

**LAPORAN PRAKTEK KERJA LAPANGAN  
MAC SECURITY NORTEL BASED PADA PT.PUPUK  
SRIWIDJAJA PALEMBANG**

Laporan ini diajukan untuk memenuhi persyaratan dalam matakuliah  
Kuliah Kerja Praktek(KKP)

**DI  
PT.PUPUK SRIWIDJAJA PALEMBANG**

Oleh

**R.M.ATTHORIQ**

**NIM :10142264**

**IMAM JAKA WIJAYA**

**NIM : 10142229**

**PROGRAM STUDI TEKNIK INFORMATIKA  
UNIVERSITAS BINA DARMA  
PALEMBANG  
2013**

**MAC SECURITY NORTEL BASED PADA PT PUPUK  
SRIWIDJAJA PALEMBANG**

**OLEH :**

**R.M.ATTHORIQ 10.142.264  
IMAM JAKA WIJAYA 10.142.229**

**LAPORAN PRAKTEK KERJA LAPANGAN**

Disusun sebagai syarat menyelesaikan Mata Kuliah Praktek Kerja Lapangan  
di Universitas Bina Darma

Disetujui,

Dosen Pembimbing



**Prihambodo Hendro Saksono ST.,M.Sc.,P.hd.**

Program Studi Teknik Informatika  
Universitas Binadarma,  
Ketua,



**Syahril Rizal, S.T.,M.M.,M.Kom.**

## *Motto*

*"Ketidaktahuan bukanlah penyakit, tetapi itu adalah kebiasaan,,  
dan kecerdasan bukanlah keuntungan tetapi merupakan sebuah prestasi "*

*Kupersembahkan Kepada :*

- *Allah SWT*
- *Kedua Orang tuaku yang selalu memberikan dukungan, motivasi dan doa*
- *Adik-adik ku tersayang.*
- *Jeman-temanku seperjuangan*
- *Almamaterku.*

**ABSTRAK**  
**Aplikasi Memo Permohonan Evaluasi Pengadaan Barang Berbasis PHP**  
**pada PT Pupuk Sriwidjaja Palembang**  
**Jalan. Mayor Zen, Palembang 30118 – INDONESIA**

---

**Bagus Apri Susandi**  
**Dayat Suhaimi**  
**Teknik Informatika**  
**Universitas Bina Darma**

Departemen IT terutama pada bagian IT infrastruktur jaringan pada PT. Pupuk Sriwidjaja Palembang menghadapi permasalahan, seringkali perangkat yang tidak dikenal mencoba mengakses LAN, Selama ini akses LAN pada PT Pusri tidak pembatasan, sehingga sering terjadi perangkat yang tidak dikenal mengakses LAN pada PT Pusri, dan melakukan hal-hal yang tidak diinginkan seperti Sniffing paket atau Pemutusan Koneksi secara Paksa.

Nortel merupakan perusahaan IT yang besar, Salah satu Produk keluaran Nortel adalah Switch.

Memanfaatkan Teknologi pada Switch keluaran Nortel dengan fitur Mac-Security dapat membatasi hak akses pada jaringan LAN PT Pusri Palembang. Mac-Security bekerja berdasarkan *Media Access Controler*(MAC), hanya MAC yang terdaftar pada Switch yang dapat mengakses jaringan LAN pada PT Pusri Palembang.

Berdasarkan Masalah diatas penulis maka Hipotesis sementara masalah tersebut adalah: untuk menanggulangi perangkat yang tidak diinginkan mengakses jaringan LAN pada PT Pusri, pembatasan akses pada LAN PT Pusri harus diterapkan m

Simpulan yang didapat adalah dengan diterapkannya Mac Security pada Switch Nortel yang ada pada pada PT. PUSRI PALEMBANG, jaringan LAN pada PT Pusri Palembang tidak terganggu dengan perangkat yang tidak dikenal yang mencoba masuk, dan juga dapat menghindari serangan-serangan seperti Paket Sniffing atau DNS Spoofing.

Kata Kunci :  
Mac Security Nortel, Nortel User Manual.

# KATA PENGANTAR

**Assalamu'alaikum Wr. Wb.**

Puji syukur penulis panjatkan atas kehadiran Allah SWT. atas segala rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan tugas laporan PKL ini. Laporan PKL yang berjudul “ **MAC SECURITY NORTEL BASED PADA PT PUPUK SRIWIDJAJA PALEMBANG**”.

Adapun maksud dari pembuatan laporan Kerja Praktek ini adalah sebagai persyaratan untuk mengakhiri Kerja Praktek di PT.Pupuk Sriwidjaja.

Pada kesempatan ini, Penulis menyampaikan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan segala kemudahan, derongan, bantuan baik moril maupun materil kepada penulis selama penyusunan Laporan Kerja Praktek ini.

Ucapan terima kasih penulis ditujukan kepada yang terhormat :

1. Orang tua dan semua keluarga saya yang telah bersedia memberikan doa dan dukungannya.,
2. Bapak Prof. Ir. H. Bochari Rachman, M.Sc. selaku Rektor Universitas Binadarma Palembang.
3. Bapak M.Izman Herdiansyah, M.M., Ph.D. selaku Dekan fakultas Ilmu Komputer Universitas Binadarma Palembang.
4. Bapak Syahril Rizal, S.T., M.M., M.Kom. selaku Ketua Program Studi Teknik Informatika Universitas Binadarma Palembang.

5. Bapak Prihambodo Hendro Saksono, ST., M.Sc., Ph.D selaku Pembimbing Laporan Praktik Kerja Lapangan di Universitas Binadarma Palembang.
6. PT.Pupuk Sriwidjaja Palembang yan telah bersedia menerima penulis dalam melaksanakan Kerja Praktek.
7. Diklat PT.Pupuk Sriwidjaja Palembang yang telah membantu penulis dalam melaksanakan Kerja Praktek.
8. Departement Teknologi Informasi yang telah memberi Tempat dan fasilitas kepada penulis dalam melaksanakan Kerja Praktek.
9. Bapak Muhammad Nur Hidayat selaku Pembimbing dalam melaksanakan Kerja Praktek di PT.Pupuk Sriwidjaja Palembang.
10. Seluruh Karyawan divisi Teknologi Informasi PT.Pupuk Sriwidjaja atas segala bantuan dan bimbingannya.
11. Semua pihak yang telah membantu penyelesaian Laporan Kerja Praktek ini.

Harapan penulis semoga Allah SWT membalas segala kebaikan pada semua pihak yang tersebut diatas.

Penulis sadar masih banyak kekurangan yang harus disempurnakan dalam penyusunan laporan Kerja Praktek ini.Akhir kata semoga laporan ini bermanfaat bagi semua pihak yang membutuhkan.

**Assalamu'alaikum Wr. Wb.**

Palembang , 15 Maret 2013

Penulis

# DAFTAR ISI

|                                    |            |
|------------------------------------|------------|
| <b>LEMBAR PENGESAHAN.....</b>      | <b>i</b>   |
| <b>MOTO &amp; PERSEMBAHAN.....</b> | <b>ii</b>  |
| <b>ABSTRAK.....</b>                | <b>iii</b> |
| <b>KATA PENGANTAR.....</b>         | <b>iv</b>  |
| <b>DAFTAR ISI.....</b>             | <b>vi</b>  |
| <b>DAFTAR GAMBAR.....</b>          | <b>ix</b>  |

## **BAB I PENDAHULUAN**

|                                       |   |
|---------------------------------------|---|
| 1.1 Latar Belakang.....               | 1 |
| 1.2 Rumusan Masalah.....              | 2 |
| 1.3 Tujuan dan Manfaat.....           | 3 |
| 1.3.1 Tujuan.....                     | 3 |
| 1.3.2 Manfaat.....                    | 3 |
| 1.4 Lokasi dan Waktu PKL.....         | 4 |
| 1.4.1 Lokasi PKL.....                 | 4 |
| 1.4.2 Waktu PKL.....                  | 4 |
| 1.5 Sistematik Penulisan Laporan..... | 4 |

## **BAB II LANDASAN TEORI**

|                                       |    |
|---------------------------------------|----|
| 2.1 Mac Address.....                  | 6  |
| 2.2 Mac Address Based Attacks.....    | 7  |
| 2.2.1 Mac Address Based Attack.....   | 7  |
| 2.2.2 Sniffing Paket.....             | 8  |
| 2.2.3 Arp Spoofing dan Netcut.....    | 10 |
| 2.3 Nortel.....                       | 11 |
| 2.3.1 Switch.....                     | 12 |
| 2.4 Paket Jaringan/Network Paket..... | 13 |

|                |    |
|----------------|----|
| 2.5 Putty..... | 14 |
|----------------|----|

### **BAB III TINJAUAN OBJEK**

|  |    |
|--|----|
| 3.1 Sejarah Singkat PT.Pusri Palembang.....              | 15 |
| 3.2 Visi dan Misi PT.Pusri Palembang.....                | 17 |
| 3.2.1 Visi PT.Pusri Palembang.....                       | 17 |
| 3.2.1 Misi PT.Pusri Palembang.....                       | 17 |
| 3.3 Struktur PT.Pusri Palembang.....                     | 17 |
| 3.4 Gambaran Teknologi Informasi PT.Pusri Palembang..... | 18 |
| 3.5 Bagan Wan dan Lan PT.Pusri Palembang.....            | 20 |
| 3.6 Bagan Server PT.Pusri Palembang.....                 | 21 |
| 3.7 Infrastruktur di PT.Pusri Palembang.....             | 22 |
| 3.8 Sistem-Sistem di PT.Pusri Palembang.....             | 23 |
| 3.9 Implementasi TI PT.Pusri Beberapa Tahun Depan.....   | 24 |

