaringan. Pilihan lain yang dapat digunakan dengan enkripsi adalah dengan menggunakan jaringan yang terpisah untuk penularan dari data rahasia.
2. *Integrity;* adalah perubahan data yang dibuat atau dilakukan hanya oleh yang berwenang individu/sistem. Korupsi data adalah kegagalan untuk menjaga *integrity* data.

3. *Availlability;* Hal ini berlaku untuk sistem dan data. Jika jaringan atau datanya tidak tersedia untuk pengguna dikarenakan oleh serangan *denial-of-service* (DoS) atau mungkin karena jaringan umum menaglami kegagalan, pengaruh signifikan kepada perusahaan dan pengguna yang mengandalkan jaringan yang sebagai alat bisnis. Kegagalan sistem, untuk memasukkan data, aplikasi, perangkat, dan jaringan, umumnya setara dengan kehilangan pendapatan.

Salah satu konesp dari kemana jaringan adalah firewall. Di dalam sistem keamanan jaringan komputer istilah firewall ini tidaklah sangat asing di dengarkan. Menurut [11] menjelaskan :

> Konsep firewall dalam konteks jaringan komputer mengambil gagasan dasar dari firewall (tembok penahan api) sebuah perangkat fisik yang dipasang di gedung-gedung. Tujuan utama pemasangan firewall fisik ini pada gedung-gedung adalah mencegah menjalarnya api dari sumbernya ke area di belakang firewall. Di kompleks-kompleks apartemen, misalnya, jika antara tiap-tiap unit apartemen dibatasi oleh sebuah firewall, maka api kebakaran yang timbul di salah satunya tidak akan menjalar degan mudah ke unit-unit yang bersebelahan karena terhalang firewall.



Sumber : www.gohacking.com/how-firewalls-work/

Gambar 2
Firewall

Menurut [4] mengatakan bahwa "Firewall adalah sebuah perangkat lunak atau perangkat keras yang menyaring semua lalu lintas jaringan antara komputer, jaringan rumah, atau jaringan perusahaan dan internet". Sedangkan karakteristik dari firewall di rancang dengan tujuan adalah sebagai berikut :

1. Semua lalu lintas yang berasal dari dalam jaringan komputer menuju keluar jaringan, harus melewati firewall.
2. Hanya lalu lintas yang berwenang dapat melewati firewall seperti membatasi kebijakan kemanan.
3. Sebuah firewall dapat sebagai kekebalan terhadap serangan dari luar.

Menurut [6] mengatakan bahwa "untuk dapat menjalankan tujuannya, sebuah firewall mempunyai empat teknik dalam mengontrol akses dan menegakkan kebijakan keamanan yang diterapkannya. Secara original, firewall terfokus pada keutamaan dalam mengontrol pelayanan, yaitu :

1. *Service Control*, Menentukan jenis layanan internet yang dapat diakses, *inbound* atau *outbound*. firewall dapat menyaring lalu lintas atas dasar alamat IP, protokol, atau nomor port; dapat menyediakan *software* proxy yang menerima dan menafsirkan setiap permintaan layanan sebelum dilewati atau mungkin host server perangkat lunak itu sendiri, seperti Web atau layanan mail.
2. *Direction Control*, Menentukan arah layanan tertentu di mana permintaan dapat dimulai dan dibiarkan mengalir melalui firewall.
3. *User Control*, Kontrol akses terhadap pengguna dengan layanan sesuai mencoba mengaksesnya. Fitur ini biasanya diterapkan untuk pengguna di dalam firewall perimeter (*user local*). Hal ini juga dapat diterapkan untuk lalu lintas masuk dari pengguna eksternal; yang terakhir membutuhkan beberapa bentuk teknologi otentikasi, seperti disediakan dalam Ipsec.
4. *Behavior Control*, Mengontrol bagaimana layanan tertentu yang digunakan. Sebagai contoh, firewall dapat menyaring e-mail untuk menghilangkan spam, atau memungkinkan akses eksternal untuk hanya sebagian dari informasi pada server Web lokal

Dengan empat teknik tersebut diatas implementasi firewall dapat menjalankan penyaringan paket, maka diberlakukan seperangkat aturan untuk setiap paket IP yang masuk dan yang keluar dan kemudian bisa dibiarkan untuk dilewati atau membuang paket tersebut. Firewall biasanya dikonfigurasi untuk penyaringan paket akan di kedua arah (dari dan ke internal jaringan). Aturan penyaringan didasarkan pada informasi yang terkandung dalam sebuah paket jaringan, yaitu :

1. *Source IP address*: Alamat IP dari sistem yang berasal paket IP.
2. *Destination IP address*:
3. *Source* dan *destination transport-level address*: Transportasi-tingkat (misalnya, TCP atau UDP) nomor port, yang mendefinisikan aplikasi seperti SNMP atau TELNET
4. *IP protocol field*: Mendefinisikan protokol transport.
5. *Interface*: Untuk firewall dengan tiga atau lebih port, interface firewall paket berasal dari atau interface firewall paket ditakdirkan untuk

C. Packet Filtering

Menurut [12] mengatakan "Packet filtering adalah mekanisme keamanan jaringan yang bekerja dengan mengontrol data apa yang dapat mengalir ke dan dari jaringan". Sebuah pakcket data dihantarkan melalui kendaraan yang disebut protokol, sedangkan protokol yang berfungsi sebagai pembawa packet data ini disebut sebagai IP (*Internet Protocol*) yang dapat mendefinisikan alamat sumber pengirim packet data dan alamat penerima packet data tersebut.

Selanjutnya didalamnya perjalanan packet data tersebut akan berjalan jika keluar dari jaringan komputer maka ada sebuah perangkat hardware yang harus dilewati paket data tersebut untuk dapat menentukan ke mana tujuan packet data tersebut akan ditujukan. Hardware tersebut disebut router.

Selanjutnya perangkat router ini akan mencek aturan yang diterapkan pada diri router tersebut dalam melakukan pengiriman packet data keluar maupun kedalam jaringan.

Hal tersebut diatas dijelaskan oleh [12] mengenai apa yang dilakukan oleh router pada sebuah paket data, beliau mengemukakan "Dalam menentukan bagaimana meneruskan paket ke tujuan, pada router yang normal dengan paket normal juga hanya terlihat alamat tujuan dan router hanya meminta "Bagaimana saya bisa meneruskan paket ini?" Sedangkan pada sebuah router packet filtering router akan mempertimbangkan pertanyaan "Haruskah saya meneruskan paket ini?" Paket filtering router menjawab pertanyaan yang sesuai dengan kebijakan keamanan diprogram didalam router melalui aturan penyaringan paket".

Sehingga yang terjadi pada paket dengan router paket filtering, paket tersebut akan ditahan dan selanjutnya dibuang jika paket tersebut terkena larangan untuk dilanjutkan ke luar jaringan oleh aturan penyaringan paket yang diterapkan oleh router. Sedangkan akan dibiarkan melewati atau diteruskan ke luar jaringan jika paket tersebut diberi izin oleh aturan penyaringan paket pada router untuk dilanjutkan ke luar jaringan.

D. Access List Control

Menurut [5] mengatakan bahwa "*Access Control Lists* (ACL) memungkinkan spesifikasi beberapa parameter yang merupakan dasar untuk kegiatan packet filtering, terlepas dari apakah penyaringan bergantung pada metode stateless atau stateful". Implementasi dari sebuah *access control list* yang dipergunakan oleh router mempunyai format penulisan :

Router> enable
Router# configure terminal
Router(config)# access-list standart/extended permit/deny source(hostname/ip/network) wildcard destination(hostname/ip/network) wildcard paket data

Menurut [8] mengatakan bahwa "ACL sangat membantu dalam pengontrolan lalu lintas dalam akses sebuah jaringan". Pada format penerapan ACL pada router cisco akan menyaring paket-paket data yang akan dilewati atau ditolak berdasarkan pada :

1. Alamat sumber
2. Alamat tujuan
3. Tipe protocol
4. Dan nomor port dari paket

Tetapi dalam implementasinya keempat format penerapan ACL tersebut tidak selalu digunakan, ini akan bergantung pada jenis ACL yang digunakan. Di dalam *access control list* mempunyai 2 jenis, yaitu :

1. Standart ACL hanya menggunakan alamat sumber IP di dalam paket IP sebagai kondisi yang diproses. Dan jenis ACL ini tidak dapat membedakan spesifik dari paket data yang akan diproses apakah itu akan diizinkan atau ditolak, dan jenis ACL ini diidentifikasikan dengan penomoran < 1 – 99 >
2. Extended ACL bisa melakukan pemrosesan banyak field lain pada header layer 3 dan layer 4 pada paket IP. Jenis ACL ini amat spesifik terhadap paket data yang akan diproses dari Alamat sumber, alamat tujuan, tipe protokol dan nomor port dari paket tersebut. Jenis ACL ini diidentifikasikan dengan penomoran < 100 – 199 >.

