**BAB I**

**PENDAHULUAN**

* 1. **Latar belakang Masalah**

Perkembangan teknologi komputer dan informasi saat ini sangatlah cepat, salah satunya adalah komputer. Hampir semua pengolahan dan penyimpanan informasi dilakukan dengan perangkat komputer, dan ini lebih mudah dilakukan apabila sebuah perangkat komputer terhubung ke sebuah jaringan.

Seiring dengan berkembangnya kebutuhan dalam jaringan komputer, jaringan LAN masih terdapat beberapa kelemahan yang harus dikembangkan seperti dalam satu LAN hanya terdiri dari satu broadcast domain jadi semakin banyak penggunaan pc dalam jaringan LAN maka akan semakin lambat pengiriman data, dalam mengatasi permasalah ini diperlukanlah pengembangan jaringan LAN dan muncullah konsep Virtual Local Area Network (VLAN).

VLAN digunakan untuk mengatasi kelemahan yang ada pada LAN, seperti penggunaan alat-alat jaringan yang kurang efisien, untuk membagi beberapa broadcast domain membutuhkan beberapa switch. Dengan mengaplikasikan VLAN maka satu switch yang biasanya hanya mampu digunakan untuk membuat satu LAN dengan satu wilayah teritorial, dapat digunakan untuk membuat beberapa VLAN dengan wilayah teritorialnya masing-masing. Meskipun secara fisik tidak berbeda, namun secara konsep logika VLAN memiliki perbedaan dengan LAN. Penerapan VLAN pada suatu instansi atau perusahaan dapat meningkatkan efisiensi dan efektivitas sistem jaringan. Hal tersebut yang membuatnya menjadi lebih unggul daripada LAN.

Selain penggunaan alat-alat jaringan yang efisien, VLAN juga dapat berhubungan komunikasi antara VLAN yang berbeda dengan menggunakan router sebagai penghubung antar VLAN, untuk itu dibutuhkan lah sebuah metode VLAN Trunk pada switch. VLAN Trunkdibutuhkan dari sistem jaringan yang memiliki lebih dari satu *switch* yang saling terhubung atau dihubungkan ke router.

VLAN dapat saling terhubung karena adanya device yang berperan dalam layer 3 yaitu router yang di sambungkan dengan switch (layer 2), sehingga disebut dengan inter VLAN.

Selain dari pada itu pengalamatan juga dibutuhkan dalam suatu jaringan computer atau lebih tepatnya IP address, dalam pengalamatan IP dibutuhkan sebuah cara untuk membagi sebuah alamat secara otomatis tanpa harus membuat IP host secara satu per satu, agar dapat mempermudah dalam mengatur pengalamatan jaringan pada setiap host muncullah suatu cara pembagian IP secara otomatis yaitu Dynamic Host Configuration Protocol (DHCP) server.

Adapun dari keamanan VLAN sendiri yang masih rentan terhadap serangan-seranganyang mungkin masih akan terjadi, dalam hal ini penulis mengambil masalah dari penggunaan NetCut (tool hacking). NetCut menggunakan jenis serangan ARP Spoofing yang dapat memutuskan koneksi computer korban ke gateway sehingga computer korban akan langsung terputus ke server hingga kejaringan luar (internet). Dari masalah yang ditemukan penulis mencoba membuat suatu pencegahan dengan menggunakan Private VLAN (protected port) yang artinya setiap user tidak bisa berkomunikasi dengan user lain tetapi user masih dapat menjangkau server sehingga user tidak bisa melakukan penyerangan ke user lainya, di sinilah yang akan menjadi keamanan dari VLAN ini.

Dari beberapa kumpulan permasalahan di atas penulis akan mencoba untuk membuat Tugas Akhir ini dengan judul “Hardening Inter VLAN Menggunakan Protected Port dan Port Security”.

* 1. **Rumusan masalah**

Berdasarkan latar belakang di atas, permasalahan yang ditemukan yaitu :

1. Bagaimana membuat Virtual Local Area Network
2. Bagaimana membuat VLAN Trunk
3. Bagaimana membuat DHCP server untuk setiap VLAN
4. Bagaimana membuat Inter VLAN
5. Bagaimana membuat kamanan (hardening) pada VLAN
	1. **Tujuan penelitian**

Tujuan penulisan tugas akhir ini adalah untuk membuat keamanan di dalam jaringan VLAN dengan menggunakan DHCP server dengan system keamanan Protected Port dan Port Security .