### **BAB IV HASIL DAN PEMBAHASAN**

|                                |    |
|--------------------------------|----|
| 4.1 Hasil.....                 | 25 |
| 4.2 Pembahasan.....            | 28 |
| 4.2.1 Status Mac Security..... | 28 |
| 4.2.2 Security List.....       | 29 |
| 4.2.3 Mac Address Table.....   | 30 |
| 4.2.4 Intrusion Detect.....    | 31 |
| 4.2.5 Intrusion Timer.....     | 32 |
| 4.2.6 Mac Filtering.....       | 32 |
| 4.2.7 Auto Learning.....       | 33 |
| 4.2.8 Status Port.....         | 34 |

**BAB V PENUTUP**

|                     |    |
|---------------------|----|
| 5.1 Kesimpulan..... | 35 |
| 5.2 Saran.....      | 36 |

**DAFTAR PUSTAKA**

**LAMPIRAN**

# DAFTAR GAMBAR

|  |           |
|--|-----------|
| <b>Gambar 2.1 MAC Address Format.....</b>                          | <b>6</b>  |
| <b>Gambar 2.2 Paket Sniffing.....</b>                              | <b>9</b>  |
| <b>Gambar 2.3 Nortel Networks.....</b>                             | <b>11</b> |
| <b>Gambar 2.4 Switch Keluaran Nortel Networks.....</b>             | <b>12</b> |
| <b>Gambar 3.3 Bagan LAN dan Wan di PT.PUSRI.....</b>               | <b>20</b> |
| <b>Gambar 3.4 Bagan Server PT.PUSRI.....</b>                       | <b>21</b> |
| <b>Gambar 4.1 Status Mac Security Pada Saat Disable.....</b>       | <b>28</b> |
| <b>Gambar 4.2 Status Mac Security pada Saat Enable.....</b>        | <b>28</b> |
| <b>Gambar 4.3 Daftar Security List.....</b>                        | <b>29</b> |
| <b>Gambar 4.4 Daftar Mac-Address-Table.....</b>                    | <b>30</b> |
| <b>Gambar 4.5 Status Intrusion Detect dan Intrusion Timer.....</b> | <b>32</b> |
| <b>Gambar 4.6 Status Mac Filtering.....</b>                        | <b>32</b> |
| <b>Gambar 4.7 Status Automatic Learning.....</b>                   | <b>33</b> |
| <b>Gambar 4.8 Status Pada Setiap Port.....</b>                     | <b>34</b> |

# BABI PENDAHULUAN

## 1.1 LATAR BELAKANG

Maraknya kejahatan cyberyang mengancam data perusahaan, menuntut perusahaan meningkatkan keamanan terhadap resiko kebocoran data. Salah satu kejahatan cyber yang marak saat ini adalah Sniffing, ARP spoofing, serta *pemutusankoneksi internet secara paksa* (netcut) demi melancarkan pembocoran data pada situasi normal, sewaktu komputer kita terhubung ke jaringan internet (browsing, download file, dll) komputer kita memerlukan nomor *Media Access Control* (MAC) , Walaupun tidak ada yang bertanya, *netcut* akan mengirimkan paket ARP berisi jawaban nomor MAC, hal yang sama terjadi pada sniffing, salah satu untuk menanggulangnya adalah dengan menggunakan *Mac filtering* untuk mengontrol MAC yang masuk.

Product Switch keluaran Nortel menyediakan fitur Mac-security yang berfungsi sebagai *control* MAC. Hanya MAC yang terdaftar yang dapat mengakses jaringan. Fitur ini dapat juga digunakan untuk mengkonfigurasi mode deteksi agar MAC dapat dikelola dengan baik serta meningkatkan keamanan data dari Snifing dan sejenisnya.

## **1.2 RUMUSAN MASALAH**

Berdasarkan latar belakang diatas, maka penulis merumuskan permasalahan dalam Laporan Praktek Kerja Lapangan ini yaitu bagaimana menciptakan keamanan MAC yang tepat demi mengamankan data dari paket sniffing atau sejenisnya.

## **1.3 TUJUAN DAN MANFAAT**

### **1.3.1 TUJUAN**

Tujuan Kerja Praktek di PT.PUSRI yaitu:

1. Memahami dan menganalisa konsep jaringan yang diterapkan di PT.Pusri
2. Mempelajari Konfigurasi pada Switch keluaran Nortel
3. Mengkonfigurasi dan merancang MAC-Security pada PT.PUSRI.

### **1.3.2 MANFAAT**

Dengan mengaktifkann MAC-Security switch Nortel, maka keamanan paket data dalam setiap pengiriman dapat aman dan mudah untuk dikelola MAC *addressnya*. Disamping itu jika terjadi penyadapan paket data, mode Mac-Security dapat di pilih sesuai keperluan. Ada tiga jenis mode yang dapat dipilih untuk merespon penyadapan paket data, yaitu :

1. Enable, jika mode enable dipilih maka apabila ada Mac address yang tidak terdaftar pada port masuk, maka port akan *shutdown* (mati) dalam jangka waktu tertentu.
2. Disable, jika mode disable dipilih, maka apabila ada Mac address yang tidak terdaftar pada port masuk maka port tidak akan mati, hanya saja Mac tersebut tidak dapat broadcast data.
3. Forever, sama halnya dengan mode enable, jika Mac yang tidak terdaftar pada port masuk, port tersebut akan mati, tapi port yang mati tersebut tidak akan bisa aktif kecuali diaktifkan secara manual.

## **1.4 LOKASI DAN WAKTU PKL**

### **1.4.1 LOKASI PKL**

Lokasi praktek kerja lapangan bertempat di PT.Pupuk Sriwidjaja Palembang yang beralamatkan di jalan Mayor Zen Palembang 30118.

### **1.4.2 WAKTU PKL**

Waktu pelaksanaan kerja praktek di PT.Pupuk Sriwidjaja Palembang selama 6 minggu kerja yang berlangsung antara tanggal 1 Februari 2013 sampai 31 Maret 2013. Dimulai pada pukul 07.30 WIB sampai dengan pukul 16.30 WIB kecuali pada hari Jumat di mulai pukul 07.30 WIB sampai dengan pukul 17.00 WIB.

## **1.5 SISTEMATIK PENULISAN LAPORAN**

Untuk memudahkan penyusunan laporan ini, penulis menggunakan sistematika penulisan yang bertujuan untuk mempermudah dalam penyusunan laporannya. Adapun sistematika laporan ini adalah sebagai berikut:

### **BAB I : PENDAHULUAN**

Berisikan latar belakang, rumusan masalah, tujuan dan manfaat, lokasi dan waktu PKL, sistematika penulisan laporan.

### **BAB II : LANDASAN TEORI**

Bab ini mengulas landasan teoritik yang berhubungan dengan penelitian yang akan dilakukan. Perlu ditegaskan bahwa bagian ini bukan hanya menampilkan definisi-definisi tetapi juga diskusi tentang apa yang menjadi tinjauan.

### **BAB III : TINJAUAN OBJEK**

Bab ini berisikan sejarah singkat perusahaan, visi dan misi perusahaan, struktur organisasi, kegiatan organisasi, membahas keadaan TIK secara umum.

### **BAB IV : HASIL DAN PEMBAHASAN**

Bab ini berisikan hasil-hasil penelitian serta pembahasan yang telah di lakukan.

### **BAB V : KESIMPULAN DAN SARAN**

Bab ini berisikan kesimpulan dari penelitian yang telah dilakukan dan saran yang di berikan untuk penelitian selanjutnya.

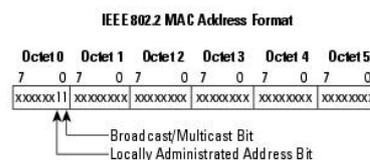
# BAB II

## LANDASAN TEORI

### 2.1 MAC ADDRESS

**MAC Address** (*Media Access Control address*) adalah alamat fisik suatu interface  jaringan  (seperti ethernet card pada komputer, interface/port pada router, dan node  jaringan  lain) yang bersifat unik dan berfungsi sebagai identitas perangkat tersebut. Secara umum **MAC Address** dibuat dan diberikan oleh pabrik pembuat NIC (Network Interface Card) dan disimpan secara permanen pada ROM (Read Only Memory) perangkat tersebut. **MAC address** juga biasa disebut *Ethernet Hardware Address (EHA)*, *Hardware Address*, atau *Physical Address*.

**MAC Address** memiliki panjang 48-bit (6 byte). **Format standard MAC Address** secara umum terdiri dari 6 kelompok digit yang masing-masing kelompok berjumlah 2 digit heksa desimal. masing-masing kelompok digit dipisahkan tanda (-) atau (:), misalnya 01-23-45-67-89-ab atau 01:23:45:67:89:ab.



**Gambar 2.1 MAC Address Format**

## **2.2 MAC ADDRESS ATTACKS**

### **2.2.1 MAC ADDRESS-BASED ATTACKS**

Serangan yang dilakukan dengan membanjiri *MAC address* (MAC flooding). Teknik yang dilakukan pada *MAC address flooding* yaitu si penyerang mengisi tabel CAM(*content addressable memory*) pada switch, dengan MAC address yang tidak valid.

Setelah tabel CAM penuh traffic yang address-nya tidak ada di tabel akan di-flood ke semua interface, efek yang ditimbulkan adalah meningkatnya beban(load) pada traffic dan meningkatnya traffic pada LAN. Kondisi ini dapat menyebabkan tabel CAM milik switch yang berdekatan mengalami *overflow*.

