# HALAMAN JUDUL

**DETEKSI SERANGAN PADA**

**ARP (Address Resolution Protocol)**

**PROYEK TUGAS AKHIR**

Diajukan untuk memenuhi salah satu syarat

Mencapai derajat Sarjana S-1 Program Studi Teknik Informatika



Disusun oleh:

Ardika Rommy Sanjaya

5130411060

**PROGRAM STUDI TEKNIK INFORMATIKA**

**FAKULTAS BISNIS DAN TEKNOLOGI INFORMASI**

**UNIVERSITAS TEKNOLOGI YOGYAKARTA**

**2017**

# HALAMANPENGESAHAN

**DETEKSI SERANGAN PADA**

**ARP (Address Resolution Protocol)**

**PROYEK TUGAS AKHIR**

Disusun oleh

Ardika Rommy Sanjaya

5130411060

TelahdipertanggungjawabkandidalamSidang Proyek Tugas Akhir  
padatanggal, (PelaksanaanSidang)

TimPenguji:

(tandatangan ketua)  
Ketua

(tandatangan anggota)

Anggota

(tandatangan anggota)

Anggota

Tugas akhir ini telah diterima sebagai salah satu syarat untuk mencapai derajat Sarjana S-1 Program Studi Teknik Informatika

Yogyakarta ,…………….

Ketua Program Studi Teknik Informatika/ Sistem Informasi

Fakultas Bisnis dan Teknologi Informasi, Universitas Teknologi Yogyakarta

Nama Kaprodi

# LEMBARPERNYATAAN

Sayayangbertandatangandibawahini:

N a m a : Ardika Rommy Sanjaya

NPM : ………………………………...

Program Studi : Teknik Informatikd

Menyatakan bahwa Proyek Tugas Akhir yang berjudul:

Deteksi Serangan Pada ARP (Address Resolution Protocol)

merupakan karya ilmiah asli saya dan belum pernah dipublikasikan oleh orang lain, kecuali yang tertulis sebagai acuan dalam naskah ini dan disebutkan dalam daftar pustaka. Apabila dikemudian hari, karya saya disinyalir bukan merupakan karya asli saya, maka saya bersediamenerima konsekuensi apa yang diberikan Program Studi Teknik Informatika Fakultas Bisnis dan Teknologi Informasi Universitas Teknologi Yogyakarta kepada saya.

Demikian surat pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Yogyakarta

Pada tanggal :   
Yang menyatakan

Ardika Rommy Sanjaya

# ABSTRAK

# ABSTRACT

# KATA PENGANTAR

PujisyukurdipanjatkanataskehadiratAllah SWT,karenadenganlimpahankarunia-NyapenulisdapatmenyelesaikanProyek Tugas Akhir denganjudulDeteksi Serangan Pada ARP (Address Resulution Protocol).

Penyusunan Proyek Tugas AkhirdiajukansebagaisalahsatusyaratuntukmemperolehgelarsarjanapadaProgram StudiTeknikInformatikaFakultasTeknologiInformasiUniversitas Teknologi Yogyakarta.

Kerja Praktikinidapatdiselesaikantidaklepasdarisegalabantuan,bimbingan,dorongandandoadariberbagaipihak,yangpadakesempataninipenulisinginmenyampaikanucapanterimakasihkepada:

1. Kepada Rektor Universitas
2. Kepada Dekan Fakultas
3. Kepada Ketua Program Studi
4. Kepada Dosen Pembimbing Tugas Akhir

Akhirkata,penulismenyadaribahwasepenuhnyaakanterbatasnyapengetahuanpenyusun,sehinggatidakmenutupkemungkinanjikaadakesalahansertakekurangandalampenyusunanKerja Praktik,untukitusumbangsarandaripembacasangatdiharapkansebagaibahanpelajaranberhargadimasayangakandatang.

Yogyakarta, Agustus 2016

Penulis

# DAFTAR ISI

[HALAMAN JUDUL i](#_Toc484945390)

[HALAMANPENGESAHAN ii](#_Toc484945391)

[LEMBARPERNYATAAN iii](#_Toc484945392)

[ABSTRAK iv](#_Toc484945393)

[ABSTRACT v](#_Toc484945394)

[KATA PENGANTAR vi](#_Toc484945395)

[DAFTAR ISI vii](#_Toc484945396)

[DAFTAR GAMBAR x](#_Toc484945397)

[DAFTAR TABEL xi](#_Toc484945398)

[BAB I PENDAHULUAN 1](#_Toc484945399)

[1.1 Latar Belakang 1](#_Toc484945400)

[1.2 Rumusan Masalah 2](#_Toc484945401)

[1.3 Batasan Masalah 2](#_Toc484945402)

[1.4 Tujuan Penelitian 3](#_Toc484945403)

[1.5 ManfaatPenelitian 3](#_Toc484945404)

[1.6 Sistematika Penulisan 3](#_Toc484945405)

[BAB II KAJIAN PUSTAKA DAN TEORI 5](#_Toc484945406)

[2.1 Kajian Hasil Penelitian 5](#_Toc484945407)

[2.2 Dasar Teori 7](#_Toc484945408)

[2.2.1 Intrusion Detection System (IDS) 7](#_Toc484945409)

[2.2.2 Protokol 7](#_Toc484945410)

[2.2.3 ARP (Address Resolution Protocol) 9](#_Toc484945411)

[2.2.4 Ethernet 10](#_Toc484945412)

[2.2.5 Ethernet II 10](#_Toc484945413)

[2.2.6 IP Address 11](#_Toc484945414)

[2.2.7 IPv4 (Internet Protocol Version 4) 11](#_Toc484945415)

[2.2.8 TCP (Transmission Control Protocol) 12](#_Toc484945416)

[2.2.9 Sniffing dan Spoofing 18](#_Toc484945417)

[2.2.10 Promiscuous Mode 19](#_Toc484945418)

[2.2.11 Maximum Transmission Unit (MTU) 19](#_Toc484945419)

[2.2.12 Pcap File Format 19](#_Toc484945420)

[BAB III METODE PENELITIAN 20](#_Toc484945421)

[3.1 Obyek Penelitian 20](#_Toc484945422)

[3.2 Metode Penelitian 20](#_Toc484945423)

[3.2.1 Pengumpulan Data 20](#_Toc484945424)

[3.2.2 Analisis Perancangan 21](#_Toc484945425)

[3.2.3 Pembuatan Program 21](#_Toc484945426)

[3.2.4 Implementasi dan Pengujian 21](#_Toc484945427)

[BAB IV ANALISA DAN PERANCANGAN SISTEM 22](#_Toc484945428)

[4.1 Analisa Sistem yang Berjalan 22](#_Toc484945429)

[4.2 Analisa Kebutuhan 22](#_Toc484945430)

[4.2.1 Kebutuhan Fungsional 22](#_Toc484945431)

[4.2.2 Kebutuhan Non Fungsional 23](#_Toc484945432)

[4.3 Analisa Pengembangan sistem 23](#_Toc484945433)

[4.4 Rancangan Sistem 23](#_Toc484945434)

[4.5 Rancangan Menu Dan Antar Muka 25](#_Toc484945435)

[4.6 Rancangan *Graphical User Interface (GUI)* 26](#_Toc484945436)

[4.6.1 Serangan Pada ARP 26](#_Toc484945437)

[4.6.2 Deteksi Serangan Pada ARP 28](#_Toc484945438)

[BAB V IMPLEMENTASI SISTEM 29](#_Toc484945439)

[5.1 Implementasi 29](#_Toc484945440)

[5.2 Perangkat Keras (*Hardware*) yang Digunakan 29](#_Toc484945441)

[5.3 Perangkat Lunak (*Software*) yang digunakan 29](#_Toc484945442)

[5.4 ImplementasiWEB 30](#_Toc484945443)

[5.4.1 ImplementasiHalaman User 30](#_Toc484945444)

[5.4.2 Koneksi.php 30](#_Toc484945445)

[5.4.3 TampilanHalaman Home 30](#_Toc484945446)

[BAB VI PENUTUP 32](#_Toc484945447)

[6.1 Kesimpulan 32](#_Toc484945448)

[6.2 Saran 32](#_Toc484945449)

[DAFTAR PUSTAKA 33](#_Toc484945450)

# DAFTAR GAMBAR

[Gambar 2.1. Satellite Map **Error! Bookmark not defined.**](#_Toc461058044)

[Gambar 3.1. DFD level 0 24](#_Toc461058053)

[Gambar 3.2. Struktur Menu User **Error! Bookmark not defined.**](#_Toc461058054)

[Gambar 3.3. Struktur Menu Admin 25](#_Toc461058055)

[Gambar 4.1. Script koneksi.php 29](#_Toc461058063)

[Gambar 4.2. Tampilan Home 30](#_Toc461058064)

# DAFTAR TABEL

[Tabel 2.1. NotasidalamERD **Error! Bookmark not defined.**](#_Toc461058207)

[Tabel 2.2. DFD (Data Flow Diagram) **Error! Bookmark not defined.**](#_Toc461058208)

# PENDAHULUAN

## Latar Belakang

Address Resolution Protocol (ARP) memiliki tanggung jawab untuk mencari Media Access Control (MAC) Address dari setiap komputer (host) yang akan berkomunikasi (pertukaran data) melalui jaringan Local Area Network (LAN) dengan memanfaatkan Internet Protocol (IP) Address, khususnya IP Address Version 4 yang telah didapat saat sebuah host berhasil melakukan koneksi ke jaringan. MAC Address yang telah didapatkan dari ARP akan disimpan di dalam ARP Cache/ARPTable dengan tujuan agar jaringan tidak menjadi sibuk karena penggunaan ARP secara terus-menerus ketika setiap host ingin berkomunikasi dengan host lainnya. Dalam Open System Interconnection (OSI) protokol ini sering digambarkan sebagai yang berada antara lapisan (layer) ke 2 dan 3 dimana juga dienkaptulasi oleh protokol layer 2 (Ethernet).

