JARINGAN KOMPUTER

ANDRY MAULANA, M.KOM

AHMAD FAUZI, M.KOM

KATA PENGANTAR

Segala puji bagi Allah SWT yang telah memberikan kami kemudahan sehingga kami dapat menyelesaikan buku ajar ini dengan tepat waktu. Tanpa pertolongan-Nya tentunya kami tidak akan sanggup untuk menyelesaikan buku ajar ini dengan baik. Sholawat serta salam semoga terlimpah curahkan kepada baginda tercinta kita yaitu Nabi Muhammad SAW yang kita nanti-natikan syafa'atnya di akhirat nanti.

Penulis mengucapkan syukur kepada Allah SWT atas limpahan nikmat sehat-Nya, baik itu berupa sehat fisik maupun akal pikiran, sehingga penulis mampu untuk menyelesaikan pembuatan buku ajar sebagai dari tri darma untuk dari mata kuliah administrasi jaringan.

Penulis tentu menyadari bahwa makalah ini masih jauh dari kata sempurna dan masih banyak terdapat kesalahan serta kekurangan di dalamnya. Untuk itu, penulis mengharapkan kritik serta saran yang membangun dari pembaca untuk buku ajar ini, supaya maka buku ajar lah ini nantinya dapat menjadi acuan dalam pembelajaran yang lebih baik lagi. Demikian, dan apabila terdapat banyak kesalahan pada makalah ini penulis mohon maaf yang sebesar-besarnya.

Jakarta, 9 Oktober 2018

Tim Penulis

DAFTAR ISI

DAFTAR GAMBAR

PERTEMUAN 1
PENGENALAN KEAMANA JARINGAN

1.1. DATA PRIBADI

1.1.1. Pengantar Data Pribadi

1. Apa itu Keamanan Jaringan?

Jaringan informasi elektronik yang terhubung telah menjadi bagian integral dari kehidupan kita sehari-hari. Semua jenis organisasi, seperti lembaga medis, keuangan, dan pendidikan, menggunakan jaringan ini untuk beroperasi secara efektif. Mereka memanfaatkan jaringan dengan mengumpulkan, memproses, menyimpan, dan berbagi sejumlah besar informasi digital. Karena semakin banyak informasi digital dikumpulkan dan dibagikan, perlindungan informasi ini menjadi semakin penting bagi keamanan nasional dan stabilitas ekonomi kita. Keamanan siber adalah upaya berkelanjutan untuk melindungi sistem jaringan ini dan semua data dari penggunaan atau bahaya yang tidak sah. Pada tingkat pribadi, Anda perlu melindungi identitas Anda, data Anda, dan perangkat komputasi Anda. Di tingkat korporat, merupakan tanggung jawab setiap orang untuk melindungi reputasi, data, dan pelanggan organisasi. Di tingkat negara bagian, keamanan nasional, serta keselamatan dan kesejahteraan warga dipertaruhkan.

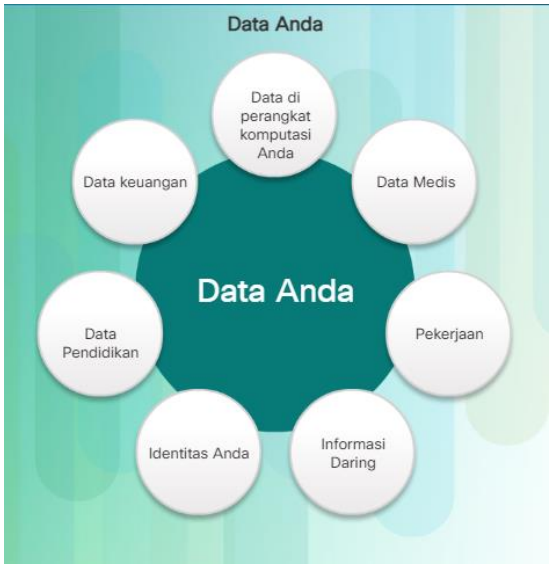
2. Status Identitas Seorang Saat Online dan Offline

Semakin banyak waktu yang dihabiskan untuk online, identitas Anda, baik online maupun offline, dapat memengaruhi hidup Anda. Identitas offline Anda adalah orang yang berinteraksi dengan teman dan keluarga Anda setiap hari di rumah, di sekolah, atau di tempat kerja. Mereka mengetahui informasi pribadi Anda, seperti nama, usia, atau tempat tinggal Anda. Identitas online Anda adalah siapa Anda di dunia maya. Identitas online Anda adalah bagaimana Anda menampilkan diri Anda kepada orang lain secara online. Identitas

online ini seharusnya hanya mengungkapkan sedikit informasi tentang Anda. Anda harus berhati-hati saat memilih nama pengguna atau alias untuk identitas online Anda. Nama pengguna tidak boleh menyertakan informasi pribadi apa pun. Itu harus sesuatu yang pantas dan terhormat. Nama pengguna ini tidak boleh membuat orang asing berpikir bahwa Anda adalah sasaran empuk kejahatan dunia maya atau perhatian yang tidak diinginkan.

3. Data Anda

Setiap informasi tentang Anda dapat dianggap sebagai data Anda. Informasi pribadi ini dapat secara unik mengidentifikasi Anda sebagai individu. Data ini mencakup gambar dan pesan yang Anda tukarkan dengan keluarga dan teman Anda secara online. Informasi lain, seperti nama, nomor jaminan sosial, tanggal dan tempat lahir, atau nama gadis ibu, diketahui oleh Anda dan digunakan untuk mengidentifikasi Anda. Informasi seperti informasi medis, pendidikan, keuangan, dan pekerjaan, juga dapat digunakan untuk mengidentifikasi Anda secara online.



Gambar 1. Data anda tersimpan

a. Rekam medis

Setiap kali Anda pergi ke kantor dokter, lebih banyak informasi ditambahkan ke catatan kesehatan elektronik (EHR) Anda. Resep dari dokter keluarga Anda menjadi bagian dari EHR Anda. EHR Anda mencakup kesehatan fisik, kesehatan mental, dan informasi pribadi lainnya yang mungkin tidak terkait secara medis. Misalnya, jika Anda memiliki konseling sebagai seorang anak ketika ada perubahan besar dalam keluarga, ini akan berada di suatu tempat dalam catatan medis Anda. Selain riwayat kesehatan dan informasi pribadi Anda, EHR juga dapat menyertakan informasi tentang keluarga Anda. Perangkat medis, seperti gelang kebugaran, menggunakan platform cloud untuk memungkinkan transfer nirkabel, penyimpanan, dan tampilan data klinis seperti detak jantung, tekanan darah, dan gula darah. Perangkat ini dapat menghasilkan sejumlah besar data klinis yang dapat menjadi bagian dari catatan medis Anda.

b. Catatan Pendidikan

Saat Anda maju melalui pendidikan Anda, informasi tentang nilai dan nilai ujian Anda, kehadiran Anda, kursus yang diambil, penghargaan dan gelar yang diberikan, dan laporan disipliner apa pun mungkin ada dalam catatan pendidikan Anda. Catatan ini juga dapat mencakup informasi kontak, catatan kesehatan dan imunisasi, dan catatan pendidikan khusus termasuk program pendidikan individual (IEPs).

c. Catatan Ketenagakerjaan dan Keuangan

Catatan keuangan Anda mungkin termasuk informasi tentang pendapatan dan pengeluaran Anda. Catatan pajak dapat mencakup slip gaji, laporan kartu kredit, peringkat kredit Anda, dan informasi perbankan lainnya. Informasi pekerjaan Anda dapat mencakup pekerjaan Anda sebelumnya dan kinerja Anda.

4. Dimana Data Anda?

Semua informasi ini tentang Anda. Ada berbagai undang-undang yang melindungi privasi dan data Anda di negara Anda. Tapi apakah Anda tahu di mana data Anda? Ketika Anda berada di kantor dokter, percakapan Anda dengan dokter dicatat dalam bagan medis Anda. Untuk tujuan penagihan, informasi ini dapat dibagikan dengan perusahaan asuransi untuk memastikan penagihan dan kualitas yang sesuai. Sekarang, bagian dari rekam medis Anda untuk kunjungan itu juga ada di perusahaan asuransi. Kartu loyalitas toko mungkin merupakan cara yang nyaman untuk menghemat uang untuk pembelian Anda. Namun, toko sedang menyusun profil pembelian Anda dan menggunakan informasi itu untuk penggunaannya sendiri. Profil menunjukkan pembeli membeli pasta gigi merek dan rasa tertentu secara teratur. Toko menggunakan informasi ini untuk menargetkan pembeli dengan penawaran khusus dari mitra pemasaran. Dengan menggunakan kartu loyalitas, toko dan mitra pemasaran memiliki profil untuk perilaku pembelian pelanggan. Ketika Anda membagikan foto Anda secara online dengan teman-teman Anda, apakah Anda tahu siapa yang mungkin memiliki salinan foto tersebut? Salinan gambar ada di perangkat Anda sendiri. Teman Anda mungkin memiliki salinan gambar yang diunduh ke perangkat mereka. Jika foto-foto itu dibagikan secara publik, orang asing mungkin juga memiliki salinannya. Mereka dapat mengunduh gambar-gambar itu atau mengambil tangkapan layar dari gambar-gambar itu. Karena gambar-gambar tersebut diposting secara online, mereka juga disimpan di server yang berlokasi di berbagai belahan dunia. Sekarang gambar tidak lagi hanya ditemukan di perangkat komputasi Anda.

5. Perangkat Komputasi

Perangkat komputasi Anda tidak hanya menyimpan data Anda. Sekarang perangkat ini telah menjadi portal ke data Anda dan menghasilkan informasi tentang Anda. Kecuali Anda telah memilih untuk menerima laporan tertulis untuk semua akun Anda, Anda menggunakan perangkat komputasi Anda untuk mengakses data. Jika Anda menginginkan salinan digital dari laporan kartu kredit terbaru, Anda menggunakan perangkat komputasi Anda untuk mengakses situs web penerbit kartu kredit. Jika Anda ingin membayar tagihan kartu kredit Anda secara online, Anda mengakses situs web bank Anda untuk mentransfer dana menggunakan perangkat komputasi Anda. Selain memungkinkan Anda untuk mengakses informasi Anda, perangkat komputasi juga dapat menghasilkan informasi tentang Anda. Dengan semua informasi tentang Anda ini tersedia secara online, data pribadi Anda menjadi menguntungkan bagi hackers.

1.1.2. Data Pribadi Sebagai Target

1. Mereka Menginginkan Uang Anda

Jika Anda memiliki sesuatu yang berharga, para penjahat menginginkannya. Kredensial online Anda sangat berharga. Kredensial ini memberi pencuri akses ke akun Anda. Anda mungkin berpikir bahwa frequent flyer miles yang Anda peroleh tidak berharga bagi penjahat dunia maya. Pikirkan lagi. Setelah sekitar 10.000 akun American Airlines dan United diretas, penjahat dunia maya memesan penerbangan gratis dan upgrade menggunakan kredensial yang dicuri ini. Meskipun miles frequent flyer dikembalikan ke pelanggan oleh maskapai, ini menunjukkan nilai kredensial login. Seorang penjahat juga bisa memanfaatkan hubungan Anda. Mereka dapat mengakses akun online Anda dan reputasi Anda untuk menipu Anda agar mengirimkan uang ke teman atau keluarga Anda. Penjahat dapat mengirim pesan yang menyatakan bahwa keluarga atau teman Anda

membutuhkan Anda untuk mengirim uang kepada mereka sehingga mereka dapat pulang dari luar negeri setelah kehilangan dompet mereka. Para penjahat sangat imajinatif ketika mereka mencoba menipu Anda untuk memberi mereka uang. Mereka tidak hanya mencuri uang Anda; mereka juga bisa mencuri identitas Anda dan menghancurkan hidup Anda.

2. Mereka Menginginkan Identitas Anda

Selain mencuri uang Anda untuk keuntungan moneter jangka pendek, para penjahat menginginkan keuntungan jangka panjang dengan mencuri identitas Anda. Ketika biaya medis meningkat, pencurian identitas medis juga meningkat. Pencuri identitas dapat mencuri asuransi kesehatan Anda dan menggunakan manfaat medis Anda untuk diri mereka sendiri, dan prosedur medis ini sekarang ada dalam catatan medis Anda. Prosedur pengajuan pajak tahunan dapat bervariasi dari satu negara ke negara lain; Namun, penjahat dunia maya melihat waktu ini sebagai peluang. Misalnya, rakyat Amerika Serikat harus mengajukan pajak mereka paling lambat tanggal 15 April setiap tahun. Internal Revenue Service (IRS) tidak memeriksa pengembalian pajak terhadap informasi dari majikan sampai Juli. Pencuri identitas dapat mengajukan pengembalian pajak palsu dan mengumpulkan pengembalian dana. Pelapor yang sah akan melihat ketika pengembalian mereka ditolak oleh IRS. Dengan identitas yang dicuri, mereka juga dapat membuka rekening kartu kredit dan membayar hutang atas nama Anda. Ini akan menyebabkan kerusakan pada peringkat kredit Anda dan membuat Anda lebih sulit untuk mendapatkan pinjaman. Kredensial pribadi juga dapat mengarah ke data perusahaan dan akses data pemerintah.

1.2. DATA ORGANISASI

1.2.1. Pengantar Data Organisasi

1. Jenis Data Organisasi

a. Data Tradisional

Data perusahaan mencakup informasi personalia, kekayaan intelektual, dan data keuangan. Informasi kepegawaian mencakup materi aplikasi, penggajian, surat penawaran, perjanjian karyawan, dan informasi apa pun yang digunakan dalam membuat keputusan ketenagakerjaan. Kekayaan intelektual, seperti paten, merek dagang, dan rencana produk baru, memungkinkan bisnis memperoleh keuntungan ekonomi atas para pesaingnya. Kekayaan intelektual ini dapat dianggap sebagai rahasia dagang; kehilangan informasi ini dapat menjadi bencana bagi masa depan perusahaan. Data keuangan, seperti laporan laba rugi, neraca, dan laporan arus kas suatu perusahaan memberikan wawasan tentang kesehatan perusahaan.

b. Internet of Things dan Big Data

Dengan munculnya Internet of Things (IoT), ada lebih banyak data untuk dikelola dan diamankan. IoT adalah jaringan besar objek fisik, seperti sensor dan peralatan yang melampaui jaringan komputer tradisional. Semua koneksi ini, ditambah fakta bahwa kami telah memperluas kapasitas penyimpanan dan layanan penyimpanan melalui cloud dan virtualisasi, mengarah pada pertumbuhan data yang eksponensial. Data ini telah menciptakan bidang minat baru dalam teknologi dan bisnis yang disebut "Big Data". Dengan kecepatan, volume, dan variasi data yang dihasilkan oleh IoT dan operasi bisnis sehari-hari, kerahasiaan, integritas, dan ketersediaan data ini sangat penting. penting bagi kelangsungan hidup organisasi.