* 1. **Manfaat penelitian**

Ada pun manfaat yang dapat diperoleh yaitu :

1. Memudahkan dalam mengontrol jaringan VLAN
2. Meningkatkan keamanan jaringan pada VLAN
	1. **Batasan masalah**

Dalam perangcangan VLAN ini terdapat beberapa batasan ruang lingkup permasalahan, yaitu :

1. Pembahasan Tugas Akhir ini hanya membahas tentang pembagian jaringan LAN dalam satu switch dengan mongkonfigurasi VLAN serta membuat Inter VLAN dengan menggunakan trunking ke router
2. VLAN di konfigurasi berdasarkan port switch.
3. Hardening yang akan di bahas dalam penelitian ini menggunakan sistem keamanan Protected Port dan Port Security.
4. Pengujian untuk sistem keamanan Protected Port dilakukan menggunakan tools bantuan “NetCut”.
	1. **Sistematika Penulisan**

Dalam laporan tugas akhir ini, pembahasan akan disajikan dalam beberapa bab dengan sistematika penulisannya adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan yang digunakan dalam laporan tugas akhir ini.

BAB II TINJAUAN PUSTAKA

Pada bab ini berisi tentang teori-teori dan penjelasan yang berkaitan dengan permasalahan dan penyelesaian masalah dari laporan tugas akhir.

BAB III METODOLOGI PENELITIAN

Pada bab ini berisi tentang analisis, perancangan, dan pengujian dari hasil penelitian tugas akhir ini.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini berisi tentang pembahasan dari hasil konfigurasi yang telah terselesaikan. Serta hasil uji coba konfigurasi VLAN dan keamanan VLAN.

BAB V PENUTUP

Pada bab ini berisi tentang kesimpulan yang dapat diambil dari keseluruhan isi laporan tugas akhir, dan saran yang diharapkan dapat bermanfaat untuk pengembangan selanjutnya.

DAFTAR PUSTAKA

Pada bagian ini dipaparkan tentang sumber-sumber literatur yang digunakan dalam pembutan laporan tugas akhir ini.

**BAB II**

**TINJAUAN PUSTAKA**

1. **Pengertian Hardening**

Hardening secara umum berarti melakukan proses pengerasan suatu lapisan yang lembut sehingga lapisan tersebut menjadi lebih kuat dan lebih tahan terhadap kerusakan (Andika Agus Slameto, 2015).

Prinsip itu juga yang digunakan untuk menerapkan hardening inter VLAN yang berpengaruh terhadap keamanan pada VLAN.

1. **Pengertian Jaringan Komputer**

Jaringan computer adalah sekelompok komputer yang saling berhubungan antara satu dengan lainnya menggunakan protocol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi programprogram, penggunaan perangkat keras bersama seperti printer, hardisk, dan sebagainya.1 Jaringan yaitu kombinasi perangkat keras, perangkat lunak, dan pengkabelan(cabling), yang memungkinkan berbagi alat komputasi untuk berkomunikasi satu sama lain (Saputra, H.B, 2014)

* 1. **Alamat IP**

Alamat Internet Protokol (IP) adalah alamat yang diberikan pada jaringan komputer dan perangkat jaringan. Alamat IP terdiri atas 32 bit angka  biner yang dapat dituliskan sebagai empat kelompok angka desimal yang dipisahkan oleh tanda titik seperti 192.168.0.1. Alamat IP terdiri atas dua bagian yaitu network ID dan host ID, dimana network ID menentukan alamat jaringan komputer, sedangkan host ID menentukan Alamat host (komputer, router, switch). Oleh sebab itu alamat IP memberikan alamat lengkap suatu host beserta alamat jaringan di host itu berada (Saputra, H.B, 2014)

* 1. **VLAN (Virtual Local Area Network)**
		1. **Pengertian VLAN**

Virtual Local Area Network (VLAN) merupakan suatu kumpulan perangkat dalam Local Area Network (LAN) yang dikonfigurai sehingga dapat berkomunikasi seolah-olah dihubungkan dengan kabel padahal berada pada segment yang berbeda dalam LAN. Sebuah jaringan LAN dapat dikatakan sebagai sebuah broadcast domain dan VLAN berfungsi untuk membagi broadcast domain yang semula lebih besar menjadi dua atau lebih broadcast domain yang lebih kecil.