Protokol ini sangat sering dimanfaatkan oleh penyerang *(hacker/attacker)* untuk melakukan serangan *Man In The Middle (MITM)* dengan berbagai tujuan. Ketika *attacker* mengirimkan paket *ARP Reply* yang telah dimodifikasi sedemikian rupa dengan tujuan *host* target maka *ARP Cache* dari target akan ter-*update* sesuai dengan apa yang diinginkan oleh *attacker*. Setiap *host* yang ingin berkomunikasi dengan *host* lainnya menggunakan *MAC Address* agar setiap *frame* data dapat diteruskan ke tujuan dan diletakan di atas media transmisi dan diproses oleh *Network Interface Card (NIC)* dimana *MAC Address* tersebut tersimpan di dalam *ARP Cache* yang telah ter-*update*. Hal ini dapat menyebabkan paket yang dikirimkan tidak sampai pada *host* tujuan atau justru dapat diterima oleh *attacker*. Misalkan seseorang yang telah terkena serangan ini melakukan *login* pada suatu aplikasi di sisi *server* yang tidak menggunakan protokol yang aman (ter-enkripsi) misalkan HTTP, FTP, Telnet, dan lain sebagainya maka *username* dan *password* yang digunakan untuk *login* akan dapat dibaca oleh penyerang. Bahkan penyerang juga dapat melakukan perubahan terhadap paket yang dikirimkan dari sisi *client* maupun *server.*

Serangan menggunakan *ARP* ini dapat dideteksi dengan meng-*capture* paket *ARP Reply* yang mana jika terjadi paket tersebut dapat mengubah *Mac Address* pada *ARP Table* maka *host* yang diserang dapat mingirimkan paket *TCP* dengan *destination* pada *IPv4* paket adalah *IP Address* miliknya dan paket tersebut dikirimkan kepada *attacker*. Jika *IP Packet Routing* dari *attacker* di-aktifkan maka paket *TCP* yang tadi dikirimkan akan di *forward* secara otomatis oleh *attacker* dan dapat dipastikan bahwa itu merupakan serangan dengan menggunakan *ARP*.

## Rumusan Masalah

Berdasarkan latar belakang diatas dapat dirumuskan beberapa masalah dalam peneliatan “Deteksi Serangan Pada ARP (Address Resolution Protocol)”, yaitu:

* Bagaimana mencari kartu jaringan yang terkoneksi dengan jaringan LAN *(Local Area Network)*?
* Bagaimana setiap paket yang melewati *Network Interface Card (NIC)* dapat di-*capture*?
* Bagaimana mengolah paket-paket yang berhasil di-*capture* agar dapat dilakukan pengecekan (pembanding) terhadap *ARP Cache*?
* Bagaimanamengirimkan paket *TCP* untuk mendeteksi apakah *IP Packet Routing* milik *attacker* aktif?

## Batasan Masalah

Mengingat dengan banyaknya perkembangan masalah yang bisa ditemukan pada penelitian ini, maka perlu adanya batasan-batasan masalah yang jelas mengenai apa yang dibuat dan diselesaikan. Adapun batasan-batasan masalah pada penelitian ini, sebagai beribut:

* Mencarikartu jaringan yang dapat digunakan.
* Mencari data paket hasil *capture* yang akan menjadi *input-*an untuk proses deteksi.
* Menganalisa *input-*an berupa paket data.
* Memastikan komputer yang digunakan sedang mendapatkan serangan atau tidak.

## Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah untuk membuat sistem yang dapat melakukan pengecekan paket-paket *ARP* sehingga dapat menciptakan sebuah sistem yang dapat mendeteksi serangan yang menggunakan *ARP (ARP Spoofing)*.

## ManfaatPenelitian

Diharapkan penelitian ini dapat memberikan manfaat, diantaranya:

* Penelitian ini diharapkan dapat memberikan manfaat secara teoritis, sekurang-kurangnya dapat berguna sebagai sumbangan pemikiran bagi dunia pendidikan.
* Menambah wawasan penulis khususnya mengenai keamanan jaringan komputer.
* Sebagai referensi dalam ilmu pendidikan sehingga dapat memeperkaya dan menambah wawasan khususnya menyenai keamanan jaringan komputer.
* Sistem dapat mengurangi tingkat penyalahgunaan jaringan *LAN* baik untuk pencurian *password*, manipulasi paket data dan sebagainya.
* Penelitian ini juga diharapkan dapat bermanfaat bagi penelitian berikutnya.

## Sistematika Penulisan

Sistematika yang digunakan dalam penulisan ini adalah sebagai berikut:

1. Pendahuluan.

Menjelaskan latar belakang permasalahan yang diangkat dalam penelitian ini serta solusi yang ditawarkan oleh peneliti. Selain itu juga disertakan rumusan masalah, tujuan penelitian, dan manfaat penelitian.

1. Kajian Pustaka dan Teori.

Menjelaskan teori, konsep, metodologi, dan teknologi yang relevan terhadap objek penelitian. Dimana nantinya kajian pustaka dan teori ini akan dijadikan landasan dalam analisis dan perancangan sistem.

1. Metode Penelitian.

Berisi penjelasan tentang objek yang akan diteliti dan sekumpulan metode ataupun tatacara yang lebih terperinci mengenai tahap-tahap melakukan penelitian untuk menyelesaikan suatu masalah. Metode tersebut diantaranya metode pengumpulan data, analisis dan perancangan, pembuatan program, implementasi, dan pengujian program.

1. Analisis dan Perancangan.

Pada bab ini akan dibahas pengenai perancangan maupun analisa sistem baik berupa pembahasan, algoritma maupun *flow chart*.Analisi dan perancangan ini akan digunakan sebagai landasan bagi pembuatan/implementasi program pada bab selanjutnya.

1. Implementasi sistem.

Pada bab ini hasil dari analisis dan perancangan sistem akan diimplementasikan ke dalam program. Selain itu akan dilakukan pengujian terhadap program yang telah dibuat.

1. Penutup.

Menjelaskan kesimpulan dari hasil penelitian yang telah dilakukan serta disajikan juga beberapa saran yang mungkin akan berguna bagi peneliti selanjutnya.

Daftar Pustaka

Lampiran

# KAJIAN PUSTAKA DAN TEORI

## Kajian Hasil Penelitian

Penelitian oleh Vinay dan Rahman (2015), dengan judul *“ARP Spoof Detection System using ICMP Protocol: An Active Approach”* menggunakan teknik deteksi aktif dengan cara meng-capture paket *ARP* dan menyimpannya paket pertama ke dalam *database(IP* dan *MAC Address)*. Ketika hasil capture paket *ARP* berikutnya telah ada (telah disimpan ke *database* sebelumnya) maka paket tersebut dinyatakan aman (*IP* dan *MAC Address* sama), namun jika yang sama hanya *IP Address* yang sama maka *IP* tersebut akan digunakan untuk melakukan pengiriman paket *ICMP (Internet Control Messaege Protocol)*. Jika *IP packet routing (IP forwarding)* pada penyerang diaktifkan maka paket yang tadi dikirimkan ke penyerang akan diteruskan kembali oleh penyerang sesuai dengan *IP Address* tujuan. Dari paket tersebut dapat dilakukan pencocokan paket pada *layer* 2 dengan paket *ARP* hasil *capture* yang sebelumnya untuk memastikan apakah paket *ARP* tersebut aman atau tidak. Namun hal ini dapat diatasi oleh penyerang dengan membuat *firewall* untuk meblokir setiap paket *ICMP* yang masuk. Oleh karena itu peneliti tidak menggunakan paket *ICMP* sebuagai parameter untuk deteksi namun berbagai macam parameter lainnya yang masih mungkin dapat digunakan.