2. Confidentiality, Integrity, and Availability

Confidentiality, integrity and availability yang dikenal sebagai triad adalah pedoman untuk keamanan informasi bagi suatu organisasi. Kerahasiaan memastikan privasi data dengan membatasi akses melalui enkripsi otentikasi. Integritas memastikan bahwa informasi tersebut akurat dan dapat dipercaya. Ketersediaan memastikan bahwa informasi dapat diakses oleh orang yang berwenang.

a. Confidentiality

   Istilah lain untuk kerahasiaan adalah privasi. Kebijakan perusahaan harus membatasi akses ke informasi untuk personel yang berwenang dan memastikan bahwa hanya individu yang berwenang yang melihat data ini. Data dapat dikotak-kotakkan sesuai dengan tingkat keamanan atau sensitivitas informasi. Misalnya, pengembang program Java tidak harus mengakses informasi pribadi semua karyawan. Selanjutnya, karyawan harus menerima pelatihan untuk memahami praktik terbaik dalam menjaga informasi sensitif untuk melindungi diri mereka sendiri dan perusahaan dari serangan. Metode untuk memastikan kerahasiaan termasuk enkripsi data, ID nama pengguna dan kata sandi, otentikasi dua faktor, dan meminimalkan paparan informasi sensitif.

b. Integrity

   Integritas adalah akurasi, konsistensi, dan kepercayaan data selama seluruh siklus hidupnya. Data tidak boleh diubah selama transit dan tidak diubah oleh entitas yang tidak berwenang. Izin file dan kontrol akses pengguna dapat mencegah akses yang tidak sah. Kontrol versi dapat digunakan untuk mencegah perubahan yang tidak disengaja oleh pengguna yang berwenang. Cadangan harus tersedia untuk memulihkan data yang rusak, dan hashing checksum dapat digunakan untuk memverifikasi integritas data selama transfer.

Checksum digunakan untuk memverifikasi integritas file, atau string karakter, setelah ditransfer dari satu perangkat ke perangkat lain melalui jaringan lokal Anda atau Internet. Checksum dihitung dengan fungsi hash. Beberapa checksum yang umum adalah MD5, SHA-1, SHA-256, dan SHA-512. Fungsi hash menggunakan algoritma matematika untuk mengubah data menjadi nilai panjang tetap yang mewakili data, seperti yang ditunjukkan pada Gambar 2. Nilai hash hanya ada untuk perbandingan. Dari nilai hash, data asli tidak dapat diambil secara langsung. Misalnya, jika Anda lupa kata sandi, kata sandi Anda tidak dapat dipulihkan dari nilai hash. Kata sandi harus diatur ulang.

Setelah file diunduh, Anda dapat memverifikasi integritasnya dengan memverifikasi nilai hash dari sumber dengan yang Anda buat menggunakan kalkulator hash apa pun. Dengan membandingkan nilai hash, Anda dapat memastikan bahwa file tidak dirusak atau rusak selama transfer.

c. Availability

Memelihara peralatan, melakukan perbaikan perangkat keras, memperbarui sistem operasi dan perangkat lunak, dan membuat cadangan memastikan ketersediaan jaringan dan data kepada pengguna yang berwenang. Harus ada rencana untuk segera pulih dari bencana alam atau bencana buatan manusia. Peralatan atau perangkat lunak keamanan, seperti firewall, menjaga dari waktu henti akibat serangan seperti penolakan layanan (DoS). Penolakan layanan terjadi ketika penyerang mencoba membanjiri sumber daya sehingga layanan tidak tersedia bagi pengguna.

3. LAB PRAKTIKUM – Membandingkan data dengan Aplikasi HASH

Tujuan :

Gunakan program hashing untuk memverifikasi integritas data.

Latar Belakang / Skenario:

Penting untuk dipahami ketika data telah rusak atau telah dirusak. Program hashing dapat digunakan untuk memverifikasi apakah data telah berubah, atau apakah tetap sama. Program hashing melakukan fungsi hash pada data atau file, yang mengembalikan nilai (biasanya jauh lebih pendek). Ada banyak fungsi hash yang berbeda, beberapa sangat sederhana dan beberapa sangat kompleks. Ketika hash yang sama dilakukan pada data yang sama, nilai yang dikembalikan selalu sama. Jika ada perubahan yang dilakukan pada data, nilai hash yang dikembalikan akan berbeda.

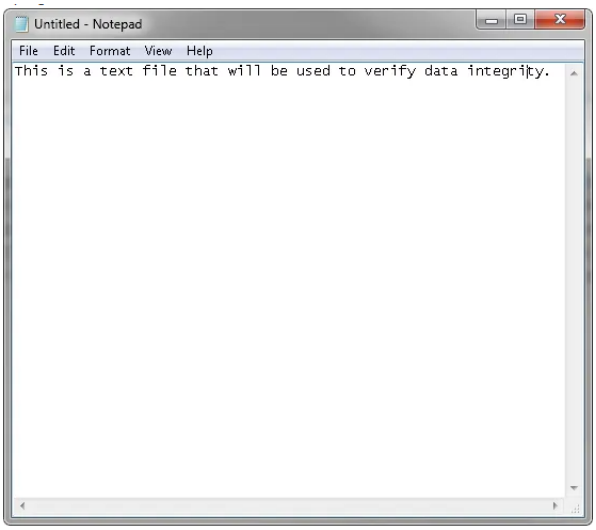
Catatan : Anda akan memerlukan hak instalasi dan beberapa pengetahuan tentang proses untuk menginstal program Windows.

Sumber Daya yang Diperlukan:

PC dengan akses Internet

Langkah 1: Buat file Teks

a. Buka Aplikasi Notepad
b. Ketik beberapa kata dalam Notepad tersebut



Gambar 2. Ketik beberapa kata dalam aplikasi notepad

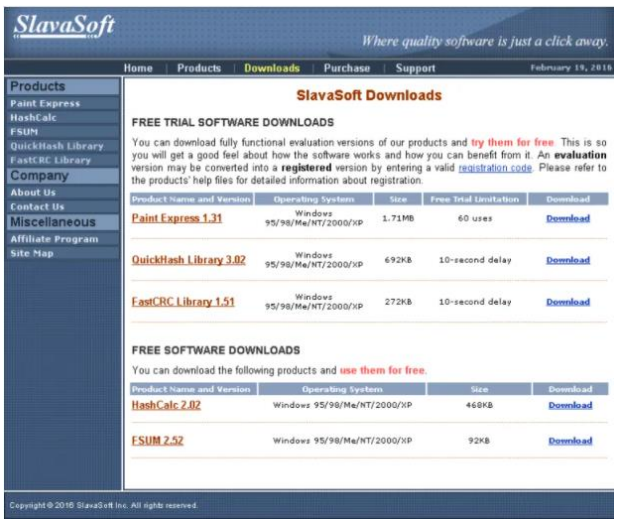
c. Pilih File > save

d. Simpan pada penyimpanan Desktop

e. Dengan nama File " Hash" lalu simpan

Langkah 2: Instal HashCalc

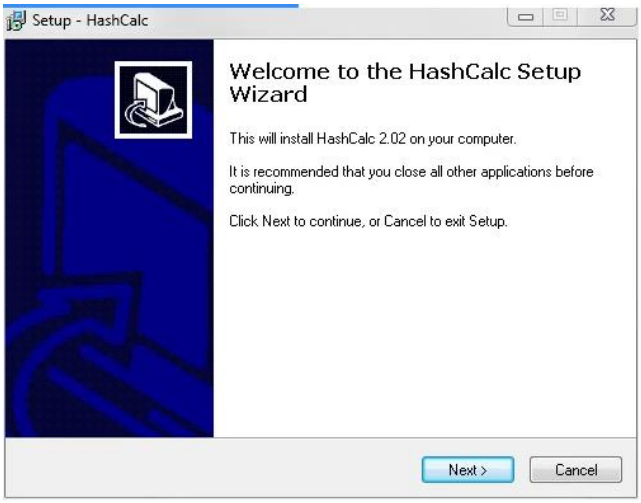
a. Buka browser web dan navigasikan ke http://www.slavasoft.com/download.htm



Gambar 3. Tampilan download Hash

b. Klik download pada baris HashCalc 2.02

c. Buka file hashcalc.zip dan jalankan file setup.exe di dalamnya.



Gambar 4. Install HashCalc

d. Ikuti wizard penginstalan untuk menginstal HashCalc.

e. Klik Finish pada layar terakhir, dan tutup file README jika dibuka. Anda dapat membaca file tersebut jika Anda mau.

f. HashCalc sekarang diinstal dan berjalan.

Gambar 5. Tampilan aplikasi HashCalc

Langkah 3: Hitung hash dari file Hash.txt

a. Perhatikan pemilihan menu dalam Hashcalc

1) Data Format : File
2) Data : klik button … selanjutkan ambil data notepad yang sudah dibuat sebelumnya pada Desktop dengan nama file Hast.txt
3) Hilangkan tanda cheklist pada HMAC
4) Hilangkan semua tanda cheklist pada aplikasi Kecuali MD5

b. Klik tombol Button Calculate
   1) Berapa nilai di sebelah MD5 ? -Jawaban silakan diisi-
   2) Buka file Hash.txt pada penyimpanan Dekstop
   3) Buat perubahan kecil pada teks, seperti menghapus huruf, atau menambahkan spasi atau titik.
   4) Klik File > Save , dan tutup Notepad .

Langkah 5: Hitung hash baru dari file Hash.txt

a. Klik tombol Button Calculate pada HashCalc lagi.
   Berapa nilai di sebelah MD5 ? -Jawaban silakan diisi-
   Apakah nilainya berbeda dengan nilai yang tercatat di Langkah 3? -Jawaban silakan diisi-
b. Beri tanda ceklist di semua jenis hash.
c. Klik tombol Button Calculate
d. Perhatikan bahwa banyak tipe hash membuat hash dengan panjang yang berbeda.
   Mengapa? -Jawaban silakan diisi-

Dalam peraktikum mandiri yang kita lakukan pada aplikasi Hash menjelakan bahwa sebuah data memiliki sebuat nilai bit yang dapat dikonveriskan berdasarkan isi yang

terdapat dalam data tersebut, bila nilai bit sudah tidak sesuai dengan versi original yang kita miliki sudah dijamin bahwa data tersebut sudah mengalami perubahan isi dan perlu di curigai terkait perubahan data yang tidak dapat dilakukan oleh orang lain selain diri anda yang memang sebagai pemilik hak penuh atas data tersebut.

1.2.2. Dampak Pelanggaran Keamanan

1. Konsekuensi dari Pelanggaran Keamanan

Untuk melindungi organisasi dari setiap kemungkinan serangan siber tidak mungkin dilakukan, karena beberapa alasan. Keahlian yang diperlukan untuk menyiapkan dan memelihara jaringan yang aman bisa mahal. Penyerang akan selalu terus mencari cara baru untuk menargetkan jaringan. Akhirnya, serangan siber yang canggih dan tepat sasaran akan berhasil. Prioritas selanjutnya adalah seberapa cepat tim keamanan Anda dapat merespons serangan tersebut untuk meminimalkan hilangnya data, waktu henti, dan pendapatan. Sekarang Anda tahu bahwa apa pun yang diposting online dapat hidup online selamanya, bahkan jika Anda dapat menghapus semua salinan yang Anda miliki. Jika server Anda diretas, informasi personel rahasia dapat dipublikasikan. Seorang peretas (atau grup peretas) dapat merusak situs web perusahaan dengan memposting informasi yang tidak benar dan merusak reputasi perusahaan yang membutuhkan waktu bertahun-tahun untuk dibangun. Peretas juga dapat menghapus situs web perusahaan yang menyebabkan perusahaan kehilangan pendapatan. Jika situs web tidak aktif untuk jangka waktu yang lebih lama, perusahaan mungkin tampak tidak dapat diandalkan dan mungkin kehilangan kredibilitas. Jika situs web atau jaringan perusahaan telah dilanggar, hal ini dapat menyebabkan kebocoran dokumen rahasia, pengungkapan rahasia dagang, dan pencurian kekayaan intelektual. Hilangnya semua informasi ini dapat menghambat pertumbuhan dan ekspansi perusahaan. Biaya moneter dari pelanggaran jauh lebih tinggi daripada hanya mengganti perangkat yang hilang atau dicuri, berinvestasi dalam keamanan yang ada dan memperkuat

keamanan fisik bangunan. Perusahaan mungkin bertanggung jawab untuk menghubungi semua pelanggan yang terkena dampak tentang pelanggaran tersebut dan mungkin harus bersiap untuk proses pengadilan. Dengan semua gejolak ini, karyawan dapat memilih untuk meninggalkan perusahaan. Perusahaan mungkin perlu kurang fokus pada pertumbuhan dan lebih banyak pada perbaikan reputasinya.

2. Contoh Pelanggaran Keamanan 1

Pengelola kata sandi online, LastPass, mendeteksi aktivitas yang tidak biasa di jaringannya pada Juli 2015. Ternyata peretas telah mencuri alamat email pengguna, pengingat kata sandi, dan hash otentikasi. Untungnya bagi para pengguna, para peretas tidak dapat memperoleh brankas kata sandi terenkripsi siapa pun. Meskipun terjadi pelanggaran keamanan, LastPass tetap dapat mengamankan informasi akun pengguna. LastPass memerlukan verifikasi email atau otentikasi multi-faktor setiap kali ada login baru dari perangkat atau alamat IP yang tidak dikenal. Peretas juga memerlukan kata sandi utama untuk mengakses akun. Pengguna LastPass juga memiliki tanggung jawab dalam menjaga akun mereka sendiri. Pengguna harus selalu menggunakan kata sandi utama yang rumit dan mengubah kata sandi utama secara berkala. Pengguna harus selalu waspada terhadap serangan Phishing. Contoh serangan Phishing adalah jika penyerang mengirim email palsu yang mengaku berasal dari LastPass. Email meminta pengguna untuk mengklik tautan yang disematkan dan mengubah kata sandi. Tautan dalam email mengarah ke versi situs web palsu yang digunakan untuk mencuri kata sandi utama. Pengguna tidak boleh mengklik tautan yang disematkan dalam email. Pengguna juga harus berhati-hati dengan pengingat kata sandi mereka. Pengingat kata sandi tidak boleh memberikan kata sandi Anda. Yang terpenting, pengguna harus mengaktifkan otentikasi multi-faktor bila tersedia untuk situs web mana pun yang menawarkannya. Jika pengguna dan penyedia layanan sama-sama menggunakan alat

dan prosedur yang tepat untuk melindungi informasi pengguna, data pengguna masih dapat dilindungi, bahkan jika terjadi pelanggaran keamanan.