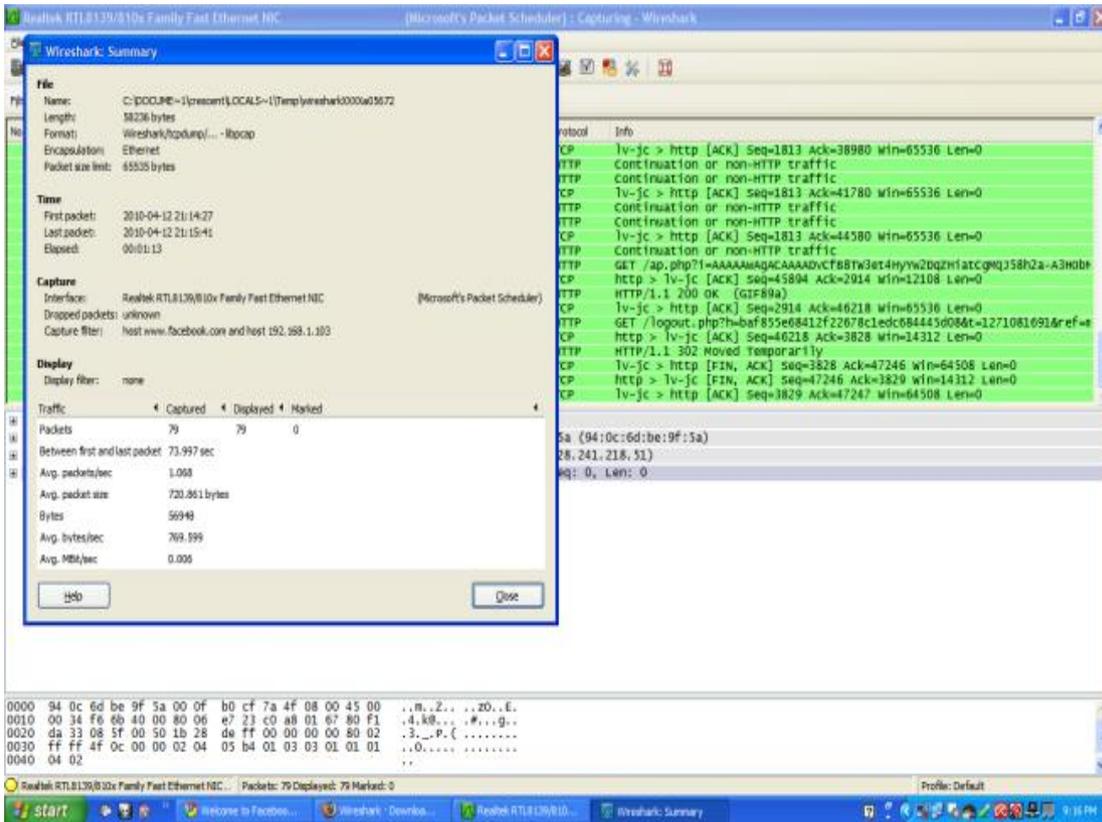
Untuk mengatasi atau mengurangi MAC address attack dapat digunakan teknik yang disebut Mac-Security.

### **2.2.2 SNIFFING PAKET**

*Sniffing* adalah kegiatan penyadapan pada lalu lintas data di jaringan komputer. Contohnya apabila anda pemakai komputer yang terhubung dengan suatu jaringan dikantor. saat melakukan pengiriman email ke teman anda atau rekan anda yang berada diluar kota maka email tersebut akan dikirimkan dari komputer anda trus melewati jaringan komputer kantor anda (mungkin server atau gateway internet), trus keluar dari kantor melalui jaringan internet, lalu akan sampai diinbox email teman anda. Pada saat email tersebut melalui jaringan komputer kantor itulah *sniffing* bisa dilakukan. sniffing bisa dilakukan oleh administrator jaringan yang mengendalikan server, atau oleh pemakai komputer

lain yang terhubung pada jaringan komputer, Sangat berbahaya apabila isi email tersebut ternyata penting. *sniffing* dibagi menjadi 2 bagian :

1. Passive sniffing adalah suatu kegiatan penyadapan tanpa merubah data atau paket apapun di jaringan. paket sniffing yang umumnya dilakukan yaitu pada Hub, hal ini disebabkan karena prinsip kerja hub yang hanya bertugas meneruskan signal ke semua komputer (broadcast). berbeda dengan switch yang mempunyai cara untuk menghindari collision atau bentrokan yang terjadi pada hub dengan membaca MAC address komputer. Beberapa program yang umumnya digunakan untuk melakukan aktifitas ini yaitu wireshark, Cain-Abel, dsb.
2. Active sniffing adalah kegiatan sniffing yang dapat melakukan perubahan paket data dalam jaringan agar bisa melakukan sniffing, active sniffing dengan kata lain merupakan kebalikan dari passive sniffing. Active sniffing umumnya dilakukan pada Switch, hal ini di dasar karena perbedaan prinsip kerja antara Hub dan Switch, seperti yang dijelaskan di atas. Active sniffing yang paling umum dilakukan adalah ARP Poisoning, Man in the middle attack (MITM).



**Gambar 2.2 Paket yang di Sniffing**

### 2.2.3 ARP SPOOFING DAN NETCUT

Pada situasi normal, sewaktu komputer kita terhubung ke jaringan untuk berinternet ria (browsing internet, download file, dll) komputer kita memerlukan nomor Media Access Control (MAC) router/modem internet.

Jadi yang dilakukan oleh komputer anda adalah sebagai berikut:

1. Mengirimkan paket ARP berisi pertanyaan tentang nomor MAC crouter/modem.
2. Menerima paket ARP berisi jawaban dari router/modem tentang nomor MAC dirinya.

3. Mengirimkan paket data dengan menggunakan nomor MAC yang didapat sebagai tujuan.

Netcut mengganggu proses ini dengan cara sbb:

1. Walaupun tidak ada yang bertanya, netcut akan mengirimkan paket ARP berisi jawaban nomor MAC router/modem (tentunya nomor MACnya adalah nomor MAC komputer yang menjalankan netcut)
2. Komputer anda menerima informasi palsu tentang nomor MAC router dan dengan polosnya percaya saja
3. Pada saat komputer anda mau mengirimkan data ke internet, nomor MAC yang digunakan bukan lagi nomor MAC router/modem melainkan nomor MAC komputer netcut.

## **2.3 NORTEL**

**Nortel Networks** (disingkat **Nortel** NYSE: NT) adalah sebuah perusahaan telekomunikasi multi-nasional yang berkantor pusat di Toronto, Kanada. Salah satu perangkatnya adalah Switch.

Kini Nortel Networks telah diambil oleh **Avaya**. **Avaya** berdiri sebagai perusahaan mandiri pada 2 Oktober 2000. Sebelumnya Avaya menjadi bagian dari **Western Electric, ATT, dan Lucent Technologies**. Setelah mandiri, avaya memulai bisnisnya pada New York Stock Exchange dengan menggunakan symbol AV.



**Gambar 2.3 Nortel Networks**

### **2.3.1 SWITCH**

Sebuah alat jaringan yang melakukan penjembutan taktampak (penghubung penyekatan (*segmentation*) banyak jaringan dengan pengalihan berdasarkan alamat MAC).

Switch jaringan dapat digunakan sebagai penghubung komputer atau penghala pada satu area yang terbatas, pengalih juga bekerja pada lapisan taut data (*data link*), cara kerja pengalih hampir sama seperti jembatan (*bridge*), tetapi switch memiliki sejumlah porta sehingga sering dinamakan jembatan pancaporta (*multi-port bridge*).



**Gambar 2.4 Switch Keluaran Nortel Networks**

## 2.4 PAKET JARINGAN/NETWORK PAKET

Paket jaringan atau network packet adalah satuan informasi dasar yang dapat ditransmisikan di atas jaringan atau melalui saluran komunikasi digital. Sebuah paket berisi *packet header* yang berisi informasi mengenai protokol tersebut (informasi mengenai jenis, sumber, tujuan, atau informasi lainnya), data yang hendak ditransmisikan yang disebut dengan *data payload*, dan *packet trailer* yang bersifat opsional. Sebuah paket memiliki struktur logis yang dibentuk oleh protokol yang digunakannya. Ukuran setiap paket juga dapat bervariasi, tergantung struktur yang dibentuk oleh arsitektur jaringan yang digunakan. Paket jaringan juga dapat disebut datagram, frame, atau cell.

Jika dilihat dari perspektif model tujuh lapis *Open Systems Interconnection* (OSI), istilah packet dan frame memiliki definisi yang jauh berbeda. Sebuah paket merupakan "amplop elektronik" yang mengandung informasi yang dibentuk pada lapisan 3 hingga lapisan 7 dari model tujuh lapis OSI tersebut, sementara sebuah *frame* adalah "amplop elektronik" yang mengandung informasi mengenai paket dan informasi lainnya dari semua lapisan dari tujuh lapisan OSI.

### 3.6 PuTTY

**PuTTY** adalah sebuah program klien untuk protokol jaringan SSH, Telnet, dan Rlogin. Semua protokol ini digunakan untuk menjalankan sebuah remote session pada sebuah komputer, menggunakan sebuah jaringan.

**PuTTY** mengimplementasikan client end pada session tersebut: end di mana session tersebut ditampilkan, bukan end di mana ia berjalan. Contoh sederhananya: jalankan **PuTTY** pada sebuah mesin Windows, dan beri perintah kepadanya untuk terhubung dengan (sebagai contoh) sebuah mesin Unix.

**PuTTY** membuka sebuah window. Lalu, apa pun yang diketik di dalam window itu akan dikirim langsung ke mesin Unix, dan segala sesuatu yang mesin Unix kirim kembali ditampilkan di window. Jadi saat bekerja pada mesin Unix terlihat seolah-olah pengguna sedang duduk pada konsolnya, padahal sebenarnya sedang duduk di tempat lain.