Kaur (2013) penah melakukan penelitian dengan judul *“Detection and Prevention of ARP Cache Poisoning”* untuk mendeteksi dan mengatasi serangan *ARP Spoofing (ARP Cache Poisoning)* dengan mendeteksi paket-paket yang mencurigakan dan ketika telah dipastikan ada yang melakukan serangan segera diambil tindakan dengan mengirimkan paket *ARP Request* ke *gateway* dengan tujuan untuk memperbaharui *ARP Cache*. Selain itu digunakan juga *ICMP* (*Internet Control Message Protocol*) untuk melakukan pengecekan apakah penyerang meng-aktifkan fungsi *IP Forwarding (IP Routing)* untuk meneruskan paket *IPv4* pada tujuan. Berdasarkan penelitian tersebut peneliti akan menambakan fitur untuk melakukan penyimpanan hasil *capture* paket pada format yang umum digunakan seperti pcap dan pcapng agar lebih mudah untuk dianalisis oleh peneliti lain.

Srinath dkk (2015) telah melakukan penelitian dengan judul *“Detection and Prevention of ARP Spoofing using Centralized Server”* dengan menggunakan tiga model untuk mengatasi serangan *ARP Spoofing* yaitu model perspektif komputer (*host*), perspektif *server*, dan otentikasi. Dimodel pertama setiap komputer mengirimkan informasi yang didapat setelah terhubung ke jaringan melalui *DHCP* ke *server* dan tugas *server* adalah menyimpan informasi tersebut ke *database* sekaligus melakukan pengecekan informasi. Informasi yang disimpan di *database* dapat ditampilkan dengan menggunakan diagram agar mempermudah pembacaan. Sistem yang peneliti buat hanya digunakan di sisi *client* dengan alasan kebiasaan pengguna jaringan seperti *wifi* yang selalu berpindah-pindah (tidak hanya menggunakan satu jaringan).

**Tabel 2.1.** Perbandingan Tinjauan Pustaka

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | Judul | Penulis | Metode | Hasil/Kesimpulan |
| 1 | *ARP Spoof Detection System using ICMP Protocol: An Active Approach* | Vinay K. R. dan T. R. Mahibur Rahman | *ICMP Modul* | Tiknik ini juga dapat mendeteksi *IP* dan *MAC* *Address* yang asli *(Correct Address)* selain itu teknik ini cukup simple dan effisien. |
| 2 | *Detection and Prevention of ARP Cache Poisoning* | Inderjeet Kaur | *ARP dan ICMP* | Metode ini cukup efisian untuk mendeteksi dan mengatasi *ARP Cache Poisoning*. |
| 3 | *Detection and Prevention of ARP Spoofing using Centralized Server* | D. Srinath, S. Panimalar, A. Jerrin Simla dan J. Deepa | *Centralized Server* | Metode ini cukup baik digunakan untuk mengatasi *ARP Spoofing* selain itu dapat pula digunakan untuk mengatasi *IP Spoofing*. |

Seperti terlihat pada table 2.1. perbedaan dari ketiga referensi dengan judul yang diangkat oleh penulis terletak pada metode yang digunakan, masing-masing metode memiliki keunggulannya masing-masing. Peneliti akan menggunakan beberapa keunggulan dari masing-masing referensi dan menambahkan beberapa metode untuk meingkatkan kemampuan dari sistem pendeteksi serangan pada penelitian ini.

## Dasar Teori

### Intrusion Detection System (IDS)

Intrusion Detection System merupakan sebuah sistem yang dapat digunakan untuk melakukan deteksi terhadap aktivitas yang mencurigakan dalam sebuah sistem atau jaringan yang dapat menggangu konfidensialitas, integritas dan ketersediaan data. IDS dapat melakukan inspeksi terhadap lalu lintas *inbound* dan *outbound* dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi.

### Protokol

Protokol pada jaringan komputer merupakan sebuah prosedur atau aturan yang harus disetujui secara bersama oleh perangkat yang akan berkomunikasi. Banyaknya protokol yang berbeda pada jaringan mengakibatkan sulitnya komunikasi antar perangkat yang terkoneksi melalui jaringan.

Salah satu model arsitektur yang banyak digunakan adalah OSI (*Open System Interconnection*) yang berupaya membentuk standar umum jaringan komputer untuk menunjang interoperatibilitas antar pemasok (*vendor*) dari yang berbeda. OSI memiliki 7 lapisan/*layer* yang setiap lapisan memiliki fungsinya masing-masing. Menurut Sugeng, W dan Putri, T.D fungsi dari masing-masing lapisan/*layer* yang terdapat pada OSI sebagai berikut:

1. Lapisan Fisik (*Physical Layer*), berfungsi dalam mengiriman *raw* bit ke kanal komunikasi. Masalah-masalah yang harus diperhatikan adalah masalah desain (Jika dikirim bit 1 harus diartikan bit 1 disisi penerima), masalah debain ini ditemukan ada hubungannya dengan mekanika, kelistrikan, prosedur *interface*, dan medium transmisi fisik yang berada di lapisan fisik.
2. Lapisan Jalur Data (*Data Link Layer*), tugas utamanya sebagai fasilitas transmisi *raw* data dan mentransfirmasikan data tersebut ke saluran yang bebas dari kesalahan transmisi. Dimungkinnya melalukan pemecahan data input menjadi sejumlah data *frame* (biasanya jumlahnya ratusan atau ribuan byte). Selanjutnya *frame* tersebut dikirim secara perurutan, dan memproses *acknowledgment frame* yang dikirim kembali oleh penerima. Penambahan bit-bit khusus diawal dan diakhir data guna pengenalan *frame* merupakan bagian pekerjaannya. Jika terjadi *noise* dan *frame* rusak *frame* dikirim ulang, tapi akibatnya akan terjadi duplikasi *frame* jika  *acknowledgment frame* hilang.
3. Lapisan Jaringan (*Network Layer*)*,* berfungsi sebagai pengendalian operasi *subnet*. Masalah desain yang penting adalah menentukan *route* pengiriman *packet* dari sumber ke tujuannya. Desain *route* dapat berupa statik atau dinamik. Masalah pengendalian kemacetan (*bottlenect*) merupakan tugasnya. Pada jaringan *broadcast,* masalah penentuan *route* hal yang sederhana, lapisan jaringan bisa tidak ada atau tidak diperlukan.
4. Lapisan Transport (*Transport Layer*), fungsi dasarnya adalah menerima data dari Lapisan Sesi, bila perlu memecah data menjadi bagian-bagian yang lebih kecil, meneruskan potongan ke lapisan jaringan dan menjamin seluruh potongan data sampai dengan benar disisi lainnya. Harus dilaksanakan secara efisien. Tujuan lainnya adalah melindungi seluruh lapisan diatasnya dari perubahan teknologi perangkat keras yang mungkin timbul. Bila diperlukan *throughput* yang tinggi, maka lapisa *transport* hubungan jaringan yang banyak, tetapi dapat pula menggabungkan beberapa hubungan *transport* ke hubungan jaringan yang sama. Penentuan jenis layanan (yang populer adalah saluran *error-free point tot point*) merupakan tugasnya pula. Merupakan *layer end-to-end* sejati dari sumber ke tujuan. Banyak *host* diprogram dengan *multiprogrammed* (banyak hubungan yang masuk dan meninggalkan *host* untuk menyatakan pesan mana). TH adalah tempat informasi tersebut ditempatkan. Pengendalian aliran (*Flow Control*) adalah merupakan tugasnya agar tidak membanjiri *host* yang lambat.
5. Lapisan Sesi (*Session Layer*), mengizinkan para pengguna untuk menetapkan *session* di antara mereka. Sebuah *session* digunakan untuk memungkinkan seseorang pengguna lelakukan *log* ke dalam suatu *remote time sharing system* atau memindahkan suatu *file* dari satu mesin ke mesin yang lain. Jadi tugasnya adalah pengendalian dialog. Funsi lainnya dalah manajemen *token (token management)*, sinkronisasi (*synchronization*), penyisipan *checkpoint* diperlukan jika akan mengulangi pengiriman akibat terjadinya *crash* sehingga tidak perlu seluruh data diulang pengirimannya.
6. Lapisan Presentasi (*Presentation Layer*),melakukan fungsi tertentu yang sering diminta untuk menjamin penemuan sebuah penyelesaian umum bagi masalah tertentu. Lapisan Presentasi tidak mengizinkan pengguna untuk menyelesaikan sendiri suatu masalah. Lapisan Presentasi memperhatikan *sytax* dan semantik informasi yang dikirimkan. Contoh layanannya adalah pengodean data (*data encoding*).
7. Lapisan Aplikasi (*Appilcation Layer*), tugasnya melayani *remote* terminal. Lapisan aplikasi terdiri dari bermacam-macam protocol yang bisa digunakan. Diperlukan adanya terminal virtual jaringan (*network virtual terminal*) sebelum suatu editor *remote* digunakan. Fungsi lainnya adalah pemindahan … (biasanya satu sistem ke sistem lain mempunyai konvensi yang berbeda). Tugasnya seperti: E-mail, Telnet, FTP, WWW dan lain sebagainya.