3. Contoh Pelanggaran Keamanan 2

Pembuat mainan berteknologi tinggi untuk anak-anak, Vtech, mengalami pelanggaran keamanan pada basis datanya pada November 2015. Pelanggaran ini dapat memengaruhi jutaan pelanggan di seluruh dunia, termasuk anak-anak. Pelanggaran data mengekspos informasi sensitif termasuk nama pelanggan, alamat email, kata sandi, gambar, dan log obrolan. Sebuah tablet mainan telah menjadi target baru bagi para peretas. Pelanggan telah berbagi foto dan menggunakan fitur obrolan melalui tablet mainan. Informasi tidak diamankan dengan benar, dan situs web perusahaan tidak mendukung komunikasi SSL yang aman. Meskipun pelanggaran tersebut tidak mengekspos informasi kartu kredit dan data identifikasi pribadi, perusahaan tersebut ditangguhkan di bursa saham karena kekhawatiran atas peretasan tersebut begitu besar. Vtech tidak melindungi informasi pelanggan dengan benar dan itu terungkap selama pelanggaran. Meskipun perusahaan memberi tahu pelanggannya bahwa kata sandi mereka telah di-hash, masih mungkin bagi para peretas untuk menguraikannya. Kata sandi dalam database diacak menggunakan fungsi hash MD5, tetapi pertanyaan keamanan dan jawaban disimpan dalam teks biasa. Sayangnya, fungsi hash MD5 memiliki kerentanan yang diketahui. Peretas dapat menentukan kata sandi asli dengan membandingkan jutaan nilai hash yang telah dihitung sebelumnya. Dengan informasi yang terungkap dalam pelanggaran data ini, penjahat dunia maya dapat menggunakannya untuk membuat akun email, mengajukan kredit, dan melakukan kejahatan sebelum anak-anak cukup umur untuk pergi ke sekolah. Untuk orang tua dari anak-anak ini, penjahat dunia maya dapat mengambil alih akun online karena banyak orang menggunakan kembali kata sandi mereka di situs web dan akun yang berbeda. Pelanggaran keamanan tidak hanya berdampak

pada privasi pelanggan, tetapi juga merusak reputasi perusahaan, seperti yang ditunjukkan oleh perusahaan ketika kehadirannya di bursa ditangguhkan. Bagi orang tua, ini adalah peringatan untuk lebih waspada tentang privasi online anak-anak mereka dan menuntut keamanan yang lebih baik untuk produk anak-anak. Untuk produsen produk yang terhubung ke jaringan, mereka harus lebih agresif dalam melindungi data dan privasi pelanggan sekarang dan di masa depan, seiring berkembangnya lanskap serangan siber.

4. Contoh Pelanggaran Keamanan 3

Equifax Inc. adalah salah satu agen pelaporan kredit konsumen nasional di Amerika Serikat. Perusahaan ini mengumpulkan informasi tentang jutaan pelanggan individu dan bisnis di seluruh dunia. Berdasarkan informasi yang dikumpulkan, skor kredit dan laporan kredit dibuat tentang pelanggan. Informasi ini dapat mempengaruhi pelanggan ketika mereka mengajukan pinjaman dan ketika mereka mencari pekerjaan. Pada bulan September 2017, Equifax secara terbuka mengumumkan peristiwa pelanggaran data. Para penyerang mengeksploitasi kerentanan dalam perangkat lunak aplikasi web Apache Struts. Perusahaan percaya bahwa jutaan data pribadi sensitif konsumen AS diakses oleh penjahat cyber antara Mei dan Juli 2017. Data pribadi termasuk nama lengkap pelanggan, nomor Jaminan Sosial, tanggal lahir, alamat dan informasi pribadi lainnya. Ada bukti bahwa pelanggaran tersebut mungkin telah mempengaruhi pelanggan di Inggris dan Kanada. Equifax mendirikan situs web khusus yang memungkinkan konsumen untuk menentukan apakah informasi mereka telah disusupi, dan mendaftar untuk pemantauan kredit dan perlindungan pencurian identitas. Menggunakan nama domain baru, alih-alih menggunakan subdomain equifax.com, ini memungkinkan pihak jahat untuk membuat situs web tidak sah dengan nama yang mirip. Situs web ini dapat digunakan sebagai bagian dari skema phishing untuk mengelabui Anda agar memberikan informasi pribadi. Selanjutnya, seorang karyawan dari

Equifax memberikan tautan web yang salah di media sosial untuk pelanggan yang khawatir. Untungnya, situs web ini dihapus dalam waktu 24 jam. Itu dibuat oleh seorang individu yang menggunakannya sebagai kesempatan pendidikan untuk mengekspos kerentanan yang ada di halaman respons Equifax. Sebagai konsumen yang peduli, Anda mungkin ingin memverifikasi dengan cepat apakah informasi Anda telah disusupi, sehingga Anda dapat meminimalkan dampaknya. Dalam masa krisis, Anda mungkin ditipu untuk menggunakan situs web yang tidak sah. Anda harus berhati-hati dalam memberikan informasi pribadi agar tidak menjadi korban lagi. Selain itu, perusahaan bertanggung jawab untuk menjaga keamanan informasi kami dari akses yang tidak sah. Perusahaan perlu secara teratur menambal dan memperbarui perangkat lunak mereka untuk mengurangi eksploitasi kerentanan yang diketahui. Karyawan mereka harus dididik dan diinformasikan tentang prosedur untuk melindungi informasi dan apa yang harus dilakukan jika terjadi pelanggaran. Sayangnya, korban sebenarnya dari pelanggaran ini adalah individu yang datanya mungkin telah disusupi. Dalam hal ini, Equifax memiliki beban untuk melindungi data konsumen yang dikumpulkan saat melakukan pemeriksaan kredit karena pelanggan tidak memilih untuk menggunakan layanan yang disediakan oleh Equifax. Konsumen harus mempercayai perusahaan untuk melindungi informasi yang dikumpulkan. Selanjutnya, penyerang dapat menggunakan data ini untuk mengasumsikan identitas Anda, dan sangat sulit untuk membuktikan sebaliknya karena penyerang dan korban mengetahui informasi yang sama. Dalam situasi ini, yang paling dapat Anda lakukan adalah waspada ketika Anda memberikan informasi identitas pribadi melalui Internet. Periksa laporan kredit Anda secara teratur (sekali per bulan atau sekali per kuartal). Segera laporkan informasi palsu.

5. LAB PRAKTIKUM – APA YANG DICURI?

Tujuan:

Cari dan baca tentang beberapa kejadian pelanggaran keamanan yang pernah terjadi pada sebuah organisasi.

Latar Belakang / Skenario:

Pelanggaran keamanan terjadi ketika individu atau aplikasi mencoba mendapatkan akses tidak sah ke data, aplikasi, layanan, atau perangkat. Selama pelanggaran ini, penyerang, apakah mereka orang dalam atau bukan, berusaha mendapatkan informasi yang dapat mereka gunakan untuk keuntungan finansial atau keuntungan lainnya. Di lab ini, Anda akan mempelajari beberapa pelanggaran keamanan untuk menentukan apa yang diambil, eksploitasi apa yang digunakan, dan apa yang dapat Anda lakukan untuk melindungi diri sendiri.

Sumber Daya yang Diperlukan

PC atau perangkat seluler dengan akses Internet

Penelitian Pelanggaran Keamanan

a. Cari sebuah artikel tentang sebuah Pencurian data untuk mengisi table dibawah ini sertakan link berita informasinya.

Tanggal Insiden	Organisasi yang Terkena Dampak	Berapa banyak korban? Apa yang Diambil?	Eksploitasi apa yang digunakan?	Sumber Referensi

1.3. PENYERANG DAN PROFESIONAL KEAMANA CYBER

1.3.1. Profil Penyerangan Cyber

1. Jenis Penyerang

Penyerang adalah individu atau kelompok yang mencoba mengeksploitasi kerentanan untuk keuntungan pribadi atau finansial. Penyerang tertarik pada segalanya, mulai dari kartu kredit hingga desain produk dan apa pun yang bernilai.

Amateurs – Orang-orang ini terkadang disebut Script Kiddies. Mereka biasanya penyerang dengan sedikit atau tanpa keterampilan, sering kali menggunakan alat atau instruksi yang ada di Internet untuk melancarkan serangan. Beberapa dari mereka hanya ingin tahu, sementara yang lain mencoba untuk menunjukkan keterampilan mereka dan menyebabkan kerusakan. Mereka mungkin menggunakan alat dasar, tetapi hasilnya masih bisa menghancurkan.

Hackers – Kelompok penyerang ini membobol komputer atau jaringan untuk mendapatkan akses. Bergantung pada maksud pembobolan, penyerang ini diklasifikasikan sebagai topi putih, abu-abu, atau hitam. Para penyerang topi putih membobol jaringan atau sistem komputer untuk menemukan kelemahan sehingga keamanan sistem tersebut dapat

ditingkatkan. Pembobolan ini dilakukan dengan izin sebelumnya dan hasil apa pun dilaporkan kembali ke pemilik. Di sisi lain, penyerang topi hitam memanfaatkan kerentanan apa pun untuk keuntungan pribadi, finansial, atau politik yang ilegal. Penyerang topi abu-abu berada di antara penyerang topi putih dan hitam. Penyerang topi abu-abu mungkin menemukan kerentanan dalam suatu sistem. Peretas topi abu-abu dapat melaporkan kerentanan kepada pemilik sistem jika tindakan itu sesuai dengan agenda mereka

Organized Hackers – Peretas ini termasuk organisasi penjahat dunia maya, peretas, teroris, dan peretas yang disponsori negara. Penjahat dunia maya biasanya adalah kelompok penjahat profesional yang berfokus pada kontrol, kekuasaan, dan kekayaan. Para penjahat sangat canggih dan terorganisir, dan mereka bahkan mungkin menyediakan kejahatan dunia maya sebagai layanan untuk penjahat lain. Hacktivists membuat pernyataan politik untuk menciptakan kesadaran akan isu-isu yang penting bagi mereka. Penyerang yang disponsori negara mengumpulkan intelijen atau melakukan sabotase atas nama pemerintah mereka. Penyerang ini biasanya sangat terlatih dan didanai dengan baik, dan serangan mereka difokuskan pada tujuan tertentu yang bermanfaat bagi pemerintah mereka.

2. Ancaman Internal dan Eksternal

a. Ancaman Keamanan Internal

Serangan dapat berasal dari dalam organisasi atau dari luar organisasi, seperti yang ditunjukkan pada gambar. Pengguna internal, seperti karyawan atau mitra kontrak, dapat secara tidak sengaja atau sengaja:

- Salah menangani data rahasia
- Mengancam operasi server internal atau perangkat infrastruktur jaringan
- Memfasilitasi serangan dari luar dengan menghubungkan media USB yang terinfeksi ke dalam sistem komputer perusahaan

- Secara tidak sengaja mengundang malware ke jaringan melalui email atau situs web berbahaya.

Ancaman internal juga berpotensi menimbulkan kerusakan yang lebih besar daripada ancaman eksternal, karena pengguna internal memiliki akses langsung ke gedung dan perangkat infrastrukturnya. Karyawan juga memiliki pengetahuan tentang jaringan perusahaan, sumber dayanya, dan data rahasianya, serta berbagai tingkat hak istimewa pengguna atau administratif.

b. Ancaman Keamanan Eksternal

Ancaman eksternal dari amatir atau penyerang terampil dapat mengeksploitasi kerentanan dalam jaringan atau perangkat komputasi, atau menggunakan rekayasa sosial untuk mendapatkan akses.

1.4. Cyberwarfe

1.4.1. Pengantar Cyberwarfe

1. Apa itu Cyberwarfe

Dunia maya telah menjadi dimensi penting lain dari peperangan, di mana negara dapat melakukan konflik tanpa bentrokan pasukan dan mesin tradisional. Hal ini memungkinkan negara-negara dengan kehadiran militer minimal menjadi sekuat negara lain di dunia maya. Cyberwarfare adalah konflik berbasis Internet yang melibatkan penetrasi sistem komputer dan jaringan negara lain. Penyerang ini memiliki sumber daya dan keahlian untuk meluncurkan serangan berbasis Internet besar-besaran terhadap negara lain untuk menyebabkan kerusakan atau mengganggu layanan, seperti mematikan jaringan listrik. Contoh serangan yang disponsori negara melibatkan malware Stuxnet yang dirancang untuk merusak pabrik pengayaan nuklir Iran. Malware Stuxnet tidak membajak komputer yang ditargetkan untuk mencuri informasi. Itu dirancang untuk merusak peralatan fisik yang

dikendalikan oleh komputer. Itu menggunakan pengkodean modular yang diprogram untuk melakukan tugas tertentu di dalam malware. Itu menggunakan sertifikat digital curian sehingga serangan itu tampak sah bagi sistem.

2. Tujuan Cyberwarfe

Tujuan utama dari cyberwarfare adalah untuk mendapatkan keuntungan atas musuh, apakah mereka negara atau pesaing. Suatu negara dapat terus menginvasi infrastruktur negara lain, mencuri rahasia pertahanan, dan mengumpulkan informasi tentang teknologi untuk mempersempit kesenjangan dalam industri dan militernya. Selain spionase industri dan militeristik, perang siber dapat menyabotase infrastruktur negara lain dan merenggut nyawa di negara yang ditargetkan. Misalnya, serangan dapat mengganggu jaringan listrik kota besar. Lalu lintas akan terganggu. Pertukaran barang dan jasa dihentikan. Pasien tidak bisa mendapatkan perawatan yang dibutuhkan dalam situasi darurat. Akses ke Internet juga dapat terganggu. Dengan mempengaruhi jaringan listrik, serangan itu dapat mempengaruhi kehidupan sehari-hari warga biasa. Selain itu, data sensitif yang disusupi dapat memberi penyerang kemampuan untuk memeras personel di dalam pemerintahan. Informasi tersebut memungkinkan penyerang untuk berpura-pura menjadi pengguna yang berwenang untuk mengakses informasi atau peralatan sensitif. Jika pemerintah tidak dapat mempertahankan diri dari serangan siber, warga dapat kehilangan kepercayaan pada kemampuan pemerintah untuk melindungi mereka. Cyberwarfare dapat mengacaukan suatu negara, mengganggu perdagangan, dan mempengaruhi kepercayaan warga negara pada pemerintah mereka tanpa pernah secara fisik menyerang negara yang ditargetkan.