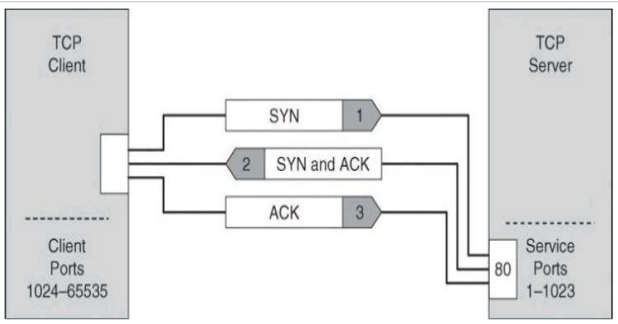
E. Protokol

Di dalam jaringan komputer ada beberapa arsitektur dan model. Arsitektur dan model di dalam jaringan komputer amat sangat penting, ini dikarenakan bagaimana sistem di dalam jaringan komputer dapat mengkomunikasikan perangkat-perangkat *hardware* maupun *software* yang ada didalamnya dapat berkomunikasi satu sama lain. Untuk sebuah model didalam jaringan banyak dikenal, contohnya *Systems Network Architecture* (SNA-IBM), AppleTalk, Novell Netware (IPX/SPX), dan *Open System Interconnection* (OSI).

Menurut [4] mengatakan "Sebuah protokol adalah sekumpulan aturan yang digunakan oleh komputer untuk dapat berkomunikasi dengan komputer lain atau satu sama lain. Kadang-kadang, beberapa protokol yang diperlukan untuk berkomunikasi, yang tidak jauh berbeda dari dunia nyata'.

Untuk memahami bagaimana firewall memproses lalu lintas jaringan, Anda harus tahu sedikit tentang TCP/IP. TCP/IP adalah bahasa yang digunakan oleh komputer untuk berbicara ketika mereka (komputer) berkomunikasi satu sama lain melalui Internet. Untungnya, TCP/IP jauh lebih mudah untuk dipelajari dibandingkan dengan bahasa asing (Protokol) lainnya, dan hanya komputer perlu memahami semua nuansa atau fitur-fitur yang ada di dalam TCP/IP.

Dibawah ini konsep komunikasi TCP dijelaskan oleh [7] adalah "TCP menggunakan desain *connection-oriented*. Desain ini berarti bahwa peserta dalam TCP harus terlebih dahulu membangun sambungan menggunakan *three-way-hanshake.*



Gambar 3
TCP Three-way-handshake

Keterangannya adalah :

1. Klien memilih dan mengirimkan *initial number sequence*
2. Server melakukan *acknowlegdes* dari *initila number squence* klient dan mengirimkan *number sequence* sendiri sendiri.

3. Klien melakukan *acknowlegdes* dari *number sequence* server dan koneksi yang terbuka untuk transmisi data.

Internet dan hampir semua jaringan kamputer menggunakan standarisasi pada model TCP / IP. Hal ini sering disebut sebagai bahasa internet, karena aplikasi biasanya dibangun di sekitar protokol ini. Menurut [2] mengatakan bahwa"pada Layer 4, sebenarnya ada dua protokol dihadirkan pada model ini, yaitu *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP). Banyak operasi didasarkan pada UDP, sehingga pada Layer 4 sebenarnya bersama oleh dua protokol. Lapisan 1 dan 2 diatur oleh *Local Area Network Protocol*, tapi Layer 3 milik IP dengan *Internet Control Message Protocol* (ICMP) dan *Internet Group Keanggotaan Protocol* (IGMP) komponen operasi berbasis IP".

Aplication	FTP, telnet, email, games, printing, http
Transport	Transmission Control Protocol (TCP), User Datagram Protocol (UDP)
Internet (internetwork)	Internet Protocol (IP), ICMP, IGMP
Link Layer (Network)	Ethernet, 802.11
Physical	Ethernet, 802.11

Sumber : Hartpence (2011:9)

Gambar 4
TCP/IP Model dan Protokol

F. Wildcard Mask

Wildcard mask merupakan pasangan dari sebuah IP Address di dalam konfigurasi pada sebuah aturan *access control list*yang berfungsi sebagai penyaring dari IP Address tersebut. Konsep dalam penulisannya sama dengan subnet mask yaitu terdiri dari 32-bit yang dibagi menjadi empat octet. Tetapi fungsi dari subnet mask dan wildcard mempunyai beberapa perbedaan, adalah subnet mask berfungsi sebagai pengidentifikasikan Network ID dan Host ID pada IP Address sedangkan Wildcard mask berfungsi sebagai filtering IP Address untuk dapat diijinkan atau ditolak dalam mengakses sesuatu pada firewall.

Konsep penyaringan di dalam *Wildcard* mask apakah sebuah address akan diberikan izin atau tidak berdasarkan pada *Wildcard* mask berdasarkan pada angka bineri "0" (null) atau "1" (satu) yang terkandung di dalam *Wildcard* mask tersebut. Sedangkan aturannya di dalam angka bineri tersebut adalah :

1. Bineri 0 (null) mengidentifikasikan pada bit address harus benar-benar sama, dan jika bineri alamat IP bertemu dengan nilai "0" (null) pada bineri *Wildcard* mask maka bineri alamat IP itu akan di proses.
2. Bineri 1 (satu) mengidentifikasikan pada bit address akan diabaikan, dan jika bineri alamat IP bertemu dengan nilai "1" (satu) pada bineri *Wildcard mask* maka bineri alamat IP itu akan tidak diproses atau diabaikan.

Dibawah ini tabel yang akan menjelaskan pernyataan diatas :

Tabel II
Cara konversi alamat ip dengan wildcard mask

Contoh Mask	
Network Address	10.1.1.0
Subnet mask	255.255.255.0
Wildcard Mask	0.0.0.255
Network Address dalam binery	00001010.00000001.00000001.00000000
Mask dalam binery	00000000.00000000.00000000.11111111

Penjelasan dari tabel tersebut adalah, dasar dari sebuah *Wildcard mask* yang telah dikonversi ke dalam angka biner, Network address dari IP Address diatas adalah 3 (tiga) octet pertama, yaitu (10.1.1), sedangkan pada octet 4 (empat) merupakan Host ID (0). Pada Wildcard mask tabel diatas adalah 3 (tiga) oktet pertama bernilai 0.0.0 atau jika Wildcard mask tersebut di konversikan ke dalam biner, maka (00000000.00000000.00000000), sedangkan pada oktet 4 (empat) pada Wildcard mask bernilai 255 atau dalam konversi ke biner (11111111).

Padankan antara nilai biner Network ID dengan nilai biner Wildcard mask akan terbentuk tabel 3 :

Tabel III
Padanan alamat ip dengan *Wildcard mask*

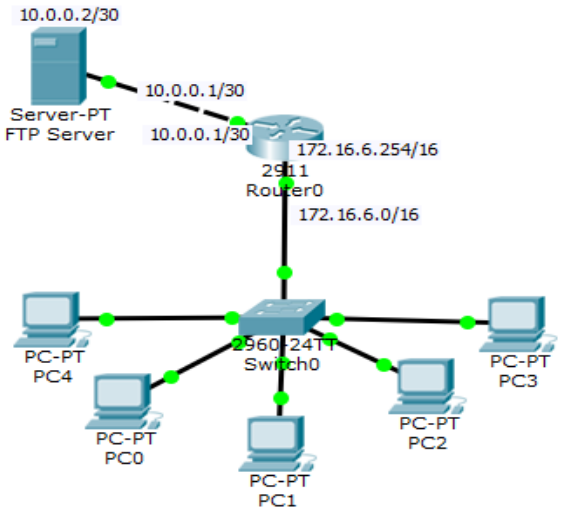
Net ID	00001010	00000001	00000001	
Wildcard	00000000	00000000	00000000	11111111

Maka nilai network ID tersebut di dalam tabel akan diproses dalam pemfilteran. Didalam *wildcard* ada 2 buah nilai yang diberikan spesial, yaitu :

1. 255.255.255.255 adalah nilai ini akan mengabaikan semua address yang ada atau bisa juga dengan mengganti perintah "any".
2. 0.0.0.0 adalah nilai ini akan memproses secara spesifik address yang dimilikinya. Contohnya : IP Address 172.16.0.1 Wildcard mask 0.0.0.0, maka nilai address yang akan diproses hanya address 172.16.0.1.

III METODE PENELITIAN

Metode penelitian yang digunakan adalah studi literatur dengan pengamatan menggunakan tools simulator jaringan komputer yaitu Packet Tracer. Di dalam simulator program Packet Tracer tersebut penulis membuat skema jaringan sebagai berikut :



Gambar 4
Skema Jaringan

Ruang lingkup pembahasan *Access Control List* (ACL) jenis extended yang menggunakan spesifik dari sebuah alamat sumber, alamat tujuan, tujuan protokol dari paket. Di dalam sebuah skenario terdapat sebuah ftp server dengan IP Address 10.0.0.2/32 yang terhubung dengan router pada interface GigaEthernet 0/1 dengan alamat IP 10.0.0.1/32. Dan pada perangkat router tersebut mempunyai 2 buah perangkat GigaEthernet, yaitu : GigaEthernet 0/1 terhubung ke server ftp dan yang satu lagi adalah GigaEthernet 0/2 terhubung ke swtich dengan IP Address 172.16.6.254/16. Sedangkan alamat IP untuk host/client pada jaringan tersebut adalah 172.16.0.1 sampai dengan 172.16.255.254/16.