### ARP (Address Resolution Protocol)

Menurut Sugeng, W dan Putri, T.D, ARP (Address Resolution Protocol) adalah protokol yang bertugas untuk menemukan *hardware address* suatu *host* dengan alamat *IP* tertentu. Berikut format dari protokol ini:

**Tabel 2.2** Format *ARP*

|  |  |  |
| --- | --- | --- |
| Octet Offset | 0 | 1 |
| 0 | Hardware type | |
| 2 | Protocol type | |
| 4 | Hardware Address Length | Protocol Address Length |
| 6 | Operation | |
| 8 | Sender Hardware Address | |
| 10 |
| 12 |
| 14 | Sender Protocol Address | |
| 16 |
| 18 | Target Hardware Address | |
| 20 |
| 22 |
| 24 | Target Protocol Address | |
| 26 |

### Ethernet

Menurut Sugeng, W dan Putri, T.D, pada awalnya Ethernet didesain untuk dijalankan di atas kabel koaksial pada kecepatan maksumum 10 Mbps. Sekarang Ethernet berjalan pada kabel koaksial *thin-wide* (10base2) dan *unshielded twisted-pair (UTP) telephone wiring* (10base3). *Device* pada *network-PC, workstation, printer, server,* dll secara fisik terhubung ke kabel tunggal yang dikenal sebagai *bus.*

Pada perkembangan berikutnya, muncul teknologi *Switch Ethernet,* untuk menghindari *problem* tabrakan paket. Sebuah *Switch Ethernet* menggantikan pengabelan *hub.* Berikutnya ada *Fast Ethernet,* yang membesarkan *bandwith* LAN dari 10 Mbps menjadi 100 Mbps. Ia menggunakan 2 standar: Gigabit 100base-I (IEEE 802.3u) dan Gigabit 100VG-AnyLAN (IEEE 803.12).

### Ethernet II

Ethernet II adalah sebuah standar enkapsulasi paket data jaringan berbasis teknologi Ethernet yang digunakan oleh protokol TCP/IP. Standar ini dikembangkan oleh Digital Equipment Corporation (DEC), Intel Corporation, dan Xerox sebelum akhirnya diserahkan kepada komite IEEE 802 untuk menjadi standar IEEE 802.3. Ethernet II juga disebut sebagai Ethernet II frame format atau DIX frame format (mengingat pihak-pihak yang mengembangkannya adalah DEC, Intel dan Xerox).

**Table 2.3.** Ethernet II Frame Format

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MAC Destination | MAC Source | Ethertype | Payload | FCS |
| 6 octets | 6 octets | 2 octets | 46-1500 octets | 4 octet |

### IP Address

Menurut Sugeng, W dan Putri, T.D, *IP (Internet Protocol)* *address* atau alamat *IP* yang bahasa awamnya bisa disebut dengan kode pengenal komputer pada jaringan merupaan komponen vital pada internet, karena tanpa alamat *IP* sesorang tidak akan dapat terhubung ke *internet.* Setiap komputer yang terhubung ke *internet* setidaknya harus memiliki satu buah alamat *IP* pada setiap perangkat yang terhubung ke *internet* dan alamat *IP* itu sendiri harus unik karena tidak boleh ada komputer/*server/*perangkat jaringan lainnya yang menggunakan alamat *IP* yang sama di *Internet.*

### Mac Address

Mac Address (Media Access Control) Addres adalah., sebuah alamat jaringan yang diimplementasikan pada lapisan data-link dalam tujuh lapisan model OSI, yang merepresentasikan sebuah node tertentu dalam jaringan. Dalam sebuah jaringan berbasis Ethernet, MAC address merupakan alamat yang unik yang memiliki panjang 48-bit (6 byte) yang mengidentifikasikan sebuah komputer, interface dalam sebuah router, atau node lainnya dalam jaringan. MAC Address juga sering disebut sebagai Ethernet address, physical address, atau hardware address.

Dalam sebuah komputer, MAC address ditetapkan ke sebuah kartu jaringan (network interface card/NIC) yang digunakan untuk menghubungkan komputer yang bersangkutan ke jaringan. MAC Address umumnya tidak dapat diubah karena telah dimasukkan ke dalam ROM. Beberapa kartu jaringan menyediakan utilitas yang mengizinkan pengguna untuk mengubah MAC address, meski hal ini kurang disarankan. Jika dalam sebuah jaringan terdapat dua kartu jaringan yang memiliki MAC address yang sama, maka akan terjadi konflik alamat dan komputer pun tidak dapat saling berkomunikasi antara satu dengan lainnya. Beberapa kartu jaringan, seperti halnya kartu Token Ring mengharuskan pengguna untuk mengatur MAC address (tidak dimasukkan ke dalam ROM), sebelum dapat digunakan.

MAC address memang harus unik, dan untuk itulah, Institute of Electrical and Electronics Engineers (IEEE) mengalokasikan blok-blok dalam MAC address. 24 bit pertama dari MAC address merepresentasikan siapa pembuat kartu tersebut, dan 24 bit sisanya merepresentasikan nomor kartu tersebut. Setiap kelompok 24 bit tersebut dapat direpresentasikan dengan menggunakan enam digit bilangan heksadesimal, sehingga menjadikan total 12 digit bilangan heksadesimal yang merepresentasikan keseluruhan MAC address. Berikut merupakan tabel beberapa pembuat kartu jaringan populer dan nomor identifikasi dalam MAC Address.

Agar antara komputer dapat saling berkomunikasi satu dengan lainnya, frame-frame jaringan harus diberi alamat dengan menggunakan alamat Layer-2 atau MAC address. Tetapi, untuk menyederhanakan komunikasi jaringan, digunakanlah alamat Layer-3 yang merupakan alamat IP yang digunakan oleh jaringan TCP/IP. Protokol dalam TCP/IP yang disebut sebagai Address Resolution Protocol (ARP) dapat menerjemahkan alamat Layer-3 menjadi alamat Layer-2, sehingga komputer pun dapat saling berkomunikasi.

### IPv4 (Internet Protocol Version 4)

Menurut Sugeng, W dan Putri, T.D, alamat *IP (IPv4)* pada awalnya adalah sederetan bilangan biner sepanjang 32 bit yang dipakai untuk mengidentifikasikan *host* pada jaringan. Alamat *IP* ini diberikan secara unik pada masing-masing komputer/*host* yang terhubung ke *internet.* Prinsip kerjanya adalah paket yang membawa data dimuati alamat *IP* dari komputer pengirim data kepada alamat *IP* pada komputer yang akan dituju, kemudian data tersebut dikirim ke jaringan. Paket ini kemudian dikirim dari *router* ke *router* dengan berpedoman pada alamat *IP* tersebut menuju ke komputer yang dituju. Seluruh komputer/*host* yang tersambung ke iinternet, dibedakan hanya berdasarkan alamat *IP* untuk setiap komputer yang terhubung ke jaringan *internet.*

*IPv4* terdiri dari 14 *field*, namun satu *field* terakhir hanya bersifat  *optional*. Berikut format dari paket *IPv4*.

**Tabel 2.4.** Format IPv4

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Offsets | Octet | 0 | | | | 1 | | | | 2 | | | | | 3 | | | |
| Octet | Bit | 0 | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | | 20 | 22 | 24 | 26 | 28 | 30 |
| 0 | 0 | Version | | IHL | | DSCP | | | E | Total Length | | | | | | | | |
| 4 | 32 | Identification | | | | | | | | Flags | | Fragment Offset | | | | | | |
| 8 | 64 | Time to Live | | | | Protocol | | | | Header Checksum | | | | | | | | |
| 12 | 96 | Source IP Address | | | | | | | | | | | | | | | | |
| 16 | 128 | Destinatin IP Address | | | | | | | | | | | | | | | | |
| 20 | 160 | Options (if IHL > 5) | | | | | | | | | | | | | | | | |
| 24 | 192 |
| 28 | 224 |
| 32 | 256 |

### TCP (Transmission Control Protocol)

*Transmission Control Protocol (TCP)* merupakan protokol yang terletak pada *transport layer*. Protokol ini menyediakan layanan yang dikenal sebagain *connection oriented* yang berarti sebelum melakukan pertukaran data dua *host* yang menggunakan *TCP* harus melakukan pembentukan hubungan *(handshake)* terlebih dahulu. Berikut karakteristik *TCP*:

* Berorientasi sambungan (*connection-oriented*): Sebelum data dapat ditransmisikan antara dua host, dua proses yang berjalan pada lapisan aplikasi harus melakukan negosiasi untuk membuat sesi koneksi terlebih dahulu. Koneksi TCP ditutup dengan menggunakan proses terminasi koneksi TCP (TCP connection termination).
* *Full-duplex*: Untuk setiap host *TCP*, koneksi yang terjadi antara dua *host* terdiri atas dua buah jalur, yakni jalur keluar dan jalur masuk. Dengan menggunakan teknologi lapisan yang lebih rendah yang mendukung *full-duplex*, maka data pun dapat secara simultan diterima dan dikirim. *TCP Header* berisi nomor urut *(TCP sequence number)* dari data yang ditransmisikan dan sebuah *acknowledgment* dari data yang masuk.
* Dapat diandalkan (*reliable*): Data yang dikirimkan ke sebuah koneksi *TCP* akan diurutkan dengan sebuah nomor urut paket dan akan mengharapkan paket *positive acknowledgment* dari penerima. Jika tidak ada paket *Acknowledgment* dari penerima, maka segmen *TCP* (*protocol data unit* dalam protokol *TCP*) akan ditransmisikan ulang. Pada pihak penerima, segmen-segmen duplikat akan diabaikan dan segmen-segmen yang datang tidak sesuai dengan urutannya akan diletakkan di belakang untuk mengurutkan segmen-segmen *TCP*. Untuk menjamin integritas setiap segmen *TCP, TCP* mengimplementasikan penghitungan *TCP Checksum*.
* *Byte stream*: *TCP* melihat data yang dikirimkan dan diterima melalui dua jalur masuk dan jalur keluar *TCP* sebagai sebuah *byte stream* yang berdekatan (kontigu). Nomor urut *TCP* dan nomor *acknowlegment* dalam setiap *TCP Header* didefinisikan juga dalam bentuk *byte*. Meski demikian, *TCP* tidak mengetahui batasan pesan-pesan di dalam *byte stream TCP* tersebut. Untuk melakukannya, hal ini diserahkan kepada protokol lapisan aplikasi (dalam *DARPA Reference Model*), yang harus menerjemahkan *byte stream TCP* ke dalam "bahasa" yang ia pahami.
* Memiliki layanan *flow control*: Untuk mencegah data terlalu banyak dikirimkan pada satu waktu, yang akhirnya membuat "macet" jaringan *internetwork IP*, *TCP* mengimplementasikan layanan *flow control* yang dimiliki oleh pihak pengirim yang secara terus menerus memantau dan membatasi jumlah data yang dikirimkan pada satu waktu. Untuk mencegah pihak penerima untuk memperoleh data yang tidak dapat disangganya (*buffer*), *TCP* juga mengimplementasikan *flow control* dalam pihak penerima, yang mengindikasikan jumlah *buffer* yang masih tersedia dalam pihak penerima.
* Melakukan segmentasi terhadap data yang datang dari lapisan aplikasi (dalam *DARPA Reference Model*).
* Mengirimkan paket secara "*one-to-one*": hal ini karena memang *TCP* harus membuat sebuah sirkuit logis antara dua buah protokol lapisan aplikasi agar saling dapat berkomunikasi. *TCP* tidak menyediakan layanan pengiriman data secara *one-to-many*.

**Table 2.5.** Penjelasan *Field-field TCP*

|  |  |  |
| --- | --- | --- |
| **Nama field** | **Ukuran** | **Keterangan** |
| Source Port | 16 bit | Mengindikasikan sumber protokol lapisan aplikasi yang mengirimkan segmen TCP yang bersangkutan. Gabungan antara field Source IP Address dalam header IP dan field Source Port dalam field header TCP disebut juga sebagai source socket, yang berarti sebuah alamat global dari mana segmen dikirimkan. Lihat juga Port TCP. |
| Destination Port | 16 bit | Mengindikasikan tujuan protokol lapisan aplikasi yang menerima segmen TCP yang bersangkutan. Gabungan antara field Destination IP Address dalam header IP dan field Destination Port dalam field header TCP disebut juga sebagai *socket* tujuan, yang berarti sebuah alamat global ke mana segmen akan dikirimkan. |
| Sequence Number | 32 bit | Mengindikasikan nomor urut dari oktet pertama dari data di dalam sebuah segmen TCP yang hendak dikirimkan. Field ini harus selalu diset, meskipun tidak ada data (payload) dalam segmen. Ketika memulai sebuah sesi koneksi TCP, segmen dengan flag SYN (Synchronization) diset ke nilai 1, field ini akan berisi nilai Initial Sequence Number (ISN). Hal ini berarti, oktet pertama dalam aliran byte (byte stream) dalam koneksi adalah ISN+1. |
| Acknowledgment Number | 32 bit | Mengindikasikan nomor urut dari oktet selanjutnya dalam aliran byte yang diharapkan oleh untuk diterima oleh pengirim dari si penerima pada pengiriman selanjutnya. Acknowledgment number sangat dipentingkan bagi segmen-segmen TCP dengan flag ACK diset ke nilai 1. |
| Data Offset | 4 bit | Mengindikasikan di mana data dalam segmen TCP dimulai. Field ini juga dapat berarti ukuran dari header TCP. Seperti halnya field *Header Length* dalam header IP, field ini merupakan angka dari word 32-bit dalam header TCP. Untuk sebuah segmen TCP terkecil (di mana tidak ada opsi TCP tambahan), field ini diatur ke nilai 0x5, yang berarti data dalam segmen TCP dimulai dari oktet ke 20 dilihat dari permulaan segmen TCP. Jika field Data Offset diset ke nilai maksimumnya (24=16) yakni 15, header TCP dengan ukuran terbesar dapat memiliki panjang hingga 60 byte. |
| Reserved | 6 bit | Direservasikan untuk digunakan pada masa depan. Pengirim segmen TCP akan mengeset bit-bit ini ke dalam nilai 0. |
| Flags | 6 bit | Mengindikasikan flag-flag TCP yang memang ada enam jumlahnya, yang terdiri atas: URG (Urgent), ACK (Acknowledgment), PSH (Push), RST (Reset), SYN (Synchronize), dan FIN (Finish). |
| Window | 16 bit | Mengindikasikan jumlah byte yang tersedia yang dimiliki oleh buffer host penerima segmen yang bersangkutan. Buffer ini disebut sebagai Receive Buffer, digunakan untuk menyimpan byte stream yang datang. Dengan mengimbuhkan ukuran window ke setiap segmen, penerima segmen TCP memberitahukan kepada pengirim segmen berapa banyak data yang dapat dikirimkan dan disangga dengan sukses. Hal ini dilakukan agar si pengirim segmen tidak mengirimkan data lebih banyak dibandingkan ukuran Receive Buffer. Jika tidak ada tempat lagi di dalam Receive buffer, nilai dari field ini adalah 0. Dengan nilai 0, maka si pengirim tidak akan dapat mengirimkan segmen lagi ke penerima hingga nilai field ini berubah (bukan 0). Tujuan hal ini adalah untuk mengatur lalu lintas data atau *flow control*. |
| Checksum | 16 bit | Mampu melakukan pengecekan integritas segmen TCP (*header*-nya dan *payload*-nya). Nilai field Checksum akan diatur ke nilai 0 selama proses kalkulasi checksum. |
| Urgent Pointer | 16 bit | Menandakan lokasi data yang dianggap "urgent" dalam segmen. |
| Options | 32 bit | Berfungsi sebagai penampung beberapa opsi tambahan TCP. Setiap opsi TCP akan memakan ruangan 32 bit, sehingga ukuran header TCP dapat diindikasikan dengan menggunakan field Data offset. |

Proses pembuatan koneksi *TCP* disebut juga dengan *"Three-way Handshake"*. Tujuan metode ini adalah agar dapat melakukan sinkronisasi terhadap nomor urut dan nomor *acknowledgement* yang dikirimkan oleh kedua pihak dan saling bertukar ukuran *TCP Window*. Prosesnya dapat digambarkan sebagai berikut:

* *Host* pertama (yang ingin membuat koneksi) akan mengirimkan sebuah segmen *TCP* dengan *flag SYN* diaktifkan kepada *host* kedua (yang hendak diajak untuk berkomunikasi).
* *Host* kedua akan meresponsnya dengan mengirimkan segmen dengan *acknowledgment* dan juga *SYN* kepada *host* pertama.
* *Host* pertama selanjutnya akan mulai saling bertukar data dengan host kedua.

*TCP* menggunakan proses jabat tangan yang sama untuk mengakhiri koneksi yang dibuat. Hal ini menjamin dua *host* yang sedang terkoneksi tersebut telah menyelesaikan proses transmisi data dan semua data yang ditransmisikan telah diterima dengan baik. Itulah sebabnya, mengapa *TCP* disebut dengan koneksi yang *reliable*.