IP Address

IP address merupakan alamat dari sebuah komputer yang dibentuk oleh sekumpulan bilangan biner sepanjang 32 bit, yang dibagi atas 4 bagian. Setiap bagian panjangan terdiri dari 8 buah bit. IP address merupakan sebuah indetitas dari host pada jaringan computer. IP address yang digunakan untuk keperluan LAN/intrenet disebut sebagai IP address local. Sedangkan IP address yang digunakan untuk keperluan internet disebut IP address public. Ruang lingkup dari pengalamatan IPv4 mencangkup semua kemungkinan. Kombinasi angka untuk 32 bit alamat IPv4. Secara harfiah 232 nilai yang berbeda ada dengan nomor 32 bit. Kombinasi angka-angka dapat dimulai dari "0 - 255" dalam empat octad: 0.0.0.0, 0.0.0.1, 0.0.0.2 sampai ke 255.255.255.255. Contoh penulisan dari IP address sebagai berikut:

10000000.00001010.00001010.00000001

Apabila setiap bagian kita konversikan ke bilangan decimal maka IP address diatas menjadi: 192.10.10.1

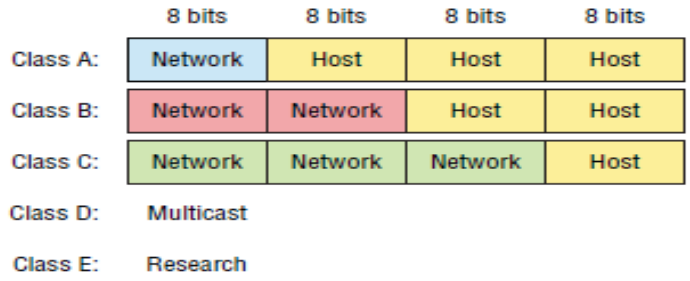
Pada bentuk penulisan IP address diatas dikenal dengan istilah notasi "doted decimal". Dalam praktiknya, IP address dalam bentuk decimal inilah yang akan kita gunakan dalam konfigurasi jaringan computer. Saat ini alokasi ataupun penyedian dari IP address versi 4 (IPv4) semakin berkurang dikarenakan semakin banyaknya pengguna IP versi 4 itu. IPv4 sudah digunakan lebih dari 20 Tahun lamanya. Untuk mengatasinya kini sudah dikembangkan penggunakan IPv6 atau IPng (IP next generation). Salah satuPraktikum Jaringan Komputer [Networking] Page 9 keuntungan dari IPv6 adalah jumlahnya yang sangat besar. Sehingga dapat mengantisipasi lonjakan permintaan dari IPv4 tersebut. IPv4 menggunakan 32 bit sedangkan IPv6 menggunakan 128 bit, sehingga kurang lebih dapat menanpung 4 Milyar computer yang terhubung ke internet. Namun, semakin tingginya penggunakan dari perangkat genggam, seperti PDA, smartphone, blackberry

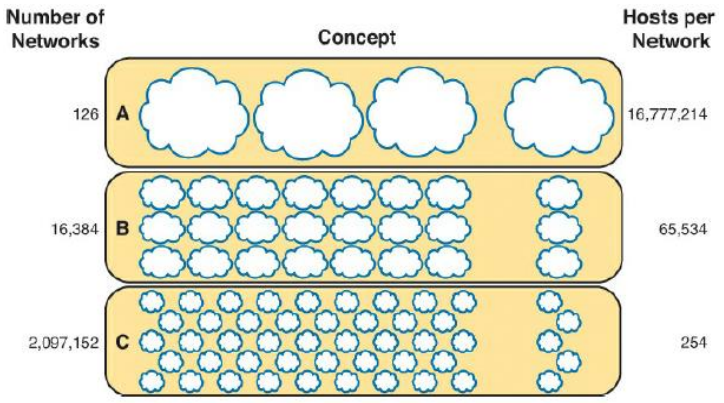
maka sitadaknya paling sedikit terdapat 1600 address tiap RT, Secara umum IP address dibagi menjadi 5 buah kelas. Kelas A, B, C, D, dan E. Namun, pada praktiknya hanya menggunakan kelas A, B dan C saja untuk keperluan umum. Sedangkan IP address kelas D dan E dipergunakan untuk keperluan khusus ataupun penelitian. IP address (kelas A, B, dan C) dapat dipisahkan menjadi 2 bagian, yakni bagian network (bit-bit networks/networks bit) dan bagian host (bit-bit host/host bits). Network bit berperan sebagai pembeda antar-network atau identifikasi (ID) network. Sedangkan host bit berperan sebagai identifikasi host. Semua host yang terhubung pada network yang sama, pasti akan memiliki network bit yang sama juga.

KELAS	IP Address
A	1.0.0.0 – 126.255.255.255
B	128.0.0.0 – 191.255.255.255
C	192.0.0.0 – 223.255.255.255

KELAS	IP Address
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

Pada jaringan TCP/IP, perbedaan network tidak ditentukan pada topologi yang digunakan, media yang digunakan, akses, system operasi dan aplikasi yang digunakan. Berikut ini penjelasan dari masing-masing kelas IP address.





1. Kelas A

   IP address kelas A dapat ditulisankan sebagai berikut:

   nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

   “n” menerangkan sebagai network, sedangkan “h” menerangkan sebagai host.

   Sebagai contoh:

   IP: 10.11.12.1

   Subnet: 255.0.0.0

   Ket:

   10 > Sebagai Network.

   11, 12, dan 1 > merupakan host yang dapat digunakan pada kelas A.

2. Kelas B

   IP address kelas B dapat ditulisankan sebagai berikut:

   nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh

   Sebagai contoh:

   IP: 172.168.10.1

   Subnet: 255.255.0.0

Ket:

172.168 > Sebagai Network

10.1> merupakan host yang dapat digunakan pada kelas B

3. Kelas C

IP address kelas C dapat ditulisankan sebagai berikut:

nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh

Sebagai contoh:

IP: 192.168.10.1

Subnet: 255.255.255.0

Ket:

192.168.10 > Sebagai Network

1 > merupakan host yang dapat digunakan pada kelas C.

Selain IP address, terdapat pula netmask yang merupakan jenis IP address khusus. Setiap kelas-kelas IP memiliki nilai netmask yang berbeda. IP kelas A dengan netmask 255.0.0.0 sedangkan kelas B 255.255.0.0 dan kelas C 255.255.255.0.

KELAS	Netmask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Penggunakan netmask dapat menentukan besarnya jumlah client yang dapat mengakses ke dalam sebuah jaringan computer. Contoh penggunaan netmask pada

kelas B adalah 172.168.10.1 dengan netmask 255.255.0.0. IP address ini jika kita konversikan ke bilangan biner maka hasil yang didapat adalah:

255.255.0.0

11111111.11111111.00000000.00000000

Ket:

1 > Network (N)

0> Host (H)

Maka untuk melakukan perhitungan jumlah client yang dapat terkoneksi kedalam sebuah jaringan computer kita dapat menggunakan rumus:

Network= 2n

Host= 2h-2

Maka dapat kita hitung jumlah host yang dapat terkoneksi adalah:

H= (216)-2 = 65524

Dapatkan anda membayangkan, sebuah kabel jaringan atau sebuah topologi jaringan yang dapat menampung sampai 65524 client??. Untuk mengatasi masalah tersebut, kita dapat memecahnya menjadi sebuah network yang lebih kecil. Network yang lebih kecil ini disebut dengan subnetwork.

Contoh IP Subneting:

1. IP Address: 192.168.0.0/24
   a. Netmask : 255.255.255.0
   b. Prefix : /24
   c. IP Network : 192.168.0.0
   d. First Host IP : 192.168.0.1
   e. Last Host IP : 192.168.0.254
   f. Broadcast : 192.168.0.255

Jadi dengan menggunakan “/24” jumlah host yang dapat terkoneksi sebanyak 254 client.

2. IP Address: 192.168.0.0/25

   a. Netmask : 255.255.255.128

   b. Prefix : /25

   c. IP Network : 192.168.0.0

   d. First Host IP : 192.168.0.1

   e. Last Host IP : 192.168.0.126

   f. Broadcast : 192.168.0.127

Jadi dengan menggunakan “/24” jumlah host yang dapat terkoneksi sebanyak 127 client.

A. Subneting

Subnetting adalah metode atau 29amper membuat net Id dengan cara mengorbankan bit host. Karena Ipv4 pengalamatan sangat terbatas dengan makin banyaknya user jaringan maka dibuat metode 29amper29r2929.

Kegunaan Subnetting

1. Untuk menentukan batas network ID dalam suatu subnet
2. Memperbanyak jumlah network (LAN)
3. Mengurangi jumlah host dalam satu network

Tujuan lain dari subnetteing yang tidak kalah penting adalah untuk mengurangi tingkat konggesti (gangguan/tabrakan) lalulintas data dalam suatu network

1. Efisiensi pengguanan IP Address
2. Pendelegasian kekuasan untuk pengaturan
3. Mempermudah manajemen jaringan
4. Mengatasi masalah perbedaan hardware dan topologi fisik jaringan

Menghitung Subbnetting

Rumus untuk menghitung jumlah subnet adalah : 2n – 2, “N” adalah jumlah bit yang diselubungi/dikorbankan

Rumus untuk menghitung jumlah host per subnet : 2N–2, “N” adalah jumlah bit yang masih tersisa untuk host ID

Contoh subnet kelas A:

IP = 10.0.0.0/25

Subnet = 25 bit

= 11111111.11111111.11111111.10000000

= 255.255.255.128

Jumlah net id baru = 2n – 2

= 217 – 2

= 131070

*n = 17 = 111111111.11111111.11111111.10000000

Jumlah host per subnet = 2N – 2

= 27 – 2

= 126

*N = 7 = 1111111.11111111.11111111.10000000

Variable Length Subnet Mask (VLSM)

Jika pada pengalokasian IP Address classfull, suatu network ID hanya memiliki satu subnetmask, maka VLSM menggunakan metode yang berbeda, yakni dengan memberikan lebih dari satu subnet.

Contoh:

Satu blok IP address (169.254.0.0/20) dibagi menjadi 16

1. Subnet 1 = 4094 host – Net Address = 169.254.0.0/20
2. Subnet 1 = 4094 host – Net Address = 169.254.16.0/20
3. Subnet 1 = 4094 host – Net Address = 169.254.32.0/20
4. Subnet 1 = 4094 host – Net Address = 169.254.64.0/20
5. Subnet 1 = 4094 host – Net Address = 169.254.240.0/20
6. Subnet Mask = 255.255.240.0

Berikutnya Subnet 2 akan dipecah menjadi 16 subnet lagi yang lebih kecil

1. Subnet 2.1 =254 host – Net Address = 169.254.16.0/24
2. Subnet 2.2 =254 host – Net Address = 169.254.17.0/24
3. Subnet 2.3 =254 host – Net Address = 169.254.18.0/24
4. .....
5. Subnet 2.16 =254 host – Net Address = 169.254.31.0/24
6. Subnet Mask = 255.255.255.0

Bila subnet 2.1 akan dipecah lagi menjadi beberapa subnet, misalnya 4 subnet, maka:

1. Subnet 2.1.1 = 62 host –Net Address = 169.254.16.0/26
2. Subnet 2.1.2 = 62 host –Net Address = 169.254.16.64/26
3. Subnet 2.1.3 = 62 host –Net Address = 169.254.16.128/26
4. Subnet 2.1.4 = 62 host –Net Address = 169.254.16.192/26
5. Subnet Mask = 255.255.255.192

Kesimpulan dari contoh:

Terlihat 32ampe pada Subnet 2 (Net Address 169.254.16.0) dapat memecah jaringannya menjadi beberapa subnet lagi dengan mengganti Subnetmask-nya menjadi:

255.255.240.0, 255.255.255.0 dan 255.255.255.192

Jika anda perhatikan, CIDR dan metode VLSM mirip satu sama lain, yaiut blok network address dapat dibagi lebih lanjut menjadi sejumlah blok IP address yang lebih kecil.

Perbedaanny adalah CIDR merupakan sebuah konsep untuk pembagian blok IP Public yang telah didistribusikan dari IANA, sedangkan VLSM merupakan implementasi pengalokasian blok IP yang dilakukan oleh pemilik network (network administrator) dari blok IP yang telah diberikan padanya (sifatnya local dan tidak dikenal di internet).

LAN DESAIN

1.1. Pengertian

Administrasi jaringan komputer adalah sebuah profesi atau pekerjaan yang bertugas untuk mengatur sebuah lalu lintas jaringan komputer dan memonitoring jaringan untuk mengamankan paket baik dalam sekala kecil atau pada sekala besar.

Seorang Administrasi bertanggung jawab penuh terhadap penggunaan user maupun akses pada setiap clinet yang terdapat pada sebuah network agar dapat berjalan dengan lancar sebuah akses yang diterima oleh client ke sebuah network.

1.2. Tugas Pokok Administrator Jaringan Komputer

Adapun tugas pokok Administrasi jaringan Komputer sebagai berikut:

1. Menginstall dan Mengkonfigurasi Server

   Tugas utama dari administrator jaringan adalah menginstall server atau komputer server beserta konfigurasinya. Untuk server jaringan biasanya dalam perusahaan atau lembaga menggunakan sistem operasi linux. Kemudian untuk konfigurasinya biasanya adalah konfigurasi alamat IP beserta koneksi jaringan.
2. Menginstall dan mengkonfirgurasi Aplication Server

   Kemudian setelah melakukan installasi dan konfigurasi server maka tugas kedua administrator jaringan adalah menentukan aplikasi dan software apa saja yang ingin digunakan dalam jaringan tersebut.
3. Membuat dan mengelola user

   Untuk tugas lainya dari administrator jaringan adalah membuat dan mengelolah user, dimana user disini sangatlah dibutuhkan agar tidak sembarangan orang yang memasuki jaringan. Oleh karena itu dibuatlah user untuk lebih mengamankan jaringan.
4. Backup dan Restore File

   Back Up dan Restore file sangatlah dibutuhkan dalam administrasi jaringan. Hal ini dilakukan karena jika terjadi masalah dalam server atau jaringan maka data yang hilang masih tetap tersimpan dan aman
5. Mengkonfirgurasi Keamanan Sistem

   Keamanan sistem sangatlah dibutuhkan untuk melindungi jaringan dan data-data dalam jaringan. Oleh karena itu server atau sistem jaringan harus dikonfigurasi.

Sehingga dapat disimpulkan bahwa tugas pokok Administrasi jaringan komputer adalah Mengetahui tentang dasar komputer baik teori maupun praktek, Melakukan instalasi, mengelola serta memecahkan permasalahan insfratruktur jaringan seperti pada: Router, Switch, Access Point dll dan Menjaga kesetabilan jaringan (QoS).

1.3. Perancangan Jaringan

1.3.1. Prinsip Administrasi jaringan komputer

Dalam menentukan perancangan jaringan komputer harus menggunakan beberapa prinsip diantaranya:

1. Perhitungkan bandwidth yang dibutuhkan jaringan

   Bandwidth adalah ukuran banyak data yang dapat ditransfer dalam satu waktu tertentu pada medium tertentu antara 2 titik lokasi, semakin besar bandwidth maka semakin cepat data keluar masuk pada koneksi Internet.

   Satuan bandwidth adalah bits per second (bps), contoh bandwidth sebuah koneksi terdaftar 80 Mbps artinya koneksi internet tersebut mampu memindahkan maksimal sebanyak 80 juta bit data tiap detiknya.