# **BAB III**

## **TINJAUAN OBJEK**

### **3.1 SEJARAH SINGKAT PT.PUSRI PALEMBANG**

PT Pupuk Sriwidjaja Palembang merupakan anak perusahaan dari PT Pupuk Indonesia (Persero) yang merupakan Badan Usaha Milik Negara (BUMN) . PT Pupuk Sriwidjaja Palembang menjalankan usaha di bidang produksi dan pemasaran pupuk. Perusahaan juga dikenal dengan sebutan PT Pusri ini, diawali didirikannya Perusahaan Pupuk pada tanggal 24 Desember 1959 adalah pencetus pertama pupuk urea di Indonesia. Sriwidjaja sebagai nama perusahaan untuk mengabadikan sejarah kejayaan Kerajaan Sriwijaya di Palembang, Sumatera Selatan yang sangat dihormati di Asia Tenggara hingga daratan Cina.

Tanggal 14 Agustus 1961 merupakan tonggak penting sejarah berdirinya Pusri, karena pada saat itu dimulai pembangunan pabrik pupuk pertama kali yang dikenal dengan Pabrik Pusri I. Pada tahun 1963, Pabrik Pusri I mulai berproduksi dengan kapasitas terpasang sebesar 100.000 ton urea dan 59.400 ton amonia per tahun. Seiring dengan kebutuhan pupuk yang terus meningkat, maka selama periode 1972-1977, perusahaan telah membangun sejumlah pabrik Pusri II, Pusri III, dan Pusri IV. Pabrik Pusri II memiliki kapasitas terpasang 380.000 ton per tahun. Pada tahun 1992 Pabrik Pusri II dilakukan proyek optimalisasi urea

menjadi 552.000 ton per tahun. Pusri III yang dibangun pada 1976 dengan kapasitas terpasang 570.000 ton per tahun. Sedangkan pabrik urea Pusri IV dibangun pada tahun 1977 dengan kapasitas sebesar 570.000 ton per tahun. Upaya peremajaan, peningkatan kapasitas produksi pabrik dilakukan dengan membangun pabrik pupuk urea Pusri IB bermuatan 570.000 ton per tahun menggantikan pabrik Pusri I yang dihentikan operasinya karena alasan usia dan tingkat efisiensi yang menurun.

Pada tahun 1979, PT Pusri diberikan tugas oleh Pemerintah melaksanakan distribusi dan pemasaran pupuk bersubsidi kepada petani sebagai bentuk pelaksanaan Public Service Obligation (PSO) untuk mendukung program pangan nasional dengan memprioritaskan produksi dan pendistribusian pupuk bagi petani di seluruh wilayah Indonesia.

Pada tahun 1997, Pusri dipilih sebagai perusahaan pusat membawahi empat BUMN yang bergerak di bidang industri pupuk dan petrokimia, yaitu PT Petrokimia Gresik di Gresik, Jawa Timur; PT Pupuk Kujang di Cikampek, Jawa Barat.

PT Pupuk Kaltim di Bontang, Kalimantan Timur; dan PT Pupuk Iskandar Muda di Lhokseumawe, NAD, serta BUMN yang bergerak di bidang engineering, procurement & construction (EPC), yaitu PT Rekayasa Industri (berkantor di Jakarta). Pada tahun 1998, anak perusahaan Pusri bertambah satu BUMN lagi, yaitu PT.Mega Eltra di Jakarta di bidang perdagangan.

Pada tahun 2010 dilakukan Pemisahan (Spin Off) dari PT Pupuk Indonesia (Persero) (saat itu masih bernama PT. Pupuk Sriwidjaja (Persero)) kepada PT

Pupuk Sriwidjaja Palembang serta telah terjadinya pengalihan hak dan kewajiban PT Pupuk Indonesia (Persero) kepada PT Pupuk Sriwidjaja Palembang sebagaimana tertuang didalan RUPS-LB tanggal 24 Desember 2010 yang berlaku efektif 1 Januari 2011. Spin Off ini tertera pada Perubahan Anggaran Dasar PT Pupuk Sriwidjaja Palembang melalui Akte Notaris Fathiah Helmi SH nomor 14 tanggal 12 November 2010 yang telah disahkan oleh Menteri Hukum dan HAM tanggal 13 Desember 2010 nomor AHU57993.AH.01.01 tahun 2010.

### **3.2 VISI DAN MISI PT.PUSRI PALEMBANG**

#### **3.2.1 VISI PT.PUSRI PALEMBANG**

Berusaha Menjadi Perusahaan Pupuk Terkemuka Tingkat Regional

#### **3.2.2 MISI PT.PUSRI PALEMBANG**

Memproduksi, memasarkan pupuk dan produk agribisnis secara efisien, berkualitas prima dan memuaskan pelanggan.

### **3.3 STRUKTUR PT.PUPUK SRIWIDJAJA PALEMBANG**

Bentuk badan usaha PT Pupuk Sriwidjaja Palembang adalah Perseroan Terbatas (PT) maka struktur Organisasi dipimpin oleh Direksidan diawasi oleh Dewan Komisaris yang ditetapkan oleh Menteri keuangan selaku pemegang saham. Struktur organisasi PT Pupuk Sriwidjaja Palembang terbagi dalam enam Direktorat utama: Produksi, Keuangan, Teknik, Perakayasa, Komersial dan Litbank .

### **3.4 GAMBARAN IT PT.PUSRI**

#### **1972-1980 (Dekade I)**

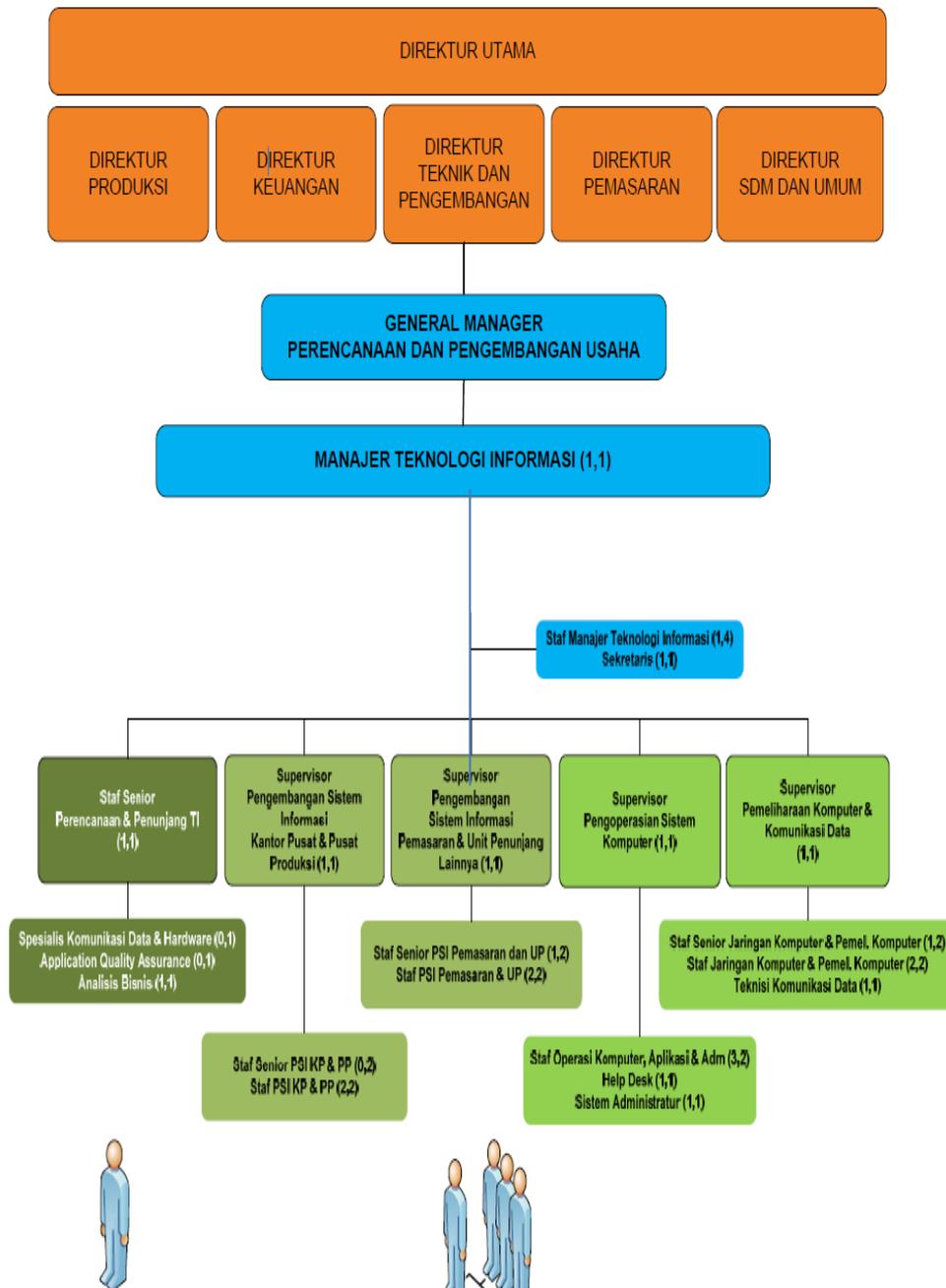
Penerapan Financial Reporting System (FRS) dengan mesin IBM 370/138 (Batch System).

#### **1980-1999 (Dekade II-III)**

Batch System ke terminal system FM-80, HP-FM dengan mesin HP-3000-947 yang bisa melayani keuangan di daerah dan anak perusahaan, penggunaan mesin mainframe, pengembangan aplikasi secara modular. Penggunaan peralatan kontrol berbasis komputer untuk operasi pabrik, penggunaan LAN untuk PMIS (Plant Management Informatin System) yang digunakan memonitor operasional pabrik secara remote.