VLAN dapat diciptakan dengan menggunakan managable switch yang mendukung VLAN. Sama seperti pada jaringan LAN, untuk berbuhungan antara satu VLAN dengan VLAN yang lain dibutuhkan sebuah router atau device layer 3 lainnya. VLAN merupakan suatu model jaringan yang tidak terbatas pada lokasi fisik seperti LAN , hal ini mengakibatkan suatu network dapat dikonfigurasi secara virtual tanpa harus menuruti lokasi fisik peralatan.

* + 1. **Keuntungan VLAN**

Beberapa tujuan utama dari implementasi VLAN pada jaringan antara lain :

1. **Security**

Implementasi VLAN dalam suatu perusahaan memungkinkan terkontrolnya keamanan data dalam tiap-tiap departemen karena berada dalam satu broadcast domain yang berbeda.

1. **Cost Reduction**

Mengurangi biaya yang akan dikeluarkan apabila terdapat penambahan jaringan dan lebih efisien dalam pemakaian *bandwidt* danuplinks

1. **Higher Performance**

Memisahkan jaringan layer 2 ke dalam berbagai logical workgroup (broadcast domain) yang dapat mengurangi traffic data yang tidak diperlukan dan meningkatkan performance jaringan.

1. **Broadcast Storm Mitigation**

Penerapan VLAN dapat mengurangi jumlah device yang turut serta dalam sebuahbroadcast storm.

1. **Improved IT Staff Efficiency**

Penerapan VLAN memudahkan pengaturan jaringan dan konfigurasi VLAN dapat langsung tersebar apabila ada sebuah switch baru yang terhubung ke dalam jaringan tersebut.

Secara keseluruhan VLAN memberikan keuntungan sebagai berikut :

1. Pemindahan, penambahan host, dan perubahan host menjadi lebih mudah.
2. Dengan menggunakan device layer 3 di antara VLAN, pengendalian administratif menjadi lebih mudah
3. Konsumsi bandwidth LAN lebih efisien jika dibandingkan konsumsi bandwidth dalam suatu broadcast domain yang besar.
4. Penggunaan CPU lebih efisien karena lebih sedikit mem-forward paket broadcast.
	* 1. **Link VLAN**

VLAN dibangun menggunakan berbagai perangkat seperti switch, router, PC dan sebagainya. Hubungan atau link di antara perangkat-perangkat tersebut. Link seringkali disebut sebagai interface. ada dua jenis link yang umum digunakan dalam VLAN yaitu :

1. Access link

Access link merupakan tipe link yang umum dan dimiliki oleh hampir semua jenis switch VLAN. Access link lazimmnya digunakan untuk menghubungkan komputer dengan switch. Access link tidak lain merupakan port switch yang sudah terkonfigurasi. Selama proses transfer data, switch akan membuang informasi tentang VLAN. Anggota suatu VLAN tidak bisa berkomunikasi dengan anggota VLAN yang lain kecuali jika dihubungkan dengan device*layer* 3 (Router).

1. Trunk link

Istilah trunk diambil dari sistem telepon yang dapat mengangkut beberapa percakapan sekaligus (multiple conversation). Trunk link digunakan untuk menghubungkan switch dengan switch yang lain, switch dengan router, atau switch dengan server. Jadi port telah dikonfigurasi untuk dilalui berbagai VLAN (tidak hanya sebuah VLAN).

Trunk link hanya mendukung teknologi Fast (100Mbps) atau Gigabit (1Gbps) Ethernet. Sebab trunk link lazimnya dihubungkan dengan network backbone berkecepatan tinggi. Wajar jika kebutuhannya lebih tinggi dibandingkan access link

* + 1. **Tipe VLAN**

Tipe-tipe VLAN dapat dibedakan menjadi :

1. Data VLAN

VLAN yang dikonfigurasi hanya untuk *user* dan tidak memiliki kemampuan untuk mengirim voic-based *traffic*.

1. Default VLAN

Ketika switch pertama kali dinyalakan maka semua port yang ada di switch akan menjadi anggota default VLAN. Default VLAN dari switch Cisco adalah VLAN 1 dimana VLAN tersebut tidak dapat diganti namanya atau dihapus.

1. Native VLAN

Link antara switch dengan switch atau switch dengan router menjadi native VLAN. Jangan menjadikan VLAN 1 sebaga native VLAN. Native VLAN berfungsi untuk *tagged*-*traffic* dan *untagged*-*traffic*. Tujuannya agar switch non-Cisco bisa terhubung dengan device Cisco yang lainnya.