2. Menganalisa aplikasi kebutuhan pengguna

   Kebutuhan terhadap aplikasi perangkat lunak harusnya disesuaikan dengan kebutuhan bisnis atau perusahaan. Karena Analisis kebutuhan merupakan langkah awal untuk menentukan gambaran sistem yang akan dihasilkan ketika akan melaksanakan sebuah proyek mengadministrasi server. Perangkat lunak yang baik dan sesuai dengan kebutuhan pengguna sangat tergantung pada keberhasilan dalam melakukan analisis kebutuhan. Untuk proyek-proyek instalasi server yang besar, analisis kebutuhan dilaksanakan setelah aktivitas installation system dan server administration planning. Analisa kebutuhan yang baik belum tentu menghasilkan sistem yang baik, tetapi analisa kebutuhan yang tidak tepat menghasilkan sistem yang tidak berguna. Mengetahui adanya kesalahan pada analisis kebutuhan pada tahap awal memang jauh lebih baik, tapi kesalahan analisis kebutuhan yang diketahui ketika sudah memasuki penulisan kode atau pengujian, bahkan hampir masuk dalam tahap penyelesaian merupakan malapetaka besar bagi pembuat perangkat lunak. Biaya dan waktu yang diperlukan akan menjadi sia sia.

3. Memperhatikan jalur-jalur kritis pada jaringan

Menentukan jalur merupakan sebuah perioritas yang harus dilakukan oleh administrator untuk menentukan jalur yang dilewati oleh sebuah clinet agar tidak terjadi traffic atau kemacetan lalulinta data.

4. Memperhatikan keseimbangan beban pada jaringan

   Agar tidak terjadi permasalahan lambatnya sebuah akses komputer clinet terhadap jaringan Internet atau Intranet maka diperlukan penentuan dan penyeimbangan beban yang ditetapkan pada setiap network.

5. Menggunakan model desain hierarki dalam mendesain jaringan

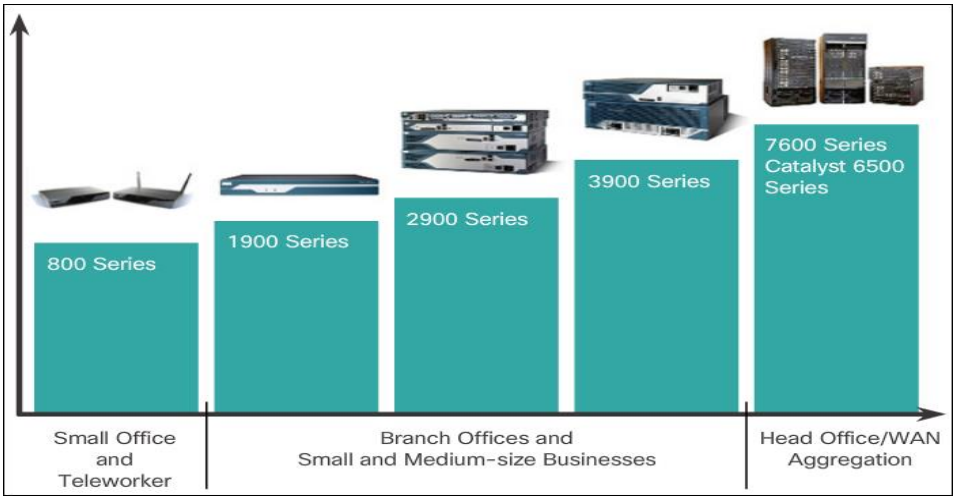
   Penentuan topologi jaringan komputer merupakan sebuah usaha agar sebuah network dapat berjalan sesuai dengan rencana dan merupakan hal pertama yang dilakukan dengan menyesuaikan kebutuhan yang akan diterapkan pada sebuah perusahan atau instansi.

6. Mengetahui tentang sistem keamanan jaringan komputer

   Kemana jaringan komputer merupakan tantangan terbesar sebagai administrator jaringan komputer selain mengetahui system kemanan seorang adminstrasi harus pandai dalam mengatasi serangan yang kemungkinan terjadi pada sebuah network.

1.3.2. Memilih Perangkat Jaringan

Administrator jaringan dilingkungan perusahaan harus mampu menentukan perangkat jaringan yang akan digunakan, seperti jenis-jenis router. Terdapat tiga katagori dari router berdasarkan spesifikasinya. Router untuk Small Office, Medium dan Head Office.



Gambar 1.1 Penentuan Hardware

Pentingnya pemilihan hardware untuk menyesuiakan kapasitas pengguna merupakan salah satu hal terpenting dalam perancangan network, seperti pada seri hardware brand cisco untuk cakup wilayah kecil atau small office dapat menggunakan switch seris RB800 dengan spesifiaksi sebagai berikut:

Spesifikasi RB800	
Product Code	RB800
Architecture	PPC
CPU	MPC8544 800MHz
Current Monitor	No
Main Storage/NAND	512MB
RAM	256MB
SFP Ports	0
LAN Ports	3
Gigabit	Yes
Switch Chip	1
MiniPCI	4
Integrated Wireless	No
MiniPCIe	1
SIM Card Slots	No
USB	No
Memory Cards	1
Memory Card Type	CF
Power Jack	10-56V
802.3af Support	Yes
POE Input	36-56V
POE Output	No
Serial Port	DB9/RS232
Voltage Monitor	Yes
Temperature Sensor	Yes
Dimentions	200mm x 140mm
Operating System	RouterOS
Temperature Range	-75C .. +65C
RouterOS License	Level6

Gambar 1.2 spesifikasi RB800 Cisco

Pada spesifikasi tersebut cukup untuk kebutuhan jaringan yang kecil dikarenakan dalam penyimpanan data menggunakan kapasitas RAM sebanyak 256 MB. Adapun untuk series network yang mulai besar atau menengah tidak dapat menggunakan seri RB 800 akan tetapi lebih meningkat ketahap selanjutnya yaitu series 1900, 2900 dan 3900. Sedangkan untuk network yang berskala besar maka menggunakan dengan jenis router yang mampu menampung beban yang sangat besar diantaranya adalah Seris RB 6500.

1.3.3. Wireless

Adalah salah satu jenis jaringan berdarsarkan media komunikasinya, yang memungkinkan perangkat-perangat didalamnya seperti komputer, hp, dll bisa saling berkomunikasi secara wireless/tanpa kabel. Wireless network umumnya diimplementasikan menggunakan komunikasi radio. Implementasi ini berada pada level lapisan fisik (pysical layer) dari OSI model.

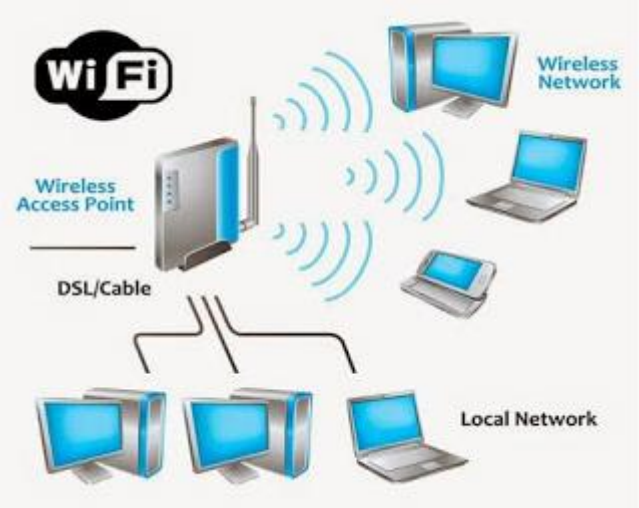
1. Wireless PAN (WPAN)

   Wireless Personal Area Network (WPAN) adalah jaringan wireless dengan jangkauan area yang kecil. Contohnya Bluetooth, Infrared, dan ZigBee.

Gambar 1.3 Wireless PAN (WPAN)

2. Wireless LAN (WLAN) / Wifi

   Wireless Local Area Network (WLAN) atau biasa disebut Wifi memiliki jangkauan yang jauh lebih luas dibanding WPAN. Saat ini WLAN mengalami banyak peningkatan dari segi kecepatan dan luas cakupannya. Awalnya WLAN ditujukan untuk penggunaan perangkat jaringan lokal, namun saat ini lebih banyak digunakan untuk mengakses internet



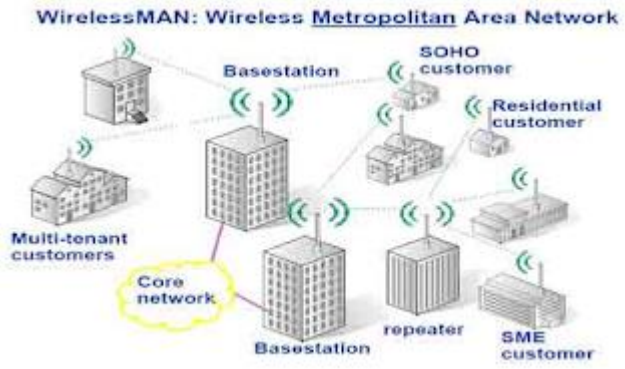
Gambar 1.4 WLAN

IEEE (Institute of Electrical dan Electronics Engineers) membentuk Kelompok 802.11 pada tahun 1990. Spesifikasi untuk standar ditulis pada tahun 1997, Kecepatan awal adalah 1 dan 2 Mbps.IEEE dimodifikasi standar pada tahun 1999 meliputi:

a. 802.11b
b. 802.11a
c. 802.11g

3. Wireless MAN (WMAN)

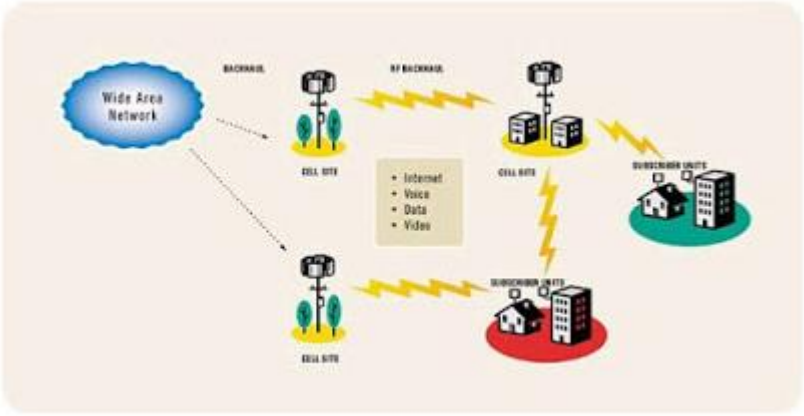
Wireless Metropolitan Area Network (WMAN) adalah jaringan wireless network yang menghubungkan beberapa jaringan WLAN. Contoh teknologi WMAN adalah WiMAX.



Gambar 1.5 WMAN

4. Wireless WAN (WWAN)

   Wireless Wide Area Network adalah jaringan wireless yang umumnya menjangkau area luas misalnya menghubungkan kantor pusat dan cabang antar provinsi.



Gambar 1.6 WWAN

5. Cellular Network

   Cellular Network atau Mobile Network adalah jaringan radio terdistribusi yang melayani media komunikasi perangkat mobile seperti handphone, pager, dll. Contoh sistem dari Cellular Network ini adalah GSM, PCS, dan D-AMPS

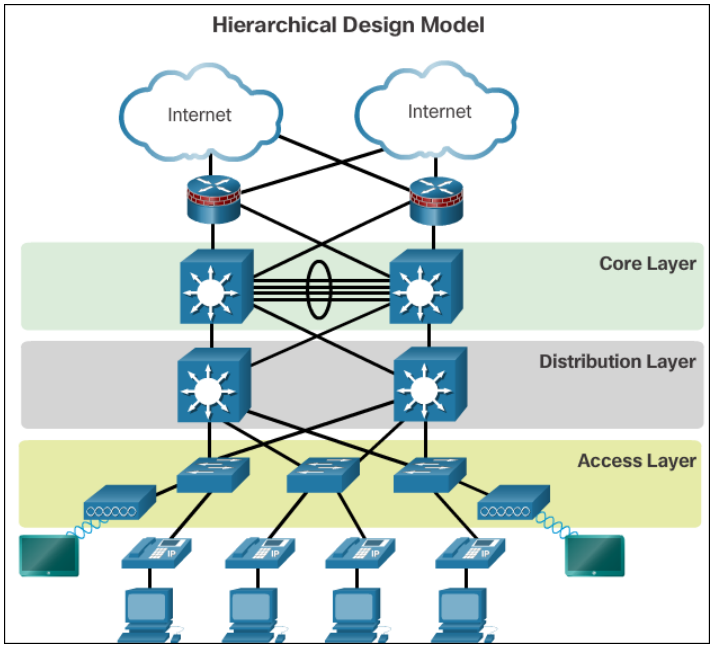
Gambar 1.7 Cellular Network

1.3.4. Kampus Wired LAN (WLAN)

1. Desain Cisco

   Desain dari hirarki LAN meliputi:

   a. Lapisan Akses
   b. Lapisan Distribusi
   c. Lapisan Inti (Core)



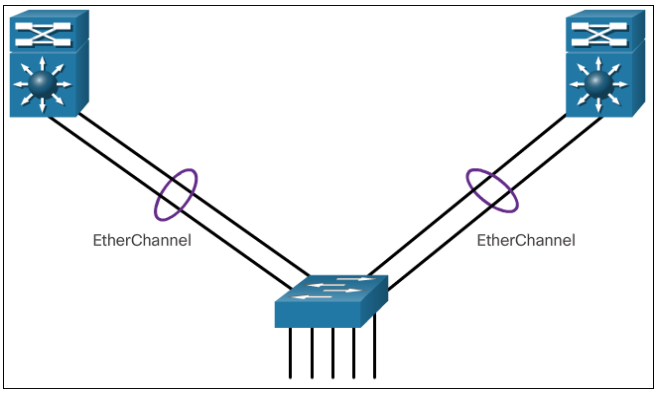
Gambar 1.8 WLAN

Untuk membangun sebuah jaringan yang lebih besar, perancangan jaringan haruslah mengembangkan strategi untuk mengoptimalkan jaringan, Salah satu metode untuk mengoptimalkan jaringan dapat menerapkan redundansi pada lalu lintas jaringan yang padat.

1.3.5. EtherChannel

EtherChannel merupakan sebuah teknologi trunking yang dilakukan oleh Switch dengan cara menghubungkan 2 buat Switch guna untuk meningkatkan kecepatan dan meminimalis terjadi adanya akses yang terputus bilamana salah satu port atau kabel terjadi sebuah gangguan.

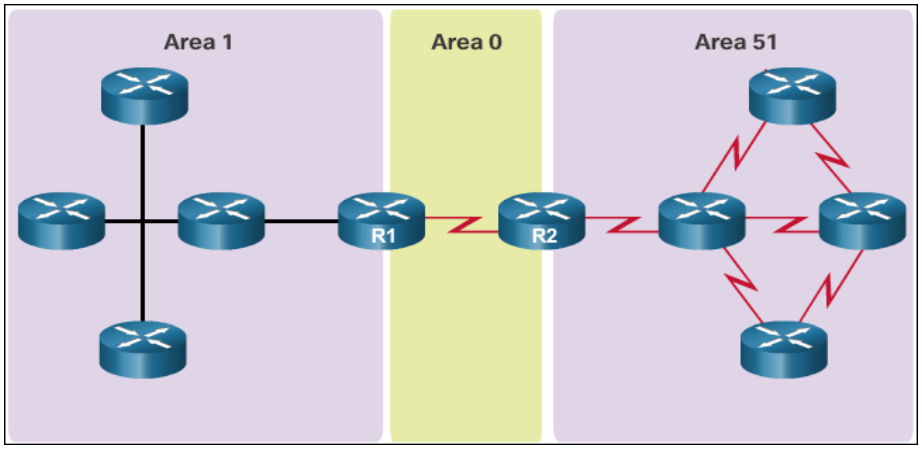
Agregasi link EtherChannel memungkinkan administrator untuk meningkatkan jumlah bandwidth antara perangkat dengan menciptakan satu link logis terdiri dari beberapa link fisik.