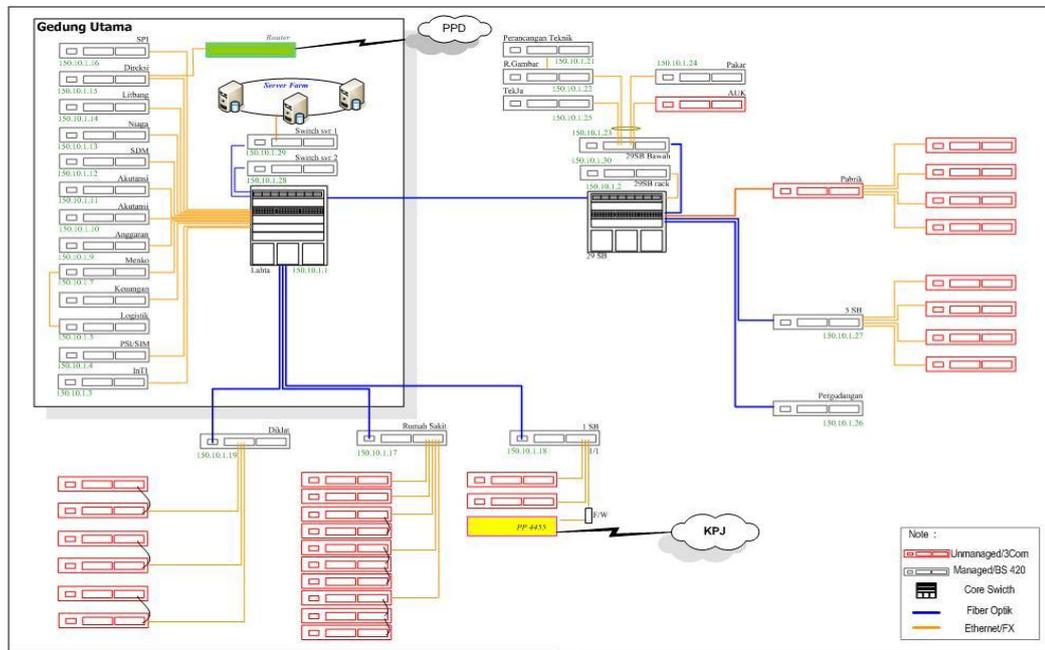
#### **2000-2009 (Dekade IV)**

Dipicu dari Y2K, Pusri mulai mengimplementasi ERP IFS, komunikasi data berbasis IP, aplikasi berbasis web dan data mobile, serta pengembangan aplikasi holding. Memanfaatkan data operasi pabrik untuk mendapatkan informasi kondisi peralatan, distribusi data evaluasi laboratorium.



**Gambar 3.2 Struktur Organisasi Departemen TI PT.PUSRI**

### 3.5 BAGAN WAN DAN LAN PT.PUSRI PALEMBANG



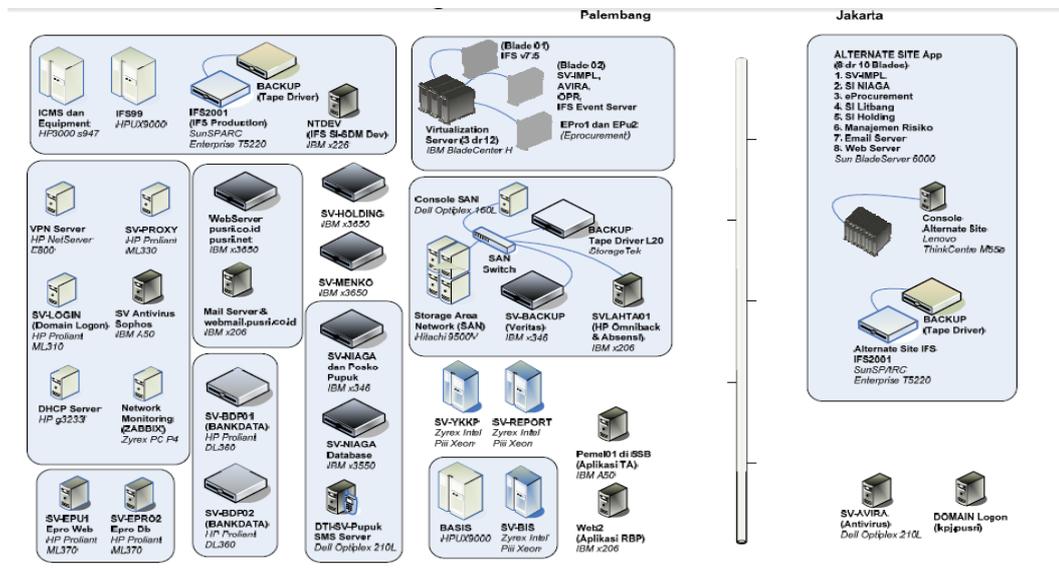
Gambar 3.3 Bagan LAN dan Wan di PT.PUSRI

Topologi jaringan WAN dan LAN PT.Pusri pada *Layer Access* menggunakan kabel Fiber Optic, dikarenakan Fiber Optic memiliki kecepatan yang baik melebihi kabel UTP CAT 6 yang kecepatannya hanya 1GB.

Layer distribusi menggunakan Switch Nortel yang keamanan tidak kalah dari Cisco, dan harganya sedikit lebih murah dari Cisco untuk menghemat biaya. Selain itu, jaringan pada PT.Pusri telah menggunakan VLAN(*virtual LAN*) agar terorganisir dengan baik.

PT.Pusri menggunakan ISP(*Internet Service Provider*) dari Telkom, WAN PT.Pusri menggunakan IP VPN(*Virtual Private Network*) dari Lintas arta untuk menghubungkan jaringan kantor pusan Palembang ke PPD dan kantor perwakilan di Jakarta.

### 3.6 BAGAN SERVER PT.PUSRI PALEMBANG



**Gambar 3.4 Bagan Server PT.PUSRI**

PT.Pusri memiliki banyak server seperti Mail Server(@Pusri.net),Proxy server untuk membatasi akses ke situs-situs tertentu,Web Server (www.Pusri.net), VPN Server, yang terbaru adalah Blade Server yang berguna sebagai Virtualisasi untuk beberapa server demi meminimalisir perangkat keras yang digunakan, dan masih banyak lagi Server lainnya.

Semua data terbackup dengan rapi pada Tape Driver yang kemudian disimpan di SAN (*Storage Area Network*), SAN pada PT.Pusri menggunakan merek Hitachi 9500V, dan keamanannya terjaga dengan baik.

### **3.7 INFRASTRUKTUR DI PT PUSRI**

#### **Hardwares :**

1. Komputer SUN-FIRE T-5220 Memory 8 Gb, Processor 1,2Gb, Harddisk 4 (146Gb).
2. Storage Area Network (SAN) dengan memory 1 Tera-byte (1 TB)
3. Back Up SAN
4. Beberapa Server (SI, eMail, Proxy, dll-nya)
5. Personal Komputer

#### **Data Communication :**

1. LAN Kantor Pusat Palembang
2. FDDI (Fiber Optic) sampai ke area pabrik
3. LAN PPJ / PPD
4. WAN Palembang – Jakarta – PPD
5. VPN IP (Virtual Private Network - IP) : 12 PPD, 1 UPP

#### **DATA BASE, SISTEM OPERASI :**

1. Database : Oracle, MSSQL Server dan MySQL
2. Sistem Operasi : Unix, MS Windows, Linux, SUN
3. Solaris 10.0
4. Aplikasi yang bersifat networking:
  - INTRANET / INTERNET (Website)
  - E-mail, Forum

### **3.8 SISTEM-SISTEM PADA PT.PUSRI**

Sistem- sampai dengan saat ini proses bisnis perusahaan yang memanfaatkan TI/SI meliputi :

#### **1. ERP**

- IFS (Industrial Financial System), Swedia
- Modul : FIN, MAINT, PROC HR

#### **2. Produksi**

- Modul PHP (Perhitungan Hasil Produksi), Laboratorium, Morning News dan e-LogSheet)
- Kerja sama dengan ITB, Bandung

#### **3. Distribusi dan Pemasaran**

- Modul Operasional Pemasaran dan Akuntansi & Keuangan
- Dikembangkan internal PT Pusri

#### **4. E-Auction / E-Procurement, sejak 2005**

- Dikembangkan dengan pihak ketiga

#### **5. IFS Project**

#### **6. Anggaran**

- Dikembangkan secara internal
- Modul Preparation, Simulation, Analisis

#### **7. SI Bank Data (data warehouse)**

- Dikembangkan dengan pihak ketiga

### **3.9 IMPLEMENTASI PT.PUSRI BEBERAPA TAHUN KEDEPAN**

1. Peralihan pengadaan komputer sewa dari PC + Monitor CRT ke PC MonitorLCD (*300unit PC per tahun*)
  - Hemat listrik dan ramah lingkungan.
  - Kepemilikan PC ada di tangan pemberi sewa
2. Migrasi dari Server yang pemakaian prosessornya rendah ke Lingkungan Virtualisasi
  - Konsumsi listrik ruang server dapat dikurangi
  - Ruang server lebih lega.
  - Penanganan Maintenance Server dapat lebih cepat diatasi
3. Penyeragaman Komunikasi antar cabang di daerah menggunakan VPN-IP.
  - IP Based PABX dan atau pemanfaatan VoIP untuk komunikasi voice dan data.
  - Memungkinkan Monitoring Jaringan Komunikasi Data secara visual
4. Pembangunan Sistem Informasi KM, Office Automation dan Virtualisasi akan meningkatkan penyimpanan berkas digital sehingga membutuhkan Storage yang berkapasitas besar : Storage Area Network >2Terrabyte

# BAB IV

## HASIL DAN PEMBAHASAN

### 4.1 HASIL

Dari kerja praktek di PT. Pupuk Sriwidjaja Palembang dari tanggal 1 Februari 2013 sampai 31 Maret 2013, Diperoleh hasil sebagai berikut :

- Untuk menghasilkan suatu keamanan yang baik , terhindar dari penyadapan data dan sebagainya. Kami mahasiswa Universitas Binadarama, perlu mengimplementasikan *Mac security* pada switch keluaran Nortel.