Dan wildcard yang digunakan sebagai bahan dalam pembahsan adalah sebagai berikut :

Tabel IV
Studi Kasus *Wildcardmask* dalam Pembahasan

Studi Kasus	Wildcard	Dalam Bineri	Keterangan
Wilcardmask Full			
1	0.0.0.255	00000000.00000000. 00000000.11111111	Smua Octet Byte Full
2	0.0.0.255	00000000.00000000. 11111111.11111111	Smua Octet Byte Full
Wildcardmask Fulless			
1	0.0.0.252	00000000.00000000. 00000000.11111100	Byte ke 4 tidak full
2	0.0.0.248	00000000.00000000. 00000000.11111000	Byte ke 4 tidak full
3	0.0.255.248	00000000.00000000. 11111111.11111000	Byte ke 3 Full dan Byte ke 4 tidak full
4	0.0.255.240	00000000.00000000. 11111111.11110000	Byte ke 3 Full dan Byte ke 4 tidak full
5	0.0.248.255	00000000.00000000. 11111000.11111111	Byte ke 3 tidak full dan Byte ke 4 full
6	0.0.240.255	00000000.00000000. 11110000.11111111	Byte ke 3 tidak full dan Byte ke 4 full
7	0.0.248.248	00000000.00000000. 11111000.11111000	Byte ke 3 dan Byte ke 4 tidak full
8	0.0.240.240	00000000.00000000. 11110000.11110000	Byte ke 3 dan Byte ke 4 tidak full

Wildcardmask tersebut diatas akan diterapkan pada sebuah perangkat Router dengan menggunakan aplikasi *Access Control List* tepatnya adalah menentukan alamat IP sumber. Dalam hal ini format penulisan ACL jenis extended yang digunakan :

Router> enable
Router# configure terminal
Router(config)# access-list 101 deny tcp 172.16.6.0 wildcardmask host 10.0.0.2 eq ftp
Router(config)# access-list 101 permit ip any any

Dan dalam penelitian ini untuk menjawab " Apakah wildcard ini berfungsi sebagai penyaring dari alamat IP sumber pada segmen berapa ?

IV. HASIL PENELITIAN

A. Wildcard mask Full

1. Studi Kasus 1 (pertama)

Dalam hal ini format penulisan ACL jenis extended yang digunakan :

Router(config)# access-list 101 deny tcp 172.16.6.0 0.0.0.255 host 10.0.0.2 eq ftp

Sebagai penjelasan dari proses penyaringan Alamat sumber berdasarkan Wildcard mask yang diterapkan pada aturan ACL diatas adalah sebagai berikut :

Tabel V
Studi Kasus 1

Alamat Sumber : 172.16.6.0/16 WILDCARD MASK : 0.0.0.255	
Network Address	172.16.0.0
Subnet Mask	255.255.0.0
Host ID yang digunakan	172.16.6.0
Wildcard Mask	0.0.0.255
Host ID dalam binery	10101100.00010000.00000110.00000000
Wildcard mask dalam binery	00000000.00000000.00000000.11111111
Bineri yang diproses	10101100.00010000.00000110.--------
Alamat Host ID yang diproses	172 . 16 . 6

Penjelasan dari tabel diatas adalah IP sumber 172.16.6.0 dengan wildcard 0.0.0.255 adalah :

a. Jika terdapat sebuah host/client dengan IP address 172.16.6. maka alamat IP ini akan diproses. Sedangkan prosesnya adalah melihat perintah sebelumnya yaitu "deny tcp".
b. Perintah "deny" adalah menolak, jadi perintah ini berfungsi sebagai penghalang dan tidak diberikan izin untuk dapat melewati interface router. Nah apa yang ditolak ?
c. Setelah perintah "deny" adalah nama aplikasi yaitu "tcp". Aplikasi tersebut kepanjangannya adalah Transmission Control Protocol. Didalam aplikasi tcp terdapat beberapa paket data yaitu ftp, pop3, smtp, telnet dan www.
d. Sedangkan Wildcard mask 0.0.0.255 berfungsi sebagai pemilih atau penentu alamat IP segmen apa saja yang akan ditolak (deny). Dilihat dari Wildcard mask yang digunakan adalah Byte ke 1 (pertama) sampai dengan Byte ke 3 merupakan angka "0" (null). Ini menandakan

bahwa 3 Byte alamat IP yang dideklarasikan akan ditolak. Sedangkan pada Byte ke 4 bernilai 255, jika dikonversikan ke dalam biner maka jumlah Byte ke 4 tersebut bernilai "1" (satu) semua dengan banyaknya 8 buah angka "1". Hal ini dikarenakan 1 Byte sama dengan 8 bit. Maka dapat dipastikan Byte ke 4 ini apapun angka yang dideklarasikan pada alamat IP source tidak akan di proses.

Maka kesimpulannya adalah dari perintah access list control yang diterapkan pada router dengan sintaks access-list 101 deny tcp 172.16.6.0 0.0.0.255 host 10.0.0.2 eq ftp, adalah setiap segment alamat IP 172.16.6.0 sampai dengan 172.16.6.255 tidak akan dapat mengakses ke ftp server. Ada hal yang tersirat juga dalam perintah access list diatas adalah selain alamat IP dengan 3 Byte segment berbeda dari alamat IP sumber tidak akan diproses dalam hal ini prosesnya adalah ditolak untuk mengakses ftp server. Dengan kata lain alamat IP selain tersebut dapat diberi akses atau izin untuk mengakses ftp server. Alamat IP yang diberi akses adalah :

Tabel VI
Alamat IP dapat Mengakses FTP Server dengan *Wildcard* 0.0.0.255

Alamat IP	Wildcard dalam Biner 0.0.0.252	Keterangan
172.16.0.1 sampai dengan 172.16.5.255	00000000.00000000. 00000000.11111100	Diizinkan ke ftp server
172.16.6.0 sampai dengan 172.16.6.255	00000000.00000000. 00000000.11111100	Ditolak ke ftp server
172.16.7.0 sampai dengan 172.16.255.254	00000000.00000000. 00000000.11111100	Diizinkan ke ftp server

2. Studi kasus yang kedua

Dalam hal ini format penulisan ACL jenis extended yang digunakan :

Router(config)# access-list 101 deny tcp 172.16.6.0 0.0.255.255 host 10.0.0.2 eq ftp

Sebagai penjelasan dari proses penyaringan Alamat sumber berdasarkan Wildcard mask yang ditetapkan pada aturan ACL diatas adalah sebagai berikut :

Tabel VIII
Studi kasus 2

Alamat Sumber : 172.16.6.0/16 Wildcard mask : 0.0.255.255	
Network Address	172.16.0.0
Subnet Mask	255.255.0.0
Host ID yang digunakan	172.16.6.0
Wildcard Mask	0.0.255.255
Host ID dalam binery	10101100.00010000.00000110.00000000
Wildcard mask dalam binery	00000000.00000000.11111111.11111111
Bineri yang diproses	10101100.00010000.--------.--------
Alamat Host ID yang diproses	172 . 16 . - . -

Penjelasan dari tabel diatas adalah IP sumber 172.16.6.0 dengan wildcard 0.0.255.255 adalah :

a. Dalam kasus ini wildcard yang digunakan di dalam ACL merupakan lawan dari subnet mask yang digunakan pada alamat IP host/clien, maka semua alamat IP host/clien akan diproses. Subnet mask yang digunakan pada alamat IP host/clien adalah 255.255.0.0 sedangkan wildcard yang digunakan adalah 0.0.255.255. Bahwa terlihat nilai Byte pertama dan kedua subnet mask 255.255 sedangkan nilai Byte pertama dan kedua Wildcardmask adalah 0.0 maka dapat dikatan bahwa NetID pada alamat IP tersebut akan diproses. Sedangkan prosesnya adalah melihat perintah sebelumnya yaitu "deny tcp".
b. Perintah "deny" adalah menolak, jadi perintah ini berfungsi sebagai penghalang dan tidak diberikan izin untuk dapat melewati interface router. Nah apa yang ditolak ?
c. Setelah perintah "deny" adalah nama aplikasi yaitu "tcp". Aplikasi tersebut kepanjangannya adalah Transmission Control Protocol. Didalam aplikasi tcp terdapat beberapa paket data yaitu ftp, pop3, smtp, telnet dan www.
d. Sedangkan Wildcardmask 0.0.255.255 berfungsi sebagai pemilih atau penentu alamat IP segmen apa saja yang akan ditolak (deny). Dilihat dari Wildcard mask yang digunakan adalah Byte ke 1 (pertama) sampai dengan Byte ke 2 merupakan angka "0" (null). Ini menandakan bahwa 2 Byte sebagai alamat Net ID yang dideklarasikan akan ditolak. Disini 2 Byte tersebut merupakan alamat NetID, jadi dapat ditarik kesimpulan bahwa Net ID 172.16.0.0 akan ditolak dan akhirnya semua host/client pada Net ID tersebut juga akan ditolak atau tidak diizinkan untuk mengakses ftp server.