1. Management VLAN

VLAN yang dibuat untuk admin dalam mengatur kapabilitas dari switch atau VLAN yang dibuat untuk me *manage device* yang terhubung.

1. Voice VLAN

VLAN yang ditujukan hanya untuk*traffic* voice (Prama, H. B, 2008)

* + 1. **VLAN Trunking**

VLAN trunk adalah Ethernet segmen di antara dua switch, dimana switch menambahkan VLAN header ke frame sebelum mengirim frame, [VLAN trunking header](http://pengertianpengertian.blogspot.com/2013/11/pengertian-vlan-trunking-header.html) mengidentifikasi VLAN mana yang menempati frame.VLAN *Trunking* dibutuhkan pada VLAN dari sistem jaringan yang memiliki lebih dari satu *switch* yang saling terhubung. Saat dilakukan pengiriman *frame* dari satu *switch* menuju *switch* yang lain, *switch-switch* tersebut memerlukan sebuah arahan untuk mengidentifikasi VLAN yang telah mengirim *frame* yang dimaksud. Dengan VLAN *Trunking*, *switch-switch* yang bersangkutan melakukan *tagging* terhadap setiap *frame* yang dikirim, sehingga *switch* penerima dapat mengenali VLAN pemilik *frame* yang dikirim kepadanya Desirable (Pusparini Dian Pertiwi, 2006).

**Gambar 2.1 contoh VLAN Trunk**

* 1. **DHCP (Dynamic Host Configuration Protocol)**
1. **Pengertian DHCP**

Dynamic Host Configuration Protocol (DHCP) merupakan layanan yang secara otomatis memberikan ip address ke komputer yang memintanya. Komputer yang memberikan nomor ip address disebut DHCP Server dan yang meminta nomor ip address disebut DHCP Client.

Dengan adanya layanan DHCP seorang administrator jaringan tidak perlu repot - repot untuk memberikan nomor ip address secara manual ke setiap [komputer](http://begal-tech.blogspot.com/search/label/Komputer) yang ada dalam jaringan saat konfigurasi TCP / IP, tetapi hanya cukup memberikan referensi ke DHCP. Selain memberikan alamat IP Address, banyak parameter jaringan yang dapat diberikan oleh DHCP, seperti Default Gateway dan DNS server (Veriztiarta Radianta, 2015).

* + 1. **Cara Kerja Dhcp Server**

DHCP menggunakan 4 tahapan proses untuk memberikan konfigurasi nomor IP. (Jika Client memiliki NIC lebih dari satu dan perlu no IP lebih dari satu maka proses DHCP dijalankan untuk setiap adaptor secara sendiri-sendiri).

1. **IP Least Request**

Client meminta nomor IP ke server (Broadcast mencari DHCP server).

1. **IP Least Offer**

DHCP server (bisa satu atau lebih server jika memang ada 2 atau lebih DHCP server) yang mempunyai nomor IP, memberikan penawaran ke client tersebut.

1. **IP Lease Selection**

Client memilih penawaran DHCP Server yang pertama diterima dan kembali melakukan broadcast dengan message menyetujui peminjaman tersebut kepada DHCP Server.

1. **IP Lease Acknowledge**

DHCP Server yang menang memberikan jawaban atas pesan tersebut berupa konfirmasi nomor IP dan informasi lain kepada Client dengan sebuah ACKnowledgment. Kemudian client melakukan inisialisasi dengan mengikat nomor IP tersebut dan client dapat bekerja pada jaringan tersebut. (Nugroho R.H, 2013).

* 1. **Inter VLAN**

Maksud dari Inter VLAN ini adalah menggabunkan jaringan antar vlan. Karena dalam switch manageable jika sudah diset memakai vlan maka antar port tidak akan bisa tersambung, tidak seperti switch pada umumnya. Untuk mengatasinya maka ditambahkan router pada switch tersebut. Dikarenakan port dari router terbatas maka dipakai trunking dan interface alias. hardware yang lebih sederhana adalah switch layer 3 (Nugroho R.H, 2013).

* 1. **Topologi Jaringan Komputer**

Topologi merupakan suatu cara untuk menghubungkan satu komputer dengan computer yang lainnya sehingga membentuk jaringan komputer. Topologi jaringan menggambarkan struktur dari jaringan computer.