Berikut *flag* yang terdapat pada *TCP:*

**Table 2.6.** Penjelasan *TCP Flags*

|  |  |
| --- | --- |
| **Nama flag** | **Keterangan** |
| URG | Mengindikasikan bahwa beberapa bagian dari segmen TCP mengandung data yang sangat penting, dan field Urgent Pointer dalam header TCP harus digunakan untuk menentukan lokasi di mana data penting tersebut berada dalam segmen. |
| ACK | Mengindikasikan field Acknowledgment mengandung oktet selanjutnya yang diharapkan dalam koneksi. Flag ini selalu diset, kecuali pada segmen pertama pada pembuatan sesi koneksi TCP. |
| PSH | Mengindikasikan bahwa isi dari TCP Receive buffer harus diserahkan kepada protokol lapisan aplikasi. Data dalam receive buffer harus berisi sebuah blok data yang berurutan (kontigu), dilihat dari ujung paling kiri dari buffer. Dengan kata lain, sebuah segmen yang memiliki flag PSH diset ke nilai 1, tidak bolah ada satu byte pun data yang hilang dari aliran byte segmen tersebut; data tidak dapat diberikan kepada protokol lapisan aplikasi hingga segmen yang hilang tersebut datang. Normalnya, TCP Receive buffer akan dikosongkan (dengan kata lain, isi dari buffer akan diteruskan kepada protokol lapisan aplikasi) ketika buffer tersebut berisi data yang kontigu atau ketika dalam "proses perawatan". Flag PSH ini dapat mengubah hal seperti itu, dan membuat akan TCP segera mengosongkan TCP Receive buffer. Flag PSH umumnya digunakan dalam protokol lapisan aplikasi yang bersifat interaktif, seperti halnya Telnet, karena setiap penekanan tombol dalam sesi terminal virtual akan dikirimkan dengan sebuah flag PSH diset ke nilai 1. Contoh dari penggunaan lainnya dari flag ini adalah pada segmen terakhir dari berkas yang ditransfer dengan menggunakan protokol FTP. Segmen yang dikirimkan dengan flag PSH aktif tidak harus segera di-acknowledge oleh penerima. |
| RST | Mengindikasikan bahwa koneksi yang dibuat akan digagalkan. Untuk sebuah koneksi TCP yang sedang berjalan (aktif), sebuah segmen dengan flag RST diset ke nilai 1 akan dikirimkan sebagai respons terhadap sebuah segmen TCP yang diterima yang ternyata segmen tersebut bukan yang diminta, sehingga koneksi pun menjadi gagal. Pengiriman segmen dengan flag RST diset ke nilai 1 untuk sebuah koneksi aktif akan menutup koneksi secara paksa, sehingga data yang disimpan dalam buffer akan dibuang (dihilangkan). Untuk sebuah koneksi TCP yang sedang dibuat, segmen dengan flag RST aktif akan dikirimkan sebagai respons terhadap request pembuatan koneksi untuk mencegah percobaan pembuatan koneksi. |
| SYN | Mengindikasikan bahwa segmen TCP yang bersangkutan mengandung Initial Sequence Number (ISN). Selama proses pembuatan sesi koneksi TCP, TCP akan mengirimkan sebuah segmen dengan flag SYN diset ke nilai 1. Setiap host TCP lainnya akan memberikan jawaban (acknowledgment) dari segmen dengan flag SYN tersebut dengan menganggap bahwa segmen tersebut merupakan sekumpulan byte dari data. Field Acknowledgment Number dari sebuah segmen SYN diatur ke nilai ISN + 1. |
| FIN | Menandakan bahwa pengirim segmen TCP telah selesai dalam mengirimkan data dalam sebuah koneksi TCP. Ketika sebuah koneksi TCP akhirnya dihentikan (akibat sudah tidak ada data yang dikirimkan lagi), setiap host TCP akan mengirimkan sebuah segmen TCP dengan flag FIN diset ke nilai 1. Sebuah host TCP tidak akan mengirimkan segmen dengan flag FIN hingga semua data yang dikirimkannya telah diterima dengan baik (menerima paket acknowledgment) oleh penerima. Setiap host akan menganggap sebuah segmen TCP dengan flag FIN sebagai sekumpulan byte dari data. Ketika dua host TCP telah mengirimkan segmen TCP dengan flag FIN dan menerima acknowledgment dari segmen tersebut, maka koneksi TCP pun akan dihentikan. |

### Sniffing dan Spoofing

*Sniffing* adalah proses penyadapan paket pada jaringan dengan menggunakan sebuah aplikasi yang biasa disebut *Network Analyzer*. Aplikasi ini menangkap tiap-tiap paket dan dapat juga menguraikan paket tersebut berdasarkan *RFC (Request of Comments)*. Sedangkan *spoofing* merupakan proses pemalsuan paket-paket jaringan yang dapat mendukung proses *sniffing*.

*Sniffing* sendiri dapat dikategorikan menjadi 2, yaitu aktif dan pasif. *Sniffing* pasif merupakan proses analisa paket jaringan tanpa melakukan perubahan atau pembuatan paket tertentu yang kemudian dikirimkan melelui jaringan. Sebaliknya *sniffing* aktif merupakan proses *sniffing* yang pada kondisi tertentu dapat melakukan perubahan ataupun pembuatan paket yang kemudian dikirimkan melalui jaringan.

### Promiscuous Mode

*Promiscuous mode* atau *promisc mode* merupakan konfigurasi pada *Network Interface Card (NIC)* yang dapat menghambat atau meneruskan setiap paket yang melewatinya. Ketika *NIC* berada pada *promiscuous mode* maka setiap paket yang melewatinya (termasuk paket yang tidak ditujukan kepadanya) akan diteruskan ke *CPU* dan diproses.

### Maximum Transmission Unit (MTU)

*Maximum Transmission Unit (MTU)* dalam jaringan komputer merupakan maksimum dari ukuran paket yang dapat ditransimikan oleh media jaringan. Ukuran dari *MTU* berfariasi tergantung pada media transmisi yang digunakan. Salah satu media transmisi yang umum digunakan adalah *Ethernet* dengan maksimum *MTU* adalah 1500 yang berarti paket yang ditransmisikan pada *Ethernet Frame (datalink layer)* tidak dapat melebihi 1500 *bytes.*

### Pcap File Format

Format .pcap *(Packet Capture)* merupakan format standar yang digunakan untuk penyimpanan hasil *capture* data jaringan. Paket yang tersimpan di dalam format pcap tidak selalu berisi semua data seperti paket yang terdapat di jaringan jika *snaphot length* yang digunakan lebih kecil dari panjang paket yang terdapat di jaringan. Untuk mengatasi permasalahan ini kita dapat menerapkan *snapshot length* sepanjang 65535 (maksimum). Versi setelah pcap adalah pcap-ng, untuk lebih detailnya dapat dilihat di https://github.com/the-tcpdump-group/pcapng.

# METODE PENELITIAN

## Obyek Penelitian

*ARP* merupakan suatu protokol yang bertanggung jawab untuk mencari *Media Access Control (MAC) Address* dari setiap komputer yang akan berkomunikasi melalui jaringan *Local Area Network (LAN)* dengan memanfaatkan *Internet Protocol Address (IP Address)* versi 4 yang telah didapat saat sebuah komputer terkoneksi ke dalam jaringan. *MAC Address* yang telah didapat akan disimpan di dalam *ARP cache* agar tidak membuat jaringan sibuk dengan selalu mengirimkan paket *ARP* setiap kali ingin berkomunikasi dengan komputer lainnya.

Ketika sebuah host menerima *ARP* reply maka secara langsung akan meng-update *ARP cache* yang dimilikinya. Hal ini menyebabkan permasalahan ketika host tesebut mendapatkan *ARP reply* yang telah di buat sedemikian rupa oleh attacker (penyerang) karena pada proses update *ARP cache* tidak dilakukan pengecekan terlebih dahulu. Disini timbul permasalahan kerena *ARP cache* tersebut akan digunakan untuk berkomunikasi antar host yang terkoneksi di jaringan yang akan berakibat tidak sampainya data kepada tujuan yang diinginkan.

## Metode Penelitian

### Pengumpulan Data

Metode dan prosedur yang penulis gunakan untuk mendapatkan suatu data atau informasi tentang apa saja yang harus dikerjakan pada saat pengembangan sistem “Pendeteksi Serangan Pada ARP” adalah sebagai berikut:

1. **Observasi**

Kegiatan yang dilakukan adalah dengan mengamati dan menganalisa setiap paket *ARP* yang dapat di-*capture* pada jaringan. Hasil dari kegiatan ini akan dijadikan acuan untuk menentukan metode yang tepat untuk menyelesaikan masalah

1. **Analisis Kebutuhan**

Pada kegiatan ini akan dilakukan analisis kebutuhan sistem baik perangkat keras maupun perangkat lunak. Selain itu juga akan dilakukan analisis akan kebutuhan calon pengguna sistem yang dibuat akan tepat guna.

### Analisis Perancangan

Dalam memenuhi kebutuhan pengguna, sistem ini membutuhkan dukungan hardware dan software diantaranya *Network Interface Card (NIC)*, Libpcap untuk GNU/Linux sebagai *packet capture library* dan Winpcap yang merupakan versi lain dari Libpcap untuk Windows dimana juga terdapat *network driver* untuk *packet capture*. Libpcap/Winpcap ini juga digunakan untuk menyimpan hasil dari paket-packet yang berhasil di-*capture*.

### Pembuatan Program

Sistem ini akan diimplementasikan dengan menggunakan bahasa pemrograman Java dan C (untuk pembuatam *library/modul* pengiriman dan pengambilan paket). Sedangkan penyimpanan hasil *capture* paket akan menggunakan format pcap ataupun pcapng.

### Implementasi dan Pengujian

Sistem ini akan diimplementasikan pada beberapa komputer yang menggunakan sistem operasi Linux dan Windows, selain itu akan dilakukan beberapa kali pengujian sebelum dan saat sistem digunakan oleh pengguna.