B. Wildcard mask Fulless

Di dalam kasus ini Wildcard mask yang akan dideklarasikan pada ACL nilai dalam binernya tidak bernilai "0" (null) semuanya atau bernilai "1" (satu) semuanya dalam binery octet Byte-nya. Tetapi nilai dalam biner pada pada salah satu octet Byte-nya terdiri dari angka "1" (satu) atau "0" (null).

1. Studi Kasus 1 (pertama)

Router(config)# access-list 101 deny tcp 172.16.6.0 0.0.0.252 host 10.0.0.2 eq ftp

Analisa dari wildcard yang digunakan yaitu 0.0.0.252 adalah :

Yang menjadi fokus perhatian pada wildcard yang dipergunakan yaitu terletak pada Byte ke 4 karna pada Byte ke 4 tersebut angka yang ada adalah 252, sedangkan angka Byte pertama sampai dengan Byte ketiga adalah "0" (null). Dan angka Byte ke 4 tidak bernilai 255 tetapi bernilai 252, berarti pada Byte ke 4 dalam 8 bit angkanya tidak sama angkanya yaitu "1" (satu) semua atau "0" (null) semua dan jika dikonversikan ke dalam angka bineri adalah 8 bit-nya 11111100 yaitu terdiri angka "1" (satu) sebanyak 6 bit dan angka "0" (nul) sebanyak 2 bit.

Tabel VIII

Penjelasan Kasus 1

WILDCARD MASK : 0.0.0.252			
Angka Desimal Byte 1	0	Angka Binery Byte 1	00000000
Angka Desimal Byte 2	0	Angka Binery Byte 2	00000000
Angka Desimal Byte 3	0	Angka Binery Byte 3	00000000
Angka Desimal Byte 4	252	Angka Binery Byte 4	11111100

Dan hasil alamat sumber dari alamat IP yang deklarasikan pada wildcard tersebut diatas dalam ACL, adalah :

Tabel IX

Hasil Penerapan Wildcard Kasus 1

Alamat IP	Wildcard dalam Biner 0.0.0.252	Keterangan
172.16.0.1 sampai dengan 172.16.5.255	00000000.00000000. 00000000.11111100	Diizinkan ke ftp server
172.16.6.0	00000000.00000000. 00000000.11111100	Ditolak ke ftp server
172.16.6.1 sampai dengan 172.16.6.3	00000000.00000000. 00000000.11111100	Diizinkan ke ftp server
172.16.6.4	00000000.00000000. 00000000.11111100	Ditolak ke ftp server
172.16.6.5 sampai dengan 172.16.6.7	00000000.00000000. 00000000.11111100	Diizinkan ke ftp server
172.16.6.8, 172.16.6.12, 172.16.6.16, 172.16.6.20, 172.16.6.24 Dan seterusnya	00000000.00000000. 00000000.11111100	Ditolak ke ftp server
172.16.7.0 sampai dengan 172.16.255.254	00000000.00000000. 00000000.11111100	Diizinkan ke ftp server

Di dalam tabel diatas alamat IP 172.16.0.1 sampai dengan 172.16.5.255 tidak akan diproses. Hal ini dikarenakan di dalam ACL mendeklarasikan alamat sumber yang menjadi acuan adalah 172.16.6.0, jadi segmen alamat IP tersebut akan diproses. Selain alamat IP dengan segmen tersebut tidak akan diproses atau diabaikan. Jadi dapat disimpulkan alamat IP 172.16.0.1 sampai dengan 172.16.5.255 dan alamat IP 172.16.7.0 sampai dengan 172.16.255.254 pasti diabaikan atau tidak akan diproses. Sedangkan untuk alamat IP dengan segmen IP 172.16.6.0 sampai dengan 172.16.255 akan diproses berdasarkan dibawah ini penjelasannya.

Sebagai penjelasan dari hasil tabel diatas fokus pada Byte ke 4 dari Wildcard mask yang sudah di deklarasikan, yaitu : 11111100 yang terdiri dari angka "1" (satu) sebanyak 6 bit dan angka "0" (null) sebanyak 2 bit. Di dalam konversi tersebut angka "0" (null) yang sebanyak 2 dan sebuah Host ID yang diproses di dalam wildcard tersebut adalah kelipatan angka 4 (empat). Jadi diambil kesimpulan sebuah Host ID yang akan diproses tergantung dari jumlah angka "0" (null) menjadi nilai pangkat 2. Jadi dapat disimpulkan Host ID yang diproses dapat menggunakan rumus pada Wildcard mask yang fulless, adalah :

$$2^w = x$$

Keterangan :

W = Jumlah angka null dalam 1 Byte Wildcard

X = Kelipatan Host ID yang akan diproses

2. Studi Kasus 2 (kedua)

Router(config)# access-list 101 deny tcp 172.16.6.0 0.0.0.248 host 10.0.0.2 eq ftp

Analisa dari wildcard yang digunakan yaitu 0.0.0.248 adalah :

Yang menjadi fokus perhatian pada wildcard yang dipergunakan yaitu terletak pada Byte ke 4 karena pada Byte ke 4 tersebut angka yang ada adalah 248, sedangkan angka Byte pertama sampai dengan Byte ketiga adalah "0" (null). Dan angka Byte ke 4 tidak bernilai 255 tetapi bernilai 248, berarti pada Byte ke 4 dalam 8 bit angkanya tidak sama angkanya yaitu "1" (satu) semua atau "0" (null) semua dan jika dikonversikan ke dalam angka bineri adalah 8 bit-nya 11111000 yaitu terdiri angka "1" (satu) sebanyak 5 bit dan angka "0" (nul) sebanyak 3 bit.

Tabel X

Penjelasan Kasus 2

WILDCARD MASK : 0.0.0.248			
Angka Desimal Byte 1	0	Angka Binery Byte 1	00000000
Angka Desimal Byte 2	0	Angka Binery Byte 2	00000000
Angka Desimal Byte 3	0	Angka Binery Byte 3	00000000
Angka Desimal Byte 4	248	Angka Binery Byte 4	11111000

Dan hasil alamat sumber dari alamat IP yang deklarasikan pada wildcard tersebut diatas dalam ACL, adalah :

Tabel XI

Hasil Penerapan Wildcard Kasus 2

Alamat IP	Wildcard dalam Biner	Keterangan
172.16.0.1 sampai dengan 172.16.5.255	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.6.0	00000000.00000000. 00000000.11111000	Ditolak ke ftp server
172.16.6.1 sampai dengan 172.16.6.7	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.6.8	00000000.00000000. 00000000.11111000	Ditolak ke ftp server
172.16.6.9 sampai dengan 172.16.6.15	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.6.16, 172.16.24, 172.16.6.32, 172.16.6.40, 172.16.6.48 Dan Seterusnya	00000000.00000000. 00000000.11111000	Ditolak ke ftp server
172.16.7.0 sampai dengan 172.16.255.254	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server

Di dalam tabel diatas alamat IP 172.16.0.1 sampai dengan 172.16.5.255 tidak akan diproses. Hal ini dikarenakan di dalam ACL mendeklarasikan alamat sumber yang menjadi acuan adalah 172.16.6.0, jadi segmen alamat IP tersebut akan diproses. Selain alamat IP dengan segmen tersebut tidak akan diproses atau diabaikan. Jadi dapat disimpulkan alamat IP 172.16.0.1 sampai dengan 172.16.5.255 dan alamat IP 172.16.7.0 sampai dengan 172.16.255.254 pasti diabaikan atau tidak akan diproses. Sedangkan untuk alamat IP dengan segmen IP 172.16.6.0 sampai dengan 172.16.255 akan diproses berdasarkan dibawah ini penjelasannya.

Sebagai penjelasan dari hasil tabel diatas fokus pada Byte ke 4 dari Wildcard mask yang sudah di deklarasikan, yaitu : 11111000 yang terdiri dari angka "1" (satu) sebanyak 5 bit dan angka "0" (null) sebanyak 3 bit. Di dalam konversi tersebut angka "0" (null) yang sebanyak 3 dan sebuah Host ID yang diproses di dalam wildcard tersebut adalah kelipatan angka 8 (delapan). Jadi diambil kesimpulan sebuah Host ID

yang akan diproses tergantung dari jumlah angka "0" (null) menjadi nilai pangkat 2. Jadi dapat disimpulkan Host ID yang diproses dapat menggunakan rumus pada Wildcard mask yang fulless berdasarkan banyaknya angka "0" (null) dalam 1 Byte ke 4 wildcard fulless, adalah :

$$2^w = x$$

Keterangan :
W = Jumlah "0" (null) dalam 1 Byte Wildcard Fulless
X = Kelipatan Host ID yang akan diproses

3. Studi Kasus 3 (Ketiga)

Router(config)# access-list 101 deny tcp 172.16.6.0 0.0.255.248 host 10.0.0.2 eq ftp

Analisa dari wildcard yang digunakan yaitu 0.0.255.248 adalah :

Yang menjadi fokus perhatian pada wildcard yang dipergunakan yaitu terletak pada Byte ke 3 dan Byte ke 4 karena pada Byte ke 3 dan Byte ke 4 tersebut angka yang ada adalah 255.248, sedangkan angka Byte pertama dan kedua adalah "0" (null). Pada angka Byte ke 3 (tiga) bernilai 255 jadi pada Byte ke 3 ini nilai 8 bit nernilai "1" (satu) semua. Dan angka Byte ke 4 tidak bernilai 255 tetapi bernilai 248, berarti pada Byte ke 4 dalam 8 bit angkanya tidak sama angkanya yaitu "1" (satu) semua dan jika dikonversikan ke dalam angka bineri adalah 8 bit-nya 11111000 yaitu terdiri angka "1" (satu) sebanyak 5 bit dan angka "0" (nul) sebanyak 3 bit.