Gambar 1.9 EtherChannel

1.3.6. Open Shortest Path First

Link-state routing protokol, seperti Open Shortest Path First (OSPF), bekerja dengan baik untuk jaringan hirarkis yang lebih besar di mana konvergensi cepat sangatlah penting.



Gambar 1.10 OSPF

BAB II
WIRELESS LAN

2.1. Wireless Wireless LAN

Adalah salah satu jenis jaringan berdarsarkan media komunikasinya, yang memungkinkan perangkat-perangat didalamnya seperti komputer, hp, dll bisa saling berkomunikasi secara wireless/tanpa kabel. Wireless network umumnya diimplementasikan menggunakan komunikasi radio. Implementasi ini berada pada level lapisan fisik (pysical layer) dari OSI model.

2.2. Wired dan Wireless

Wired adalah Pendistribusian informasi melalui kabel sebagai media penghubung dan biasanya digunakan dalam jangkuan local semisal dalam satu area Gedung, kabel yang sering digunakan adalah jenis: coaxial cabel, unshielded twisted Pair (UTP) maupun fiber optik,

Minimal dua perangkat yang akan berkomunikasi satu sama lainnya harus dihubungkan menggunakan kabel (tidak fleksibel), Kabel yang digunakan mengandung untaian logam atau bahan serat optik yang berjalan dari satu sisi ke sisi lainnya, Kabel Ethernet memiliki standar IEEE 802.3

Wireless atau jaringan Nirkabel adalah pendistribusian informasi melalui gelombang radio sebagai media transisinya yang diset untuk bekerja dibidang frekuensi tertentu sesuai dengan standar, Jaringan nirkabel mengandalkan kenyamanan dan mobilitas pengguna untuk dapat tetap terkoneksi kedalam jaringan

IEEE Standard	Maximum Speed	Frequency	Backwards Compatible
802.11	2 Mb/s	2.4 GHz	—
802.11a	54 Mb/s	5 GHz	—
802.11b	11 Mb/s	2.4 GHz	—
802.11g	54 Mb/s	2.4 GHz	802.11b
802.11n	600 Mb/s	2.4 GHz and 5 GHz	802.11a/b/g
802.11ac	1.3 Gb/s (1300 Mb/s)	5 GHz	802.11a/n
802.11ad	7 Gb/s (7000 Mb/s)	2.4 GHz, 5 GHz, and 60 GHz	802.11a/b/g/n/ac

Gambar 2.1 Standarisasi IEEE 802.11

Institute of Electrical and Electronics Engineers adalah Group dari Organisasi Insinyur yang mengatur standarisasi dalam bidang teknologi informasi. Setiap standarisasi yang diciptakan memiliki kode tersendiri. Salah satunya standarisasi di jaringan wireless yang memiliki kode 802.11. Dengan adanya standar ini dimaksudkan agar setiap perangkat wireless yang berbeda tetap dapat berkomunikasi meski berbeda vendor.

1. 802.11

   Pada Tahun 1997, IEEE menciptakan standar wireless yang pertama bekerja pada frekuensi 2,4 GHz yang dinamakan 802.11. Namun standar ini hanya mendukung bandwidth jaringan maksimal 2 Mbps, telalu kecil untuk komunikasi jaringan pada saat ini. Oleh karena itu perangkat wireless dengan standar ini tidak diproduksi lagi.

2. 802.11 b

   IEE menciptakan standar lanjutan yang dinamakan 802.11b pada tahun 1999 mendukung bandwidth mencapai 11 Mbps. Masih bekerja pada frekuensi 2,4 GHz. Vendor perangkat elektronik pada umumnya lebih memilih menggunakan frekuensi ini dikarenakan dapat menekan biaya produksi. Seperti yang diketahui, frekuensi 2,4 GHz merupakan frekuensi radio yang tidak diatur sehingga dapat menimbulkan gangguan dari perangkat elektronik lainnya seperti microwave, televisi dan perangkat lainnya yang menggunakan frekuensi 2,4 GHz. Namun hal tersebut dapat dihindari dengan mengatur jarak antar perangkat elektronik sehingga tidak menimbulkan gangguan atau interferensi.

   Router yang hanya menggunakan standar 802.11b ini juga sudah tidak diproduksi lagi. Namun beberapa router baru masih mendukung standar ini. Standar ini, secara teoritis mendukung bandwidth data mencapai 11 Mbps dan jangkauan sinyal mencapai sekitar 150 kaki (+-45 Meter).

3. 802.11 a

   Saat standar 802.11b sedang dikembangkan, IEEE membuat ekstensi untuk standar 802.11 yang dinamakan 802.11a. Standar ini diciptakan pada saat yang bersamaan dengan standar 802.11b. Standar ini sudah mendukung bandwidth data mencapai 54 Mbps dan menggunakan frekuensi 5 GHz (semakin tinggi frekuensi maka semakin pendek jangkauan sinyal). Dikarenakan berjalan pada frekuensi yang bebeda dengan standar 802.11b, kedua teknologi ini tidak kompatible satu sama lain. Beberapa vendor menawarkan perangkat jaringan hybrid 802.11a/b. Namun perangkat tersebut hanya dapat menjalankan satu standar pada satu waktu

4. 802.11 g

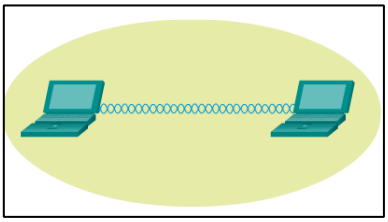
   Standar ini diciptakan pada tahun 2002 dengan menggabungkan kelebihan masing masing standar 802.11a dan 802.11b. Standar ini mendukung bandwidth 54 Mbps dan menggunakan frekuensi 2,4 GHz yang berarti memiliki jangkauan sinyal yang luas. Perangkat dengan network adapter yang mengadopsi standar ini juga kompatibel dengan standar 802.11b begitu juga sebaliknya.

5. 802.11 n

   Standar 802.11n sering dikenal dengan sebutan Wireless-N diciptakan untuk memperbaiki standar 802.11g dalam hal jumlah bandwidth yang didukung dengan memanfaatkan beberapa sinyal wireless dan antena (disebut dengan teknologi MIMO, Multiple in Multiple out). IEEE meresmikan standar ini pada tahun 2009 dengan spesifikasi menyediakan bandwidth sampai 300 Mbps. Standar ini juga menawarkan jangkauan sinyal yang lebih baik dibandingkan standar wireless sebelumnya serta memiliki kompabilitas dengan perangkat yang memiliki standar 802.11b/g. Standar wireless ini beroperasi 2 frekuensi yaitu 2,4 GHz dan 5GHz

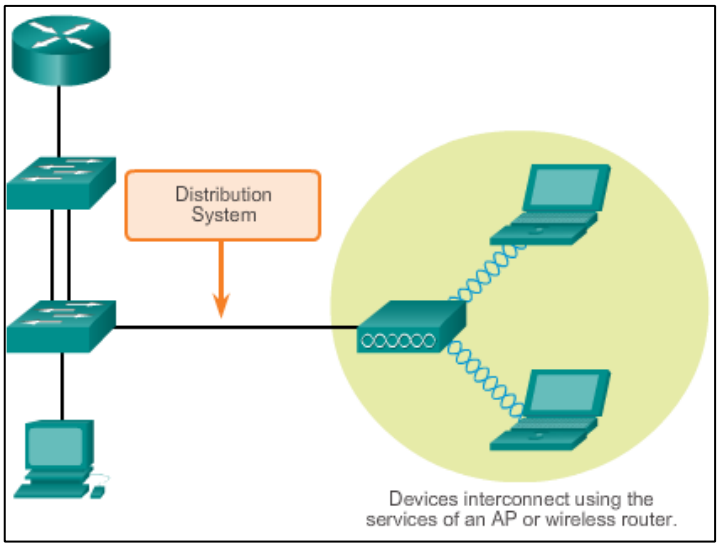
6. 802.11 ac

   Generasi terbaru dari standar Wifi yang populer digunakan. Memanfaatkan teknologi wireless dual band mendukung koneksi secara bersamaan pada frekuensi 2,4 GHz dan 5 GHz. Menawarkan kompabilitas dengan standar 802.11b/g/n serta mendukung bandwidth mencapai 1300Mbps pada frekuensi 5 GHz ditambah 450Mbps pada frekuensi 2,4 GHz



Gambar 2.2 802.11 mode Ad-Hoc

Tethering (personal hotspot): merupakan variasi dari topologi Ad Hoc, biasanya ketika ponsel pintar atau tablet dengan akses data seluler mengaktifkan fitur tethering untuk membuat hostpot pribadi



Gambar 2.3 Mode Infrastructure

2.3. TW Power & RX Sensitivity

Standard	Output power / Receive Sensitivity
802.11a	17dBm/-88dBm @ 6Mbps
	13dBm/-71dBm @ 54Mbps
802.11b	19dBm/-95dBm @ 1Mbps
	19dBm/-90dBm @ 11Mbps
802.11g	18dBm/-90dBm @ 6Mbps
	15dBm/-73dBm @ 54Mbps

Gambar 2.4 TW Power & RX Sensitivity

Wireless Card memiliki spesifikasi TX Power dan RX Sensitivity yang bervariasi sesuai dengan kualitas dari card itu sendiri. Tidak hanya pada kualitas, TX power dan RX sensitivity juga akan berubah sesuai dengan Band yang digunakan dan besar troughput yang melewati card tersebut.

2.4. Sertifikasi WIFI

Dalam fungsinya sertifikasi WIFI harus mempunya serttifikasi diantaranya adalah: IEEE 802.11a/b/g/n/ac/ad harus kompatibilitas, IEEE 802.11i, mengamankan menggunakan WPA2 dan Extensible Authentication Protocol (EAP), Wi-Fi Protected Setup (WPS), untuk menyediakan koneksi perangkat, Wi-Fi Direct, untuk berbagi media antara perangkat, Wi-Fi Passpoint, untuk menyederhanakan keamanan hubungan ke jaringan Hotspot Wi-Fi, Wi-Fi Miracast, untuk menampilkan video antara perangkat

2.5. Komponen WLAN

1. Omnidirectional Wi-Fi Antennas

   Antena Omni menyediakan cakupan 360 Derajat. Biasanya digunakan pada radio Walkie-Talkie.

2. Directional Wi-Fi Antennas

   Antena Directional berfokus terhadap sinyal radio dalam arah tertentu saja. Biasanya digunakan untuk meningkatkan sinyal AP.

3. Yagi Antennas

   Merupakan antena radio yang dapat digunakan untuk jarak jauh pada jaringan Wi-Fi.

2.6. Parameter Operasi Nirkabel

1. SSID

   SSID (Service Set Identifier) merupakan identifikasi atau nama untuk jaringan Wireless. Setiap peralatan Wi-Fi harus menggunakan SSID (Service Set Identifier) tertentu. Peralatan Wi-Fi dianggap satu jaringan jika menggunakan SSID (Service Set Identifier) yang sama. Agar dapat berkomunikasi, setiap peralatan Wireless haruslah menggunakan SSID (Service Set Identifier) bersipat case-sensitive, penulisan huruf besar dan huruf kecil akan sangat berpengaruh.

   SSID adalah sebuah metode/ cara jaringan wireless yang digunakan sebagai pengenal atau nama sebuah WLAN. Singkatnya dalam bahasa inggris “Public name of wireless network service”. Kepanjangan dari SSID itu sendiri adalah Service Set IDentifier. SSID ini pula merupakan sebuah token yang bisa mengenal jaringan wireless dengan standar perangkat bernomor 802.11. SSID mempunyai 32 karakter khusus yangmenampilkan identifier sebagai header paket yang dikirim melalui WLAN. Identifier ini bertugas sebagai password level device ketika perangkat mobile yang mencoba untuk connect ke Basic Service Set (BSS). Pada SSID. Semua access point dan semua device berusaha untuk connect ke WLAN, dan WLAN tersebut harus mempunyai SSID yang sama. Sebuah device tidak diizinkan untuk bergabung pada BSS kecuali device tersebut menyediakan SSID khusus. Karena sebuah SSID dapat mengenali suatu teks sederhana dalam sebuah paket, dan tidak menyediakan keamanan untuk sebuah jaringan. Kadang-kadang SSID berhubungan dengan jaringan sebagai nama jaringan. SSID dalam

jaringan komputer client dapat juga menset access point secara manual. Dalam penjelesan diatas bisa ditarik kesimpulan bahwa SSID tersebut merupakan tempat untuk mengisikan nama dari access point yang akan disetting. Apabila klien komputer sedang mengakses kita misalnya dengan menggunakan super scan, maka nama yang akan timbul adalah nama SSID yang diisikan tersebut.

Biasanya SSID untuk tiap Wireless Access Point adalah berbeda. Untuk keamanan jaringan Wireless bisa juga SSID nya di hidden sehingga user dengan wireless card tidak bisa mendeteksi keberadaan jaringan wireless tersebut dan tentunya mengurangi resiko di hack oleh pihak yang tidak bertanggung jawab

2. Password

   Password adalah sandi yang harus dimasukan kedalam suatu sistem baik itu sistem komputer yang menggunakan system operasi windowsatau bukan yang berupa karakter tulisan, suara, atau ciri-ciri khusus yang harus diingat.

3. Network Mode

   a. Access Point mode atau AP mode

      AP Mode lebih digunakan untuk mentransfer sambungan kabel ke nirkabel. Ia bekerja seperti switch. Biasanya, peralatan itu adalah di belakang router, Jika Anda berada di kantor, hotel dan tempat-tempat di mana hanya jaringan kabel tersedia, ada rapat kecil dan situasi lain di mana jaringan nirkabel sementara diperlukan, silakan gunakan Mode AP.

   b. Wireless Router Mode

      Dengan mode ini, kita dapat berbagi satu koneksi internet kabel ke beberapa klien. Pada saat itu, akan ada satu port WAN. Mendukung beberapa jenis koneksi, seperti Dinamis IP / Static IP / PPPoE / L2TP / PPTP, Ketika akses Internet dari DSL atau modem kabel yang tersedia hanya untuk satu user, sementara ada lebih banyak pengguna perlu berbagi internet juga, maka silakan gunakan Mode Router.

   c. Repeater mode

      Repeater Mode digunakan untuk extender (menambah) jangkauan nirkabel dengan SSID dan keamanan yang sama.