MAC Security berfungsi untuk menyaring Mac yang masuk untuk melakukan *broadcast* data dan dapat menyaring alamat sumber MAC (SA = *source address*).

Keamanan yang tersedia pada beberapa switch tingkat tinggi ini, hanya akan mengizinkan perangkat dengan alamat MAC yang sudah pasti untuk terkoneksi ke port switch, dan dalam kasus mesin tidak dikenali, switch akan mengambil aksi memperingatkan administrator dengan perangkat SNMP atau mematikan port yang salah secepatnya.

Implementasi security pada *OSI Layer 2* dilakukan berdasarkan *MAC-Address*. Kadang-kadang kita jumpai sebuah kasus di mana kita ingin

mengamankan sebuah port pada switch hanya untuk kepentingan seseorang, peralatan atau keperluan tertentu. Mengapa perlu diamankan ? Karena mungkin port switch tersebut hanya boleh digunakan untuk peralatan dengan MAC-Address tertentu, sehingga apabila ada seseorang yang berusaha ingin menggunakan port switch tersebut tidak akan dapat terkoneksi.

Adapun software remote yang digunakan untuk mengkonfigurasi Mac-security Switch keluaran Nortel pada PT.PUSRI yaitu :

1. *Putty*

**PuTTY** adalah sebuah program klien untuk protokol jaringan *SSH*, *Telnet*, dan *Rlogin*. Semua protokol ini digunakan untuk menjalankan sebuah remote *session* pada sebuah komputer, menggunakan sebuah jaringan.

**PuTTY** mengimplementasikan client end pada session tersebut: end di mana session tersebut ditampilkan, bukan end di mana ia berjalan. Contoh sederhananya: jalankan **PuTTY** pada sebuah mesin Windows, dan beri perintah kepadanya untuk terhubung dengan (sebagai contoh) sebuah mesin Unix.

**PuTTY** membuka sebuah window. Lalu, apa pun yang diketik di dalam window itu akan dikirim langsung ke mesin Unix, dan segala sesuatu yang mesin Unix kirim kembali ditampilkan di window. Jadi, saat bekerja pada mesin Unix terlihat seolah-olah pengguna sedang duduk pada konsolnya, padahal sebenarnya sedang duduk di tempat lain.

**PuTTY** adalah sebuah program klien untuk protokol jaringan SSH, Telnet, dan Rlogin. Semua protokol ini digunakan untuk menjalankan sebuah remote session pada sebuah komputer, menggunakan sebuah jaringan.

**PuTTY** mengimplementasikan client end pada session tersebut: end di mana session tersebut ditampilkan, bukan end di mana ia berjalan. Contoh sederhananya: jalankan **PuTTY** pada sebuah mesin Windows, dan beri perintah kepadanya untuk terhubung dengan (sebagai contoh) sebuah mesin Unix.

**PuTTY** membuka sebuah window. Lalu, apa pun yang diketik di dalam window itu akan dikirim langsung ke mesin Unix, dan segala sesuatu yang mesin Unix kirim kembali ditampilkan di window. Jadi, saat bekerja pada mesin Unix terlihat seolah-olah pengguna sedang duduk pada konsolnya, padahal sebenarnya sedang duduk di tempat lain.

## 2. *Hyper Terminal*

Hyper Terminal digunakan untuk komunikasi data melalui serial com port atau TCP/IP winsock. Sayangnya pada Windows 7 sudah tidak ditemukan lagi, padahal masih banyak diantara kita yang masih membutuhkannya, bukanlah sebuah solusi kalau sampai harus men\_downgrade lagi komputer ke Windows XP.

## 4.2 PEMBAHASAN

### 4.2.1 STATUS MAC SECURITY

Langkah awal untuk mengkonfigurasi Mac security adalah melihat status Mac security, kemudian aktifkan Mac security jika belum aktif dengan perintah pada gambar 4.1 dan 4.2

```
2526T>ena
2526T#show mac-
2526T#show mac-security config
MAC Address Security: Disabled
MAC Address Security SNMP-Locked: Disabled
Partition Port on Intrusion Detected: Disabled
DA Filtering on Intrusion Detected: Disabled
Generate SNMP Trap on Intrusion: Disabled
MAC Auto-Learning Age-Time: 1 minutes
Current Learning Mode: Disabled
Learn by Ports: NONE
2526T#
```

Gambar 4.1 Status Mac Security Pada Saat Disable

```
2526T#conf t
Enter configuration commands, one per line. End with CNTL/Z.
2526T(config)#mac-se
2526T(config)#mac-security enable
2526T(config)#int fa1
2526T(config-if)#mac-se
2526T(config-if)#mac-security enable
2526T(config-if)#^Z

2526T#
2526T#show mac-security config
MAC Address Security: Enabled
MAC Address Security SNMP-Locked: Disabled
Partition Port on Intrusion Detected: Disabled
DA Filtering on Intrusion Detected: Disabled
Generate SNMP Trap on Intrusion: Disabled
MAC Auto-Learning Age-Time: 1 minutes
Current Learning Mode: Disabled
Learn by Ports: NONE
2526T#
```

Gambar 4.2 Status Mac Security pada Saat Enable

### 4.2.2 Security List

Security List berfungsi memasukan daftar port pada daftar keamanan, jumlah Security List 1 sampai dengan 32 Security Lis, perintah dari Security List adalah

2526T (config)#mac-security security-list <1-32>

```
2526T>ena
2526T#conf t
Enter configuration commands, one per line. End with CNTL/Z.
2526T(config)#mac-security enable
2526T(config)#mac-security security-list 1 add 1
2526T(config)#exit
2526T#Show mac-security security-list
Security List 1: 1
Security List 2: NONE
Security List 3: NONE
Security List 4: NONE
Security List 5: NONE
Security List 6: NONE
Security List 7: NONE
Security List 8: NONE
Security List 9: NONE
Security List 10: NONE
Security List 11: NONE
Security List 12: NONE
Security List 13: NONE
Security List 14: NONE
Security List 15: NONE
Security List 16: NONE
Security List 17: NONE
Security List 18: NONE
Security List 19: NONE
Security List 20: NONE
Security List 21: NONE
Security List 22: NONE
Security List 23: NONE
Security List 24: NONE
Security List 25: NONE
Security List 26: NONE
Security List 27: NONE
Security List 28: NONE
Security List 29: NONE
Security List 30: NONE
Security List 31: NONE
Security List 32: NONE
2526T#
```

**Gambar 4.3 Daftar Security List**

### 4.2.3 MAC ADDRESS TABLE

Mac address table adalah tabel Mac address yang terdaftar pada Mac Security, Tanpa adanya pendaftaran maka Mac security tidak akan berfungsi, adapun perintah dari Mac Address Table yaitu :

```
mac-security mac-address-table address <H.H.H.> {port<portlist>|security-list
<1-32>}
```

```
-----
2526T#conf t
Enter configuration commands, one per line. End with CNTL/Z.
2526T(config)#mac-security mac-address-table address 54-04-A6-4B-75-E0 securit$
2526T(config)#exit
2526T#show mac-security mac-address-table
Number of addresses: 1

Unit Port Allowed MAC Address Automatic
-----
Security List Allowed MAC Address Automatic
-----
1          54-04-A6-4B-75-E0 No
2526T#~
```

**Gambar 4.4 Daftar Mac-Address-Table**

#### 4.2.4 INTRUSION DETECT

Intrusion detect berfungsi sebagai mode security yang akan digunakan, mode security tersebut ada 3 bagian yaitu :

1. *Enable*

Apabila ada Mac address yang mencoba masuk pada port tertentu tetapi Mac tersebut tidak terdaftar pada Mac security Mac address table maka port tersebut akan mati dalam jangka waktu tertentu. Untuk perintah Intrusion detect yaitu :

```
2526T(config)#intrusion-detect enable
```

2. *Disable*

Sedikit berbeda dengan mode Enable, mode disable apabila ada Mac yang mencoba masuk port tidak akan mati, namun Mac tersebut tidak dapat membroadcast atau tidak dapat terkoneksi.

```
2526T(config)#intrusion-detect disable
```

3. *Forever*

Hampir sama dengan mode Enable, Mac yang tidak terdaftar mencoba masuk, Mac tersebut akan mati, pada mode ini Mac tidak dibatasi waktu tertentu untuk aktif kembali namun selamanya, selamanya tidak diaktifkan secara manual.

```
2526T(config)#intrusion-detect forever
```

#### 4.2.5 INTRUSION TIMER

Intrusion timer berfungsi untuk memberikan tenggang waktu pada mode Enable, apabila tenggang waktu habis maka port akan aktif kembali. Intrusion Timer ini memiliki satuan Seconds. Adapun perintah dari Intrusion timer yaitu :

```
2526T(config)#intrusion-timer <1-65535>
```

```
2526T>ena
2526T#show mac-security config
MAC Address Security: Enabled
MAC Address Security SNMP-Locked: Disabled
Partition Port on Intrusion Detected: Disabled
DA Filtering on Intrusion Detected: Disabled
Generate SNMP Trap on Intrusion: Disabled
MAC Auto-Learning Age-Time: 1 minutes
Current Learning Mode: Disabled
Learn by Ports: NONE
2526T#
```