Tabel XII

Penjelasan Studi Kasus 3

WILDCARD MASK : 0.0.0.248			
Angka Desimal Byte 1	0	Angka Binery Byte 1	00000000
Angka Desimal Byte 2	0	Angka Binery Byte 2	00000000
Angka Desimal Byte 3	255	Angka Binery Byte 3	11111111
Angka Desimal Byte 4	248	Angka Binery Byte 4	11111000

Dan hasil alamat sumber dari alamat IP yang deklarasikan pada wildcard tersebut diatas dalam ACL, adalah :

Tabel XIII

Hasil Penerapan Wildcard Kasus 3

Alamat IP	Wildcard dalam Biner	Keterangan
172.16.0.1 sampai dengan 172.16.0.7	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.0.8	00000000.00000000. 00000000.11111000	Ditoal ke ftp server
172.16.0.9 sampai dengan 172.16.0.15	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.0.16	00000000.00000000. 00000000.11111000	Ditoal ke ftp server
172.16.0.17 sampai dengan 172.16.0.23	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.0.24	00000000.00000000. 00000000.11111000	Ditolak ke ftp server
172.16.0.25 sampai dengan 172.16.0.31	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
Dan Seterusnya		

Di dalam tabel diatas baris pertama alamat IP 172.16.0.1 sampai dengan 172.16.0.7 tidak akan diproses. Hal ini dikarenakan di dalam ACL mendeklarasikan alamat sumber yang menjadi acuan adalah 172.16.6.0 dengan Wildcard mask 0.0.255.248. Yang menjadi fokus dalam alamat IP sumber dan wildcard yang akan dibahas terletak pada Byte ke 3 (tiga) dan Byte ke 4 (empat), alamat IP yang menjadi alamat sumber pada Byte ke 3 dan Byte ke 4 adalah 6.0 sedangkan Wildcard mask yang digunakan pada Byte ke 3 dan Byte ke 4 adalah 255.248. Prinsip dalam binery wildcard adalah jika sebuah oktet Byte bertemu dengan nilai "1" (satu) pada bineri octet Byte wildcard maka nilai oktet Byte alamat IP tersebut akan diabaikan atau tidak akan diproses. Maka dapat dipastikan bahwa nilai alamat IP sumber pada Byte ke 3 akan diabaikan atau tidak akan diproses dikarenakan alamat IP sumber pada Byte ini bertemu dengan wildcard binery octet Byte ke 3 bernilai "1" (satu) semua atau dalam desimal bernilai 255.

Selanjutnya alamat IP sumber octet Byte ke 4 bertemu dengan Wildcard mask pada octet Byte ke 4 bernilai tidak full yaitu, 248. Nilai octet Byte ke 4 wildcard ini jika dikonversikan ke dalam binery adalah 11111000, angka hasil konversi tersebut terdiri dari angka "1" (satu) sebanyak 5 digit dan angka "0" (null) sebanyak 3 digit. Maka sesuai dengan ACL yang dideklarasikan pada router alamat IP yang akan diproses adalah :

$$2^w = x$$

W = 3 (Jumlah nilai "0" biner dalam 1 Byte-octet)
X = Nilai Kelipatan yang diproses ACL
Jadi :

$$2^3 = 8$$

Maka dapat disimpulakan bahwa angka alamat IP yang dapat diproses oleh ACL adalah angka kelipatan 8 (delapan) pada octet Byte ke 4 alamat IP Sumber dengan jangkauan alamat IP dari 172.16.0.1 sampai dengan 172.16.255.254.

4. Studi Kasus ke 4 (Keempat)

Router(config)# access-list 101 deny tcp 172.16.6.0 0.0.255.240 host 10.0.0.2 eq ftp

Analisa dari wildcard yang digunakan yaitu 0.0.255.240 adalah :

Yang menjadi fokus perhatian pada wildcard yang dipergunakan yaitu terletak pada Byte ke 3 dan Byte ke 4 karena pada Byte ke 3 dan Byte ke 4 tersebut angka yang ada adalah 255.248, sedangkan angka bineri Byte pertama dan bineri Byte kedua adalah "0" (null). Pada angka Byte ke 3 (tiga) bernilai 255 jadi pada Byte ke 3 ini nilai bineri 8 bit nernilai "1" (satu) semua. Dan angka Byte ke 4 tidak bernilai 255 tetapi bernilai 248, berarti pada Byte bineri ke 4 dalam 8 bit angkanya tidak sama angkanya yaitu "1" (satu) semua dan jika dikonversikan ke dalam angka bineri adalah 8 bit-nya 11110000 yaitu terdiri angka "1" (satu) sebanyak 4 bit dan angka "0" (nul) sebanyak 4 bit.

Tabel XIV

Penjelasan Kasus 4

WILDCARD MASK : 0.0.0.248			
Angka Desimal Byte 1	0	Angka Binery Byte 1	00000000
Angka Desimal Byte 2	0	Angka Binery Byte 2	00000000
Angka Desimal Byte 3	255	Angka Binery Byte 3	11111111
Angka Desimal Byte 4	240	Angka Binery Byte 4	11110000

Dan hasil alamat sumber dari alamat IP yang deklarasikan pada wildcard tersebut diatas dalam ACL, adalah :

Tabel XV

Hasil Penerapan Wildcard Kasus 4

Alamat IP	Wildcard dalam Biner	Keterangan
172.16.0.1 sampai dengan 172.16.0.15	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.0.16	00000000.00000000. 00000000.11111000	Ditoal ke ftp server
172.16.0.17 sampai dengan 172.16.0.31	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.0.32	00000000.00000000. 00000000.11111000	Ditoal ke ftp server
172.16.0.33 sampai dengan 172.16.0.47	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.0.48	00000000.00000000. 00000000.11111000	Ditolak ke ftp server
172.16.0.49 sampai dengan 172.16.0.63	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
Dan Seterusnya		

Di dalam tabel diatas baris pertama alamat IP 172.16.0.1 sampai dengan 172.16.0.15 tidak akan diproses. Hal ini dikarenakan di dalam ACL mendeklarasikan alamat sumber yang menjadi acuan adalah 172.16.6.0 dengan Wildcard mask 0.0.255.240. Yang menjadi fokus dalam alamat IP sumber dan wildcard yang akan dibahas terletak pada Byte ke 3 (tiga) dan Byte ke 4 (empat), alamat IP yang menjadi alamat sumber pada Byte ke 3 dan Byte ke 4 adalah 6.0 sedangkan Wildcard mask yang digunakan pada Byte ke 3 dan Byte ke 4 adalah 255.240. Prinsip dalam binery wildcard adalah jika sebuah oktet Byte alamat IP sumber bertemu dengan nilai "1" (satu) pada bineri octet Byte wildcard maka nilai oktet Byte alamat IP sumber tersebut akan diabaikan atau tidak akan diproses. Maka dapat dipastikan bahwa nilai alamat IP sumber pada Byte ke 3 akan diabaikan atau tidak akan diproses dikarenakan alamat IP sumber pada Byte ini bertemu dengan wildcard binery octet Byte ke 3 bernilai "1" (satu) semua atau dalam desimal bernilai 255.

Selanjutnya alamat IP sumber octet Byte ke 4 bertemu dengan Wildcard mask pada octet Byte ke 4 bernilai tidak full yaitu, 240. Nilai octet Byte ke 4 wildcard ini jika dikonversikan ke dalam binery adalah 11110000, angka hasil konversi tersebut terdiri dari angka "1" (satu) sebanyak 4 bit dan angka "0" (null) sebanyak 4 bit. Maka sesuai dengan ACL yang dideklarasikan pada router alamat IP yang akan diproses adalah :

$$2^w = x$$

W = 4 (Jumlah nilai "0" biner dalam 1 Byte-octet)
X = Nilai Kelipatan yang diproses ACL
Jadi :

$$2^4 = 16$$

Maka dapat disimpulakan bahwa angka alamat IP yang dapat diproses oleh ACL adalah angka kelipatan 16 (delapan) pada octet Byte ke 4 alamat IP Sumber dengan jangkauan alamat IP dari 172.16.0.1 sampai dengan 172.16.255.254.

