LAPORAN KERJA PRAKTEK

PERANCANGAN DAN IMPLEMENTASI ACCESS CONTROL LIST DAN VLAN PADA PT. EXPERT DATA VOICE SOLUTION

Nama : **Muhammad Syakir Kautsar**

Nim : **09.41020.0019**

Program : **S1 (Strata Satu)**

Jurusan : **Sistem Komputer**

SEKOLAH TINGGI

MANAJEMEN INFORMATIKA & TEKNIK KOMPUTER

SURABAYA

2013

LAPORAN KERJA PRAKTEK

PERANCANGAN DAN IMPLEMENTASI ACCESS CONTROL LIST DAN VLAN PADA PT. EXPERT DATA VOICE SOLUTION

Diajukan sebagai salah satu syarat untuk mengerjakan Tugas Akhir

Disusun oleh :

Nama : Muhammad Syakir Kautsar

Nim : 09.41020.0019

Program : S1 (Strata Satu)

Jurusan : Sistem Komputer

SEKOLAH TINGGI

MANAJEMEN INFORMATIKA & TEKNIK KOMPUTER

SURABAYA

2013

ABSTRAK

Dalam kerja praktek ini dilakukan seperti bekerja pada umumnya yaitu 5 kali dalam seminggu dan 8 jam kerja dalam sehari sehingga mahasiswa STIKOM benar-benar mengalami suatu kerja seperti dilapangan.

Tempat kami kerja praktek adalah PT. Expert Data Voice Solution yang beralamat di Jakarta tepatnya di Gedung Graha Pena, lt. 5 suite 515 Jl. Kebayoran Lama No. 12, Jakarta Selatan. PT. Expert Data Voice Solution ini adalah sebuah perusahaan jaringan cisco yang spesialis pada teknologi *voice* (VoIP). Di sini kami belajar tentang implementasi perangkat-perangkat cisco yang umumnya digunakan pada perusahaan salah satunya dengan penerapan Cisco Router dengan menggunakan Cisco *Call Manager Express*.

Dalam perancangan Cisco Router penulis belajar cara implementasi pembatasan hak akses lalu lintas jaringan. Pada umumnya untuk merancang jaringan dibutuhkan pembatasan akses yang mana dapat menghubungkan, mengijinkan dan memblokir akses dari jaringan satu ke yang lainnya. Maka dari itu dibutuhkan *Access Control List (ACL)* untuk membuat pembatasan hak akses dari jalur jaringan yang tersedia.

KATA PENGANTAR

Pertama-tama penulis panjatkan puji syukur ke hadirat Allah SWT. karena atas berkat dan rahmat-Nya akhirnya penulis dapat menyelesaikan laporan kerja praktek ini dengan sebaik-baiknya. Penulis membuat laporan kerja praktek yang berjudul "PERANCANGAN DAN IMPLEMENTASI ACCESS CONTROL LIST DAN VLAN PADA PT. EXPERT DATA VOICE SOLUTION" ini sebagai pertanggungjawaban penulis terhadap pelaksanaan kerja praktek yang telah berlangsung sebelumnya.

Dalam pelaksanaan kerja praktek dan pembuatan laporan kerja praktek ini, penulis mendapatkan bantuan dari berbagai pihak. Oleh karena itu, penulis ingin mengucapkan terima kasih kepada:

1. Orang tua penulis yang selalu memberikan dukungannya, baik secara material maupun spiritual kepada penulis.
2. Bapak Dr. Jusak selaku dosen pembimbing kerja praktek yang telah membimbing dan mengarahkan penulis dengan baik dan sabar.
3. Bapak Andi Chairumin selaku penyelia dan pembimbing kerja praktek yang telah bersedia memberikan tempat kerja praktek untuk penulis.
4. Teman-teman penulis yang telah memberikan dukungan dan motivasi dalam penyelesaian laporan kerja praktek ini.
5. Semua pihak yang telah membantu pembuatan makalah ini, baik secara langsung maupun secara tidak langsung.

Penulis menyadari bahwa dalam laporan kerja praktek ini masih banyak terdapat kekurangan. Oleh karena itu, penulis memohon kritik dan saran yang bersifat konstruktif dari semua pihak untuk perbaikan penulis di masa mendatang.

Penulis juga memohon maaf yang sebesar-besarnya jika ada kata-kata yang menyinggung atau menyakiti hati para pembaca. Akhir kata, penulis mengucapkan terima kasih atas perhatiannya. Semoga laporan kerja praktek ini dapat bermanfaat bagi para pembaca.

Surabaya, November 2012

Penulis

DAFTAR ISI

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR LAMPIRAN

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam perkembangan ilmu pengetahuan dan teknologi (IPTEK) yang cepat ini sangat berpengaruh pada pola kehidupan manusia karena bagaimanapun tidak dapat dipungkiri bahwasanya sebagian besar aspek kehidupan telah memanfaatkan teknologi. Teknologi jejaring yang saling terhubung menjadi salah satu kebutuhan penting bagi manusia untuk bisa bersosialisasi dengan yang lain terutama pada perusahaan.

Pada sebuah jaringan perusahaan pastinya diperlukan pemberlakuan jaringan yang maksimal dengan biaya lebih efisien dan hemat. Maka dari itu dibutuhkan *Virtual Local Area Network* (VLAN) yang mana digunakan untuk membuat satu jaringan menjadi banyak jaringan di dalam satu perangkat (*switch*).

Dalam suatu jaringan yang saling terhubung di sebuah perusahaan pastinya membutuhkan beberapa ketentuan yang berlaku supaya jaringan tetap aman dan efisien. Misalnya pada jaringan yang terhubung di perusahaan itu seperti halnya hak akses suatu bagian yang satu ke bagian yang lainnya.

Tetapi terkadang, jaringan yang terhubung di perusahaan tidak memikirkan pembatasan akses yang digunakan komputer untuk saling berhubungan. Terutama pada saat bagian perusahaan tertentu yang mempunyai hak akses penuh dan yang tidak mempunyai hak atas hak akses pada sebuah jaringan di perusahaan.

Dengan adanya permasalahan yang seperti itu dibutuhkan suatu *Access Control List (ACL)* yang mana dapat membuat aturan-aturan dalam hak akses yang berbeda-beda di suatu jaringan perusahaan tersebut.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang diatas terdapat permasalahan yang perlu pembahasan yaitu tentang:

1. Bagaimana cara melakukan pembatasan jalur hak akses pada sebuah jaringan yang saling terhubung pada Cisco Router?
2. Bagaimana membuat satu jaringan menjadi banyak jaringan berbeda pada Cisco Switch?

1.3 Batasan Masalah

Agar lebih terarah perancangan ini dibatasi oleh berberapa hal, yaitu:

1. Hanya membahas Pembatasan Akses.
2. Hanya membahas Implementasi *Access Control List*.
3. Hanya membahas Implementasi *Virtual Local Area Network*.
4. Menggunakan Cisco Router.
5. Menggunakan Cisco Switch.

1.4 Tujuan

Tujuan dari Kerja Praktek ini adalah :

a. Dapat memberikan pengalaman baru kepada Mahasiswa tentang dunia kerja, khususnya di bidang Jaringan Komputer.

b. Memberikan pengetahuan dan pemahaman kepada mahasiswa tentang penerapan berbagai pengetahuan baik teori maupun praktek yang didapat di bangku perkuliahan pada lingkungan pekerjaan, khususnya di bidang jaringan komputer.

c. Mendapatkan pengetahuan tambahan yang tidak didapat di bangku perkuliahan mengenai jaringan komputer.

d. Meningkatkan keterampilan dan wawasan baik secara teknis maupun hubungan kemanusiaan.

e. Untuk memupuk rasa kebersamaan tim secara baik, terutama dalam mensukseskan suatu program kerja.

1.5 Konstribusi

Beberapa hal yang dapat diperoleh dari kegiatan kerja praktek di PT. Expert Voice Data Solution Jakarta antara lain:

1. Mengimplementasikan ACL dengan VLAN di jaringan router Cisco.

2. Dengan adanya ACL, dapat membatasi jalur hak akses di dalam router sesuai ketentuan yang diinginkan pada suatu perusahaan.

3. Dengan adanya VLAN pada suatu jaringan dapat memberi benyak ruang jaringan yang berbeda di dalam switch.

1.6 Sistematika Penulisan

Sistematika penulisan laporan hasil praktek kerja lapangan pada PT. Expert Data Voice Solution Jakarta adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini membahas tentang latar belakang permasalahan, perumusan masalah, pembatasan masalah, tujuan, kontribusi dan sistematika penulisan laporan kerja praktek.

BAB II GAMBARAN UMUM PERUSAHAAN

Pada bab ini menjelaskan secara detil mengenai PT. Expert Data Voice Solution (Edavos) mulai uraian tentang perusahaan, sejarah singkat, visi dan misi.

BAB III LANDASAN TEORI

Landasan ini berisi tentang penjabaran yang akan dijadikan sebagai acuan analisa dan pemecahan permasalahan yang dibahas seperti konsep dasar jaringan komputer, IP adresss, ACL, VLAN dll, sehingga memudahkan penulis dalam menyelesaikan masalah.

BAB IV DESKRIPSI KERJA PRAKTEK

Bab ini membahas tentang perancangan desain/topologi jaringan dan implementasi yang telah dilakukan selama di PT. Expert Data Voice Solution (Edavos) dan pengujian dari implementasi *Access Control List* dan *VLAN*.

BAB V PENUTUP

Berisi kesimpulan serta saran sehubungan dengan adanya kemungkinan pengembangan sistem pada masa yang akan datang.

BAB II

GAMBARAN UMUM PT. EXPERT DATA VOICE SOLUTION (EDAVOS) JAKARTA

2.1 Uraian Tentang PT. EDAVOS

Edavos adalah perusahaan *System Integrator* (SI) yang menyediakan atau memberikan layanan dengan kualitas yang tinggi dalam konsultasi, desain, implementasi, *maintenance* dan *Information and Communication Technology* (ICT) *outsourcing* dalam bidang *Information Technology* (IT). Keahlian edavos adalah di bidang infrastruktur jaringan dan server, keamanan jaringan dan *unified communications*. Edavos memiliki pengalaman bertahun-tahun dalam pasar dan industri IT, yang akan memberikan solusi IT yang luar biasa dalam memenuhi permintaan dan kebutuhan pelanggan.

Edavos didirikan dan dibentuk pada tahun 2009 tepatnya pada bulan November yang dipimpin dan dijalankan oleh mantan staf senior *network system integrator* dengan *track record* di perusahaan enterprise seperti *sales, professional services* dan *managed services*. Pemimpin perusahaan ini memiliki pengalaman bertahun-tahun dalam industri ICT.

2.2 VISI dan MISI

VISI :

UNTUK MENJADI KELAS DUNIA DAN SYSTEM INTEGRATOR (SI) PALING TERKEMUKA MELALUI TCP/IP:

- Teamwork

- Commitment
- Professional Excellence
- ICT Solution that fit to customer's need
- Persistence of Customer Satisfaction

MISI :

1. Menyediakan solusi yang tepat dan baik untuk menjalankan bisnis pelanggan ke tingkat yang lebih tinggi.
2. Memberikan solusi terbaik untuk memberikan nilai kepada pelanggan dan kepuasan yang tinggi untuk meningkatkan keunggulan kompetitif klien kami dengan menggunakan solusi sistem jaringan terbaik melalui kompeten jaringan kami yang sangat profesional.

2.3 Fokus Bisnis Edavos

Edavos memfokuskan beberapa bisnisnya untuk memberikan pelayanan-pelayanan yang dimilikinya kepada pelanggan sesuai kebutuhan pelanggan. Fokus bisnis edavos terdiri dari :

1. Consulting / System Integrator

   Menyediakan atau memberikan layanan konsultasi IT dengan keahlian di bidang infrastruktur jaringan, keamanan dan komunikasi terpadu sesuai dengan praktek industri terbaik dan memberikan solusi total untuk kebutuhan pelanggan.

2. Managed Services

Managed services infrastruktur edavos meliputi *hardware* dan *software* terkenal seperti *Microsoft Windows*, *Cisco*, *Juniper*, *Netscreen*, *checkpoint*, HP, dan masih banyak lagi.

Layanan *managed network* edavos menawarkan fitur dalam kemampuan *monitoring* yang meliputi :

- *Asset management & tracking*
- *Service Level Agreement (SLA) management*
- *Network infrastructure performance monitoring*
- *Desktop periodic maintenance*
- *Server monitoring, performance management and capacity planning.*
- *Helpdesk service automation*
- Dan banyak lagi

Layanan *managed network security* meliputi :

- *Managed security services* mencakup *monitoring firewall*, analisi *log*, audit, *monitoring* alarm IPS, anomali berbasis alert, dan *monitoring* VPN
- *Managed endpoint security*
- *Desktop & Server manajemen patch*
- Laporan keamanan jaringan meliputi laporan virus, *top viruses*, *infected hosts*, laporan serangan, *top attackers*, dan banyak lagi
- *Vulnerability management* dengan *comprehensive reporting*
- *Network* dan *web application penetration testing*

Layanan *managed voice* meliputi :

- *Managed IP Telephony*
- *Live VoIP Call QoS (packet loss, delay, and jitter) monitoring*
- *VoIP call volume reporting*
- *VoIP raw packet and call flow analysis for troubleshooting*
- *Hosted unified communication solutions*
- Dan banyak lagi

3. Outsourcing

Banyak organisasi yang ingin mendapatkan keuntungan kompetitif dengan mengoptimakan efisiensi, dan meningkatkan layanan pelanggan, cara yang paling efektif untuk mencapai itu adalah dengan melalukan *outsourcing*.

Edavos menyediakan staf *outsourcing* bersertifikat IT dengan keahlian dalam infrastruktur jaringan dan *server*, keamanan jaringan, dan komunikasi terpadu.

Staf edavos sangat baik diposisikan sebagai *engineer*, konsultan, dan *project manager*.

2.4 Solution Partner

Pada November 2010, edavos memiliki solution *partner* kelas dunia meliputi :

1. Cisco System

Gambar 2.1 Cisco *Premier Partner*

Cisco *Systems* adalah perusahaan multinasional di Amerika yang mendesain dan menjual elektronik konsumen, jaringan dan teknologi komunikasi dan jasa. Cisco adalah salah satu produk untuk teknologi informasi nomor satu di dunia, terutama untuk system, perangkat keras jaringan serta telekomunikasinya.

Edavos sudah menjadi Cisco *Premier Partner* sejak juni 2010. Dengan kemitraan ini edavos memiliki pengakuan dari cisco yang menggarisbawahi standar tinggi kompetensi sumber daya perusahaan baik secara teknis, komersial dan prestasi *customer care*.

2. Crestron Electronic

Gambar 2.2 Crestron *Electronic*

Crestron *Electronics* adalah *provider* terkemuka dalam bidang kontrol dan sistem otomatisasi untuk rumah, sekolah, rumahs sakit, hotel dan banyak lagi. Crestron menyediakan gaya hidup dalam teknologi.

3. AMP Cabling

Gambar 2.3 AMP Netconnect

AMP NETCONNECT adalah unit bisnis Tyco *electronics* yang mengembangkan, memproduksi, dan memasok berbagai sistem infrastruktur komunikasi dan produk untuk jaringan pelanggan yang dimiliki pemerintahan,

pendidikan, kesehatan, keuangan, manufaktur, perumahan, listrik dan teknologi.

4. Trend Micro

Gambar 2.4 Trend Micro

Trend Micro adalah perusahaan terkemuka di dunia dengan keahlian lebih dari dua dekade dalam *endpoint, messaging* dan keamanan *web*. Dengan beroperasi di seluruh dunia, Trend Micro difokuskan untuk melakukan inovasi yang cerdas untuk solusi keamanan yang melindungi dari berbagai ancaman membahayakan dan kombinasi serangan termasuk, virus, spam, *phising*, *spyware*, *botnet*, dan serangan *web* lainnya, termasuk pencurian data atau *malware*.