      Bila kita sudah memiliki jaringan nirkabel, dan ada beberapa tempat yang tidak dapat signal, kita dapat mempertimbangkan Repeater Mode. Dengan

Repeater Mode, kita akan memiliki hanya satu SSID. Pada saat itu, klien nirkabel dapat menjelajah di seluruh tempat.

d. Bridge Mode

Bridge mode “meminjam” jaringan internet nirkabel yang telah tersedia dan ia broadcast menggunakan SSID dan password yang berbeda. Aplikasi ini dapat membuat dua jaringan individu untuk dua kelompok pengguna berbagi satu Internet, Untuk restoran kecil, bar, rumah, kantor dan lain-lain di mana layanan internet harus disediakan untuk para tamu tanpa password dari jaringan yang ada untuk host, Bridge Mode adalah pilihan terbaik.

e. Client Mode

Dengan Client Mode, device dapat terhubung ke perangkat kabel dan bekerja sebagai adapter nirkabel (wireless adapter) untuk menerima sinyal nirkabel dari jaringan nirkabel kita, Untuk Smart TV, Media Player, konsol game atau perangkat lain yang hanya memiliki port Ethernet . Gunakan Client Mode untuk membuat perangkat ini dapat akses ke jaringan nirkabel kita.

f. AP Client Router Mode (WISP user Internet sharing)

Dengan AP client router mode , dapat terhubung ke jaringan nirkabel dan berbagi koneksi ke klien. Nirkabel adalah sisi WAN nya. Hal ini juga dapat mendukung IP Dinamis / Static IP / PPPoE / L2TP / PPTP,

Ketika wireless station membatasi jumlah klien atau meminta username / password untuk terhubung, maka AP Client Router Mode adalah solusinya.

4. Security Mode

a. WEP 64

Standar protokol WEP yang lama dan sangat rentan, sehingga sebaiknya hindari penggunaan ini

b. WEP 128

Ini adalah WEP, meskipun memiliki ukuran kunci enkripsi yang lebih besar. Walaupun begitu, ia masih sangat rentan

c. WPA-PSK (TKIP)

Ini menggunakan versi asli protokol WPA (dasarnya WPA1). Biasanya fitur ini telah digantikan oleh WPA2 dan tidak aman

d. WPA-PSK (AES)

   Ini menggunakan protokol WPA yang asli, namun menggantikan TKIP dengan enkripsi AES yang lebih modern. Fitur ini ditawarkan sebagai stopgap, namun perangkat yang mendukung AES hampir selalu mendukung WPA2, sementara perangkat yang membutuhkan WPA hampir tidak akan pernah mendukung enkripsi AES. Jadi, pilihan ini tidak masuk akal.

e. WPA2-PSK (TKIP)

   Menggunakan standar WPA2 modern dengan enkripsi TKIP yang lebih tua. Ini tidak aman, dan hanya dipakai jika Anda memiliki perangkat yang lebih tua yang tidak dapat terhubung ke jaringan WPA2-PSK (AES).

f. WPA2-PSK (AES)

   Ini adalah pilihan yang paling aman dan ideal. Dengan hadirnya fitur ini, ia akan Menggunakan WPA2, standar enkripsi Wi-Fi terbaru, dan protokol enkripsi AES terbaru. Anda harus menggunakan opsi ini. Pada beberapa perangkat, Anda hanya akan melihat opsi “WPA2” atau “WPA2-PSK.” Jika Anda melakukannya, mungkin hanya menggunakan AES, karena ini adalah pilihan sangat baik.

g. WPAWPA2-PSK (TKIP / AES)

   Beberapa perangkat menawarkan atau bahkan merekomendasikan opsi mode campuran ini. Pilihan ini memungkinkan WPA dan WPA2, baik dengan TKIP dan AES. Selain itu, ia juga menyediakan kompatibilitas maksimum dengan perangkat kuno yang mungkin kita miliki. Hanya saja, ini juga memungkinkan penyerang untuk melanggar jaringan Anda dengan menerapkan protokol WPA dan TKIP yang lebih rentan.

h. Server Autentikasi User Login Hotspot

   Menggunakan validasi user dan password untuk menentukan atau mengkonfirmasi bahwa seseorang adalah autentik atau asli

i. Media Access Control (MAC) Filtering

   Setiap perangkat jaringan pasti memiliki alamat MAC Address yang unik (disediakan oleh produsen)

   MAC Filtering hanya memungkinkan melakukan akses tertentu saja

   Namun, untuk menerapkan dijaringan dengan skala besar mengalami tingkat kerumitan yang tinggi.

BAB III
SCALING VLAN

3.1. Pengertian Scaling Vlan

VLAN Trunking Protocol (VTP) mengurangi administrasi VLAN dalam jaringan switched. Saklar yang dikonfigurasi sebagai server VTP mendistribusikan dan menyinkronkan informasi VLAN melalui link trunk ke switch berkemampuan VTP di seluruh domain.

Menggunakan frame tagged untuk menandai suatu frame dari VLAN. Pada dasarnya trunking mengijinkan komunikasi antar VLAN yang sama pada switch-switch yang berbeda. Menyediakan metode untuk trunking antar perangkat/VLAN. VTP digunakan untuk menjaga konsistensi VLAN dalam melakukan penambahan, penghapusan dan perubahan VLAN didalam jaringan

3.2. Kategori VTP

1. VTP Domain

   Tujuan utama VTP adalah untuk menyediakan fasilitas sehingga switch Cisco dapat diatur sebagai sebagai suatu grup. Sebagai contoh, jika VTP dijalankan pada semua switch Cisco Anda, pembuatan VLAN baru pada satu switch akan menyebabkan VLAN tersebut tersedia pada semua switch yang terdapat VTP management domain yang sama. VTP management domain merupakan sekelompok switch yang berbagi informasi VTP. Suatu switch hanya dapat menjadi bagian dari satu VTP management domain, dan secara default tidak menjadi bagian dari VTP management domain manapun. Dari sini dapat kita lihat mengapa VTP sangat menguntungkan. Bayangkanlah suatu lingkungan di mana administrator jaringan harus mengatur 20 switch atau lebih. Tanpa VTP, untuk membuat VLAN baru administrator harus melakukannya pada semuanya switch yang diperlukan secara individu. Namun dengan VTP, administrator dapat membuat VLAN tersebut sekali dan VTP secara otomatis akan menyebarkan (advertise) informasi tersebut ke semua switch yang berada di dalam domain yang sama. Keuntungan VTP yang utama adalah efisiensi yang diberikan dalam menambah dan menghapus VLAN dan juga dalam mengubah konfigurasi VLAN dalam lingkungan yang besar.

2. VTP Mode

Server-In VTP server mode, Anda dapat membuat, memodifikasi, dan menghapus VLAN dan menentukan parameter konfigurasi lainnya, seperti versi VTP dan pemangkasan VTP, untuk seluruh domain VTP. Server VTP mengiklankan konfigurasi VLAN mereka ke switch lain di domain VTP yang sama dan menyinkronkan konfigurasi VLAN mereka dengan switch lain berdasarkan iklan yang diterima melalui link trunk. Server VTP adalah mode default. Clien VTP berperilaku sama seperti server VTP, namun Anda tidak dapat membuat, mengubah, atau menghapus VLAN pada klien VTP. Switch transparan Transparan-VTP tidak berpartisipasi dalam VTP. Switch transparan VTP tidak mengiklankan konfigurasi VLAN-nya dan tidak menyinkronkan konfigurasi VLAN-nya berdasarkan iklan yang diterima, namun switch transparan melakukan iklan VTP ke depan sehingga mereka menerima port bagasi mereka di VTP Version 2. Mati (hanya dapat dikonfigurasi di switch CatOS) -Dalam tiga mode yang dijelaskan, iklan VTP diterima dan dikirim segera setelah saklar memasuki status domain manajemen. Pada mode off VTP, switch berperilaku sama seperti pada mode transparent VTP dengan pengecualian bahwa iklan VTP tidak diteruskan.

3. VTP Advertiser

Setiap switch yang tergabung dalam VTP menyebarkan VLAN, nomor revisi, dan parameter VLAN pada port trunk-nya untuk memberitahu switch yang lain dalam management domain. VTP advertisement dikirim sebagai frame multicast. Switch akan menangkap frame yang dikirim ke alamat multicast VTP dan memproses mereka. semua switch dalam management domain mempelajari perubahan konvigurasi VLAN yang baru, suatu VLAN hanya perlu dibuat dan dikonfigurasi pada satu VTP server di dalam domain tersebut. Secara default, management domain diset ke non-secure advertisement tanpa password. Suatu password dapat ditambahkan untuk mengeset domain ke mode secure. Password tersebut harus dikonfigurasi pada setiap switch dalam domain sehingga semua switch yang bertukar informasi VTP akan menggunakan metode enkripsi yang sama. VTP advertisement dimulai dengan nomor revisi konfigurasi 0 (nol). Pada waktu dilakukan perubahan, nomor revisi akan dinaikkan sebelum advertisement dikirim ke luar. Pada waktu switch menerima suatu advertisement yang nomor revisinya

lebih tinggi dari yang tersimpan di dalam, advertisement tersebut akan menimpa setiap informasi VLAN yang tersimpan.

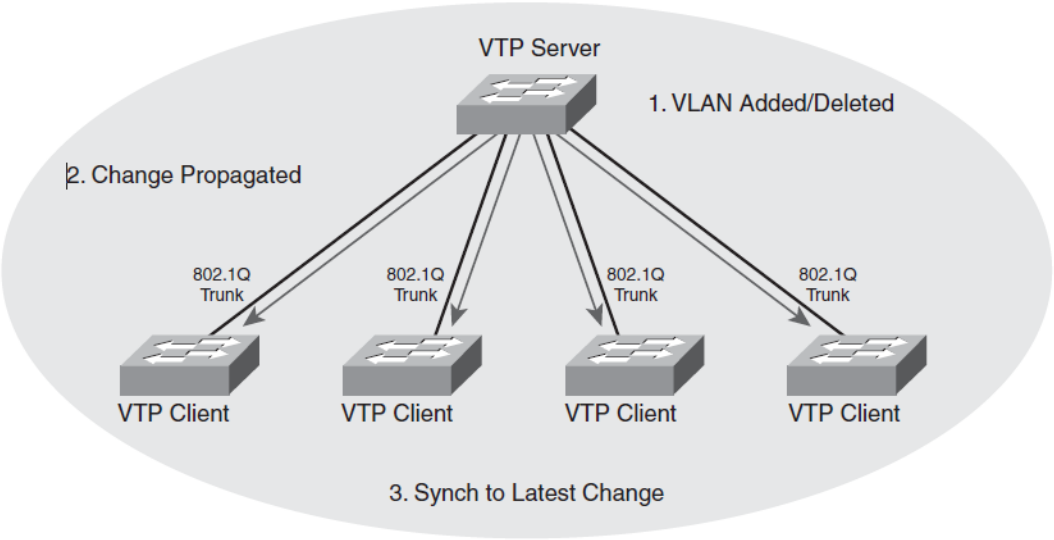
4. VTP Password

   Jika Anda mengkonfigurasi kata sandi untuk VTP, Anda harus mengkonfigurasi kata sandi pada semua switch di domain VTP. Kata sandi harus sama dengan password pada semua switch tersebut. Kata sandi VTP yang Anda konfigurasikan diterjemahkan dengan algoritma menjadi kata 16 byte (nilai MD5) yang disertakan dalam semua paket VTP ringkasan-iklan.

3.3. Manfaat VTP

Dalam penggunannya VTP memiliki beberapa manfaat yang sangat besar diantaranya:

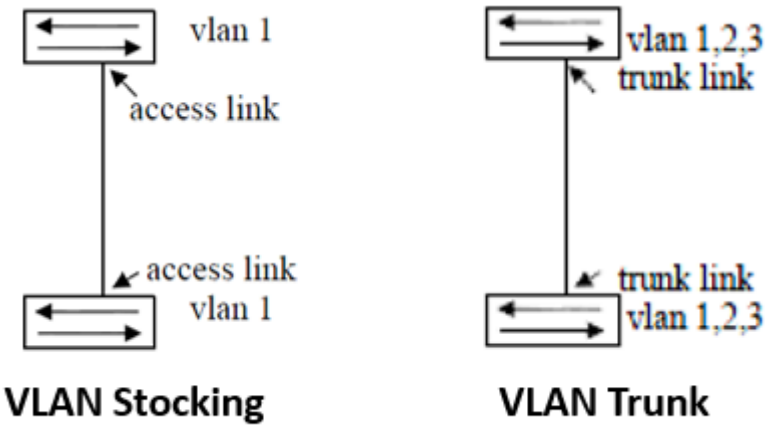
1. Konsistensi VLAN di dalam jaringan
2. Pelacakan dan pemantaun VLAN yang akurat
3. Penambahan VLAN dilakukan secara Dynamis



Gambar 3.1 Rancangan VTP

3.4. Perbedaan VLAN Stocking dengan Trunking

Pada gambar tesebut dijelaskan perbedaan antara VLAN Stocking dan VLAN Trunking dimana perbedaanya adalah pada VLAN Stocking hanya dapat membawa 1 VLAN saja dengan nama VLAN 1 atau VLAN 10 dan seterusnya selama VLAN itu memiliki nama yang sama. Sedangkan pada VLAN Trunk dapat membawa lebih dari satu VLAN dengan Asumsi VLAN yang terdaftar sama antara switch satu dengan switch lainnya.



Gambar 3.2 Konsep VLAN Stocking dab Trunk

3.5. Fungsi VTP

Fungsi utama VTP yaitu menyederhanakan pembuatan VLAN pada banyak switch.

1. VTP Server

   Dapat melakukan create, add, dan delate VLAN. Kemudian mengirimkan informasi VLAN melalui jalur Trunk

2. VTP Client

   menerima dan menyimpan informasi VLAN pada NVRAM

3. VTP Transparant

   Tidak dapat menyimpan informasi VLAN pada NVRAM. Hanya dapat meneruskan info VLAN yang diterima dari VTP Server ke VTP Client

3.6. Konfirgurasi VTP

Langkah dalam menyiapkan konfirgurasi VTP:

Gambar 3.3 Rancangan VTP

```
Switch(config)#vlan 10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#vlan 30
Switch(config-vlan)#interface fastEthernet 0/1
Switch(config-if)#switchport mode trunk
```

Pada gambar tersebut dijelaskan bahwa terdapat 2 buat Switch dimana terbagi atas VTP Server dan VTP Client.Terdaftar 3 nama VLAN diantaranya VLAN 10,20 dan 30 yang diterapkan pada port interface fastEthernet 0/1 dengan mode akses mode trunk karena membawa lebih dari satu VLAN.

```
Switch(config)#vtp domain CCNA
Changing VTP domain name from NULL to CCNA
Switch(config)#vtp mode server
Device mode already VTP SERVER.
Switch(config)#vtp password cisco
Setting device VLAN database password to cisco
```

Pada script tersebut diterapkan pada switch server menentukan nama domain dengan nama CCNA dan menjadikan switch tersebut sebagai switch server dengan password “cisco”.

```
Switch(config)#vtp domain CCNA
Domain name already set to CCNA.
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#vtp password cisco
Setting device VLAN database password to cisco
```

Pada script tersebut diterapkan pada switch Client menentukan nama domain dengan nama CCNA dan menjadikan switch tersebut sebagai switch Client dengan password “cisco”.