5. Studi Kasus ke 5 (kelima)

Router(config)# access-list 101 deny tcp 172.16.6.0 0.0.248.255 host 10.0.0.2 eq ftp

Analisa dari wildcard yang digunakan yaitu 0.0.255.240 adalah :

Yang menjadi fokus perhatian pada wildcard yang dipergunakan yaitu terletak pada Byte ke 3 dan Byte ke 4 karena pada Byte ke 3 dan Byte ke 4 tersebut angka yang ada adalah 248.255, sedangkan angka bineri Byte pertama dan bineri Byte kedua adalah "0" (null). Pada angka Byte ke 3 (tiga) bernilai 248 jadi pada Byte ke 3 jika dikoneversikan kedalam bineri 8 bit bernilai "11111000", yaitu terdiri angka "1" (satu) sebanyak 5 bit dan angka "0" (nul) sebanyak 3 bit. Dan angka Byte ke 4 bernilai 255 dalam konversi 8 bit angkanya adalah "1" (satu) semua.

Tabel XVI

Penjelasan kasus 5

WILDCARD MASK : 0.0.0.248			
Angka Desimal Byte 1	0	Angka Binery Byte 1	00000000
Angka Desimal Byte 2	0	Angka Binery Byte 2	00000000
Angka Desimal Byte 3	248	Angka Binery Byte 3	11111000
Angka Desimal Byte 4	255	Angka Binery Byte 4	11111111

Dan hasil alamat sumber dari alamat IP yang deklarasikan pada wildcard tersebut diatas dalam ACL, adalah :

Tabel XVII

Hasil penerapan wildcard kasus 5

Alamat IP	Wildcard dalam Biner	Keterangan
172.16.0.1 sampai dengan 172.16.7.255	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.8.0 sampai dengan 172.16.8.255	00000000.00000000. 00000000.11111000	Ditoal ke ftp server
172.16.9.0 sampai dengan 172.16.15.255	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.16.0 sampai dengan 172.16.16.255	00000000.00000000. 00000000.11111000	Ditoal ke ftp server
172.16.17.0 sampai dengan 172.16.23.255	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.24.0 sampai dengan 172.16.24.255	00000000.00000000. 00000000.11111000	Ditolak ke ftp server
172.16.25.0 sampai dengan 172.16.31.255	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
Dan Seterusnya		

Di dalam tabel diatas baris pertama alamat IP 172.16.0.1 sampai dengan 172.16.7.255 tidak akan diproses. Hal ini dikarenakan di dalam ACL mendeklarasikan alamat sumber yang menjadi acuan adalah 172.16.6.0 dengan Wildcard mask 0.0.248.255. Yang menjadi fokus dalam alamat IP sumber dan wildcard yang akan dibahas terletak pada Byte ke 3 (tiga) dan Byte ke 4 (empat), alamat IP yang menjadi alamat sumber pada Byte ke 3 dan Byte ke 4 adalah 6.0 sedangkan Wildcard mask yang digunakan pada Byte ke 3 dan Byte ke 4 adalah 248.255.

Selanjutnya alamat IP sumber octet Byte ke 3 bertemu dengan Wildcard mask pada octet Byte ke 3 bernilai tidak full yaitu, 248. Nilai octet Byte ke 4 wildcard ini jika dikonversikan ke dalam binery adalah 11111000, angka hasil konversi tersebut terdiri dari angka "1" (satu) sebanyak 5 bit dan angka "0" (null) sebanyak 3 bit. Maka sesuai dengan ACL

yang dideklarasikan pada router alamat IP yang akan diproses adalah :

$$2^W = x$$

W = 3 (Jumlah nilai "0" biner dalam 1 Byte-octet)
X = Nilai Kelipatan yang diproses ACL
Jadi :

$$2^3 = 8$$

Selanjutnya pada Byte ke 4 pada alamat IP sumber dan wildcard, prinsip dalam binery wildcard adalah jika sebuah oktet Byte alamat IP sumber bertemu dengan nilai "1" (satu) pada bineri octet Byte wildcard maka nilai oktet Byte alamat IP sumber tersebut akan diabaikan atau tidak akan diproses. Maka dapat dipastikan bahwa nilai alamat IP sumber pada Byte ke 4 akan diabaikan atau tidak akan diproses dikarenakan alamat IP sumber pada Byte ini bertemu dengan wildcard binery octet Byte ke 4 bernilai "1" (satu) semua atau dalam desimal bernilai 255.

Maka dapat disimpulakan bahwa angka alamat IP yang dapat diproses oleh ACL adalah angka kelipatan 8 (delapan) pada octet Byte ke 3 alamat IP Sumber dengan jangkauan alamat IP dari 172.16.0.1 sampai dengan 172.16.255.254.

6. Studi Kasus ke 6 (Keenam)

Router(config)# access-list 101 deny tcp 172.16.6.0 0.0.240.255 host 10.0.0.2 eq ftp

Analisa dari wildcard yang digunakan yaitu 0.0.255.240 adalah :

Yang menjadi fokus perhatian pada wildcard yang dipergunakan yaitu terletak pada Byte ke 3 dan Byte ke 4 karena pada Byte ke 3 dan Byte ke 4 tersebut angka yang ada adalah 240.255, sedangkan angka bineri Byte pertama dan bineri Byte kedua adalah "0" (null). Pada angka Byte ke 3 (tiga) bernilai 240 jadi pada Byte ke 3 jika dikoneversikan kedalam bineri 8 bit bernilai "11110000", yaitu terdiri angka "1" (satu) sebanyak 4 bit dan angka "0" (nul) sebanyak 4 bit. Dan angka Byte ke 4 bernilai 255 dalam konversi 8 bit angkanya adalah "1" (satu) semua.

Tabel XVIII

Penjelasan Kasus 6

WILDCARD MASK : 0.0.0.248			
Angka Desimal Byte 1	0	Angka Binery Byte 1	00000000
Angka Desimal Byte 2	0	Angka Binery Byte 2	00000000
Angka Desimal Byte 3	240	Angka Binery Byte 3	11110000
Angka Desimal Byte 4	255	Angka Binery Byte 4	11111111

Dan hasil alamat sumber dari alamat IP yang deklarasikan pada wildcard tersebut diatas dalam ACL, adalah :

Tabel XIX

Hasil Penerapan Wildcard Kasus 6

Alamat IP	Wildcard dalam Biner	Keterangan
172.16.0.1 sampai dengan 172.16.15.255	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.16.0 sampai dengan 172.16.16.255	00000000.00000000. 00000000.11111000	Ditoal ke ftp server
172.16.17.0 sampai dengan 172.16.31.255	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.32.0 sampai dengan 172.16.32.255	00000000.00000000. 00000000.11111000	Ditoal ke ftp server
172.16.33.0 sampai dengan 172.16.47.255	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.48.0 sampai dengan 172.16.48.255	00000000.00000000. 00000000.11111000	Ditolak ke ftp server
172.16.49.0 sampai dengan 172.16.63.255	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
Dan Seterusnya		

Di dalam tabel diatas baris pertama alamat IP 172.16.0.1 sampai dengan 172.16.15.255 tidak akan diproses. Hal ini dikarenakan di dalam ACL mendeklarasikan alamat sumber yang menjadi acuan adalah 172.16.6.0 dengan Wildcard mask 0.0.240.255. Yang menjadi fokus dalam alamat IP sumber dan wildcard yang akan dibahas terletak pada Byte ke 3 (tiga) dan Byte ke 4 (empat), alamat IP yang menjadi alamat sumber pada Byte ke 3 dan Byte ke 4 adalah 6.0 sedangkan Wildcard mask yang digunakan pada Byte ke 3 dan Byte ke 4 adalah 240.255.

Selanjutnya alamat IP sumber octet Byte ke 3 bertemu dengan Wildcard mask pada octet Byte ke 3 bernilai tidak full yaitu, 240. Nilai octet Byte ke 3 wildcard ini jika dikonversikan ke dalam binery adalah 11110000, angka hasil konversi tersebut terdiri dari angka "1" (satu) sebanyak 4 bit dan angka "0" (null) sebanyak 4 bit. Maka sesuai dengan ACL yang dideklarasikan pada router alamat IP yang akan diproses adalah :

$$2^W = x$$

W = 4 (Jumlah nilai "0" biner dalam 1 Byte-octet)
X = Nilai Kelipatan yang diproses ACL
Jadi :

$$2^4 = 16$$

Selanjutnya pada Byte ke 4 pada alamat IP sumber dan wildcard, prinsip dalam binery wildcard adalah jika sebuah oktet Byte alamat IP sumber bertemu dengan nilai "1" (satu) pada bineri octet Byte wildcard maka nilai oktet Byte alamat IP sumber tersebut akan diabaikan atau tidak akan diproses. Maka dapat dipastikan bahwa nilai alamat IP sumber pada Byte ke 4 akan diabaikan atau tidak akan diproses dikarenakan alamat IP sumber pada Byte ini bertemu dengan wildcard binery octet Byte ke 4 bernilai "1" (satu) semua atau dalam desimal bernilai 255.