* + 1. **Topologi Ring**

Pada topologi ring setiap komputer di hubungkan dengan komputer lain dan seterusnya sampai kembali lagi ke komputer pertama, dan membentuk lingkaran sehingga disebut ring, topologi ini berkomunikasi menggunakan data token untuk mengontrol hak akses komputer untuk menerima data, misalnya komputer 1 akan mengirim file ke komputer 4, maka data akan melewati komputer 2 dan 3 sampai di terima oleh komputer 4, jadi sebuah komputer akan melanjutkan pengiriman data jika yang dituju bukan [IP Address](http://www.adalahcara.com/2013/05/pengertian-kelas-ip-address-adalah.html) dia.



**Gambar 2.2 Topologi Ring**

* + 1. **Topologi Bus**

Topologi jaringan komputer bus tersusun rapi seperti antrian dan  menggunakan cuma satu kabel coaxial dan setiap komputer terhubung ke kabel menggunakan konektor BNC, dan kedua ujung dari kabel coaxial harus diakhiri oleh terminator.



**Gambar 2.3 Topologi Bus**

* + 1. **Topologi Star**

Topologi ini membentuk seperti bintang karena semua komputer di hubungkan ke sebuah hub atau switch dengan kabel UTP, sehingga hub/switch lah pusat dari jaringan dan bertugas untuk mengontrol lalu lintas data, jadi jika komputer 1 ingin mengirim data ke komputer 4, data akan dikirim ke switch dan langsung di kirimkan ke komputer tujuan tanpa melewati komputer lain.[Topologi jaringan komputer](http://www.adalahcara.com/2014/09/macam-pengertian-topologi-jaringan-komputer.html) inilah yang paling banyak digunakan sekarang karena kelebihannya lebih banyak.



**Gambar 2.4 Topologi Star**

* + 1. **Topologi Mesh**

Pada topologi ini setiap komputer akan terhubung dengan komputer lain dalam jaringannya menggunakan kabel tunggal, jadi proses pengiriman data akan langsung mencapai komputer tujuan tanpa melalui komputer lain ataupun switch atau hub.



**Gambar 2.5 Topologi Mes**

* + 1. **Topologi Tree**

[Topologi jaringan komputer](http://www.adalahcara.com/2014/09/macam-pengertian-topologi-jaringan-komputer.html) Tree merupakan gabungan dari beberapa topologi star yang dihubungan dengan topologi bus, jadi setiap topologi star akan terhubung ke topologi star lainnya menggunakan topologi bus, biasanya dalam topologi ini terdapat beberapa tingkatan jaringan, dan jaringan yang berada pada tingkat yang lebih tinggi dapat mengontrol jaringan yang berada pada tingkat yang lebih rendah.



**Gambar 2.6 Topologi Tree**

* 1. **Switch**

Switch adalah alat yang digunakan untuk menghubungkan beberapa LAN (Lokal Area Network) yang terpisah serta menyediakan filter paket antar LAN. Pada switch disediakan jalur tersendiri untuk setiap port, artinya setiap port di switch mempunyai Collision domain tersendiri yang sangat mempercepat pengiriman data pada jaringan.

Switch terbagi menjadi 2 berdasarkan model OSI dimana terdapat switch layer 2 dan switch layer 3.

* Switch layer 2 beroperasi pada Data link layer pada lapisan model OSI dimana switch meneruskan paket dengan melihat MAC (media access control) tujuan, switch juga melakukan fungsi bridge antara segmen - segmen LAN karena switch mengirimkan paket data dengan cara melihat alamat yang dituju tanpa mengetahui protokol jaringan yang digunakan.
* Switch layer 3 berada pada Network layer pada lapisan model OSI dimana switch meneruskan paket  data menggunakan IP address. Switch layer 3 sering disebut switch routing atau switch multilayer (Sora, 2015).
	1. **Router**

Router adalah sebuah alat jaringan komputer yang mengirimkan paket data melalui sebuah jaringan atau internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai routing. Router digunakan sebagai penghubung antar dua atau lebih jaringan untuk meneruskan paket data dari satu jaringan ke jaringan lainnya. Sedangkan PC Router adalah sebuah komputer yang dijadikan sebagai router (Nugroho R.H, 2013).