**Gambar 4.5 Status Intrusion Detect dan Intrusion Timer**

#### 4.2.5 MAC FILTERING

Mac Filtering berfungsi apabila melakukan Mac security tanpa mode maka Mac Filteringla yang diaktifkan.

```
2526T(Config)#Mac-security filtering enable
```

```
2526T(config)#mac-security filtering enable
2526T(config)#exit
2526T#show mac-security config
MAC Address Security: Enabled
MAC Address Security SNMP-Locked: Disabled
Partition Port on Intrusion Detected: Disabled
DA Filtering on Intrusion Detected: Enabled
Generate SNMP Trap on Intrusion: Disabled
MAC Auto-Learning Age-Time: 1 minutes
Current Learning Mode: Disabled
Learn by Ports: NONE
2526T#
```

**Gambar 4.6 Status Mac Filtering**

#### 4.2.6 AUTOMATIC LEARNING

Automatic learning berfungsi untuk membaca Mac yang sedang terkoneksi ke switch dengan tenggang waktu tertentu, secara otomatis Mac yang sedang terkoneksi pada Switch akan terbaca dan juga untuk maximum Max yang masuk pada Mac address table bisa disetting. Perintah automatic learning dan setting waktunya yaitu:

```
2526T(config)#int fa1
```

```
2526T(config-if)#mac-security auto-learning port 1 max-add 10
```

```
2526T(config-if)#mac-security auto-learning port 1 enable
```

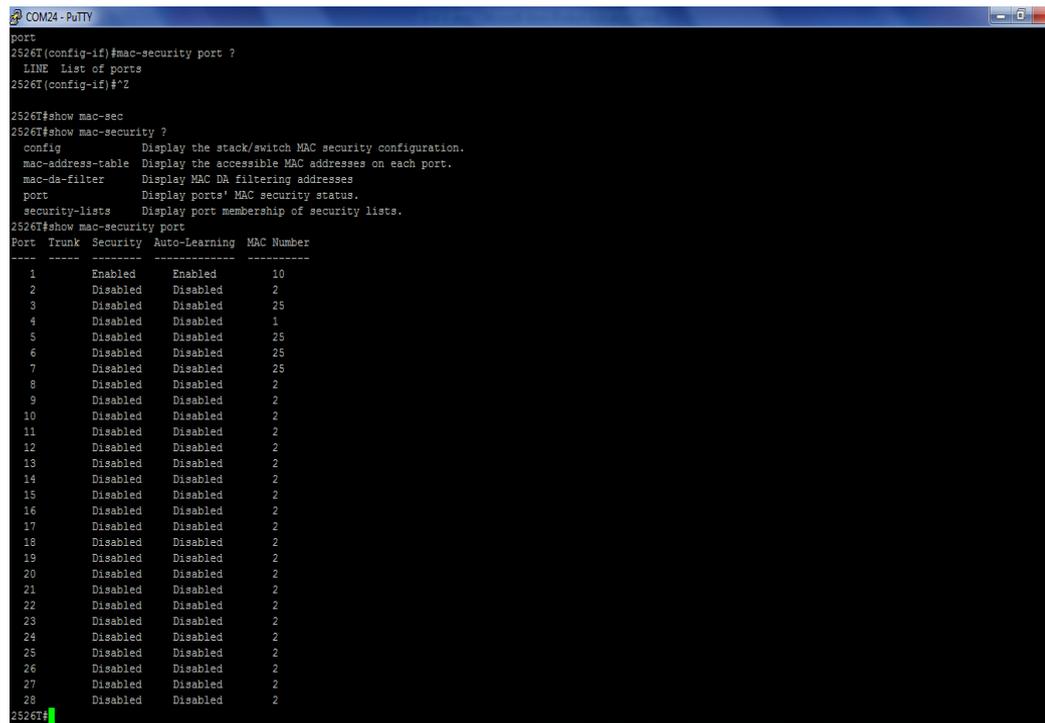
```
2526T(config)#mac-security auto-learning aging-time 60
```

```
2526T#show mac-security config
MAC Address Security: Enabled
MAC Address Security SNMP-Locked: Disabled
Partition Port on Intrusion Detected: Disabled
DA Filtering on Intrusion Detected: Enabled
Generate SNMP Trap on Intrusion: Disabled
MAC Auto-Learning Age-Time: 60 minutes
Current Learning Mode: Disabled
Learn by Ports: NONE
2526T#
```

**Gambar 4.7 Status Automatic Learning**

## 4.2.7 STATUS PADA SETIAP PORT

Pada setiap port memiliki keterangan seperti Security, Auto-Learning dan jumlah Mac yang dapat terdaftar dalam setiap port.



```
COM24 - PuTTY
port
2526T(config-if)#mac-security port ?
LINE List of ports
2526T(config-if)#^Z

2526T#show mac-sec
2526T#show mac-security ?
config          Display the stack/switch MAC security configuration.
mac-address-table Display the accessible MAC addresses on each port.
mac-da-filter   Display MAC DA filtering addresses
port           Display ports' MAC security status.
security-lists  Display port membership of security lists.
2526T#show mac-security port
Port  Trunk  Security  Auto-Learning  MAC Number
-----
1      Enabled  Enabled    Enabled         10
2      Disabled Disabled   Disabled        2
3      Disabled Disabled   Disabled       25
4      Disabled Disabled   Disabled        1
5      Disabled Disabled   Disabled       25
6      Disabled Disabled   Disabled       25
7      Disabled Disabled   Disabled       25
8      Disabled Disabled   Disabled        2
9      Disabled Disabled   Disabled        2
10     Disabled Disabled   Disabled        2
11     Disabled Disabled   Disabled        2
12     Disabled Disabled   Disabled        2
13     Disabled Disabled   Disabled        2
14     Disabled Disabled   Disabled        2
15     Disabled Disabled   Disabled        2
16     Disabled Disabled   Disabled        2
17     Disabled Disabled   Disabled        2
18     Disabled Disabled   Disabled        2
19     Disabled Disabled   Disabled        2
20     Disabled Disabled   Disabled        2
21     Disabled Disabled   Disabled        2
22     Disabled Disabled   Disabled        2
23     Disabled Disabled   Disabled        2
24     Disabled Disabled   Disabled        2
25     Disabled Disabled   Disabled        2
26     Disabled Disabled   Disabled        2
27     Disabled Disabled   Disabled        2
28     Disabled Disabled   Disabled        2
2526T#
```

Gambar 4.8 Status Pada Setiap Port

# **BAB V**

## **PENUTUP**

### **5.1 KESIMPULAN**

Dari hasil penelitian yang telah dilakukan oleh penulis pada PT.Pupuk Sriwidjaja Palembang dapat disimpulkan bahwa :

1. Mac Security sangatlah penting, sebab Mac security memberikan batas penggunaan jaringan LAN pada PT.Pusri, dengan cara membuat *Mac Address Table*, sehingga MAC yang masuk tanpa terdaftar tidak dapat mengakses jaringan LAN dan mengetahui secara pasti pemakai jaringan
2. Sniffing, Netcut, ataupun DNS Spoofing tidak akan terjadi, Mac Security sangat cocok sebagai penangkal serangan-serangan tersebut.
3. Menghemat biaya perangkat, dengan menggunakan fitur yang telah ada pada produk Switch Nortel, perusahaan tidak perlu mengamankan fisik kabel LAN dari pengguna yang tidak berhak, sehingga kabel LAN tidak cepat rusak dan tidak perlu menambah perangkat kabel LAN tambahan.

## 5.2 SARAN

Adapun saran yang penulis sampaikan adalah sebagai berikut :

1. Mac Security yang telah dirancang ini diharapkan dapat diterapkan sebagaimana mestinya, sehingga dapat membantu pekerjaan dan memberikan kenyamanan untuk mengakses data melalui jaringan intranet ataupun internet.
2. Sistem keamanan Mac Security ini sebaiknya dikolaborasikan dengan sistem keamanan lain seperti Radius authentication, Port Mirroring, dan lainnya yang ada pada Switch Keluaran Nortel ini.
3. Sebaiknya perlu diadakan Maintenance berkala pada sistem Mac Security ini, terutama jika ada Mac yang ingin ditambahkan, demi tetap terjaganya keamanan pada sistem jaringan PT.PUSRI ini.
4. Mac Address Table harus dikelola dengan baik agar tidak adanya error pada sistem Mac Security.

# DAFTAR PUSTAKA

Clara, Santa . 2006. *Using the BayStack 450 10/100/1000 Series Switch*. Di

akses tanggal 20 Februari 2013, Dari

([http://aurelie.metois85.free.fr/Maison/BTS/BTS% 20IG/cours/ VLAN](http://aurelie.metois85.free.fr/Maison/BTS/BTS%20IG/cours/VLAN)

[/Switch%20administrable%20-%20Nortel%20BatStack450-24T.pdf](http://www.scribd.com/doc/8276454/Nortel-Commands)).

Clara, Santa.2006. *Nortel Application Switch Operating System 23.0.2*

*Command Reference*. Di akses tanggal 23 Februari 2013, Dari

(<http://www.scribd.com/doc/8276454/Nortel-Commands>).

Clara,Santa.2005. *Configuring and Managing Security Nortel Ethernet*

*Switches 325 and 425 Software Release 3.6.*, User Manual (Ebook).

C.W.Aditya.2012.*100% Sukses Hacking Website Eksplorasi Teknik*

*Membobol Web Paling Berbahaya*. MediaKom: Yogyakarta.

Ir. Abdullah, M.T. 2010. *Sumber Daya TI PT Pusri Menghadapi Persaingan*

*Global*. Palembang: PT Pupuk Sriwidjaja.

Wahidin.2007.*Jaringan Komputer Untuk Orang Awam*. Maxikom:

Palembang.