Maka dapat disimpulakan bahwa angka alamat IP yang dapat diproses oleh ACL adalah angka kelipatan 16 (enam belas) pada octet Byte ke 3 alamat IP Sumber dengan jangkauan alamat IP dari 172.16.0.1 sampai dengan 172.16.255.254.

7. Studi Kasus ke 7 (Ketujuh)

Router(config)# access-list 101 deny tcp 172.16.6.0 0.0.248.248 host 10.0.0.2 eq ftp

Analisa dari wildcard yang digunakan yaitu 0.0.248.248 adalah: Yang menjadi fokus perhatian pada wildcard yang dipergunakan yaitu terletak pada Byte ke 3 dan Byte ke 4 karena pada Byte ke 3 dan Byte ke 4 tersebut angka yang ada adalah 248.248, sedangkan angka bineri Byte pertama dan bineri Byte kedua adalah "0" (null). Pada angka Byte ke 3 (tiga) dan Byte ke 4 bernilai 248 jadi jika dikoneversikan kedalam bineri 8 bit Byte ke 3 dan Byte ke 4 bernilai

"11111000", yaitu terdiri angka "1" (satu) sebanyak 5 bit dan angka "0" (nul) sebanyak 3 bit.

Tabel XX

Penjelasan Kasus 7

WILDCARD MASK : 0.0.0.248			
Angka Desimal Byte 1	0	Angka Binery Byte 1	00000000
Angka Desimal Byte 2	0	Angka Binery Byte 2	00000000
Angka Desimal Byte 3	248	Angka Binery Byte 3	11111000
Angka Desimal Byte 4	248	Angka Binery Byte 4	11111000

Dan hasil alamat sumber dari alamat IP yang deklarasikan pada wildcard tersebut diatas dalam ACL, adalah :

Tabel XXI

Hasil Penerapan Wildcard Kasus 7

Alamat IP	Wildcard dalam Biner	Keterangan
172.16.0.1 sampai dengan 172.16.0.7	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.0.8	00000000.00000000. 00000000.11111000	Ditoal ke ftp server
172.16.0.9 sampai dengan 172.16.0.15	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.0.16	00000000.00000000. 00000000.11111000	Ditoal ke ftp server
172.16.0.17 sampai dengan 172.16.0.23	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.0.24	00000000.00000000. 00000000.11111000	Ditolak ke ftp server
172.16.0.25 sampai dengan 172.16.0.31	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
Dan Seterusnya		

Di dalam tabel diatas baris pertama alamat IP 172.16.0.1 sampai dengan 172.16.0.7 tidak akan diproses. Hal ini dikarenakan di dalam ACL mendeklarasikan alamat sumber yang menjadi acuan adalah 172.16.0.0 dengan Wildcard mask 0.0.248.248. Yang menjadi fokus dalam alamat IP sumber dan wildcard yang akan dibahas terletak pada Byte ke 3 (tiga) dan Byte ke 4 (empat), alamat IP yang menjadi alamat sumber pada Byte ke 3 dan Byte ke 4 adalah 0.0 sedangkan Wildcard mask yang digunakan pada Byte ke 3 dan Byte ke 4 adalah 248.248.

Selanjutnya alamat IP sumber octet Byte ke 3 bertemu dengan Wildcard mask pada octet Byte ke 3 bernilai tidak full yaitu, 248. Nilai octet Byte ke 3 wildcard ini jika dikonversikan ke dalam binery adalah 11111000, angka hasil konversi tersebut terdiri dari angka "1" (satu) sebanyak 5 bit dan angka "0" (null) sebanyak 3 bit. Maka sesuai dengan ACL yang dideklarasikan pada router alamat IP yang akan diproses adalah :

$$2^w = x$$

W = 3 (Jumlah nilai "0" biner dalam 1 Byte-octet)
X = Nilai Kelipatan yang diproses ACL
Jadi :

$$2^3 = 8$$

Selanjutnya alamat IP sumber octet Byte ke 4 bertemu dengan Wildcard mask pada octet Byte ke 4 juga bernilai tidak full yaitu, 248. Nilai octet Byte ke 4 wildcard ini jika dikonversikan ke dalam binery adalah 11111000, angka hasil konversi tersebut terdiri dari angka "1" (satu) sebanyak 5 bit dan angka "0" (null) sebanyak 3 bit. Maka sesuai dengan ACL yang dideklarasikan pada router alamat IP yang akan diproses adalah :

$$2^w = x$$

W = 3 (Jumlah nilai "0" biner dalam 1 Byte-octet)
X = Nilai Kelipatan yang diproses ACL
Jadi :

$$2^3 = 8$$

Maka dapat disimpulakan bahwa angka alamat IP yang dapat diproses oleh ACL adalah angka kelipatan 8 (delapan) pada octet Byte ke 3 dan octet Byte ke 4 alamat IP Sumber dengan jangkauan alamat IP dari 172.16.0.1 sampai dengan 172.16.255.254.

8. Studi Kasus ke 8 (Kedelapan)

Router(config)# access-list 101 deny tcp 172.16.0.0 0.0.240.240 host 10.0.0.2 eq ftp

Analisa dari wildcard yang digunakan yaitu 0.0.240.240 adalah :

Yang menjadi fokus perhatian pada wildcard yang dipergunakan yaitu terletak pada Byte ke 3 dan Byte ke 4 karena pada Byte ke 3 dan Byte ke 4 tersebut angka yang ada adalah 240.240, sedangkan angka bineri Byte pertama dan bineri Byte kedua adalah "0" (null). Pada angka Byte ke 3 (tiga) dan Byte ke 4 bernilai 240 jadi jika dikoneversikan kedalam bineri 8 bit Byte ke 3 dan Byte ke 4 bernilai "11110000", yaitu terdiri angka "1" (satu) sebanyak 4 bit dan angka "0" (nul) sebanyak 4 bit.

Tabel XXII

Penjelasan kasus 8

WILDCARD MASK : 0.0.0.248			
Angka Desimal Byte 1	0	Angka Binery Byte 1	00000000
Angka Desimal Byte 2	0	Angka Binery Byte 2	00000000
Angka Desimal Byte 3	240	Angka Binery Byte 3	11110000
Angka Desimal Byte 4	240	Angka Binery Byte 4	11110000

Dan hasil alamat sumber dari alamat IP yang deklarasikan pada wildcard tersebut diatas dalam ACL, adalah :

Tabel XXIII

Hasil penerapan wildcard kasus 8

Alamat IP	Wildcard dalam Biner	Keterangan
172.16.0.1 sampai dengan 172.16.0.15	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.0.16	00000000.00000000. 00000000.11111000	Ditoal ke ftp server
172.16.0.17 sampai dengan 172.16.0.31	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.0.32	00000000.00000000. 00000000.11111000	Ditoal ke ftp server
172.16.0.33 sampai dengan 172.16.0.47	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
172.16.0.48	00000000.00000000. 00000000.11111000	Ditolak ke ftp server
172.16.0.49 sampai dengan 172.16.0.63	00000000.00000000. 00000000.11111000	Diizinkan ke ftp server
Dan Seterusnya		

Di dalam tabel diatas baris pertama alamat IP 172.16.0.1 sampai dengan 172.16.0.15 tidak akan diproses. Hal ini

dikarenakan di dalam ACL mendeklarasikan alamat sumber yang menjadi acuan adalah 172.16.0.0 dengan Wildcard mask 0.0.240.240. Yang menjadi fokus dalam alamat IP sumber dan wildcard yang akan dibahas terletak pada Byte ke 3 (tiga) dan Byte ke 4 (empat), alamat IP yang menjadi alamat sumber pada Byte ke 3 dan Byte ke 4 adalah 0.0 sedangkan Wildcard mask yang digunakan pada Byte ke 3 dan Byte ke 4 adalah 240.240.

Selanjutnya alamat IP sumber octet Byte ke 3 bertemu dengan Wildcard mask pada octet Byte ke 3 bernilai tidak full yaitu, 240. Nilai octet Byte ke 3 wildcard ini jika dikonversikan ke dalam binery adalah 11110000, angka hasil konversi tersebut terdiri dari angka "1" (satu) sebanyak 4 bit dan angka "0" (null) sebanyak 4 bit. Maka sesuai dengan ACL yang dideklarasikan pada router alamat IP yang akan diproses adalah :

$$2^w = x$$

W = 4 (Jumlah nilai "0" biner dalam 1 Byte-octet)
X = Nilai Kelipatan yang diproses ACL
Jadi :

$$2^3 = 16$$

Selanjutnya alamat IP sumber octet Byte ke 4 bertemu dengan Wildcard mask pada octet Byte ke 4 juga bernilai tidak full yaitu, 240. Nilai octet Byte ke 4 wildcard ini jika dikonversikan ke dalam binery adalah 11110000, angka hasil konversi tersebut terdiri dari angka "1" (satu) sebanyak 4 bit dan angka "0" (null) sebanyak 4 bit. Maka sesuai dengan ACL yang dideklarasikan pada router alamat IP yang akan diproses adalah :

$$2^w = x$$

W = 4 (Jumlah nilai "0" biner dalam 1 Byte-octet)
X = Nilai Kelipatan yang diproses ACL
Jadi :

$$2^4 = 16$$

Maka dapat disimpulakan bahwa angka alamat IP yang dapat diproses oleh ACL adalah angka kelipatan 16 (enam belas) pada octet Byte ke 3 dan octet Byte ke 4 alamat IP sumber dengan jangkauan alamat IP dari 172.16.0.1 sampai dengan 172.16.255.254.