# ANALISA DAN PERANCANGAN SISTEM

## Analisa Sistem yang Berjalan

Dalam jaringan lokal, paket *IP* umumnya dikirim melalui *Ethernet Card* (kartu jaringan/*NIC*)*.* Untuk keperluan komunikasi sesama *Ethernet Card* digunakan *Ethernet Address*, dalam hal ini ada *MAC Address* yang besarnya 48 bit dan setian kartu jaringan memiliki alamat yang berbeda-beda. Pada waktu pengiriman data dengan *IP* tertentu, suatu *host* perlu mengetahui di atas *Ethernet Card* mana *IP* tersebut terletak. Untuk keperluan pemetaan *IP Address* dengan *Ethernet Address (MAC Address)* inilah *ARP* digunakan.

Protokol yang digunakan untuk pemetaan *IP Address* dan *MAC Address* ini menyimpan hasil pemetaan yang telah dilakukan kedalam *ARP Cache/ARP Table.* Namun *ARP Cache* ini akan otomatis ter-*update* ketika sebuah *host* menerima paket *ARP* dengan *Operation Code* 0x0802 atau *ARP Reply* tanpa ada proses pengecekan lebih lanjut. Dengan begitu *ARP Cache* akan dapat di-*update* oleh penyerang sesuai dengan yang diinginkannya. Hal ini dapat menyebabkan pengiriman paket *IP* tidak sampai pada tujuan yang seharusnya, justru paket tersebut dapat dialihkan kepada penyerang. Teknik ini sering disebut dengan *MITM (Man In The Middle)*, yang mana sangat berbahaya jika paket *IP* tersebut berisi data-data penting.

## Analisa Kebutuhan

### Kebutuhan Fungsional

Sistem yang sedang berjalan ini membutuhkan sebuah fungsi tambahan untuk melakukan penyecekan pada setiap paket *ARP* untuk memastikan bahwa jaringan *LAN* tersebut cukup aman untuk digunakan. Selain itu jika dalam proses penyecekan paket *ARP* dideteksi terdapat paket yang membahayakan maka sistem membutuhkan sebuah notifikasi yang membuat pengguna tau akan tindakan apa yang harus dilakukannya.

### Kebutuhan Non Fungsional

Dibutuhkan beberapa *hardware* maupun *software* agar sistem ini dapat berjalan, diantaranya:

* Kebutuhan Perangkat Keras
  + *Ethernet Card (Network Interface Card)*
* Kebutuhan Perangkat Lunak
  + Npcap untuk sistem operasi Windows.
  + Java Runtime Environment 1.8.0 (minimal).

## Analisa Pengembangan sistem

## Rancangan Sistem

Sistem ini melakukan deteksi dengan cara melakukan *filtering* terhadap paket *ARP* yang di-*capture* oleh kartu jaringan *(Network Interface Card)* pada *promiscuous mode.* Setelah paket ARP diterima maka akan dilakukan ektraksi agar dapet diproses. Namun sebelumnya dilakukan pemilihan kartu jaringan yang akan digunakan, berikut algoritma yang digunakan:

WHILE (kartu jaringan) DO

IF (IP kartu jaringan != 0.0.0.0 AND IP kartu jaringan !=

127.0.0.1 AND Alamat Bcast kartu jaringan != 0.0.0.0

AND Alamat netmask kartu jaringan != 0.0.0.0) THEN

RETURN kartu jaringan

ENDIF

Jika paket yang diterima merupakan pakct ARP Reply (Ethertype: 0x0806, dan ARP Opcode: 2) maka akan dilakukan pengecekan untuk memastikan bahwa paket tersebut adalah paket yang memang ditujuan kepada sistem yang sedang digunakan. Jika paket tersebut memang ditujukan pada sistem yang sedang berjalan maka akan dilakukan proses deteksi sebagai berikut.

IF (EthSrc != Sender Hardware Address || EthDst !=

Target Hardware Address) THEN

Jalan mudul untuk pengecekan IP Routing

ELSE

IF (IP dan MAC Address tidak ada di Tabel ARP) THEN

Tambahkan IP dan MAC Address ke Tabel ARP

ELSE

IF (IP dan MAC Address != yang ada di Table ARP) THEN

Jalan mudul untuk pengecekan IP Routing

ELSE

IF ((Besar Eth Frame < 60 AND OUI tidak diketahui) OR

Selisih waktu pengiriman paket < 2000 ms) THEN

Jalan mudul untuk pengecekan IP Routing

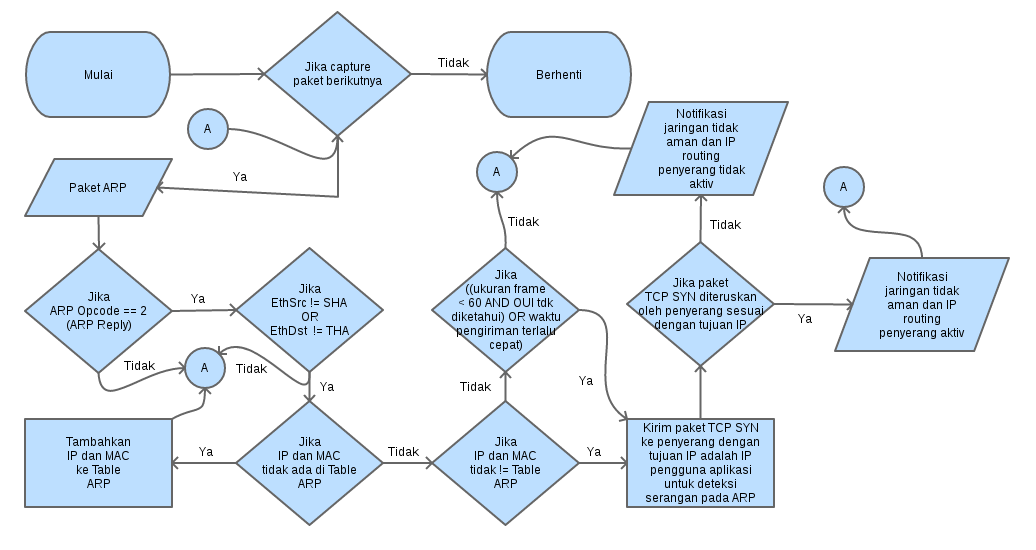
ENDIF

ENDIF

ENDIF

ENDIF

Sistem deteksi serangan pada *ARP* ini akan diperjelas dengan menggunkan *Flow Chart* berikut:



**Gambar 3.1.** Flow Chart Deteksi Serangan Pada ARP

## Rancangan Menu Dan Antar Muka

**Gambar 3.**. menunjukan rancangan struktur menu aplikasi serang pada *ARP*, yang dirancang untuk mengatur sistem.



**Gambar 3.2.** Struktur Menu Serangan

Gambar 3.4. menunjukan rancangan struktur menu aplikasi deteksi serang pada *ARP*, yang dirancang untuk mengatur sistem.

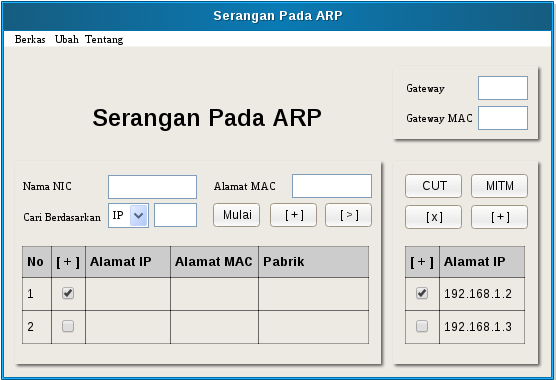


**Gambar 3.3.** Struktur Menu Deteksi Serangan

## Rancangan *Graphical User Interface (GUI)*

### Serangan Pada ARP

Jendela ini digunakan untuk melakukan pencarian *host* yang terkoneksi pada jaringan *LAN* menggunakan *ARP* dimana hasilnya dapat digunakan untuk melakukan serangan. Pada jendela ini juga ditampilkan informasi jaringan seperti, kartu jaringan yang digunakan beserta Alamat MAC-nya, Gateway address, dan Gateway MAC.



**Gambar 3.5** Serangan Pada ARP

Jendela ini digunakan untuk melakukan konfigurasi kartu jaringan yang akan digunakan untuk melakukan serangan. Namun kartu jaringan yang dapat dipilih hanyalah kartu jaringan yang terkoneksi pada jaringan *LAN*.



**Gambar 3.6.** Konfigurasi Kartu Jaringan

### Deteksi Serangan Pada ARP

Jendela berikut digunakan untuk mendeteksi serangan pada *ARP* dimana hasil deteksi akan ditampilkan dalam bentuk teks mupun notifikasi *(pop up)* yang bertujuan agar pengguna mengetahui tindakan apa yang harus dilakukan. Selain itu pada jendela ini ditambahkan fungsi untuk melakukan pengecekan *ARP Cache* (Tabel ARP) dimana dapat digunakan untuk membandingan ketika sistem sedang diserang atau tidak.



**Gambar 3.7.** Deteksi Serangan Pada ARP

# IMPLEMENTASI SISTEM

## Implementasi

Sistem ini dapat diimplementasikan pada sistem operasi GNU/Linux (i686, amd64, armv7, dsb) dan Windows (x86/amd64). Agar dapat menjalankan fungsinya sistem ini juga membutuhkan koneksi pada jaringan *LAN (Local Area Network)*.