2.5 Human Resource

Edavos saat ini mempekerjakan karyawan dengan minimal memiliki satu sertifikat profesional dari berbagai sertifikasi industri. Beberapa dari mereka memiliki berbagai sertifikat dan saat ini memiliki sertifikat antara lain:

- CCNA (Cisco Certified Network Associate)
- CCDA (Cisco Certified Design Associate)
- CSE (Cisco Sales Expert)
- CCNP (Cisco Certified Network Professional)
- CCIP (Cisco Certified Internetwork Professional)
- CCVP (Cisco Certified Voice Professional)
- CCDP (Cisco Certified Design Professional)

- MCSE (Microsoft Certified Systems Engineer)
- AMP Certified Installer

2.6 Referance Customer

Berikut adalah referensi kinerja yang menunjukkan keberhasilan yang dicapai dalam membantu pelanggan dengan semua fase sistem integrasi. Setiap *project* menjelaskan tentang lingkup dari pekerjaan yang dicapai dan tantanngan khusus dalam *project*:

- *Advertising and Public Relation*
- *Airlines*
- *Business Center*
- *Education*
- *Food and Beverages*
- *Internet Service Provider*
- *Oil and Gas*

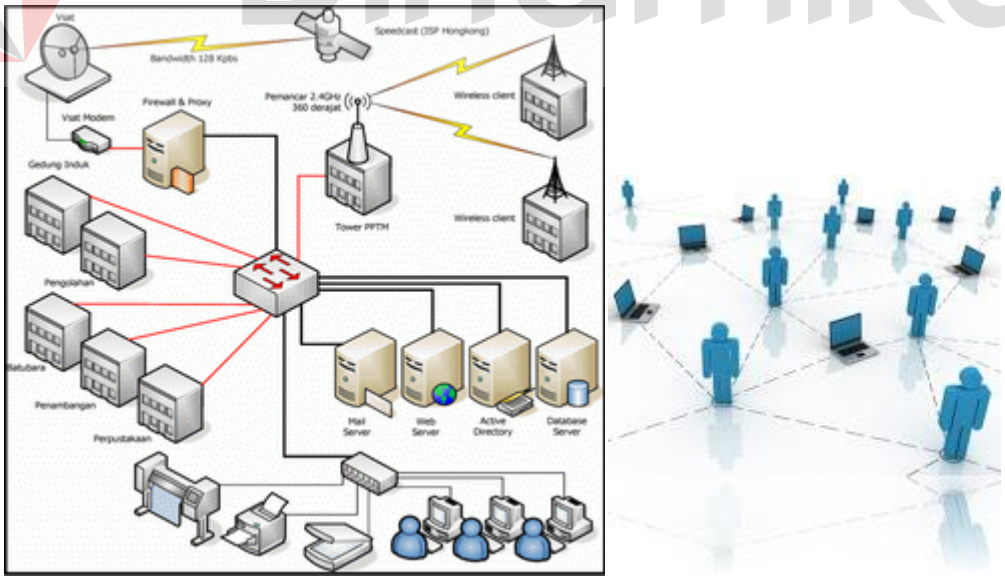
BAB III

LANDASAN TEORI

3.1 Pengertian Jaringan Komputer

Jaringan Komputer yaitu sebuah sistem terdiri dari beberapa komputer dan perangkat jaringan lainnya yang didesain saling terhubung menggunakan protokol komunikasi agar bisa bekerja bersama-sama untuk mencapai suatu tujuan yang sama. (Sukmaaji, 2003)

Tujuan Jaringan komputer adalah berbagi sumber daya (data, printer, harddisk), berkomunikasi (email, chatting), dan untuk akses informasi (web browsing).



Gambar 3.1 Topologi Jaringan

3.2 Jenis-jenis Jaringan Komputer

3.2.1 Berdasarkan Luas Areanya

Berdasarkan luas jangkauannya areanya, jaringan komputer dapat diklasikfikasikan menjadi :

1. PAN (Personal Area Network)

   PAN merupakan jaringan computer yang dibentuk oleh beberapa buah komputer dengan peralatan non-komputer (seperti : *printer, mesin fax, telepon seluler, PDA, handphone*). Teknologi PAN dapat dibangun menggunakan teknologi *wire* dan *wireless network*. Teknologi *wire* PAN biasanya mengandalkan perangkat USB dan *FireWire*. Sedangakan *wireless* PAN (WPAN) yang menggunakan Bluetooth lebih disukai penggguna. Cakupan area sebuah PAN sangat terbatas, yaitu sekitar 9-10 meter (30 feet). Namun cakupannya dapat diperluas sesuai perkembangan jaman. (Sofana, 2009)

2. LAN (Local Area Network)

   LAN berhubungan dengan area *network* yang berukuran *relative* kecil. Oleh sebab itu, LAN dapat dikembangkan dengan mudah dan mendukung kecepatan *transfer* data cukup tinggi. Kebanyakan LAN menggunakan media kabel untuk menghubungkan antara satu komputer dengan komputer lainnya. Ukuran LAN terbatas, sehingga dapat menggunakan desain tertentu. Teknologi transmisi kabel tunggal memiliki kecepatan 10 hingga 100 Mbps. (Sofana, 2009)

3. MAN (Metropolitan Area Network)

   Teknologi yang digunakan MAN hampir sama dengan LAN namun cakupan areanya lebih luas dan komputer yang dihubungkan pada jaringan

MAN lebih banyak dibanding menggunakan LAN. MAN merupakan gabungan beberapa LAN yang dihubungkan menjadi sebuah jaringan besar. MAN dapat diimplementasikan pada *wire* maupun *wireless* network. (Sofana, 2009)

4. WAN (Wide Area Network)

Jaringan area Skala Besar *Wide Area Networks* (WAN) adalah jaringan yang lingkupnya biasanya sudah menggunakan sarana Satelit ataupun kabel bawah laut sebagai contoh keseluruhan jaringan BANK BNI yang ada di Indonesia ataupun yang ada di Negara-negara lain. Menggunakan sarana WAN, Sebuah Bank yang ada di Bandung bisa menghubungi kantor cabangnya yang ada di Hongkong, hanya dalam beberapa menit. (Sofana, 2009)

3.2.2 Berdasarkan Media Penghantarnya

Berdasarkan media penghantar yang digunakan, jaringan komputer dapat dibagi menjadi:

1. Wire network atau wireline network

Wire network adalah jaringan yang menggunakan kabel sebagai media penghantarnya. Jadi, data dialirkan melalui kabel.pada jaringan LAN banyak menggunakan kabel tembaga seagai penghantarnya, namun pada jaringn MAN maupun WAN banyak menggunakan gabungan antara kabel tembaga dan serat optic. Yang dibutuhkan untuk merakit jaringan *wired*:

a. Kabel UTP
b. Konektor RJ 45
c. Tang Network
d. Switch (jika lebih dari dua komputer)

e. Modem(jika mau konek dengan internet)

2. Wireless network

Wireless network adalah jaringan komputer yang menggunakan media penghantar berupa gelombang radio atau cahaya (*infrared atau lasser*). Frekuensi yang digunakan oleh *wireless network* biasanya 2.4 GHz dan 5.8 GHz. Sedangkan penggunaan laser dan infrared umumnya hanya terbatas untuk jenis jaringan yang hanya melibatkan 2 buah itik saja (point to point). Yang dibutuhkan untuk merakit jaringan *wireless*:

a. *Wireless Network* Adapter

b. Macam *Wireless Network* Adapter:

c. USB *Wireless Network* Adapter

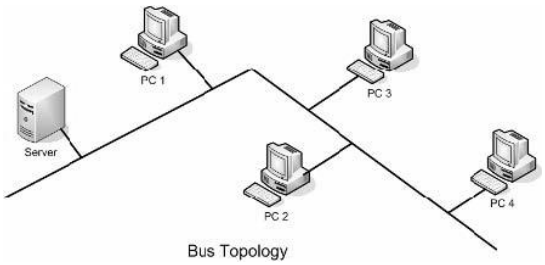
d. PCMCIA *Wireless Network* Adapter

e. PCI *Wireless Network* Adapter

f. Modem (jika mau konek dengan internet)

3.3 Topologi Jaringan

3.3.1 Topologi Bus



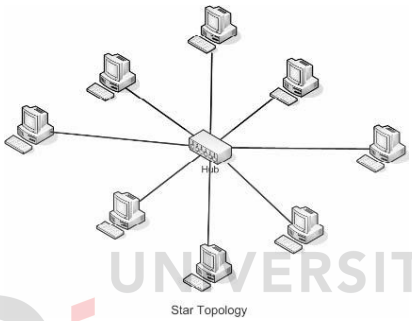
Gambar 3.2 Topologi Bus

Topologi bus menggunakan sebuah kabel *backbone* dan semua *host* terhubung secara langsung pada kabel tersebut.

Keuntungan Topologi Bus :

1. Topologi yang sederhana
2. Kabel yang digunakan sedikit untuk menghubungkan komputer-komputer atau peralatan-peralatan yang lain
3. Biayanya lebih murah dibandingkan dengan susunan pengkabelan yang lain.
4. Cukup mudah apabila kita ingin memperluas jaringan pada topologi bus.

3.3.2 Topologi Star



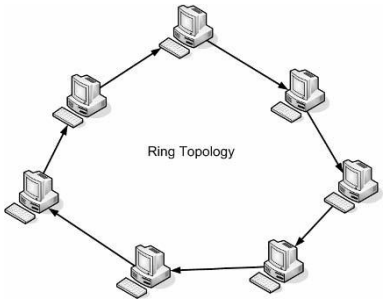
Gambar 3.3 Topologi Star

Topologi star menghubungkan semua komputer pada *sentral* atau *konsentrator*. Biasanya *konsentrator* adalah sebuah hub atau switch.

Keuntungan Topologi Star :

1. Cukup mudah untuk mengubah dan menambah komputer ke dalam jaringan yang menggunakan topologi star tanpa mengganggu aktvitas jaringan yang sedang berlangsung.
2. Apabila satu komputer yang mengalami kerusakan dalam jaringan maka komputer tersebut tidak akan membuat mati seluruh jaringan star.
3. Kita dapat menggunakan beberapa tipe kabel di dalam jaringan yang sama dengan hub yang dapat mengakomodasi tipe kabel yang berbeda.

3.3.3 Topology Ring



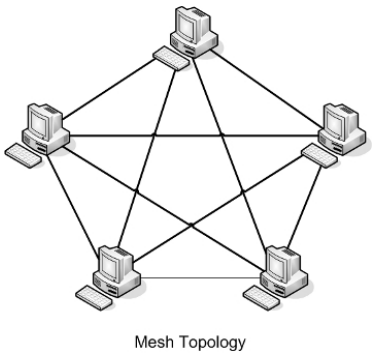
Gambar 3.4 Topologi Ring

Topologi ring menghubungkan *host* dengan *host* lainnya hingga membentuk *ring* (lingkaran tertutup).

Keuntungan Topologi Ring :

1. Data mengalir dalam satu arah sehingga terjadinya *collision* dapat dihindarkan.
2. Aliran data mengalir lebih cepat karena dapat melayani data dari kiri atau kanan dari *server*.
3. Dapat melayani aliran lalulintas data yang padat, karena data dapat bergerak kekiri atau kekanan.
4. Waktu untuk mengakses data lebih optimal.

3.3.4 Topologi Mesh atau Fully-Mesh



Gambar 3.5 Topologi Mesh

Topologi mesh menghubungkan setiap komputer secara *point-to-point*. Artinya semua *computer* akan saling terhubung satu-satu sehingga tidak dijumpai ada *link* yang putus.

Topologi mesh juga merupakan jenis topologi yang digunakan oleh internet. Dimana dapat dijumpai banyak jalur (*path*) menuju sebuah lokasi. Biasanya tiap lokasi dihubungkan oleh router.

Keuntungan Topologi Mesh :

1. Keuntungan utama dari penggunaan topologi mesh adalah *fault tolerance.*
2. Terjaminnya kapasitas *channel* komunikasi, karena memiliki hubungan yang berlebih.
3. Relatif lebih mudah untuk dilakukan *troubleshoot.*

3.4 Perangkat Jaringan Komputer

1. Modem

   Modulator-demodulator digunakan untuk mengubah informasi digital menjadi sinyal analog. Modem mengubah tegangan bernilai biner menjadi sinyal analog dengan melakukan *encoding* data digital ke dalam frekuensi carrier. Modem juga dapat mengubah kembali sinyal analog yang termodulasi menjadi data digital, sehingga informasi yang terdapat di dalamnya dapat dimengerti oleh komputer. Proses ini disebut demodulasi.

   Modem ekternal

Gambar 3.6 Modem Eksternal

Modem internal

Gambar 3.7 Modem Internal

2. Repeater

Repeater merupakan jaringan komputer yang digunakan untuk memperkuat kembali sinyal komunikasi jaringan. Setelah melalui media transmisi, sinyal dapat melemah. Repeater berfungsi untuk memperkuat kembali sinyal tersebut sehingga dapat ditransmisikan lebih jauh. *Repeater* tidak melakukan pengambilan keputusan apapun mengenai pengiriman sinyal. *Repeater* bekerja dengan menerima, memperkuat, kemudian meneruskan sinyal yang diterima agar dapat melewati agar dapat melewati media jaringan dengan jangkauan yang lebih jauh.

Gambar 3.8 Repeater

3. Hub

Hub merupakan peralatan jaringan komputer yang berfungsi untuk menerima sinyal dari satu komputer dan mentransmisikannya ke komputer yang lain. *Hub* mengambil bit-bit yang datang dari satu *port* dan mengirimkan salinannya ke setiap *port* yang lain. Setiap *host* yang tersambung ke *hub* akan melihat paket ini, tetapi hanya *host* yang dituju saja yang akan memprosesnya. Hal ini dapat mengakibatkan masalah network traffic karena paket yang dituju ke satu host sebenarnya dikirim ke semua host.

Gambar 3.9 Hub

4. Bridge

Bridge merupakan peralatan jaringan komputer yang digunakan untuk memisahkan suatu jaringan yang luas menjadi jaringan-jaringan yang lebih kecil. *Bridge* sangat berguna untuk menghubungkan beberapa LAN agar dapat mencakup daerah yang lebih luas atau membagi sebuah LAN besar menjadi beberapa LAN yang lebih kecil untuk mengurangi traffic yang melalui masing-masing LAN. Tugas *bridge* adalah melakukan pengambilan keputusan apakah *paket* harus diteruskan ke jalur yang berikutnya atau tidak. Ketika *bridge* menerima paket dari jaringan, *bridge* akan memeriksa *Media Access Control* (MAC) address tujuan dan memeriksa *MAC address* tersebut pada *bridge table*

yang dimiliki. MAC address adalah sebuah alamat jaringan yang mewakili node tertentu pada jraingan. Bridge kemudian melakukan proses pengambilan keputusan sebagai berikut :

a. Jika tujuan berada pada jalur yang sama dengan jalur paket, bridge tidak akan mengirimkan paket ke jalur yang lain. Proses ini disebut filtering.
b. Jika tujuan berada pada jalur yang berbeda, maka bridge akan meneruskan paket ke jalur yang dituju.
c. Jika MAC address tujuan tidak diketahui, bridge akan meneruskan paket ke semua jalur kecuali jalur asal paket.

Gambar 3.10 Bridge

5. Switch

Switch merupakan peralatan jaringan yang bekerja pada layer 2 model OSI, yang mampu melakukan manajemen *transfer* data yaitu hanya meneruskan data ke segmen yang dituju.*switch* tidak melakukan konversi format data. *Switch* mempelajari host mana saja yang terhubung ke suatu port dengan membaca *MAC address* asal yang ada di dalam paket, kemudian *switch* membuka sirkuit virtual antara node sumber dengan *node* tujuan. Dengan demikian, komunikasi dua port tersebut tidak mempengaruhi *traffic* dari *port* lain. Hal tersebut membuat LAN menjadi lebih efisien.