### IEEE 802Q

IEEE 802.1Q merupakan standar proses untuk membangun mekanisme yang mengizinkan multiple bridged networks secara transparan saling berbagi link jaringan fisik yang sama tanpa adanya kekurangan informasi antar jaringan. VLAN Trunking merupakan pengaplikasian dari IEEE 802.1Q. IEEE 802.1Q biasa digunakan sebagai nama dari encapsulation protocol yang digunakan untuk mengimplementasikan mekanisme ini melalui jaringan Ethernet. Selain itu, IEEE 802.1Q juga mendefinisikan arti dari VLAN itu sendiri dengan dispesifikasikan kepada model konseptual dari underpinning bridging pada layer 2 (MAC Layer) dan IEEE 802.1D Spanning Tree Protocol. Protokol tersebut mengijinkan setiap VLAN tunggal untuk berkomunikasi dengan router yang berfungsi pada layer 3 (Nugroho R.H, 2013).

### [Manageable Switch](http://andrasiok.blogspot.co.id/2011/06/manageable-switch.html)

* + 1. **Manageable Switch dan Keunggulannya**

Switch manageable adalahswitch dengan harga tinggi yang dapat dikonfigurasi karena memiliki asystem operasi didalamnya. Manageable adalah device dengan merk 'Cisco'. selain Cisco, kebanyakan hanya sebuah Switch murah yang tidak dapat dikonfigurasi (Unmanageable) dan system pakainya : tinggal colok. Switch manageable dibuat untuk meningkatkan keamanan pada sebuah jaringan lokal dan biasa dipakai pada perusahaan-perusahaan elite. karena cara kerjanya, switch manageable dapat juga dikelompokkan menjadi device yang bekerja pada layer 3 OSI Model.

* + 1. **Kemampuan Switch Manageable**
	1. Bisa membuat Virtual LAN (VLAN) Suatu kemampuan dimana bisa melakukan pembagian / segmentasi network menjadi beberapa buah network yang lebih kecil dalam satu fisik switch biasa nyauntuk tujuan keamanan data.
	2. Bisa melakukan Port Trunking untuk memperbesar bandwidth jalur Uplink Kemampuan untuk menggabungkan beberapa buah uplink menjadi satu kesatuan uplink sehingga diperoleh bandwidth yang lebih besar.
	3. Dapat mengeset Port Priority dalam komunikasi data Kemampuan yang bisa memberikan tingkat prioritas kepada suatu port tertentu sehingga data yang keluar dari port tersebut bisa segera diproses lebih dulu dari pada data yg keluar dari port lain.
		1. **Fungsi Manageable Swicth**

Fungsi Manageable Swicth menggabungkan beberapa segmen atau kelompok LAN. Switch bekerja di layer 2 pada model referensi OSI. Device ini memiliki kemampuan lebih disbanding dengan repeater atau hub.

* + 1. **Perbedaan Manageable Swicth dengan Non Manageable Swicth**
1. **Manageable Swicth**

Mendukung penyempitan broadcast jaringan dengan VLAN, pengaturan accessuser dengan access list, membuat keamanan network lebih terjamin , bisa melakukan pengaturan port yang ada (assign port with Vlan, etc), mudah dalam monitoring trafick dan maintenance network karena dapat diakses tanpa harus berada di dekat switch.

1. **Non Manageable Swicth**

Tidak memiliki kemampuan switching sederhana lainnya tapi hanya mengulangi apa yang diterima untuk sisa port, Manageable switch lebih baik jika memiliki lebih dari 1000 user sebagai jaringan yang mungkin memerlukan pembentukan dan prioritas lalu lintas seperti suara dan data dll, dan dikelola sebagai saklar mahal dibandingkan dengan unmanaged jadi berpikir sebelum berinvestasi.

* 1. **NetCut**

NetCut adalah tool untuk untuk mengalihkan/memutuskan aliran paket data antara user dengan gateway. tool ini menggunakan teknik ARP spoofing/ARP Poisoning.

ARP Poisoning dapat memanipulasi lalu lintas data dari klien target agar semua paket-paket data klien target melalui komputer penyerang terlebih dahulu. Mengapa proses ini bisa terjadi?  proses ini dapat terjadi Karena computer anda akan memberi tahu kepada klien target bahwa MAC address komputer (hardware) anda adalah MAC dari komputer server/gateway. Kemudian komputer anda juga akan memberi tahu kepada komputer server/gateway (computer yang dituju klien taget) bahwa MAC address dari klien target adalah MAC address dari computer anda sendiri (sebagai penyerang). Sekilas cara kerja netcut:

* + - 1. NetCut menjadikan laptop/komputernya sebagai gateway. Jadi dia bebas mengatur siapa yang masuk, dan siapa yang perlu ditendang keluar.
			2. Bekerja berdasarkan Address Resolution Protocol (ARP) Spoofing.