Dalam tahap ini akan diketahui bagaimana cara memulai, menjalankan, dan mengakhiri program yang telah dirancang pada bab sebelumnya.

## Perangkat Keras (*Hardware*) yang Digunakan

Perangkat keras khusus yang dibutuhkan untuk mengoperasikan sistem ini adalah:

1. Network Interface Card (Ethernet Card)

## Perangkat Lunak (*Software*) yang Digunakan

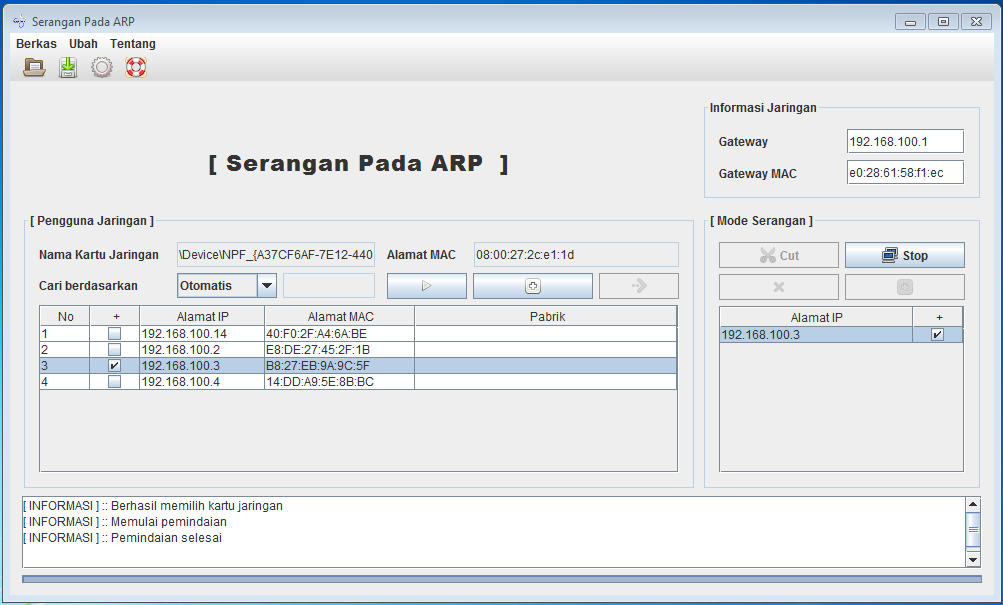
Perangkat lunak khusus yang dibutuhkan dalam membangun sistem ini adalah:

1. GNU/Linux (keluarga Debian) dan Windows (7 dan 10)
2. Netbeans dan Intellij IDEA
3. Jxnet dan Npcap (Npcap hanya untuk sistem operasi Windows)

## Implementasi Sistem

### Implementasi Serangan

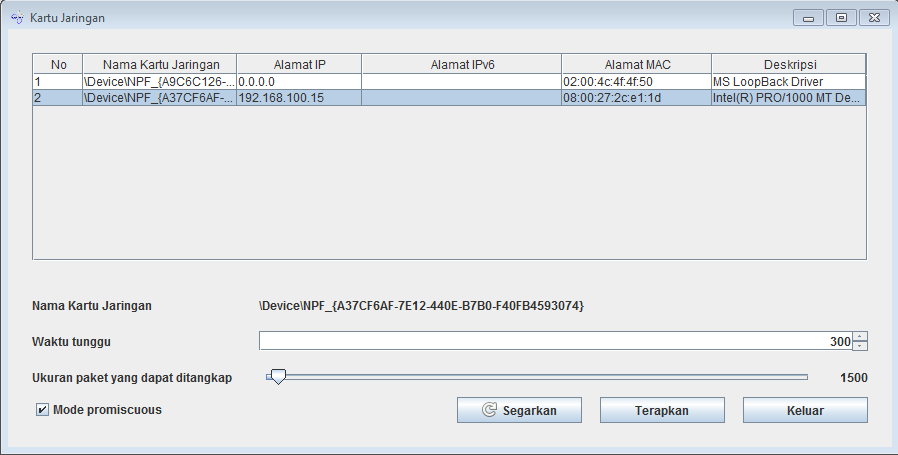
Untuk melakukan serangan menggunakan program yang telah dibuat adalah dengan melakukan pencarian target kemudian menambahkannya ke dalam tabel target. Setelah ada target di dalam tabel target makan serangan dapat dimulai dengan meng-klik tombol “Cut” ataupun “MITM”. Tombol “Cut” berfungsi untuk mengubah *ARP Cache* pada target dengan Gateway Mac Address yang acak dengan tujuan agar paket yang dikirimkan oleh target ke gateway tidak sampai. Sedangkan timbol “MITM” berfungsi untuk memberitahu kepada target bahwa penyerang adalah si­-gateway dan memberi tahu si-gateway yang sesungguhnya bahwa penyerang adalah target. Berikut tampilah dari program untuk melakukan serangan.



**Gambar 5.1** Form Serangan

### Implementasi Konfigurasi Kartu Jaringan

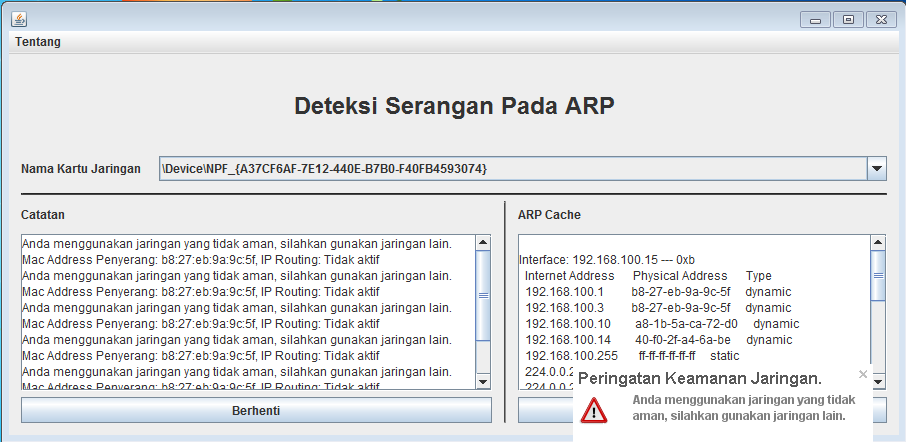
Ketika menjalankan program (untuk serangan) maka secara otomatis program akan melakukan pemilihan kartu jaringan yang akan digunakan dan terkoneksi pada jaringan LAN (Local Area Network). Namun jika ingin melakukan konfigurasi manual dapat dilakukan dengan memilih “Ubah” kemudian klik “Kartu Jaringan”. Kartu jaringan yang dapat dipilih hanyalah kartu jaringan yang digunakan (terkoneksi pada jaringan LAN). Berikut tampilan dari form konfigurasi kartu jaringan.



**Gambar 5.2** Konfigurasi Kartu Jaringan

### Implementasi Deteksi Serangan

Sebelum memulai deteksi kartu jaringan terlebih dahulu harus terkoneksi pada jaringan *LAN.* Setelah terkoneksi untuk memulai deteksi dapat meng-klik tombol “Mulai Deteksi”. Sedangkan untuk melihat “ARP Cache” untuk membandingkan antara diserang dengan tidak disertang dapat meng-klik tombol “Lihat ARP Cache”.



# PENUTUP

## Kesimpulan

Setelah sistem deteksi ini diimplementasikan dapat disimpulkan bahwa sistem ini dapat melakukan pengecekan paket-paket *ARP* sehingga dapat mendeteksi serangan yang menggunakan *ARP (ARP Spoofing/Arp Cache Poisoning)*.

## Saran

Dari hasil peng-implementasian sistem deteksi ini diharapkan adanya pengembangan sistem yang disesuaikan dengan perkembangan teknologi dan berbagai macam jenis serangan yang dapat membahayakan, diantaranya:

* Tidak hanya mampu mendeteksi *address resolution* pada *IPv4 (ARP),* namun juga *address resolution* pada *IPv6 (NDP).*
* Mampu mendeteksi serangan pengembangan dari *ARP Spoofing* seperti *Sniffing, DNS Spooing,* dan lain sebagainya.

Dimana sistem tersebut dapat memberikan rasa aman bagi para penggunanya ketika menggunakan jaringan *LAN*.

# DAFTAR PUSTAKA

Kaur, I., 2013, Detection and Prevention of ARP Cache Poisoning, Thesis, Computer Science and Engineeting Department, Thapar University, Patiala.

Srinath, D., Panimalar S., Simla, A. J., dan Deepa, J., 2015, Detection and Prevention of ARP Spoofing using Centralized Server, Internation Journal of Computer Applications*,113,* Departement of Computer science and Engineering, Panimalar Institute of Technology, India.

Vinay, K.R., Gudur, B.K., 2014, ARP Spoof Detection System Using ICMP Protocol: An Active Approach, International Journal of Engineering Research and Technologi (IJERT), Vol 3.