Gambar 3.11 Switch

6. Router

Router mempunyai semua kemampuan peralatan jaringan komputer lainnya. *Router* dapat memperkuat sinyal, mengkonsentrasikan beberapa koneksi, melakukan konversi format transmisi data, dan mengatur *transfer* data. Selain itu *router* juga bisa melakukan koneksi ke WAN, sehingga dapat menghubungkan LAN yang terpisah jauh. *Router* bertugas melakukan routing paket dar sumber ke tujuan pada LAN dan menyediakan koneksi ke WAN. Dalam lingkungan LAN, router membatasi *broadcast* dan membagi jaringan dengan menggunakan struktur *subnetwork*.

Gambar 3.12 Router

7. Access Point

Access point (AP) berperan sebgain sentral hub pada infrastruktur WLAN (*Wireless LAN*). AP dilengkapi dengan antena dan menyediakan koneksi tanpa kabel pada daerah tertentu yang disebut cell.

Gambar 3.13 Access Point

3.5 Internet

Interconnected Network atau yang lebih populer dengan sebutan Internet secara sederhana adalah sebuah sistem komunikasi global yang menghubungkan komputer-komputer dan jaringan- jaringan komputer di seluruh dunia. Setiap komputer dan jaringan terhubung secara langsung maupun tidak langsung ke beberapa jalur utama yang disebut internet *backbone* dan dibedakan satu dengan yang lainnya menggunakan *unique name* yang biasa disebut dengan alamat IP 32 bit.

Menurut pakar internet Onno. W. Purbo, "Internet dengan berbagai aplikasinya seperti *Web, VoIP, E-Mail* pada dasarnya merupakan media yang digunakan untuk mengefisiensikan proses komunikasi"

Sedangkan menurut tim penelitian dan pengembangan wahana computer, "Internet adalah metode untuk menghubungkan berbagai komputer ke dalam satu jaringan global, melalui protokol yang disebut *Transmission Control Protocol / Internet Protocol (TCP/IP).*

Komputer dan jaringan dengan berbagai *platform* yang mempunyai perbedaan dan ciri khas masing-masing (*Unix, Linux, Windows, Mac,* dll) bertukar informasi dengan sebuah protokol standar yang dikenal dengan nama TCP/IP

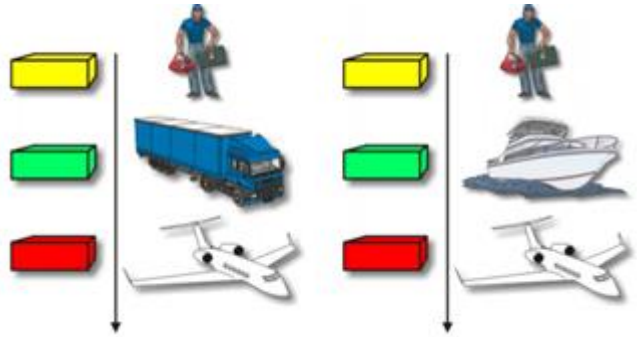
(*Transmission Control Protocol/Internet Protocol*). TCP/IP tersusun atas 4 layer (*network access*, internet, *host-to-host transport*, dan *application*) yang masing-masing memiliki protokolnya sendiri-sendiri.

3.5.1 Model Referensi Open Systems Interconnection (OSI)

Model referensi OSI merupakan model konseptual yang terdiri dari tujuh layer, dimana setiap *layer* mempunyai fungsi jaringan yng spesifik dan saling mendukung satu sama lain. Model ini telah dikembangkan oleh badan yang mengurusi permasalahan standarisasi, yaitu *International Organization Of Standardization* (ISO) di tahun 1984, dan hingga saat ini telah menjadi model arsitektur jaringan acuan dalam komunikasi antar komputer. Standard ini dikembangkan untuk industri komputer agar komputer dapat berkomunikasi pada jaringan yang berbeda secara efisien.

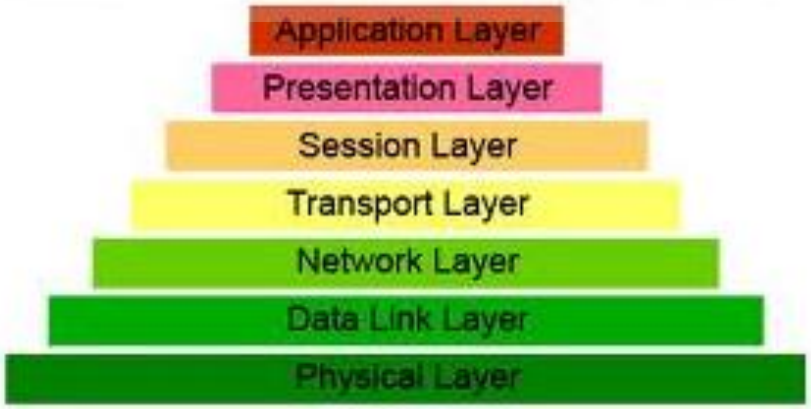
Open dalam OSI adalah untuk menyatakan model jaringan yang melakukan *interkoneksi* tanpa memandang perangkat keras "*hardware*" yang digunakan, sepanjang software komunikasi sesuai dengan standard. Hal ini secara tidak langsung menimbulkan *modularity* (dapat dibongkar pasang). *Modularity* mengacu pada pertukaran protokol di level tertentu tanpa mempengaruhi atau merusak hubungan atau fungsi dari level lainnya.

Dalam sebuah *layer*, protokol saling dipertukarkan, dan memungkinkan komunikasi terus berlangsung. Pertukaran ini berlangsung didasarkan pada perangkat keras "*hardware*" dari *vendor* yang berbeda dan bermacam-macam alasan atau keinginan yang berbeda.



Gambar 3.14 Modularity

Gambar diatas mencontohkan Jasa Antar/Kurir yang akan mengantar kiriman paket. *Modularity* pada level transportasi menyatakan bahwa tidak penting, bagaimana cara paket sampai ke pesawat. Paket untuk sampai di pesawat, dapat dikirim melalui truk atau kapal. Masing-masing cara tersebut, pengirim tetap mengirimkan dan berharap paket tersebut sampai di Toronto. Pesawat terbang membawa paket ke Toronto tanpa memperhatikan bagaimana paket tersebut sampai di pesawat itu.

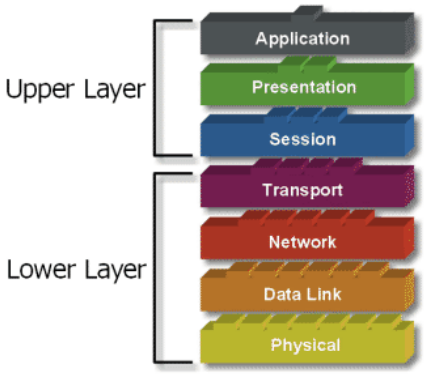


Gambar 3.15 Model OSI Layer

Setiap layer pada dasarnya dapat berdiri sendiri secara *independen* dalam implementasinya, akan tetapi tetap menyatu dalam fungsinya (berbeda-beda tetapi tetap satu fungsi yang saling mendukung). Terdapat 7 *layer* pada model OSI.

Setiap *layer* bertanggung jawab secara khusus pada proses komunikasi data. Misal, satu *layer* bertanggung jawab untuk membentuk koneksi antar perangkat, sementara *layer* lainnya bertanggung jawab untuk mengoreksi terjadinya "*error*" selama proses *transfer* data berlangsung. Dengan kemampuan ini, masing-masing *layer* dapat dikembangkan secara *independen* tanpa mempengaruhi *layer* yang lain. Beberapa keuntungan atau alasan mengapa model OSI dibuat berlapis-lapis, diantaranya :

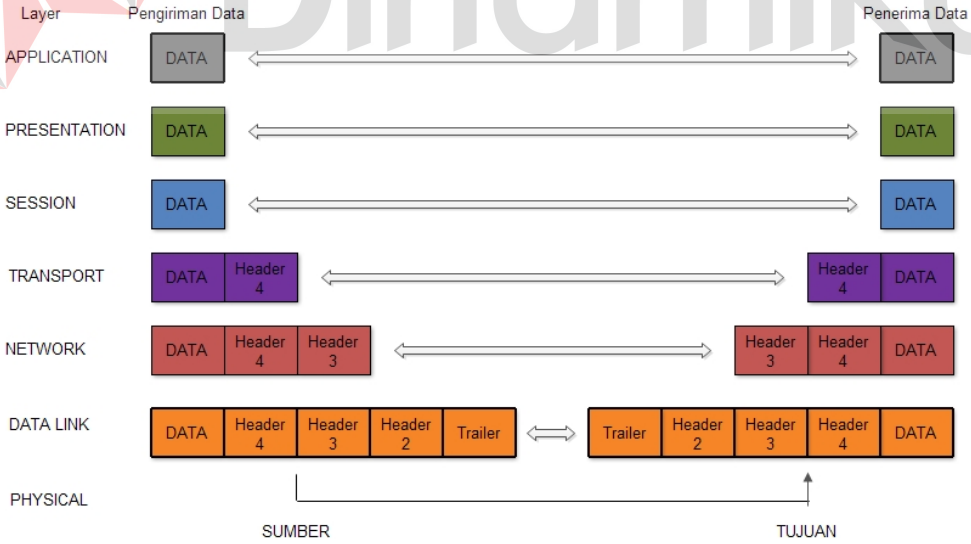
1. Memudahkan siapa saja untuk memahami cara kerja jaringan komputer secara menyeluruh
2. Memecah persoalan komunikasi data yang rumit menjadi bagian-bagian kecil yang lebih sederhana. Sehingga memudahkan *trouble shooting.*
3. Memungkinkan *vendor* atau pakar network mendesain dan mengembangkan *hardware* atau *software* yang sesuai dengan fungsi *layer* tertentu.
4. Menyediakan standar *interface* bagi pengembangan perangkat yang melibatkan *multivendor*.
5. Adanya abstraksi *layer* memudahkan pengembangan teknologi masa depan yang terkait dengan *layer* tertentu.



Gambar 3.16 Upper layer dan Lower Layer OSI Model

Dari ketujuh layer dapat diklasifikasikan secara fungsional menjadi dua bagian saja, yaitu:

1. *Layer* 5 s.d 7 dikelompokan sebagai *application layer* atau *upper layer*. Segala sesuatu yang berhubungan dengan *user interface*, *data formatting*, dan *communication session* ditangani oleh *layer* ini. *Upper layer* banyak diimplementasikan dalam bentuk *software* (aplikasi).
2. Layer 1 s.d 4 dikelompokan sebagai *data flow layer atau lower layer*. Bagimana data mengalir pada *network* ditangani oleh *layer* ini. *Lower lyer* diimpleentasikan dalam bentuk *software* maupun *hardware*. *Layer* yang paling dekat dengan media jaringan adalah *layer physical*. Pengkabelan juga termasuk dalam layer ini, yang bertugas menempatkan informasi ke dalam media yang akan ditransmisikan ke seluruh jaringan.



Gambar 3.17 Alur Pengiriman Data

Cara kerja dari OSI layer yaitu ketika data di *transfer* melalui jaringan, sebelumnya data tersebut harus melewati ke-tujuh *layer* dari satu terminal, mulai

dari *layer* aplikasi sampai *physical layer*, kemudian di sisi penerima, data tersebut melewati *layer physical* sampai aplikasi. Pada saat data melewati satu *layer* dari sisi pengirim, maka akan ditambahkan satu *header* sedangkan pada sisi penerima *header* dicopot sesuai dengan *layer* nya. Masing-masing fungsi dari tiap layer komunikasi dapat dilihat seperti berikut ini :

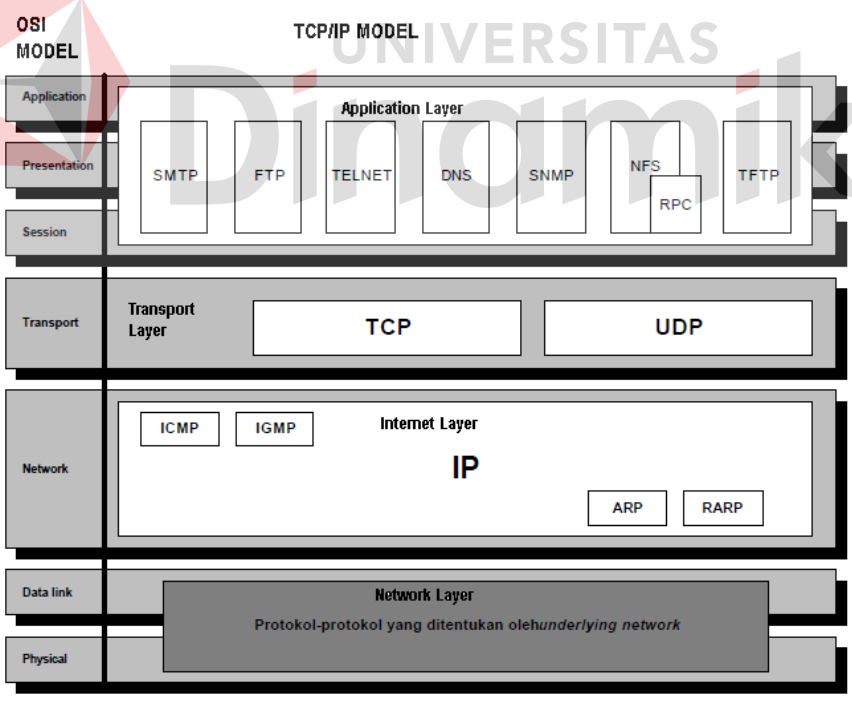
- **Application Layer:** Menyediakan jasa untuk aplikasi pengguna. *Layer* ini bertanggung jawab atas pertukaran informasi antara program komputer, seperti program e-mail, dan service lain yang jalan di jaringan, seperti server printer atau aplikasi komputer lainnya. Contuh : NNTP, HL7, Modbus, SIP, SSI, DHCP, FTP, Gopher, HTTP, NFS, NTP, RTP, SMPP, SMTP, SNMP, Telnet.
- **Presentation Layer:** Bertanggung jawab bagaimana data *dikonversi* dan *format* untuk *transfer* data. Contoh *konversi format text ASCII* untuk dokumen, gif dan JPG untuk gambar. Layer ini membentuk kode *konversi*, translasi data, *enkripsi* dan *konversi*. Contoh : TDI, ASCII, EBCDIC, MIDI, MPEG, ASCII7.
- **Session Layer:** Menentukan bagaimana dua terminal menjaga, memelihara dan mengatur koneksi,- bagaimana mereka saling berhubungan satu sama lain. Koneksi di *layer* ini disebut “session”. Contoh : SQL, X Window, Named Pipes (DNS), NetBIOS, ASP, SCP, OS, Scheduling, RPC, NFS, ZIP.
- **Transport Layer:** Bertanggung jawab membagi data menjadi *segmen*, menjaga koneksi logika “*end-to-end*” antar terminal, dan menyediakan penanganan *error (error handling).* Contoh : TCP, SPX, UDP, SCTP, IPX.

- **Network Layer:** Bertanggung jawab menentukan alamat jaringan, menentukan *rute* yang harus diambil selama perjalanan, dan menjaga antrian *trafik* di jaringan. Data pada *layer* ini berbentuk paket. Contoh : IPX, IP, ICMP, IPsec, ARP, RIP, IGRP, BGP, OSPF, NBF,Q.931.
- **Data Link Layer:** Menyediakan *link* untuk data, memaketkannya menjadi *frame* yang berhubungan dengan "*hardware*" kemudian diangkut melalui media. komunikasinya dengan
- kartu jaringan, mengatur komunikasi *layer physical* antara sistem koneksi dan penanganan error. Contoh : 802.3 (Ethernet), 802.11 a/b/g/n MAC/LLC, 802.1Q (VLAN), ATM, CDP, HDP, FDDI, Fibre Channel, Frame Relay, SDLC, HDLC, isl, ppp, Q.921, Token Ring.
- **Physical Layer:** Bertanggung jawab atas proses data menjadi bit dan mengirimkannya melalui media, seperti kabel, dan menjaga koneksi fisik antar sistem. Contoh : RS-232, V.35, V.34, I.430, I.431, T1, E1, 100BASE-TX, 10 BASE-T, POTS, SONET, DSL, 802.11a/b/g/n PHY, hub, repeater, fibre optics.