Nortel Network,2006. *Nortel Ethernet Routing Switch 5500 Series*. di akses

tanggal 15 Februari 2013, Dari

(kendrickcoleman.com/attachments/062\_NN47200-501\_2.03.).

Nur Niswati, Lutfi. 2007. *Pengertian Singkat Tentang Sniffing*. Di akses tanggal 22 Februari 2013, Dari (<http://ilmukomputer.com/Pengertian-Singkat-Tentang-Sniffing.pdf>)

PT PUSRI. \_\_\_\_\_. *Sejarah PT.Pusri Palembang*. <http://www.pusri.co.id>, 13 Februari 2013.

# DAFTAR LAMPIRAN



# PT PUPUK SRIWIDJAJA PALEMBANG

## KANTOR PUSAT

Jalan Mayor Zen  
Palembang - 30118

Website : <http://www.pusri.co.id>



Faksimili : (0711) 712100

Telepon : (0711) 712111, 712222

### DAFTAR NILAI MAHASISWA / SISWA KERJA PRAKTEK / RISET / PSG DI PT PUPUK SRIWIDJAJA

NAMA SISWA / MAHASISWA : IMAM JAKA WISATA  
 SEKOLAH / PERGURUAN TINGGI : UNIVERSITAS BINADARMA  
 JURUSAN : TEKNIK INFORMATIKA  
 NIS / NP / NIM / NIRM : 10.142.229  
 OKASI / UNIT KERJA : Perkantoran  
 DEPARTEMEN / BAGIAN : DEPARTEMEN IT

RAIAN PEKERJAAN DAN SUB PEKERJAAN YANG TELAH DILAKSANAKAN :  
 INSTALASI LAN  
 KONFIGURASI SWITCH NOKIA  
 KONFIGURASI FIREWALL PFSENSE

WAKTU MELAKSANAKAN : ..... s.d .....

| No | PARAMETER PENILAIAN                                    | KRITERIA PENILAIAN |   |      |   |       |   |        |   |
|----|--|--------------------|---|------|---|-------|---|--------|---|
|    |  | SANGAT BAIK        |   | BAIK |   | CUKUP |   | KURANG |   |
| 1  | Disiplin   | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |
| 2  | Motivasi   | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |
| 3  | Loyalitas  | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |
| 4  | Tanggung Jawab   | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |
| 5  | Kerajinan / Ketekunan                                  | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |
| 6  | Daya tangkap & pemahaman terhadap tugas yang diberikan | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |
| 7  | Kerjasama & hubungan dengan karyawan di unit kerja     | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |
| 8  | Tingkat percaya diri                                   | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |
| 9  | Tingkat kepercayaan                                    | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |
| 10 | Kecakapan dalam mengambil keputusan                    | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |
| 11 | Keterampilan   | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |
| 12 | Perawatan terhadap peralatan                           | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |
| 13 | Perhatian terhadap keselamatan kerja                   | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |
| 14 | Akhlik / prilaku                                       | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |

#### ETERANGAN :

- Penilaian diberikan dengan melingkari angka kriteria diatas.
- Butir 11 & 12 , khusus untuk Kerja Praktek

Mengetahui,  
Supervisor Pelaksana Diklat

Akhmad Noerdin Abunaim, S. Sos  
Badge No. 81.4451

Palembang, 24.11.2013  
Pembimbing Penilai

Nama : M. NUR HILDAJAT  
Badge : 070719  
Jabatan : TEKNISI KOMUNIKASI DA



# PT PUPUK SRIWIDJAJA PALEMBANG

KANTOR PUSAT

Jalan Mayor Zen  
Palembang - 30118



Telepon : (0711) 712111, 712222

Website : <http://www.pusri.co.id>

Faksimili : (0711) 712100

## DAFTAR NILAI MAHASISWA / SISWA KERJA PRAKTEK / RISET / PSG DI PT PUPUK SRIWIDJAJA

NAMA SISWA / MAHASISWA : R.M. AT THORIQ  
 SEKOLAH / PERGURUAN TINGGI : UNIVERSITAS BINADARMA PALEMBANG  
 JURUSAN : TEKNIK INFORMATIKA  
 NIS / NP / NIM / NIRM : 10.142.264  
 OKASI / UNIT KERJA : PERKANTORAN  
 DEPARTEMEN / BAGIAN : DEPT. TEKNOLOGI INFORMASI

RAIAN PEKERJAAN DAN SUB PEKERJAAN YANG TELAH DILAKSANAKAN :

INSTALASI JARINGAN KOMPUTER  
 KONFIGURASI SWITCH NORTTEL  
 KONFIGURASI & PENGUJIAN FIREWALL PFSENSE

WAKTU MELAKSANAKAN : 1 FEBRUARI 2013 s.d 28 MARET 2013

| NO | PARAMETER PENILAIAN                                    | KRITERIA PENILAIAN |   |      |   |       |   |        |   |  |
|----|--|--------------------|---|------|---|-------|---|--------|---|--|
|    |  | SANGAT BAIK        |   | BAIK |   | CUKUP |   | KURANG |   |  |
| 1  | Disiplin   | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |  |
| 2  | Motivasi   | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |  |
| 3  | Loyalitas  | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |  |
| 4  | Tanggung Jawab   | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |  |
| 5  | Kerajinan / Ketekunan                                  | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |  |
| 6  | Daya tangkap & pemahaman terhadap tugas yang diberikan | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |  |
| 7  | Kerjasama & hubungan dengan karyawan di unit kerja     | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |  |
| 8  | Tingkat percaya diri                                   | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |  |
| 9  | Tingkat kepercayaan                                    | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |  |
| 10 | Kecakapan dalam mengambil keputusan                    | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |  |
| 11 | Keterampilan   | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |  |
| 12 | Perawatan terhadap peralatan                           | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |  |
| 13 | Perhatian terhadap keselamatan kerja                   | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |  |
| 14 | Akhlak / perilaku                                      | 10                 | 9 | 8    | 7 | 6     | 5 | 4      | 3 |  |

KETERANGAN :

- Penilaian diberikan dengan melingkari angka kriteria diatas.
- Butir 11 & 12, khusus untuk Kerja Praktek

Mengetahui,  
Supervisor Pelaksana Diklat

Akhmad Noerdin Abunaim S. Sos  
Badge No. 81.4451

Palembang, 18 MARET 2013  
Pembimbing Penilai

Nama : M. NUR HIDAYAT  
Badge : 070714  
Jabatan : TEKNIK KOMUNIKASI DATA



**UNIVERSITAS BINADARMA**  
**FAKULTAS ILMU KOMPUTER**

SK. Menteri Pendidikan Nasional Republik Indonesia No.112/D/O/2002  
Jalan Jenderal Ahmad Yani No.12 Palembang 30264  
Telp (0711) 515581, 515582, 515583 Fax. (0711) 518000  
Website : [www.binadarma.ac.id](http://www.binadarma.ac.id) email : [bidar@binadarma.ac.id](mailto:bidar@binadarma.ac.id)



**LEMBAR KONSULTASI**

Nama Ketua : R.M. Atthoriq (10 142 264)  
Anggota : Imam Jaka Wijaya (10 142 229)  
(10 142 251)

Program Studi : Teknik Informatika  
Judul : MAC Security Nortel Based pada PT.PUSRI  
Pembimbing : Prihambodo Hendro Saksono ST.,MSC.,PHD.

| No | Tanggal    | Keterangan   | Paraf |
|----|------------|--|-------|
| 1  | 25-02-2013 | Perbaiki Bab I sesuai petunjuk.  |       |
| 2  | 28-02-2013 | Lanjutan BAB III   |       |
| 3  | 13-03-2013 | - Gambar harus ada penjelasan.<br>- Bab IV perbaiki sesuai petunjuk<br>- Bab V kesimpulan dibuat lebih spesifik (sistem yang di terapkan di PUSRI) |       |
| 4  | 14-03-2013 | Acc Laporan Pkl.   |       |

**PT PUPUK SRIWIDJAJA PALEMBANG**  
Antar Unit Kerja

Palembang, 11 Januari 2013

Nomor : 118 /VB300.DL/2013  
Kepada : Manajer Teknologi Informasi  
Dari : Departemen Diklat  
Hal : **Kerja Praktek**

Sesuai surat persetujuan Manajer Teknologi Informasi 007/NC300.DL/2013 tanggal 4 Januari 2013 perihal tersebut diatas, dengan ini kami tugaskan 2 (dua) orang mahasiswa Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Bina Darma, untuk melaksanakan kerja praktek/penelitian di Departemen Teknologi Informasi dengan jadwal pelaksanaan t.m.t. **01 Februari - 28 Maret 2013.**

Mahasiswa yang dimaksud adalah sbb. :

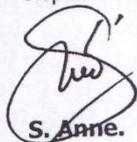
1. Nama/Nim : RM. AT Thoriq / 10142264
2. Nama/Nim : Imam Jaka Wijaya / 10142229

Disamping kegiatan utamanya, kepada mahasiswa/siswa yang bersangkutan diwajibkan :

- Mengetahui/mempelajari sejarah & perkembangan PT Pupuk Sriwidjaja Palembang melalui pengarahan staf Departemen Humas dan Departemen K3 & LH
- Mengisi daftar hadir setiap hari kerja yang dipantau oleh pembimbing serta mematuhi peraturan tata tertib yang berlaku.

Demikian disampaikan, atas bantuan dan kerjasamanya diucapkan terima kasih.

Kepala Diklat



**S. Anne.**

Badge No. 83.0514

Tembusan :

- Supervisor Adm Sitem Sekuriti
- Perpustakaan
- Pembimbing : - M. Nur Hidayat # 07.0714

*Stv / Staf*