V. KESIMPULAN

Berdasarkan hasil penelitian maka dapat disimpulkan sebagai berikut :

1. Pada studi kasus 1 (pertama) dan ke 2 (dua) alamat IP sumber 172.16.6.0 dengan wildcard 0.0.0.252 dan 0.0.0.248 terletak pada Byte ke 4 (empat). Dapat disimpulkan bahwa, alamat IP sumber yang akan diproses adalah Byte 1 Byte 2 dan Byte 3 alamat IP sumber 172.16.6 karena Byte-Byte alamat IP sumber tersebut dipandankan dengan nilai "0" (null) wildcard, sedangkan alamat IP sumber Byte ke 4 dipadankan dengan nilai kombinasi antara nilai "0" (null) dan nilai "1" (satu) dalam satu Byte octet wildcardnya. Dan untuk mencari angka alamat IP sumber pada Byte ke 4 ini akan mengikuti jumlah angka "0" (null) bineri octet Byte ke 4 wildcardnya. Dan untuk menghitung angka Byte ke 4 alamat IP sumber berdasarkan angka "0" (null) dengan menggunakan rumus :

   $$2^w = x$$

   Keterangan :
   W = Jumlah "0" (null) dalam 1 Byte Wildcard Fulless
   X = Kelipatan Host ID yang akan diproses

2. Pada studi kasus 3 (tiga) dan ke 4 (empat) alamat IP sumber 172.16.0.0 dengan wildcard 0.0.255.248 dan 0.0.255.240 terletak pada Byte ke 3 (tiga) dan ke 4 (empat). Dapat disimpulkan bahwa, alamat IP sumber yang akan diproses adalah Byte 1 dan Byte 2 alamat IP sumber 172.16. karena Byte-Byte alamat IP sumber tersebut dipandankan dengan nilai "0" (null) wildcard, sedangkan alamat IP sumber Byte ke 3 dipandakan dengan angka 255 pada wildcard Byte ke 3 maka angka alamat IP sumber pada Byte ke 3 ini akan diacuhkan (artinya bahwa angka yang berada pada Byte ke 3 alamat IP sumber berapapun yaitu 1 sampai dengan 255 tidak akan diproses atau diacuhkan).
   Dan Byte ke 4 dipadankan dengan nilai kombinasi antara angka "0" (null) dan angka "1" (satu) dalam satu Byte octet wildcardnya. Dan untuk mencari angka alamat IP sumber pada Byte ke 4 ini akan mengikuti jumlah angka "0" (null) bineri octet Byte ke 4 wildcardnya. Dan untuk menghitung angka Byte ke 4 alamat IP sumber berdasarkan angka "0" (null) dengan menggunakan rumus :

   $$2^w = x$$

   Keterangan :
   W = Jumlah "0" (null) dalam 1 Byte Wildcard Fulless
   X = Kelipatan Host ID yang akan diproses

3. Pada studi kasus 5 (tiga) dan ke 6 (empat) alamat IP sumber 172.16.0.0 dengan wildcard 0.0.248.255 dan 0.0.240.255 terletak pada Byte ke 3 (tiga) dan ke 4 (empat). Dapat disimpulkan bahwa, alamat IP sumber yang akan diproses adalah Byte 1 dan Byte 2 alamat IP sumber 172.16. karena Byte-Byte alamat IP sumber tersebut dipandankan dengan nilai "0" (null) wildcard.
   Byte ke 3 dipadankan dengan nilai kombinasi antara angka "0" (null) dan angka "1" (satu) dalam satu Byte octet wildcardnya. Dan untuk mencari angka alamat IP sumber pada Byte ke 3 ini akan mengikuti jumlah angka "0" (null) bineri octet Byte ke 3 wildcardnya. Dan untuk menghitung angka Byte ke 3 alamat IP sumber berdasarkan angka "0" (null) dengan menggunakan rumus :

   $$2^w = x$$

   Keterangan :
   W = Jumlah "0" (null) dalam 1 Byte Wildcard Fulless
   X = Kelipatan Host ID yang akan diproses

   Sedangkan alamat IP sumber Byte ke 4 dipandakan dengan angka 255 pada wildcard Byte ke 4 maka

angka alamat IP sumber pada Byte ke 4 ini akan diacuhkan (artinya bahwa angka yang berada pada Byte ke 4 alamat IP sumber berapapun yaitu 1 sampai dengan 255 tidak akan diproses atau diacuhkan).

4. Pada studi kasus 7 (tiga) dan ke 8 (empat) alamat IP sumber 172.16.0.0 dengan wildcard 0.0.248.248 dan 0.0.240.240 terletak pada Byte ke 3 (tiga) dan ke 4 (empat). Dapat disimpulkan bahwa, alamat IP sumber yang akan diproses adalah Byte 1 dan Byte 2 alamat IP sumber 172.16. karena Byte-Byte alamat IP sumber tersebut dipandankan dengan nilai "0" (null) wildcard. Byte ke 3 alamat IP sumber dipadankan dengan nilai kombinasi antara angka "0" (null) dan angka "1" (satu) dalam satu Byte octet wildcardnya. Dan untuk mencari angka alamat IP sumber pada Byte ke 3 yang nantinya akan diproses oleh ACL ini akan mengikuti jumlah angka "0" (null) bineri octet Byte ke 3 wildcardnya. Dan untuk menghitung angka Byte ke 3 alamat IP sumber berdasarkan angka "0" (null) dengan menggunakan rumus :

$$2^W = x$$

Keterangan :
W = Jumlah "0" (null) dalam 1 Byte Wildcard Fulless
X = Kelipatan Host ID yang akan diproses

Dan Byte ke 4 alamat IP sumber juga dipadankan dengan nilai kombinasi antara angka "0" (null) dan angka "1" (satu) dalam satu Byte octet wildcardnya. Sehingga untuk mencari angka alamat IP sumber pada Byte ke 4 yang nantinya akan diproses oleh ACL ini akan mengikuti jumlah angka "0" (null) bineri octet Byte ke 3 wildcardnya. Dan untuk menghitung angka Byte ke 3 alamat IP sumber berdasarkan angka "0" (null) dengan menggunakan rumus :

$$2^W = x$$

Keterangan :
W = Jumlah "0" (null) dalam 1 Byte Wildcard Fulless
X = Kelipatan Host ID yang akan diproses

REFERENSI

[1] A Jesin. 2014. Packet Tracer Network Simulator. Packt Publishing : Birmingham-UK.
[2] Hartpence, Bruce. 2011. Packet Guide to Core Network Protocols. O,Reilly Media : California-USA.
[3] Hikmaturokhman, Alfin, etc. 2010. Analisa Perancangan dan Implementasi Firewall dan Traffic Filtering menggunakan Cisco Router. Seminar Nasional Informatika 2010 (senmasIF 2010) UPN "Veteran" Yogyakarta, 22 Mei 2010. ISSN : 1979-2328.
[4] Komar, Brian etc. 2003. Firewall for Dummies, 2nd Edition. Wiley Publishing : New York-USA.
[5] Moraes, Alexandre M.S.P. 2011. Cisco Firewall. Cisco Press : Indianapolis-USA.
[6] Networking, ProCurve. 2005. Configuration Guide 5991-2119. HP Innovation
[7] Paquet, Catherine. 2013. Implementing Cisco IOS Network Security (IINS 640-554) Foundation Learning Guide (2nd Edition). Cisco Press : Indianapolis-USA.
[8] Simamora, S.N.M.P, et all. 2011. Metode Access Control List sebagai Solusi Alternatif Seleksi Permintaan Layanan Data pada Koneksi Internet. Jurnal Teknologi Informasi Politeknik Telkom Vol.1, No.1, Mei 2011
[9] Santos, Omar dan Stuppi, John. 2015. CCNA Security 210-260 Official Cert Guide. Cisco Press : Indianapolis-USA.
[10] Syafina, Dea Chadiza. 2015. Indonesia Urutan Kedua Terbesar Negara Asal "Cyber Crime" di Dunia http://nasional.kompas.com/read/2015/05/12/06551741/Indonesia.Urutan.Kedua.Terbesar.Negara.Asal.Cyber.Crime.di.Dunia.
[11] Tittel, Ed. 2002. Schaum's Outline : Computer Networking (Jaringan Komputer). Jakarta : Penerbit Erlangga.
[12] Zwicky, Elizabeth D, etc. 200. Building Internet Firewalls. ISSBN : 1-56592-871-7.