3.5.2 Protokol TCP/IP

TCP/IP *suite* (*Transport Control Protocol/Internet Protocol*) merupakan sekelompok protokol yang mengatur komunikasi data komputer dan memungkinkan komputer berbagai jenis dan berbagai *vendor* serta berbeda sistem operasi untuk berkomunikasi bersama dengan baik. TCP/IP memiliki karakteristik yang membedakan dari protokol-protokol komunikasi yang lain, diantaranya:

1. Bersifat standar, terbuka dan tidak bergantung pada perangkat keras atau sistem operasi tertentu.
2. Bebas dari jaringan fisik tertentu, memungkinkan integrasi berbagai jenis jaringan (*ethernet*, *token ring*, *dial-up*).
3. Menggunakan pengalamatan yang unik dalam skala global. Dengan demikian memungkinkan komputer dapat saling terhubung walaupun jaringannya seluas internet sekarang ini
4. Standarisasi protokol TCP/IP dilakukan secara konsisten dan tersedia secara luas untuk siapapun tanpa biaya. Hal ini diwujudkan dalam RFC (*Request For Comment)*



Gambar 3.18 Susunan Protokol TCP/IP dan Model OSI

Sekumpulan protokol TCP/IP ini dimodelkan dalam empat lapisan yang bertingkat.

1. Lapisan pertama (*Network Access Layer*). Indentik dengan lapisan *physical* dan data link layer pada OSI. Pada lapisan ini, didefinisikan bagaimana penyaluran data dalam bentuk farme-frame data pada media fisik yang digunakan secara handal. Lapisan ini biasanya memberikan *servis* untuk deteksi dan koreksi kesalahan dari data yang ditransmisikan. beberapa contoh protokol yang digunakan pada lapisan ini adalah X.25 untuk jaringan publik, Ethernet untuk Ethernet, dsb.
2. Lapisan kedua (*Internet Layer*). Identik dengan *network layer* pada OSI. Lapisan ini bertugas untuk menjamin agar suatu paket yang dikirimkan dapat menemukan tujuannya. Lapisan ini memiliki peranan penting terutama dalam mewujudkan *internetworking* yang meliputi wilayah luas (*worldwide Internet*). Beberapa contoh protokol pada lapisan ini yaitu IP, ARP, RARP, ICMP, IGMP, dsb.
3. Lapisan Ketiga (*Transport Layer*). Identik dengan *Transport Layer* pada OSI. Pada lapisan ini di definisikan cara-cara untuk melakukan pengiriman data antara *end to end host*. Lapisan ini menjamin bahwa informasi yang dikirim pada sisi penerima akan sama dengan informasi yang dikirim oleh pengirim. Dua buah protokol yang digunakan pada layer ini yaitu *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP).
4. Lapisan Keempat (*Application Layer).* Identik dengan *Application, Presentasi, Session layer* pada OSI. Lapisan ini mendefinisikan aplikasi-aplikasi yang dijalankan oleh jaringan. Contoh lapisan yang dikembangkan pada layer ini yaitu *Simple Mail Transport Protocol* (SMTP), *Hyper Text Transfer Protocol* (HTTP),dsb.

3.6 IP Address

Pada Layer Internet banyak dijumpai sebuah protokol yang populer, yaitu *Internet Protocol* (IP). IP merupakan merupakan protokol yang bersifat *connectionless* dan *unreliable*. IP Addrees berbeda dengan MAC address. Baik IP address maupun MAC Address, keduanya diperlukan pada *internetworking*. Ip address dibentuk oleh sekumpulan bilangan biner sepanjang 32 bit, yang dibagi atas 4 bagian. Setiap bagian panjangnya 8 bit. IP address merupakan *identifikasi* setiap *host* pada jaringan Internet. Contoh IP address sebagai berikut:

01000100 10000001 11111111 00000001

Dapat di *konversi* ke dalam bilangan desimal, sehingga diperoleh alamat IP :

68.129.255.1

Bentuk penulisan IP address di atas dikenal dengan notasi "*doted decimal*". Dalam prakteknya, bentuk *doted* digunakan sebagai alamat *host*. Dalam penggunaanya, tidak semuanya *IP address* dapat digunakan. Ada yang digunakan untuk keperluan khusus, seperti untuk keperluan alamat network, alamat *broadcast*, alamat *local host*, LAN, dsb. *IP address* berkut digunakan sebagai cadangan keperluan jaringan intranet/LAN:

1. Dimulai dari 10.0.0.0 hingga 10.255.255.255
2. Dimulai dari 127. 0.0.0 hingga 127.255.255.255
3. Dimulai dari 169.254 hingga 169.254.255.255
4. Dimulai dari 172.16.0.0 hingga 172.31.255.255
5. Dimulai dari 192.168.0.0 hingga 192.168.255.255

IP address yang digunakan untuk keperluan LAN/intranet disebut sebagai *IP private*, sedangkan yang dapat digunakan untuk keperluan internet disebut *IP publik*.

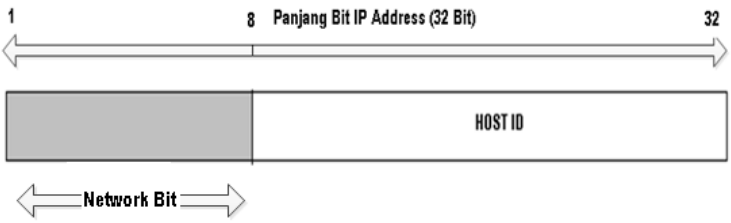
Secara umum, *IP address* dapat dibagi menjadi 5 buah kelas. Kelas A.B,C,D,dan E. namun dalam praktiknya hanya kelas A, B, C saja yang digunakan untuk keperluan umum, sedangkan *IP address* kelas D, dan E digunakan untuk keperluan khusus. *IP address* kelas D disebut juga *IP address multicast*. Sedangkan *IP address* kelas E digunakan untuk keperluan *riset.*

IP address (kelas A, B, dan C) dapat dipisahkan menjadi dua bagian, yakni bagian *network* (*bit-bit network / network bit*) dan bagian *host* (*bit-bit host / host bit*). *Network bit* berperan sebagai pembeda antar *network* atau identifikasi (ID) *network*. Sedangkan *host bit* berperan sebagai identifikasi (ID) host

Gambar 3.19 Bit IP Address

1. Kelas A

Bagan IP Address kelas A sebagai berikut:



Gambar 3.20 Bit IP Address Kelas A

Bit pertama bernilai 0. Bit ini dan 7 bit berikutnya (8 bit pertama) merupakan *bit-bit network (network bit)* dan boleh bernilai berapa saja (kombinasi angka 1 dan 0). Sisanya, yaitu 24 bit terakhir merupakan bit-bit untuk host. Dapat dituliskan sebagai berikut:

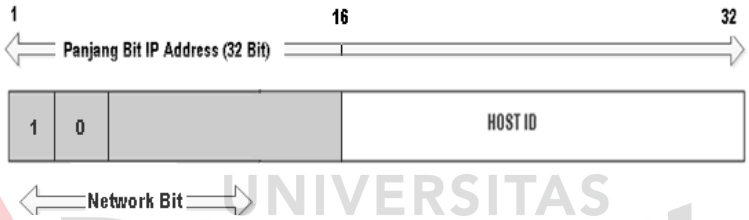
Nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

Dimana : n menyatakan *network*

h menyatakan *host*

2. Kelas B

Bagan IP Address kelas B sebagai berikut:



Gambar 3.21 Bit IP Address Kelas B

Dua bit pertama bernilai 10. Dua bit ini dan 14 bit berikutnya (16 bit pertama) merupakan *bit-bit network (network bit*) dan boleh bernilai berapa saja (kombinasi angka 1 dan 0). Sisanya, yaitu 16 bit terakhir merupakan bit-bit untuk *host*. Dapat dituliskan sebagai berikut:

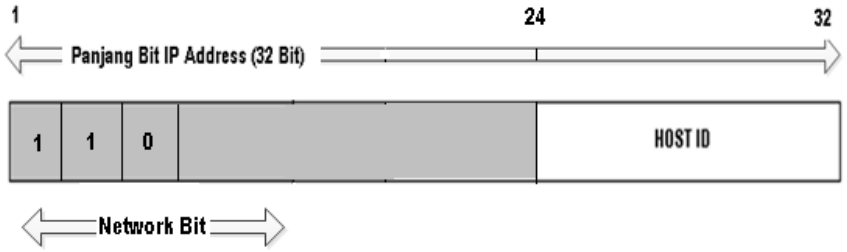
nnnnnnnn. nnnnnnnn.hhhhhhhh.hhhhhhhh

Dimana : n menyatakan *network*

h menyatakan *host*

3. Kelas C

Bagan IP Address kelas C sebagai berikut:



Gambar 3.22 Bit IP Address Kelas C

Tiga bit pertama bernilai 110. Tiga bit ini dan 21 bit berikutnya (24 bit pertama) merupakan *bit-bit network (network bit)* dan boleh bernilai berapa saja (kombinasi angka 1 dan 0). Sisanya, yaitu 8 bit terakhir merupakan bit-bit untuk *host.* Dapat dituliskan sebagai berikut:

nnnnnnnn. nnnnnnnn.hhhhhhhh.hhhhhhhh

Dimana : n menyatakan *network*

h menyatakan *host*

3.7 Virtual Local Area Network (VLAN)

VLAN (*Virtual Local Area Network*) adalah merupakan pengembangan dari LAN. VLAN adalah suatu model jaringan yang mirip dengan LAN namun tidak terbatas pada lokasi fisik. Oleh karena itu, jaringan ini dapat di konfigurasikan secara virtual dan tidak bergantung pada lokasi fisik peralatan.

Penggunaan VLAN akan membuat pengaturan jaringan menjadi sangat *fleksibel* dimana dapat dibuat segmen yang bergantung pada organisasi atau *departemen*, tanpa bergantung pada lokasi *workstation*.

VLAN ID adalah suatu informasi yang ditambahkan pada setiap frame untuk mengijinkan pengiriman frame melalui switch mode trunk, serta untuk memberikan identitas sebuah VLAN dan digunakan nomor identitas VLAN yang dinamakan VLAN ID. Dalam menandai VLAN yang terkait terdapat dua *range* VLAN ID yaitu:

1. Normal Range VLAN (1 – 1005)

- Digunakan untuk jaringan skala kecil dan menengah.
- Nomor ID 1002 s.d. 1005 dicadangkan untuk *Token Ring* dan FDDI VLAN.
- ID 1, 1002 - 1005 secara *default* sudah ada dan tidak dapat dihilangkan.
- Konfigurasi disimpan di dalam file *database* VLAN, yaitu vlan.dat. file ini disimpan dalam memori flash milkik *switch*.
- VLAN trunking protocol (VTP), yang membantu manaejemen VLAN, nanti dipelajari di bab 4, hanya dapat bekerja pada *normal range* VLAN dan menyimpannya dalam file *database* VLAN.

2. Extended Range VLANs (1006 – 4094)

Memampukan para *seervice provider* untuk memperluas infrastrukturnya kepada konsumen yang lebih banyak. Dibutuhkan untuk perusahaan skala besar yang membutuhkan jumlah VLAN lebih dari normal.

- Memiliki fitur yang lebih sedikit dibandingakn VLAN *normal range*.
- Disimpan dalam NVRAM (file *running configuration*).
- VTP tidak bekerja di sini.

3.7.1 Tipe-tipe VLAN

1. DataVLAN

Sebuah VLAN data adalah VLAN yang dikonfigurasi untuk hanya membawa user-*generated* lalu lintas. Sebuah VLAN dapat membawa suara berbasis trafik atau lalu lintas digunakan untuk mengelola saklar, namun lalu lintas ini tidak akan menjadi bagian dari VLAN data. Ini adalah praktek umum untuk memisahkan lalu lintas suara dan manajemen dari lalu lintas data. Pentingnya memisahkan data pengguna dari data switch control manajemen dan lalu lintas suara disorot oleh penggunaan istilah khusus yang digunakan untuk mengidentifikasi VLAN yang hanya membawa data pengguna - sebuah "data VLAN". Sebuah VLAN data kadang-kadang disebut sebagai VLAN pengguna.

2. Default VLAN

Semua port switch menjadi anggota VLAN *default* setelah *boot up* awal dari saklar. Memiliki semua port switch berpartisipasi dalam VLAN default membuat mereka semua bagian dari domain broadcast yang sama. Hal ini memungkinkan setiap perangkat yang terhubung ke *port switch* untuk berkomunikasi dengan perangkat lain pada port switch lainnya. *Default* VLAN untuk *switch* Cisco adalah VLAN 1. VLAN 1 memiliki semua fitur dari setiap VLAN, kecuali bahwa Anda tidak dapat mengubah nama itu dan Anda tidak dapat menghapusnya. Layer 2 kontrol lalu lintas, seperti CDP dan mencakup lalu lintas protokol pohon, akan selalu dikaitkan dengan VLAN 1 - ini tidak dapat diubah. Dalam gambar, VLAN 1 lalu lintas diteruskan selama batang VLAN

menghubungkan switch S1, S2, dan S3. Ini adalah praktek keamanan terbaik untuk mengubah default VLAN ke VLAN lain dari VLAN 1; ini memerlukan mengkonfigurasi semua port pada switch untuk dihubungkan dengan default VLAN selain VLAN 1. Batang VLAN mendukung transmisi lalu lintas dari lebih dari satu VLAN. Meskipun VLAN batang disebutkan seluruh bagian ini, mereka dijelaskan pada bagian berikutnya pada *trunking* VLAN. Catatan: Beberapa *administrator* jaringan menggunakan "VLAN *default*" untuk berarti VLAN selain VLAN 1 didefinisikan oleh *administrator* jaringan sebagai VLAN bahwa semua port yang ditugaskan untuk ketika mereka tidak digunakan. Dalam hal ini, peran hanya itu VLAN 1 memainkan adalah bahwa penanganan *Layer* 2 kontrol lalu lintas untuk jaringan.

3. NativeVLAN

Sebuah VLAN asli ditugaskan ke port trunk 802.1Q. Sebuah port trunk 802.1Q mendukung lalu lintas yang datang dari banyak VLAN (tagged traffic) serta lalu lintas yang tidak datang dari sebuah VLAN (untagged lalu lintas). Port trunk 802.1Q menempatkan untagged lalu lintas pada VLAN asli. Dalam gambar, VLAN asli adalah VLAN 99. Lalu lintas untagged dihasilkan oleh komputer terpasang ke port switch yang dikonfigurasi dengan VLAN asli. VLAN asli ditetapkan dalam spesifikasi IEEE 802.1Q untuk menjaga kompatibilitas dengan lalu lintas tanpa tanda umum untuk skenario warisan LAN. Untuk tujuan kita, VLAN asli berfungsi sebagai pengenal umum pada lawan ujung sebuah link trunk. Ini adalah praktek terbaik untuk menggunakan VLAN selain VLAN 1 sebagai VLAN asli.

4. Management VLAN

Sebuah VLAN manajemen adalah setiap VLAN Anda mengkonfigurasi untuk mengakses kemampuan manajemen dari *switch*. VLAN 1 akan melayani sebagai VLAN manajemen jika Anda tidak secara proaktif menentukan VLAN unik untuk melayani sebagai VLAN manajemen. Anda menetapkan VLAN manajemen alamat IP dan subnet mask. *Switch* dapat dikelola melalui HTTP, Telnet, SSH, atau SNMP. Karena konfigurasi *out-of-the-box* sebuah switch Cisco memiliki VLAN 1 sebagai VLAN default, Anda melihat bahwa VLAN 1 akan menjadi pilihan yang buruk sebagai VLAN manajemen; Anda tidak ingin pengguna sewenang-wenang menghubungkan ke saklar untuk default ke VLAN manajemen. Ingat bahwa Anda mengkonfigurasi VLAN manajemen VLAN 99 di Konsep Beralih Dasar dan bab Konfigurasi.