Jadi dia mengelabuhi mac address komputer satu Dengan IP address Komputer lain (Waliulu Raditya Faisal, 2012).

* 1. **Mac Address**

Media Access Control Address (MAC Address) adalah alamat fisik suatu interface [jaringan](http://www.transiskom.com/2010/06/jaringan-komputer.html) (seperti ethernet card pada [komputer](http://www.transiskom.com/2010/08/definisi-komputer.html), interface/port pada router, dan node [jaringan](http://www.transiskom.com/2010/06/jaringan-komputer.html) 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[heksadesimal](http://id.wikipedia.org/wiki/Heksadesimal).

* 1. **Protected Port**

Protected Port fungsinya adalah untuk mencegah port satu berkomunikasi dengan port protected yang lain, jadi protected port dalam suatu switch hanya bisa berhubungan dengan yang NON-protected.

* 1. **Port Security**

Port Securityadalah sebuah trafik kontrol yang bekerja di layer 2 data link

berfungsi untuk mendaftarkan dan membatasi perangkat end devices mana saja yang dapat terkoneksi pada suatu port di switch melalui mac address yang sudah terdaftar di switch. implementasi port security pada switch antara lain adalah :

1. menentukan sekelompok end devices yang diijinkan mengakses port.
2. mengijinkan hanya 1 mac-address tertentu yang dapat mengakses port.
3. menentukan tindakan yang akan dilakukan apabila terdeteksi mac address yang diijinkan.



**Gambar 2.7 contoh Port Security**

**langkah-langkah :**

1. menentukan port pada switch yang akan diberikan fungsi *port security.*
2. menentukan tipe dari port, apakah *access/trunk*. tidak boleh dynamic.
3. menaktifkan fungsi *port security* pada port tersebut.
4. mendaftarkan mac-address dari end devices yang diijinkan.
5. menentukan hukuman bagi end devices yang tidak terdaftar.

Selain itu, ada dua hukuman yang dapat diterapkan pada port security apabila ada MAC address yang tidak terdaftar berusaha mengakses port.

1. **shutdown,** saat terjadi pelanggaran, port akan dimatikan (default port-security)
2. **protect,** saat terjadi pelanggaran, port akan tetap menyala tetapi tidak bisa digunakan (Sulaiman Oris Krianto**, 2015)**
	1. **Internet**

internet ( interconnection networking) sendiri adalah jaringan komunikasi global yang terbuka dan menghubungkan jutaan bahkan milyaran jaringan komputer dengan berbagai tipe dan jenis, dengan menggunakan tipe komunikasi seperti telepon, satelit dan lain sebagainya.

Awalnya internet merupakan[jaringan komputer](http://nesabamedia.com/pengertian-manfaat-dan-macam-macam-jaringan-komputer/) yang dibentuk oleh Departemen Pertahanan Amerika Serikat pada tahun 1969 melalui sebuah proyek yang disebut dengan ARPANET. Misi awal dari proyek ini awalnya hanya untuk keperluan militer saja, tetapi lambat laun terus berkembang dan bisa dinikmati oleh semua kalangan Terciptanya internet telah membawa perubahan yang sangat berarti dalam berbagai aspek kehidupan manusia.

Selain itu, internet juga telah melahirkan dunia baru yang memiliki pola, corak sekaligus karakteristik yang berbeda dengan dunia nyata (Saputra H. B, 2015)

* 1. **Putty**

PuTTY adalah sebuah program open source yang dapat Anda gunakan untuk melakukan protokol jaringan SSH, Telnet dan login. Protokol ini dapat digunakan untuk menjalankan sesi remote pada sebuah komputer melalui sebuah jaringan, baik itu LAN, maupun internet. Program ini banyak digunakan oleh para pengguna komputer tingkat menengah ke atas, yang biasanya digunakan untuk menyambungkan, mensimulasi, atau mencoba berbagai hal yang terkait dengan jaringan. (Rizki Putra, 2014)

**Gambar 2.8 Putty**