3.7.2 Pengertian Mode Access dan Trunk

Ø Mode Access adalah mengatur config yang ada pada suatu vlan agar terhubung dengan jaringan vlan yang lainnya.

Ø Trunk pada VLAN adalah link point-to-point diantara satu atau lebih dari *interface Ethernet* dan perangkat lain jaringan, yang dimana merupakan saluran untuk VLAN antara *switch* dan *router*. *Trunk* membawa lalu lintas untuk memperluas VLAN melintasi seluruh jaringan.

3.7.3 Proses Tagging pada VLAN

VLAN Tagging adalah sebuah standar jaringan yang ditulis oleh kelompok kerja IEEE 802.1 mengizinkan beberapa jaringan bridge untuk transparan berbagi link jaringan fisik yang sama tanpa kebocoran informasi antara jaringan. IEEE 802.*1Q* - bersama dengan bentuk singkat dot1q - biasanya digunakan untuk merujuk pada protokol *enkapsulasi* yang digunakan untuk menerapkan mekanisme ini melalui jaringan *Ethernet*.

IEEE 802.1Q mendefinisikan arti dari sebuah *Virtual LAN* (VLAN) yang berkaitan dengan model konseptual tertentu yang mendukung *bridging* pada lapisan MAC dan 802.1D IEEE protokol *spanning tree*. Protokol ini memungkinkan untuk setiap VLAN untuk berkomunikasi dengan satu sama lain dengan menggunakan sebuah *switch* dengan kemampuan lapisan-3, atau *router*.

3.8 Pengertian DHCP

DHCP (*Dynamic Configuration Protocol*) adalah layanan yang secara otomatis memberikan nomor IP kepada komputer yang memintanya. Komputer yang memberikan nomor IP disebut sebagai ***DHCP server***, sedangkan komputer yang meminta nomor IP disebut sebagai DHCP Client. Dengan demikian administrator tidak perlu lagi harus memberikan nomor IP secara manual pada saat konfigurasi TCP/IP, tapi cukup dengan memberikan referensi kepada DHCP Server.

Pada saat kedua DHCP client dihidupkan , maka komputer tersebut melakukan request ke DHCP-Server untuk mendapatkan nomor IP. DHCP

menjawab dengan memberikan nomor IP yang ada di database DHCP. DHCP Server setelah memberikan nomor IP, maka server meminjamkan (lease) nomor IP yang ada ke DHCP-*Client* dan mencoret nomor IP tersebut dari daftar pool. Nomor IP diberikan bersama dengan subnet mask dan *default gateway*. Jika tidak ada lagi nomor IP yang dapat diberikan, maka *client* tidak dapat menginisialisasi TCP/IP, dengan sendirinya tidak dapat tersambung pada jaringan tersebut.

Setelah periode waktu tertentu, maka pemakaian DHCP *Client* tersebut dinyatakan selesai dan client tidak memperbaharui permintaan kembali, maka nomor IP tersebut dikembalikan kepada DHCP Server, dan server dapat memberikan nomor IP tersebut kepada *Client* yang membutuhkan. Lama periode ini dapat ditentukan dalam menit, jam, bulan atau selamanya. Jangka waktu disebut *leased period.*

Kelebihan DHCP

1. Memudahkan dalam *transfer* data kepada PC *client* lain atau PC *server*.
2. DHCP menyediakan alamat-alamat IP secara dinamis dan konfigurasi lain. DHCP ini didesain untuk melayani network yang besar dan konfigurasi TCP/IP yang kompleks.
3. DHCP memungkinkan suatu client menggunakan alamat IP yang reusable, artinya alamat IP tersebut bisa dipakai oleh client yang lain jika client tersebut tidak sedang menggunakannya (off).
4. DHCP memungkinkan suatu *client* menggunakan satu alamat IP untuk jangka waktu tertentu dari server.

5. DHCP akan memberikan satu alamat IP dan parameter-parameter kofigurasi lainnya kepada client.

3.9 Routing

Routing adalah proses dimana suatu *router* meneruskan paket ke jaringan yang dituju. Suatu *router* membuat keputusan berdasarkan IP address yang dituju oleh paket. Semua *router* menggunakan *IP address* tujuan untuk mengirim paket. Agar keputusan routing tersebut benar, *router* harus belajar bagaimana untuk mencapai tujuan.

Terdapat dua macam penghalaan, yaitu:

1. *Static Routing*
2. *Dynamic Routing*

3.9.1 Static Routing

Router meneruskan paket dari sebuah network ke *network* yang lainnya berdasarkan *rute* (catatan: seperti rute pada bis kota) yang ditentukan oleh administrator. Rute pada *static routing* tidak berubah, kecuali jika diubah secara manual oleh *administrator.*

kekurangan dan kelebihan *static routing:*

- Dengan menggunakan *next hop*

Next hop adalah *ip address* pertama yang akan didapat pertama kali ketika mengirim paket ke jaringan berikutnya.

(+) Dapat mencegah terjadinya eror dalam meneruskan paket ke router tujuan apabila *router* yang akan meneruskan paket memiliki *link* yang terhubung dengan banyak *router*.itu disebabkan karena *router* telah mengetahui *next hop*, yaitu ip address *router* tujuan

(–) *Static routing* yang menggunakan *next hop* akan mengalami *multiple lookup* atau *lookup* yg berulang. *lookup* yg pertama yang akan dilakukan adalah mencari *network* tujuan,setelah itu akan kembali melakukan proses *lookup* untuk mencari *interface* mana yang digunakan untuk menjangkau *next* hopnya.

- Dengan menggunakan exit interface

Exit interface adalah *interface* yang akan dilewati ketika akan mengirim sebuah paket yang akan keluar dari router.

(+) Proses *lookup* hanya akan terjadi satu kali saja (*single lookup*) karena *router* akan langsung meneruskan paket ke *network* tujuan melalui *interface* yang sesuai pada *routing table.*

(–) Kemungkinan akan terjadi *error* ketika meneruskan paket. jika *link router* terhubung dengan banyak *router*, maka *router* tidak bisa memutuskan *router* mana tujuanya karena tidak adanya *next hop* pada tabel *routing*. karena itulah, akan terjadi *error*.

Routing static dengan menggunakan *next hop* cocok digunakan untuk jaringan *multi-access network* atau *point to multipoint* sedangkan untuk jaringan *point to point,* cocok dengan menggunakan *exit interface* dalam mengkonfigurasi *static route.*

Recursive route lookup adalah proses yang terjadi pada *routing* tabel untuk menentukan *exit interface* mana yang akan digunakan ketika akan meneruskan paket ke tujuannya.

Default routing digunakan untuk meneruskan paket dengan tujuan yang tidak sama dengan *routing* yang ada dalam *table routing*. Secara tipikal *router* dikonfigurasi dengan cara *routing default* untuk trafik internet. *Routing default* secara actual menggunakan format:

- **ip route 0.0.0.0 0.0.0.0** [*next-hop-address* | *outgoing interface*]
- Mask 0.0.0.0, secara logika jika kita AND-kan dengan IP address tujuan selalu menunjuk ke jaringan 0.0.0.0. Jika paket tidak cocok dengan rute yang ada dalam table routing, maka paket akan diteruskan ke jaringan 0.0.0.0.

3.9.2 Dynamic Routing

Dynamic router mempelajari sendiri *Rute* yang terbaik yang akan ditempuhnya untuk meneruskan paket dari sebuah *network* ke *network* lainnya. Administrator tidak menentukan rute yang harus ditempuh oleh paket-paket tersebut. Administrator hanya menentukan bagaimana cara *router* mempelajari paket, dan kemudian *router* mempelajarinya sendiri. Rute pada *dynamic routing* berubah, sesuai dengan pelajaran yang didapatkan oleh *router*.

Apabila jaringan memiliki lebih dari satu kemungkinan rute untuk tujuan yang sama maka perlu digunakan *dynamic routing*. Sebuah *dynamic routing* dibangun berdasarkan informasi yang dikumpulkan oleh protokol *routing*. Protokol ini didesain untuk mendistribusikan informasi yang secara dinamis mengikuti perubahan kondisi jaringan. Protokol routing mengatasi situasi routing yang kompleks secara cepat dan akurat. Protokol routng didesain tidak hanya untuk mengubah ke rute backup bila rute utama tidak berhasil, namun juga didesain untuk menentukan rute mana yang terbaik untuk mencapai tujuan tersebut.

Pengisian dan pemeliharaan tabel *routing* tidak dilakukan secara manual oleh admin. *Router* saling bertukar informasi routing agar dapat mengetahui alamat tujuan dan menerima tabel *routing*. Pemeliharaan jalur dilakukan berdasarkan pada jarak terpendek antara *device* pengirim dan *device* tujuan.

dibawah ini adalah dinamik *routing* yang sering digunakan :

1. Routing Information Protocol (RIP)
2. Interior Gateway Routing Protocol (IGRP)
3. Open Shortest Path First (OSPF)
4. Enchanced Interior Gatway Routing Protocil (EIGRP)
5. Exiterior Gateway Protocol (EGP)

3.10 Access Control List (ACL)

Access Control List biasa disebut dengan *Access list* adalah pengelompokan paket berdasarkan kategori. *Access list* bisa sangat membantu ketika membutuhkan pengontrolan dalam lalu lintas *network. access list* menjadi *tool* pilihan untuk pengambilan keputusan pada situasi ini. Penggunaan *access list* yang paling umum dan paling mudah untuk dimengerti adalah penyaringan paket yang tidak diinginkan ketika mengimplementasikan kebijakan keamanan. Sebagai contoh kita dapat mengatur *access list* untuk membuat keputusan yang sangat spesifik tentang peraturan pola lalu lintas sehingga *access list* hanya memperbolehkan *host* tertentu mengakses sumber daya WWW sementara yang lainnya ditolak. Dengan kombinasi *access list* yang benar, network manajer mempunyai kekuasaan untuk memaksa hamper semua kebijakan keamanan yang bisa mereka ciptakan. (Rochmad, 2010)

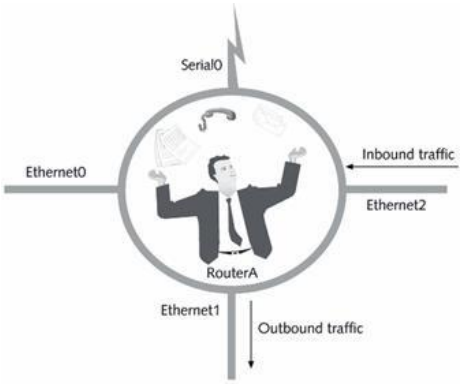
Access list juga bisa digunakan pada situasi lain yang tidak harus meliputi penolakan paket. Sebagai contoh *access list* digunakan untuk mengontrol *network* mana yang akan atau tidak dinyatakan oleh *protocol dynamic routing*. Konfigurasikan *access list* dengan cara yang sama. Perbedaannya disibni hanyalah bagaimana menerapkannya ke *protocol routing* dan bukan ke *interface*. Kita juga bisa menggunakan access list untuk mngkategorikan paket atau antrian /layanan QOS, dan mengontrol tipe lalu lintas data nama yang akan mengaktifkan link ISDN.

Membuat *access list* sangat mirip dengan statement pada programming if – then jika sebuah kondisi terpenuhi maka aksi yang diberikan akan dijalankantidak terpenuhi, tidak ada yang terjadi dan statemen berikutnya akan dievaluasi.

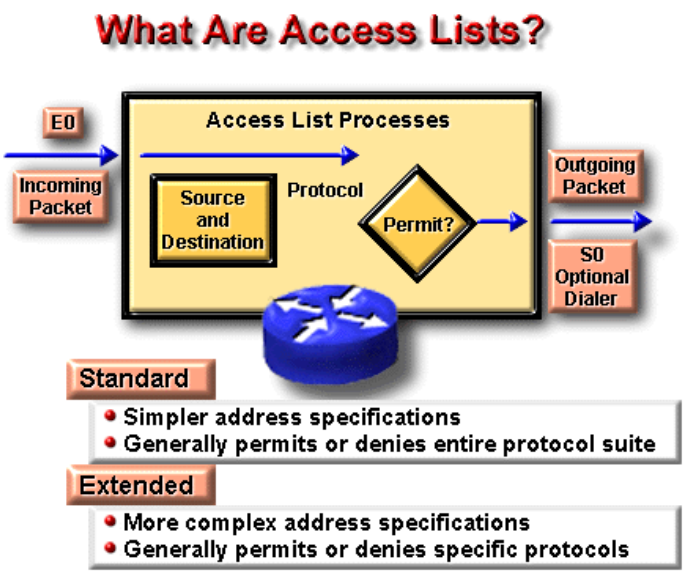
Statement ACL pada dasarnaya dalah paket *filter* dimana paket dibandingkan, dimana paket dikategorikan dan dimana suatu tindakan terhadap paket dilakukan.

List(daftar) yang telah dibuat bisa diterpakan baik kepada lalulintas inbound maupun *outbound* pada *interface* mana saja. Menerapkan ACL menyebabkan *router* menganalisa setiap paket arah spesifik yang melalui *interface* tersebut dan mengmbil tindakan yang sesuai. Ketika paket dibandingkan dengan ACL, terdapat beberapa peraturan (*rule*) penting yang diikuti:

- Paket selalu dibandingkan dengan setiap baris dari ACL secara berurutan, sebagai contoh paket dibandingkan dengan baris pertama dari ACL, kemudian baris kedua, ketiga, dan seterusnya.
- Paket hanya dibandingkan baris-baris ACL sampai terjadi kecocokan. Ketika paket cocok dengan kondisi pada baris ACL, paket akan ditindaklanjuti dan tidak ada lagi kelanjutan perbandingan.
- Terdapat statement "tolak" yang tersembunyi (*impilicit deny*) pada setiap akhir baris ACL, ini artinya bila suatu paket tidak cocok dengan semua baris kondisi pada ACL, paket tersebut akan ditolak



Gambar 3.23 Implementasi Router



Gambar 3.24 Ketentuan ACL

3.10.1 Jenis ACL

1. Standard ACL

Standard ACL hanya menggunakan alamat sumber IP di dalam paket IP sebagai kondisi yang ditest. Semua keputusan dibuat berdasarkan alamat IP sumber. Ini artinya, standard ACL pada dasarnya melewatkan atau menolak seluruh paket *protocol*. ACL ini tidak membedakan tipe dari lalu lintas IP seperti WWW, telnet, UDP, DSP.

2. Extended ACL

Extended ACL bisa mengevalusai banyak *field* lain pada *header layer* 3 dan layer 4 pada paket IP. ACL ini bisa mengevaluasi alamat IP sumber dan tujuan, *field protocol* pada *header network layer* dan nomor *port* pada *header*

transport layer. Ini memberikan *extended ACL* kemampuan untuk membuat keputusan-keputusan lebih spesifik ketika mengontrol lalu lintas.

Gambar 3.25 Tempat peletakan ACL

3.10.2 Jenis Lalu Lintas ACL

1. Inbound ACL

Ketika sebuah ACL diterapkan pada paket *inbound* di sebuah *interface*, paket tersebut diproses melalui ACL sebelum di-*route* ke *outbound interface*. Setiap paket yang ditolak tidak bisa di-*route* karena paket ini diabaikan sebelum proses *routing* diabaikan.

2. Outbond ACL

Ketika sebuah ACL diterapkan pada paket *outbound* pada sebuah *interface*, paket tersebut di-route ke outbound *interface* dan diproses melalui ACL malalui antrian.

3.10.3 Panduan Umum ACL

Terdapat beberapa panduan umum ACL yang seharusnya diikuti ketika membuat dan mengimplementasikan ACL pada *router* :

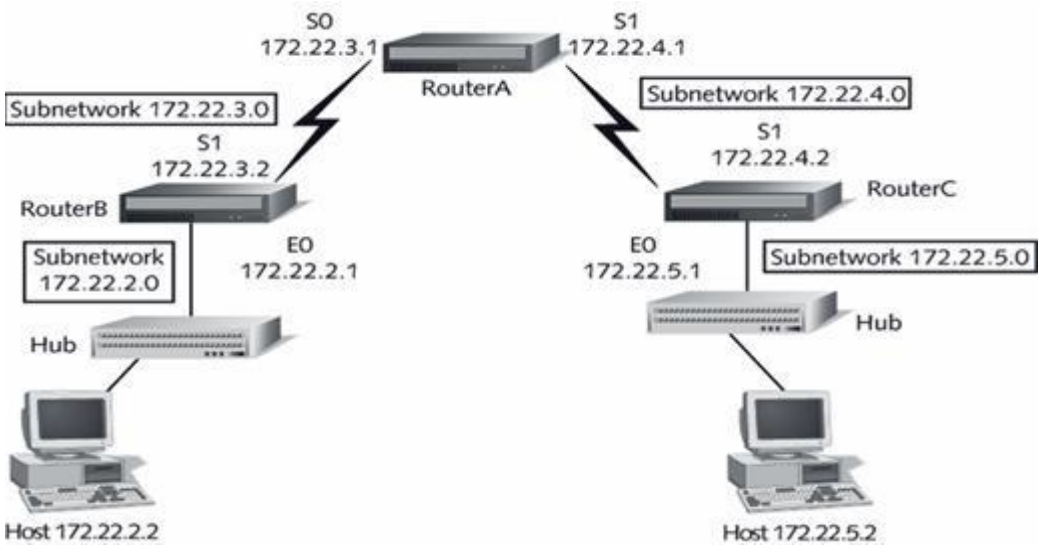
- Hanya bisa menerapkan satu ACL untuk setiap *interface*, setiap *protocol* dan setiap arah. Artinya bahwa ketika membuat ACL IP, hanya bisa membuat sebuah *inbound ACL* dan satu *Outbound ACL* untuk setiap *interface*.
- Organisasikan ACL sehingga test yang lebih spesifik diletakkan pada bagian atas ACL
- Setiap kali terjadi penambahan *entry* baru pada ACL, *entry* tersebut akan diletakkan pada bagian bawah ACL. Sangat disarankan menggunakan *text editor* dalam menggunakan ACL
- Tidak bisa membuang satu baris dari ACL. Jika kita mencoba demikian, kita akan membuang seluruh ACL. Sangat baik untuk mengcopy ACL ke *text editor* sebelum mencoba mengubah *list* tersebut.

3.10.4 Wildcard Masking

Wildcard masking digunakan bersama ACL untuk menentukan *host* tunggal, sebuah jaringan atau *range* tertentu dari sebuah atau banyak *network.* Untuk mengerti tentang *wildcard*, kita perlu mengerti tentang blok *size* yang digunkan untuk menentukan range alamat. Beberapa blok *size* yang berbeda adalah 4, 8, 16, 32, 64.

Ketika kita perlu menentukan *range* alamat, kita memilih blok *size* selanjutnya yang terbesar sesuai kebutuhan. Sebagai contoh, jika kita perlu menentukan 34 *network*, kita memerlukan blok *size* 64. jika kita ingin menentukan 18 *host*, kita memerlukan blok size 32. jiak kita perlu menunjuk 2 network, maka blok size 4 bisa digunakan. *Wildcard* digunakan dengan alamat *host* atau *network* untuk memberitahukan kepada *router* untuk difilter. Untuk menentukan sebuah host, alamat akan tampak seperti berikut 172.16.30.5 0.0.0.0 keempat 0 mewakili setiap *oktet* pada alamat. Dimanapun terdapat 0, artinya oktet pada alamat tersebut harus persis sama. Untuk menentukan bahwa sebuah *oktet* bisa bernilai apa saja, angka yang digunakan adalah 255. sebagai contoh, berikut ini adalah *subnet* /24 dispesifikasikan dengan *wildcard*: 172.16.30.0 0.0.255 ini memberitahukan pada *router* untuk menentukan 3 oktet secara tepat, tapi *oktet* ke-4 bisa bernilai apa saja.

3.10.5 Gambaran Standart Access List dan Extended Access List



Gambar 3.26 Contoh jaringan yang terhubung

1. **Standard Access List**

Standard IP ACL memfilter lalu lintas *network* dengan menguji alamat sumber IP didalam paket. Kita membuat *standard IP ACL* dengan menggunakan nomor ACL 1-99 atau 1300-1999(*expanded range*). Tipe ACL pada ummnya dibedakan berdasarkan nomor yang digunakan ketika ACL dibuat, *router* akan mengetahui tipe *syntax* yang diharapkan untuk memesukkan daftar. Dengan menggunakan nomor 1-99 atau 1300-1999, kita memberitahukan kepada *router* bahwa kita ingin membuat IPACL, jadi *router* akan mengharapkan *syntax* yang hanya menspesifikasikan alamat sumber IP pada baris pengujian. Banyak *range* nomor ACL pada contoh dibawah ini yang bisa kita gunakan untuk memfilter lalu lintas pada jaringan kita (*protocol* yang bisa kita terapkan ACL bisa tergantung pada versi IOS kita) :

Table 3.1 Perberdaan *Standart dan Extended*

TIPE ACL	NUMBER RANGE/IDENTIFIER
Standard	1-99, 1300-1999
Extended	100-1999, 2000-2699

Contoh *Standard ACL* untuk menghentikan *user* tertentu mendapatkan akses ke LAN *Department Finance*. Pada gambar, *router* mempunyai 3 koneksi LAN dan 1 koneksi WAN ke internet. *User* pada LAN Sales tidak boleh mempunyai akses ke LAN *finance*, tapi mereka boleh mengakses internet dan *Department Marketing*. LAN Marketing perlu mengakses LAN Finance untuk layanan aplikasi Pada router yang digambar, *standard IP ACL* berikut dikonfigurasi :

```
Lab_A#config t

Lab_A(config)#access -list 10 deny 172.16.40.0
0.0.0.255

Lab_A(config)#access-list 10 permit any
```

Sangatlah penting untuk diketahui bahwa perintah *any* sama halnya dengan menggunakan *wildcard* masking berikut :

```
Lab_A(config)#access-list 10 permit 0.0.0.0
255.255.255.255
```

Karena *wildcard* mask menyatakan bahwa tidak ada oktet yang diperiksa, setiap alamat akan sesuai dengan kondisi *test*. Jadi fungsi ini sama dengan penggunaan kata *any*. Saat ini, ACL dikonfigurasi untuk menolak alamat sumber dari LAN sales yang mengakses LAN *finance*, dan memperbolehkan dari akses yang lain. Tetapi untuk diingat, tidak ada tindakan yang diambil sampai akses *list* diterapkan pada arah yang spesifik. Tetapi dimana ACL ini seharusnya ditempatkan? Jika kita menempatkannya pada E0, kita mungkin akan mematikan juga *interface Ethernet* karena semua peralatan LAN Sales akan ditolak akses ke semua *network* yang terhubung ke *router*.

Tempat terbaik untuk menerapkan ACL ini adalah pada E1 sebagai *outbound list:*

```
Lab_A(config)#Int E1

Lab_A(config-if)#ip access-group  10 out
```

Ini menghentikan secara tuntas lalu lintas 172.16.40.0 keluar dari *Ethernet* 1. Ini tidak ada pengaruhnya terhadap *host* dari LAN Sales yang mengakses LAN *marketing* dan internet, karena lalu lintas ke tujuan tersebut tidak melalui *interface* E1. Setiap paket yang mencoba keluar dari E1 harus melalui ACL terlebih dahulu. JIka terdapat *inbound list* yang ditempatkan pada E0, maka setiap paket yang mencoba masuk ke *interface* E0 akan harus melalui ACL terlebih dahulu sebelum di *route* ke *interface* keluar.

Keistimewaan Standard Access List

Software Cisco IOS dapat memprovide pesan *logging* tentang paket – paket. Yang diijinkan atau ditolak oleh *standard IP access list*. Itulah sebabnya beberapa paket dapat cocok dengan *access list*.yang disebabkan oleh informasi pesan *logging*.tentang paket yang telah dikirimkan ke *console*. *Level* dari pesan *logging* ke *console* yang dikendalikan oleh perintah *logging console*.Kemampuan ini hanya terdapet pada *extended IP access lists.*

Triggers paket pertama *access list* menyebabkan *logging message* yang benar, dan paket – paket berikutnya yang dikumpulkan lebih dari *interval* 5-menit sebelum ditampilkan. Pesan *logging* meliputi nomor *access list*, apakah paket tersebut diterima atau ditolak, alamat IP sumber dari paket dan nomor asal paket yang diterima sumber atau ditolak dalam *interval* 5 menit.

KEUNTUNGAN

Kita dapat memantau berapa banyak paket yang diijinkan atau ditolak oleh *access list* khusus termasuk alamat tujuan setiap paket.

Membuat Standard Access List Menggunakan Nomor

Untuk membuat nomor *standard access list* dan menerima pesan *logging*, ditampilkan dalam *mode global* konfigurasi, sebagai berikut :

Tabel 3.2 *Standart* ACL dengan nomor

Task	Command
Mendefinisikan *standard IP access list* menggunakan alamat tujuan dan *wildcard.*	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] **log**
Mendefinisikan *standard access list* menggunakan singkatan untuk *sumber mask* dari 0.0.0.0.	**access-list** *access-list-number* {**deny** | **permit**} **any log**

Membuat Standard Access List Menggunakan Nama

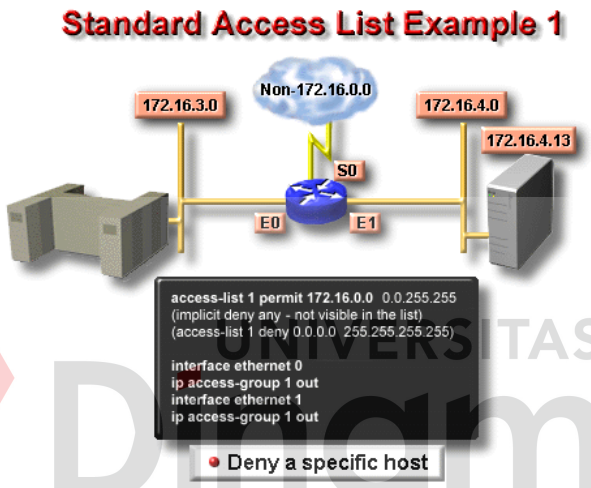
Untuk membuat nama *standard access list* dan menerima pesan *logging*, berikut adalah permulaan dalam *mode global* konfigurasi.

Tabel 3.3 *Standart ACL* dengan nama

Task	Command
Step 1. Definisikan standard IP access list berdasarkan nama	**ip access-list standard** *name*
Step 2. Dalam mode konfigurasi *access list* menspesifikasikan satu atau lebih kondisi yang diperbolehkan atau ditolak. Ini menentukan apakah paket itu dilewatkan atau diterima.	**deny** {*source* [*source-wildcard*] | **any**} **log** or **permit** {*source* [*source-wildcard*] | **any**} **log**
Step 3. Keluar dari mode konfigurasi *access list.*	**exit**

Untuk mendefinisikan standard IP access list dengan nomor, menggunakan *standard version* dari ***acess-list*** *ration* untuk memindahkan sebuah *standard access list*, maka digunakan perintah berikut

access-list *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**] **no access-list** *access-list-number*

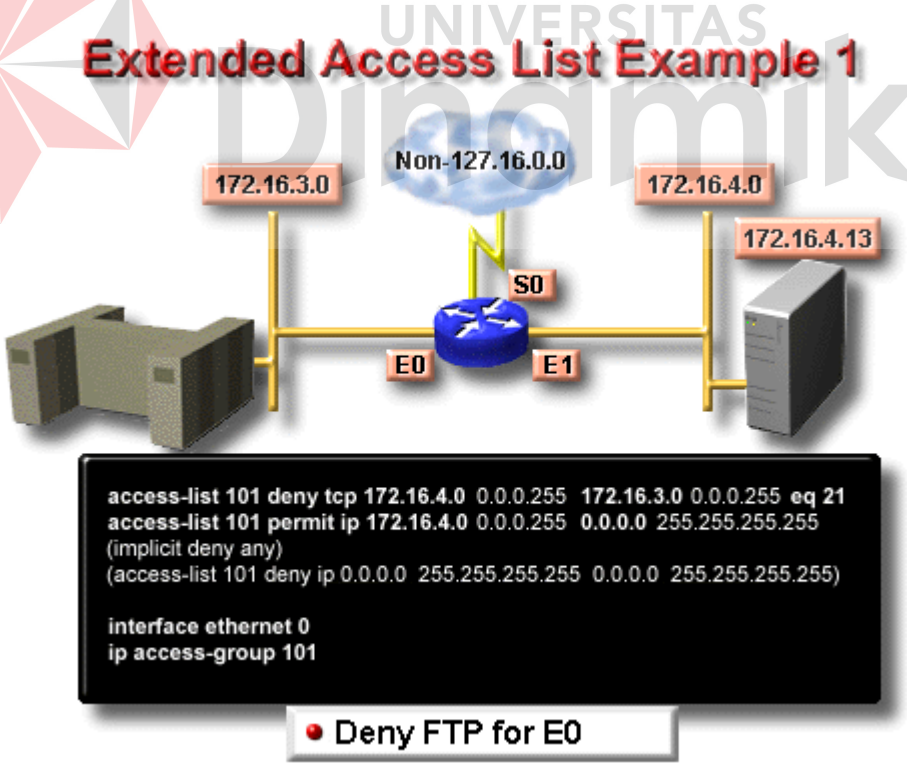


Gambar 3.27 Contoh *Standart ACL*

2. Extended ACL

Extended ACL bisa mengevaluasi banyak field lain pada *header layer* 3 dan *layer* 4 pada paket IP. ACL ini bisa mengevaluasi IP sumber dan tujuan, *field protocol* dalam *network header Network Layer* dan nomor *port* pada *Transport Layer*. Ini memberikan *extended ACL* kemampuan untuk membuat keputusan – keputusan lebih spesifik ketika mengontrol lalu lintas. Pada contoh *Standard ACL*, perhatikan bagaimana kita harus memblok semua akses dari LAN Sales ke *Department Finance*. Bagaimana jika untuk urusan keamanan, kita membutuhkan

Sales mendapatkan akses ke *server* tertentu pada *LAN Finance* tapi tidak ke layanan *network* lainnya ? Dengan *standard IP ACL*, kita tidak memperbolehkan user mendapat satu layanan sementara tidak untuk yang lainnya. Dengan kata lain, ketika kita membutuhkan membuat keputusan berdasarkan alamat sumber dan tujuan, *standard ACL* tidak memperbolehkan kita melakukannya karena ACL ini hanya mambuta kaputusan berdasrkan alamat sumber. Tetapi *extended ACL* akan membantu kita karena *extended ACL* memperbolehkan kita menentukan alamat sumber dan tujuan serta protocol dan nomor *port* yang mengidentfikasikan *protocol upper layer* atau aplikasi. Dengan menggunakan *extended ACL* kita bisa secara efisien memperbolehkan user mengakses ke fisik LAN dan menghentikan host tertentu atau bahkan layanan tertentu pada host tertentu.



Gambar 3.28 Contoh *Extended ACL*

Contoh *Extended Access List* adalah Layanan lain pada *host* ini dan *host* lainnya bisa diakses oleh departertmen seles dan marketing. Berikut adalah *access list* yang dibuat:

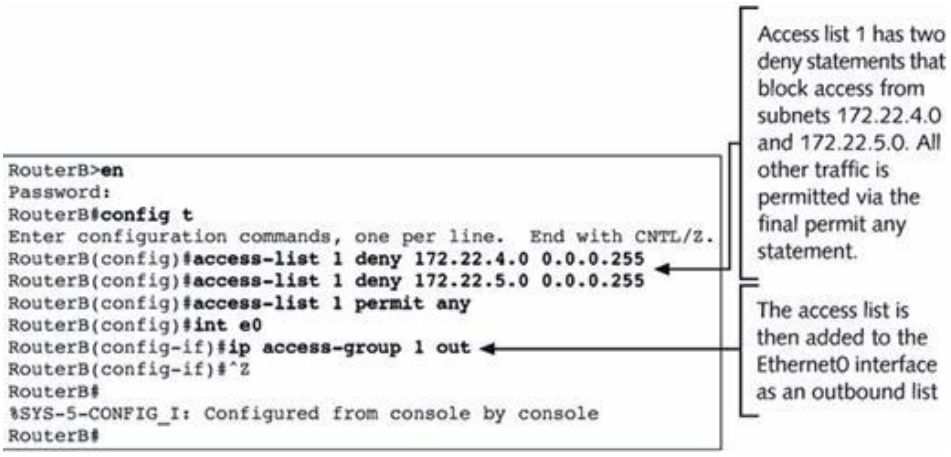
```
Lab_A#config t

Lab_A(config)#access-list 110 deny tcp any host
172.16.30.5 eq 21

Lab_A(config)#access-list 110 deny tcp any host
172.16.30.5 eq 23

Lab_A(config)#access-list 110 permit ip any any
```

Access list 110 memberitahukan ke *router* bahwa anda membuat *Extended* IP *Access List*. TCP adalah field procol pada *heather layer network*. Jika pada *list* tidak terdapat TCP disini, anda tidak bisa menyaring berdasarkan nomor port 21 dan 23 seperti yang diperlihatkan pada contoh (yaitu FTP dan Telnet dan keduanya menggunakan TCP untuk layanan *conection - oriented*). Perintah *any* disini adalah sumber, yang berarti semua alamat IP dan *host* adalah alamat IP tujuan. Setelah *list* dibuat, maka selanjutnya perlu diterapkan pada *outbound interface ethernet* 1.



Gambar 3.29 Konfigurasi ACL

- Hukum *Access List*
- Daftar aplikasi *router* secara berurutan menunjukan apa yang ditulis ke daalm *router*.
- Daftar aplikasi *router* untuk paket yang berurutan.
- Packet akan diproses jika cocok dan berdasarkan *criteria access list* termasuk pernyataan *access list.*
- *Implicit deny any*
    - Semua paket yang tidak memenuhi syarat dari *acces list* akan di blok oleh perintah permit any yang digunakan pada akhir list.
- Hanya satu list, per *protocol*, per perintah yang dapat diaplikasikan pada *interface.*
- Kita tidak dapat memindahkan satu baris dari *access list*.
- *Access list* akan efektif segera setelah diaplikasikan.

3.11 Network Address Translation (NAT)

Network Address Translation (NAT) adalah suatu teknik untuk mengubah suatu IP address ke IP address yg lain. NAT dirancang untuk menghemat penggunaan IP address dan memungkinkan jaringan untuk menggunakan IP address *private* pada jaringan *internal* NAT memungkinkan alat secara khas beroperasi di perbatasan dari *stub network*. *Stub network* adalah jaringan yang mempunyai koneksi tunggal ke jaringan tetangganya. Ketika suatu host dalam *stub network* ingin mengirim paket ke host yang luar, host tersebut meneruskan paket ke perbatasan *gateway router*. Diperbatasan *gateway router* ini dilakukan proses NAT, menterjemahkan alamat *private internal* ke *public* atau alamat *routable eksternal*.

Keterbatasan alamat IPv.4 merupakan masalah pada jaringan global atau Internet.Untuk memaksimalkan penggunakan alamat IP yang diberikan oleh *Internet Service Provider* (ISP) dapat digunakan *Network Address Translation* Untuk memaksimalkan penggunakan alamat IP yang diberikan oleh Internet *Service Provider* (ISP) dapat digunakan *Network Address Translation* atau NAT.

Keuntungan menggunakan NAT:

a. Menghemat alamat IP legal (yang ditetapkan oleh *Network Interface Card* (NIC) atau *service provider*)
b. Mengurangi terjadnya penggandaan alamat jaringan IP
c. Meningkatkan fleksibilitas untuk koneksi ke internet
d. Menghindarkan proses pengalamatan kembali pada saat jaringan berubah

Kerugian menggunakan NAT :

a. Translasi menimbulkan *delay switching*

b. Menghilangkan kemampuan *trace end to end IP*

c. Aplikasi tertentu tidak dapat berjalan jika menggunakan NAT

3.11.1 Dua Tipe NAT

Dua tipe NAT adalah *Static* dan Dinamik yang keduanya dapat digunakan secara terpisah maupun bersamaan.

a. Statik

Translasi *Static* terjadi ketika sebuah alamat lokal (*inside*) di petakan ke sebuah alamat *global*/internet (*outside*). Alamat lokal dan global dipetakan satu lawan satu secara Statik.

b. Dinamik

1. NAT dengan *Pool* : Translasi Dinamik terjadi ketika *router* NAT diset untuk memahami alamat lokal yang harus ditranslasikan, dan kelompok (*pool*) alamat *global* yang akan digunakan untuk terhubung ke internet. Proses NAT Dinamik ini dapat memetakan bebarapa kelompok alamat lokal ke beberapa kelompok alamat *global*.
2. *NAT Overload*: Sejumlah IP lokal/*internal* dapat ditranslasikan ke satu alamat IP *global/outside*. Hal ini sangat menghemat penggunakan alokasi IP dari ISP. *Sharing*/pemakaian bersama satu alamat IP ini menggunakan metoda *port multiplexing*.

3.11.2 Komponen NAT

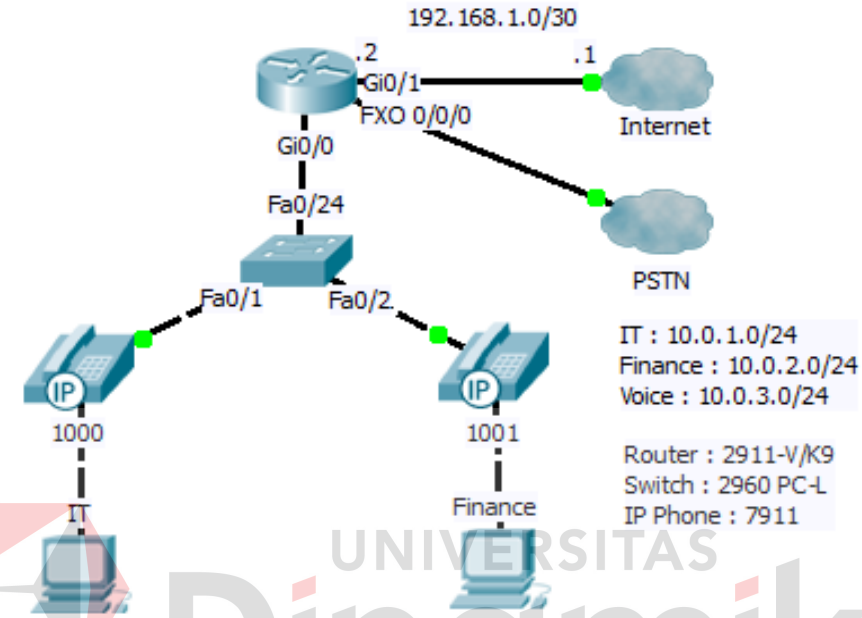
NAT dapat melewatkan alamat jaringan lokal (‘*private*’) menuju jaringan ‘*public*’ seperti Internet. Alamat ‘private’ yang berada pada jaringan lokal

/"*inside*", mengirim paket melalui router NAT, yang kemudian dirubah oleh *router* NAT menjadi alamat IP ISP sehingga paket tersebut dapat diteruskan melewati jaringan publik atau internet. Awalnya fitur ini hanya tersedia pada *gateway pass-through firewall* saja. Tapi sekarang sudah tersedia di semua *router* Cisco.

BAB IV

DESKRIPSI KERJA PRAKTEK

4.1 Topologi Jaringan



Gambar 4.1 Topologi Jaringan

Gambar diatas adalah konfigurasi jaringan LAN kantor Edavos Jakarta yang menggunakan Cisco *router* 2911-V/K9 *support Call Manager Express* (CME), modul FXO, cisco *switch* 2960 PC-L (*support* PoE), cisco IP *phone* 7911, dan 2 PC atau *notebook*. Pada perancangan tersebut penulis mengkonfigurasi dengan ketentuan seperti berikut :

1. Konfigurasi semua IP dapat dari DHCP router.
2. Konfigurasi PC 1 (IT) dengan PC 2 (Finance) pada jaringan yang berbeda.
3. Konfigurasi PC agar saling terhubung.

4. Konfigurasi PC1 dapat menghubungi PC2, namun PC2 tidak dapat menghubungi PC1 ataupun internet.
5. IP PC 1 : 10.0.1.0/24 dan IP PC 2 : 10.0.2.0/24
6. IP ke isp : 192.168.1.x/24

4.2 Perankat yang digunakan

Switch

Switch yang digunakan adalah *switch* yang mendukung PoE (*Power of Ethernet*) yang mana digunakan untuk sumber daya listrik melalui *port ethernet*.

Gambar 4.2 Switch 2960

Router

Router yang digunakan untuk menyelesaikan topologi diatas adalah *router* yang mendukung CME (*Call Manager Express*).

Gambar 4.3 2911-V/K9

4.3 Mengkoneksikan Notebook ke Cisco Switch Cisco Router CME

ada beberapa cara yang bisa dilakukan untuk setting dan konfigurasi *router* maupun *switch*. Berikut adalah beberapa cara yang umum digunakan:

- Console

  Cara yang paling aman dan mudah untuk mengkonfigurasi *switch* dan *router*.. Cara ini menggunakan software bantuan hyperterminal yang sudah secara default terinstall di Windows XP atau menggunakan software putty.

- Telnet

  Cara ini kurang aman karena *user* memasukkan *username* dan *password router* atau *switch* dalam format *plain text* tidak terenkripsi. Cara ini menggunakan bantuan command prompt pada windows atau terminal pada linux dengan mengetikkan telnet.

- SSH

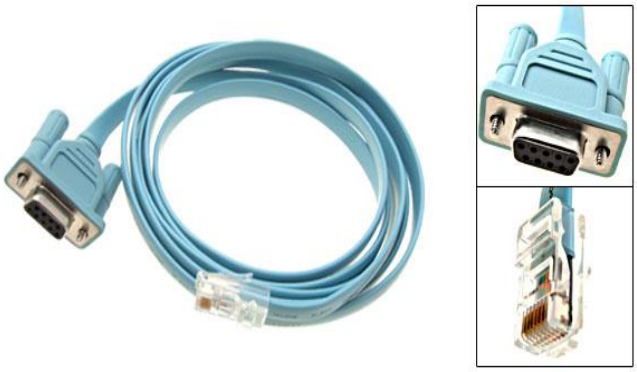
  Cara ini lebih aman dibandingkan dengan telnet, karena *username* dan *password* yang dikirim ke *router* atau *switch* di-enkripsi. Cara ini dapat dilakukan dengan bantuan *software* putty atau ssh client.

- Web Login

  Cara ini menjadikan router sebagai web server. Cara ini kurang aman sehingga banyak administrator jaringan menonaktifkan fitur ini. *Software* bantuan yang dibutuhkan adalah web *browser* seperti IE, Mozilla Firefox, Opera, Chrome, dll. Cara setting-nya cukup mudah, cukup memasukkan alamat IP *router* ke URL *browser* anda.

Untuk bisa setting dan konfigurasi router secara console, diperlukan beberapa tool dan software. Berikut ini adalah tool dan software yang diperlukan:

- *Notebook* untuk konfigurasi *router* atau *switch.*
- Kabel *rollover.*



Gambar 4.4 Kabel *Rollover*

- Kabel serial to usb untuk koneksi dari cisco *router* atau *switch* ke *notebook.*

Gambar 4.5 Kabel Serial to USB

Gambar 4.6 Kabel Rollover dan Kabel Serial to USB yang Saling Terhubung

- Hyperterminal atau bisa diganti dengan putty

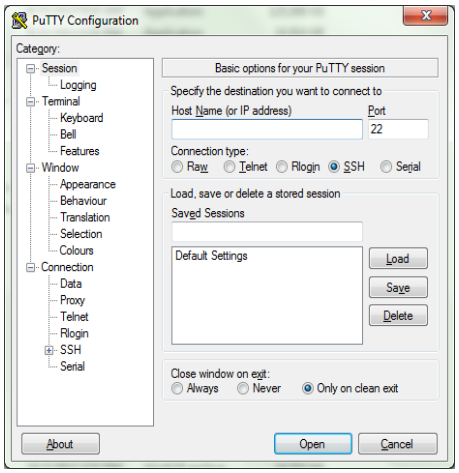
Hubungkan kabel *rollover* dan kabel serial to usb, lalu hubungkan ujung kabel *rollover* yang berupa konektor RJ45 ke *port console* yang ada di *router* atau *switch*. Sedangkan ujung kabel serial to usb yang berupa usb dihubungkan dengan *port* usb pada *notebook*.

Gambar 4.7 *Port Console* pada *Router*

Gambar 4.8 *Port Console* pada *Switch*

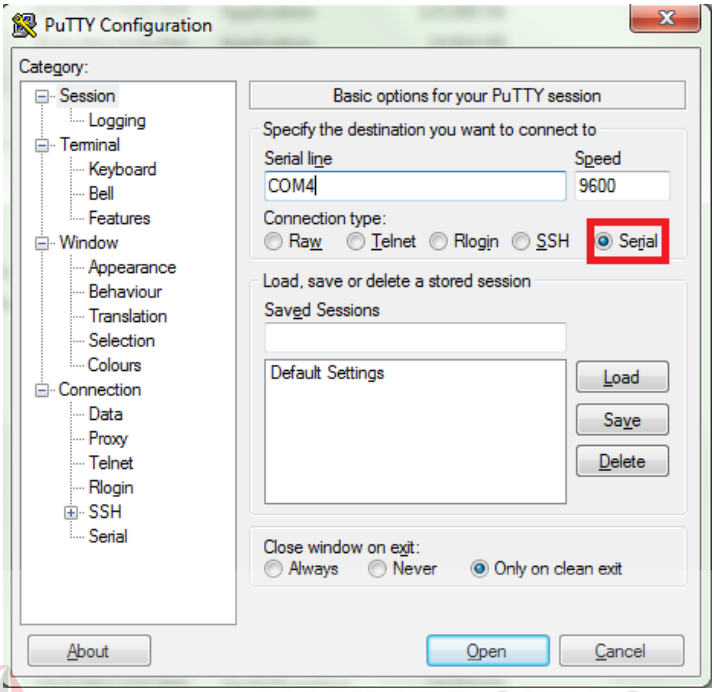
4.4 Setting Parameter Putty

Buka *software* atau aplikasi putty pada *notebook*. Kemudian akan muncul window seperti gambar dibawah ini.



Gambar 4.9 *Putty Configuration*

Setelah itu pilih koneksi serial, karena *notebook* menggunakan kabel *console* untuk terhubung ke *router*. Kemudian klik *open*.



Gambar 4.10 Serial pada *Putty*

4.4 Langkah-langkah

- **Konfigurasi Switch :**

Membuat Vlan

- PC1 : IT = Vlan 10 : 10.0.1.0
- PC2 : Finance = Vlan 11 : 10.0.2.0

Setting mode

- fa0/24 mode trunk (agar satu jalur dapat dilewati banyak vlan).
- fa0/1 mode access vlan 10 dan fa0/2 mode access vlan 11.

- **Konfigurasi Router :**

Setting interface dari jaringan local

- Memasukkan ip di *subinterface* sebagai *gateway* setiap vlan dan agar vlan yang berbeda dapat berkomunikasi (misal utk vlan 10: di *subinterface* fa0/0.10 dan untuk vlan 11: di *subinterface* fa0/0.11)
- Menyalakan interface fa0/0 (no shutdown)

Setting interface ke luar jaringan local (ISP)

- Memasukkan IP di interface fa0/1 dan Menyalakan interface (no shutdown)
- Merouting jaringan (agar router jaringan local dapat mengenali jalur ke internet)

Setting DHCP

- Membuat dhcp untuk PC dengan *range* IP (10.0.1.0/24)
- Membuat dhcp untuk IP Phone dengan *range* IP (10.0.2.0/24)

Setting NAT

- Membuat identitas jaringan (pada fa0/0.10 nat *inside* dan pada fa0/1 : nat outside)
- Membuat *acces list* yang dapat mengijinkan jaringan local (fa0/0.10) ke jalur yang ke arah jaringan internet (fa0/1)
- Membuat nat agar ip d dalam jaringan local dapat akses internet melalui ip yang ada di int fa0/1

4.6 Konfigurasi Switch

Dalam konfigurasi *switch*, yang terpenting adalah menetapkan VLAN dan trunk yang dipakai masing-masing port.

1. **Membuat nama vlan**

Switch(config)#vlan 10

Switch(config-vlan)#name IT

Switch(config-vlan)#vlan 11

Switch(config-vlan)#name finance

Switch(config-vlan)#exit (agar tersimpan terlebih dahulu)

2. **Memasukkan VLAN pada tiap port**

Switch(config)#int fa0/1

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10

Switch(config)#int fa0/2

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 11

Switch(config)#int fa0/3

Switch(config-if)#switchport mode trunk

Untuk memverifikasi apakah vlan yang dibuat telah berhasil atau tidak, maka masukkan perintah : *show vlan database* (ketika di *Previledge Mode*) atau *do show vlan database* (ketika di *Global Configuration Mode*).

Misal :

- Pada *previledge mode* : Switch# *show vlan database*
- Pada *Global Configuration Mode*: Switch(config)#*do show vlan database*

4.7 Konfigurasi Router

Setting Interface

R.Local(config)#int fa0/1

R.Local(config-if)#ip add 192.168.1.253 255.255.255.0

R.Local(config-if)#no shutdown

Setting Subinterface Untuk Gateway Vlan Masing-masing

R.Local(config-if)#int fa0/0.10

R.Local(config-subif)#encapsulation dot1Q 10

R.Local(config-subif)#ip address 10.0.1.254 255.255.255.0

R.Local(config-if)#int fa0/0.11

R.Local(config-subif)#encapsulation dot1Q 11

R.Local(config-subif)#ip address 10.0.2.254 255.255.255.0

Setting DHCP pada Router

R.Local(config)#ip dhcp pool IT

R.Local(dhcp-config)#default-router 10.0.1.254

R.Local(dhcp-config)#network 10.0.1.0 255.255.255.0

R.Local(config)#ip dhcp pool finance

R.Local(dhcp-config)#default-router 10.0.2.254

R.Local(dhcp-config)#network 10.0.2.0 255.255.255.0

Setting Routing Static

R.Local(config)#ip route 0.0.0.0 0.0.0.0 fa0/1 192.168.1.254

Setting ACL

R.Local(config)#access-list 101 permit icmp 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255 echo-reply

R.Local(config)#int fa0/0.11

R.Local(config-subif)# ip access-group 101 in

Setting Nat

R.Local(config)#access-list 1 permit any (Mengelompokkan Jar.local ke list 1)

R.Local(config-if)#int fa0/0.10

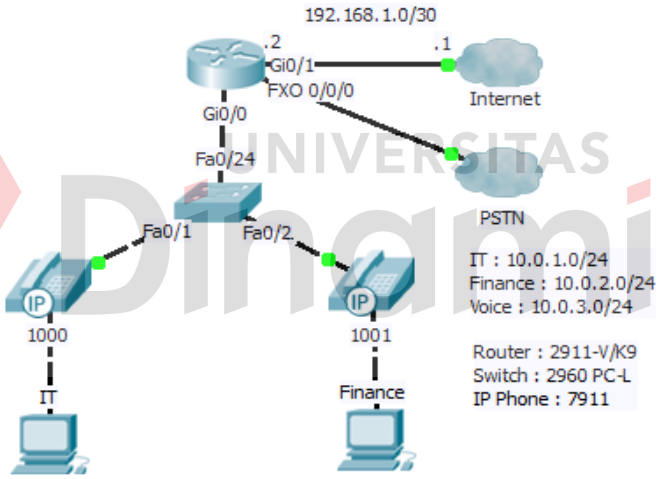
R.Local(config-subif)#ip nat inside

R.Local(config)#int fa0/1

R.Local(config-if)#ip nat outside

R.Local(config)#ip nat inside source list 1 interface fa0/1 overload (Menyambungkan Jar inside keluar ke fa0/1).

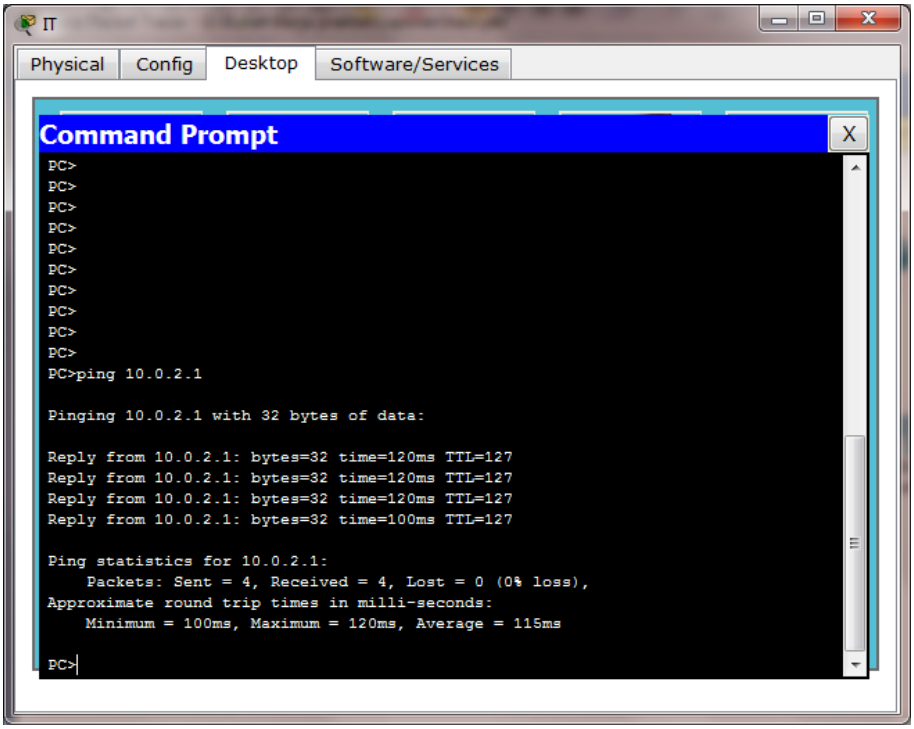
4.8 Hasil Konfigurasi



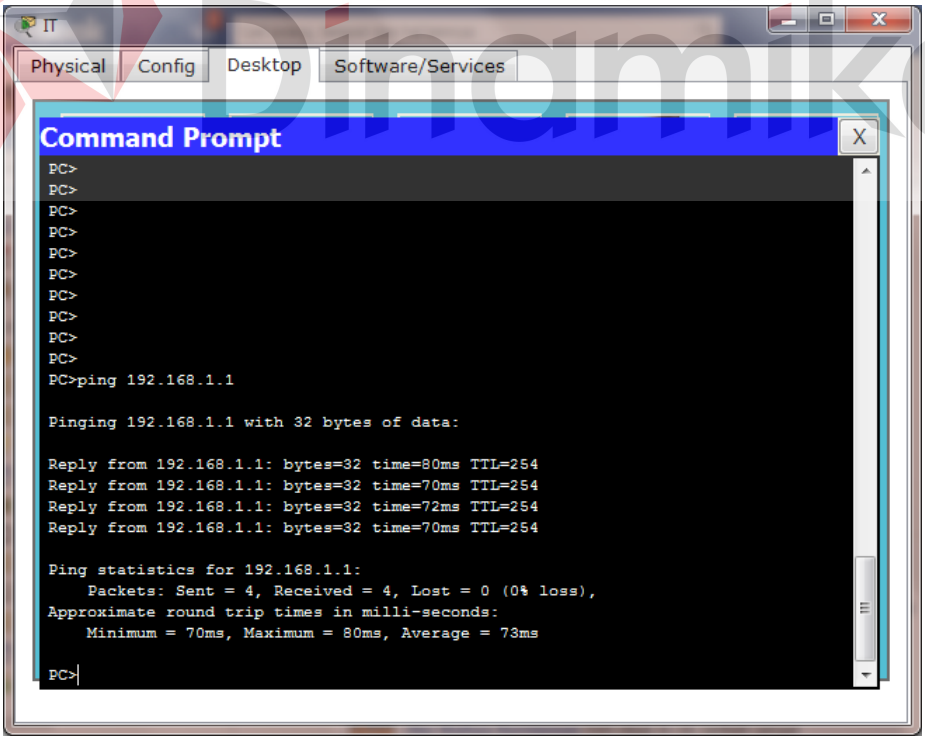
Gambar 4.11 Hasil Konfigurasi

Hasil konfigurasi yang diperoleh dari rancangan gambar dan ketentuan sesuai yang tertera di atas antara lain:

1. Komputer dari IT dapat melakukan *access* ke komputer Finance dan ke internet.

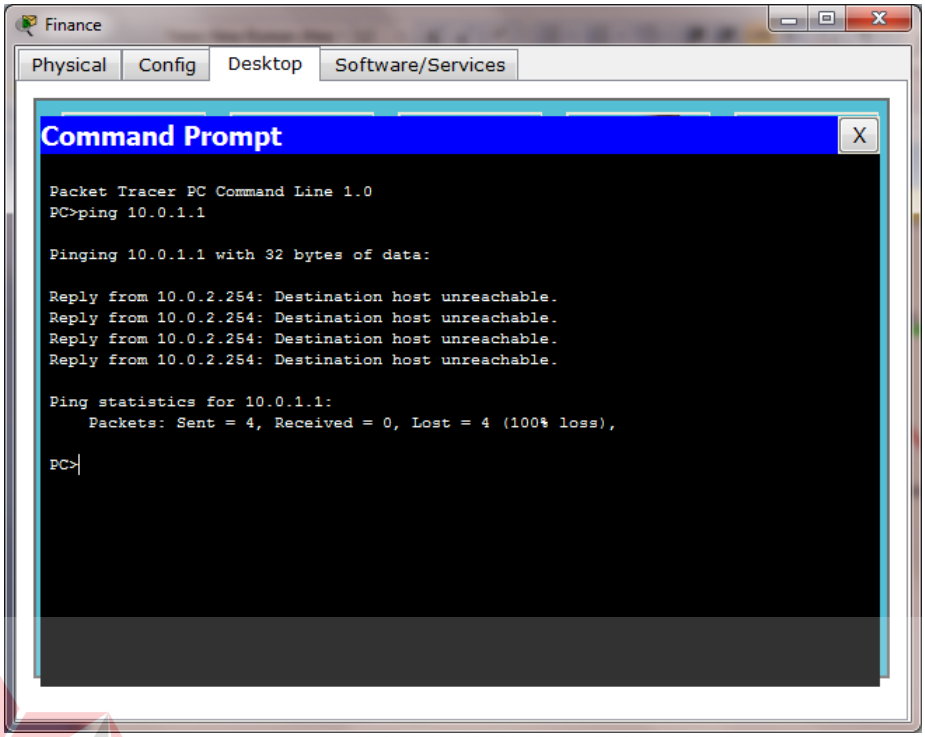


Gambar 4.12 Akses IT ke Finance

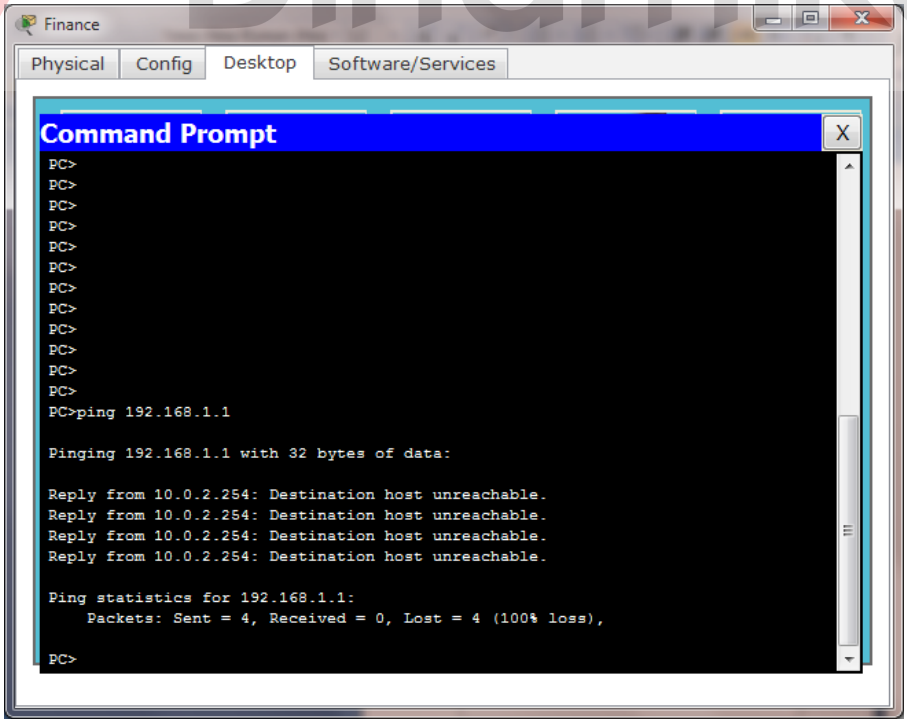


Gambar 4.13 Akses IT ke Internet

2. Komputer finance tidak dapat melakukan *access* ke komputer IT dan Internet.



Gambar 4.14 Akses Finance ke IT



Gambar 4.15 Akses Finance ke Internet

BAB V

PENUTUP

5.1 Kesimpulan

Dari hasil pembahasan laporan PKL ini penulis memberikan kesimpulan sebagai berikut:

1. Dengan adanya VLAN, dapat membuat banyak jaringan berbeda dalam satu *switch.*
2. Dengan adanya VLAN, dapat mempermudah administrator untuk membagi jaringan sesuai divisi pada sebuah perusahaan.
3. Untuk dapat melakukan pembatasan hak akses pada Cisco *Router*, dibutuhkan konfigurasi ACL.
4. Dengan adanya ACL, dapat membatasi paket-paket yang akan diblok atau yang diijinkan.

5.2 Saran

Berdasarkan kesimpulan dan analisis yang dilakukan selama PKL, penulis ingin memberikan saran-saran sebagai berikut:

1. Untuk penggunaan VLAN, lebih baik menggunakan selain VLAN 1.
2. Untuk penggunaan VLAN, lebih baik menggunakan jalur *trunk* sebagai penghemat jalur yang mengarah ke *router*.
3. Untuk penggunaan ACL, penulis menyarankan untuk menggunakan *standart* ACL apabila tidak ada batasan secara spesifik seperti : pembatasan UDP, TCP, ICMP, dll.

4. Untuk peletakkan ACL, apabila *standart* ACL, baiknya diletakkan sedekat mungkin dengan alamat tujuan dan *extended* ACL, baiknya diletakkan sedekat dengan alamat asal.

DAFTAR PUSTAKA

Rochmad, M. T. (2010). *Pengantar Jaringan Komputer.* Retrieved from Scribd: www.scribd.com

Sofana, I. (2009). *CISCO CCNA & JARINGAN KOMPUTER.* Bandung: Informatika.

Sukmaaji, A. (2003). *Jaringan Komputer.* Surabaya: Perpustakaan STIKOM.

System, C. (2007). *Configuring IP Access Lists.* Retrieved from Cisco: www.cisco.com