Switch# Show vlan brief

Digunakan untuk memverifikasi VLAN yang sudah terdaftar pada setiap Switch Client dan Server.

3.7. Extended VLAN

Memungkinkan para service 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.

1. VLAN Normal memiliki range ID antara 1 sampai 1005
2. VLAN Extended memiliki range ID antara 1006 sampai 4096
3. VTP tidak dapat dijalankan pada VLAN Extended

VLAN Range	Range	Usage	Popagated via VTP?
0, 4095	Reserved	For system use only. You cannot see or use these.	n/a
1	Normal	Cisco default. You can use this VLAN, but you cannot delete it.	Yes
2 – 1001	Normal	For Ethernet VLANs. You can create, use, and delete these.	Yes
1002 – 1005	Normal	Cisco defaults for FDDI and Token Ring. You cannot delete these.	Yes
1006 – 1024	Reserved	For system use only. You cannot see or use these.	n/a
1025 - 4094	Reserved	For Ethernet VLANs only.	VTP v 3 only. Not supported in VTP v1 or v2. Requires VTP transparent mode for configuration.

Gambar 3.4 Penentuan angka VLAN

3.8. Dynamic Trunking Protocol (DTP)

Dynamic Trunking Protocol (DTP) adalah protokol berpemilik Cisco yang diaktifkan secara otomatis pada switch Catalyst 2960 dan Catalyst 3560 Series. Switch dari vendor lain tidak mendukung DTP. DTP mengelola negosiasi batang hanya jika port pada switch tetangga dikonfigurasi dalam mode bagasi yang mendukung DTP, DTP dapat mengelola negosiasi dari trunk. Untuk mengaktifkan trunking pada switch cisco yang tidak mendukung DTP, dapat menggunakan perintah switchport mode trunk dan switchport nonegotiate pada interface yang akan digunakan.

Switchport nonegotiate Mencegah Interface menghasilkan frame DTP. Anda bisa menggunakan perintah ini hanya bila mode interface switchport adalah access atau trunk. Anda harus secara manual mengkonfigurasi antarmuka tetangga sebagai antarmuka bagasi untuk membuat link trunk.

Mode switchport dinamis yang diinginkan Membuat interface secara aktif mencoba mengubah link ke trunk link. Antarmuka menjadi antarmuka bagasi jika antarmuka tetangga diatur ke mode otomatis, diinginkan, atau dinamis. Ini adalah mode switchport default pada switch yang lebih tua, seperti switch Catalyst 2950 dan 3550 Series.

3.9. Troubleshoot VTP dan DTP

Terdapat 4 masalah umum terhadap VTP:

1. Versi VTP tidak kompatibel
2. Masalah Sandi/Password pada VTP
3. Nama VTP Domain salah/tidak sama

4. Semua Switch tersetting ke Mode Client

Sedangkan, ada tiga masalah umum dengan DTP terkait dengan mode trunk:

1. Ketidaksesuaian mode trunk
2. Allowed VLAN pada trunk
3. Ketidaksesuaian Native VLAN

3.10. Perbandingan VLAN Layer 2 dan Layer 3

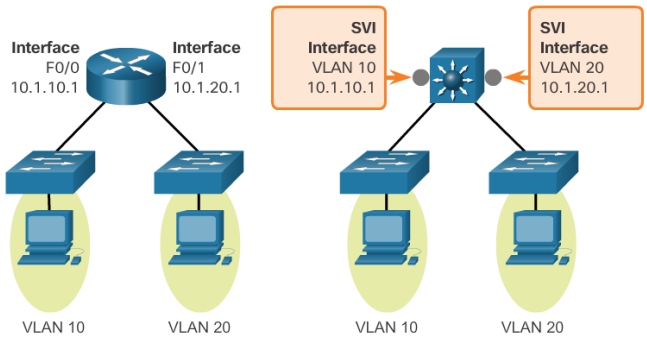
1. Layer 2 Switching

   Switch layer 2 tidak dapat meneruskan paket data yang menghubungkan antara 2 buah VLAN berbeda.

2. Layer 3 Switching
   a. Switch Layer 3 dapat meneruskan paket data dari VLAN yang berbeda
   b. Jaringan perusahaan modern menggunakan switch multilayer untuk mencapai pengolahan paket yang tinggi

3.11. Inter-VLAN Routing

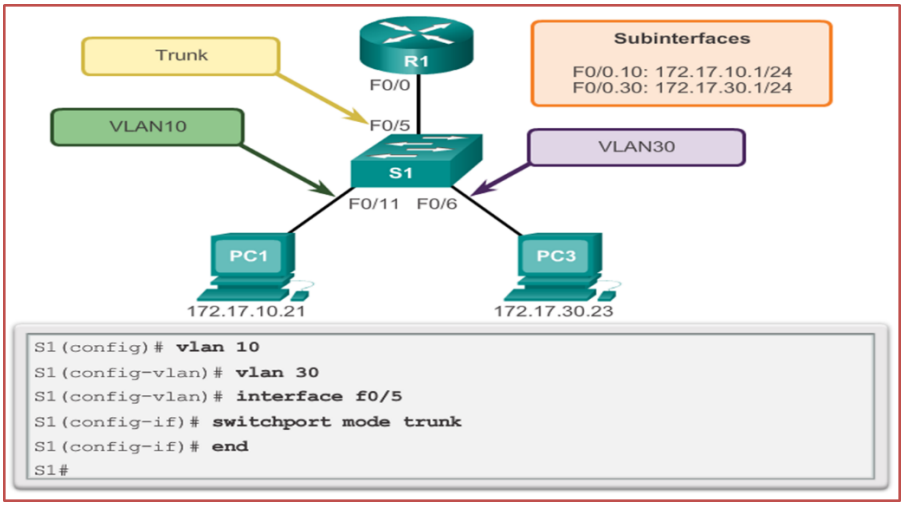
Routing dapat ditransfer ke lapisan core dan distribution (dan kadang-kadang bahkan lapisan akses) tanpa mempengaruhi kinerja jaringan.



Gambar 3.5 Model Inter-VLAN

Inter-VLAN memungkinkan sebuah network dapat melakukan akses pada network tersebut tanpa ada pembatasan sebuah segment vlan yang nantinya VLAN 10 dapat terhubung dengan VLAN 20 dengan menentukan jalur perioritas yaitu dengan mengutamakan akses ke VLAN yang sama terlebih dahulu.

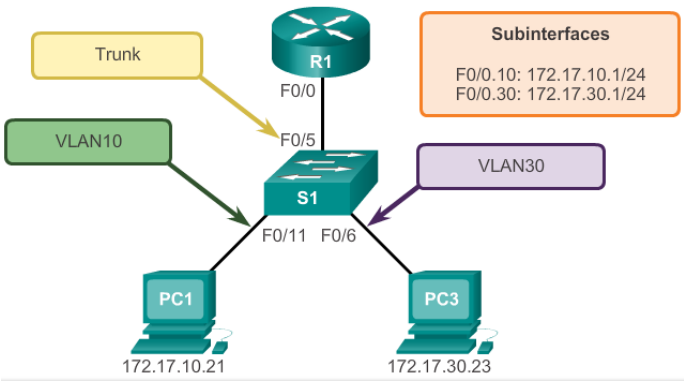
1. Konfigurasi Inter-VLAN Routing Router On a Stick



Gambar 3.6 Konsep Inter VLAN router on a Stik

Pada skema tersebut dijelaskan untuk akses Switch S1 hanya menggunakan 1 akses port dengan FA0/5 dan dengan Roter R1 pada port F0/0 sehingga dengan pola tersebut maka disebut dengan Konfigurasi Inter-VLAN Routing Router On a Stick dan pada Port Fa0/5 Switch S1 memakai mode Trunk dikarenakan agar dua buah VLAN dapat mengakses sebuah router yaitu VLAN 10 dan VLAN 20.

a. Konfigurasi Inter-VLAN Routing Router On a Stick



Gambar 3.7 Skema Inter VLAN Router On a Stick

Pada skema tersebut dijelakan bahwa ada 2 penamaan VLAN yaitu VLAN 10 dan VLAN 30 dalam pembagiannya terdapat 2 buah client dengan network 172.17.10.0 terdaftar dengan nama VLAN 10 dan network 172.17.30.0 terdaftar dengan nama VLAN 30 sehingga semua konfirgurasi penamaan VLAN dilakukan pada Switch S1 dengan mendaftarkan Vlan 10 pada port F0/1 dan VLAN 30 pada Port F0/6 dengan mode akses karena hanya dapat dilewati oleh 1 VLAN sedangkan unutk dapat mengakses Router dari Switch S1 didaftarkan

pada port F0/5 Switch S1 dengan mode trunk karena membawa dua buah VLAN yaitu VLAN 10 dan VLAN 30

```
R1(config)# interface g0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# interface g0/0.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0
R1(config)# interface g0/0
R1(config-if)# no shutdown
```

Gambar 3.8 Konfigurasi Inter-VLAN Routing Router On a Stick

Pada konfirgurasi terdapat subinterface yang merupakan pembagian dari sebuah interface artinya satu interface port dibagi menjadi beberapa IP address dengan penulisan interface g0/0.10 berarti masuk kedalam sub interfacenya g0/0 router dengan penamaan dotIq 10.

Sedangkan pada interface g0/0.30 berarati kita masih menggunakan port yang sama yaitu port g0/0 yang terdapat 2 buat IP address dengan subnetwork .10 dan .30.

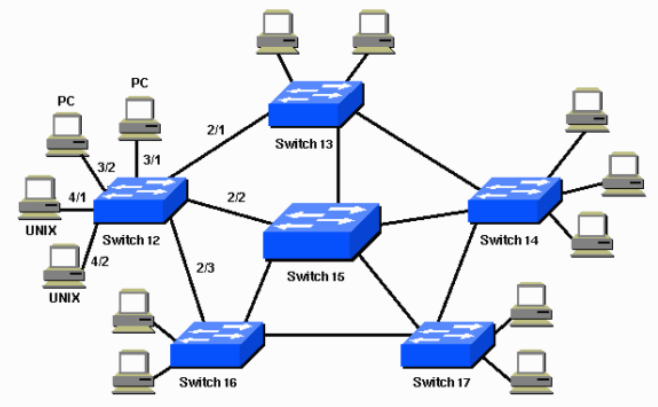
BAB IV
SPANNING TREE PROTOCOL

4.1. Pengertian STP

Spanning Tree Protocol (STP) adalah protokol Layer 2 yang berjalan pada bridge dan switch. Spesifikasi untuk STP adalah IEEE 802.1D. Tujuan utama STP adalah untuk memastikan bahwa Anda tidak membuat loop ketika Anda memiliki jalur redundan di jaringan Anda. Loop mematikan ke jaringan.

Konfigurasi dalam dokumen ini berlaku untuk Catalyst 2926G, 2948G, 2980G, 4500/4000, 5500/5000, dan 6500/6000 Switch yang menjalankan Catalyst OS (CatOS). Lihat dokumen-dokumen ini untuk informasi tentang konfigurasi STP pada platform sakelar lain:

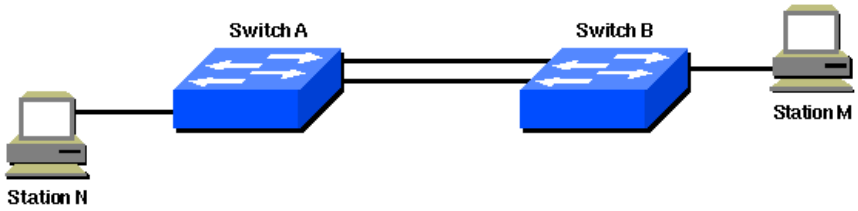
1. Mengkonfigurasi STP dan IEEE 802.1s MST (Catalyst 6500/6000 Switches yang menjalankan Perangkat Lunak Cisco IOS®)
2. Memahami dan Mengkonfigurasi STP (Catalyst 4500/4000 Switch yang menjalankan Perangkat Lunak Cisco IOS)
3. Mengkonfigurasi bagian STP dari Mengkonfigurasi Sistem (Switch Catalyst 2900XL / 3500XL)
4. Mengkonfigurasi STP (Catalyst 3550 Switches)
5. Mengkonfigurasi STP (Catalyst 2950 Switches)



Gambar 4.1 Konsep Spanning Tree Protocol (STP)

STP berjalan pada jembatan dan sakelar yang kompatibel dengan 802.1D. Ada rasa STP yang berbeda, tetapi 802.1D adalah yang paling populer dan diimplementasikan secara

luas. Anda menerapkan STP pada jembatan dan sakelar untuk mencegah loop dalam jaringan. Gunakan STP dalam situasi di mana Anda ingin tautan yang berlebihan, tetapi bukan loop. Tautan redundan sama pentingnya dengan cadangan jika terjadi kegagalan pada jaringan. Kegagalan utama Anda mengaktifkan tautan cadangan sehingga pengguna dapat terus menggunakan jaringan. Tanpa STP pada jembatan dan sakelar, kegagalan seperti itu dapat mengakibatkan loop. Jika dua sakelar yang terhubung menjalankan rasa STP yang berbeda, mereka memerlukan pengaturan waktu yang berbeda untuk menyatu. Ketika berbagai rasa digunakan di sakelar, itu menciptakan masalah waktu antara status Blocking dan Forwarding. Karena itu, disarankan untuk menggunakan rasa STP yang sama. Pertimbangkan jaringan ini:

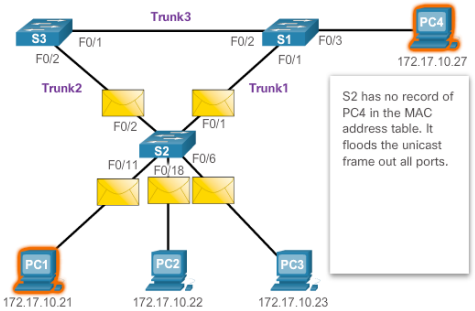


Gambar 4.2 Hubungan 2 Switch

Di jaringan ini, tautan redundan direncanakan antara Switch A dan Switch B. Namun, pengaturan ini menciptakan kemungkinan bridging loop. Sebagai contoh, paket broadcast atau multicast yang mentransmisikan dari Station M dan diperuntukkan untuk Station N hanya terus beredar di antara kedua switch.

Protokol jaringan yang menjamin topologi jaringan bebas melakukan perulangan untuk penghubung Ethernet LAN, STP mempunyai standart IEEE 802.1D, STP aktif secara default pada setiap switch cisco. STP memblok port-port yang dapat menyebabkan broadcast storm.

STP juga dapat memastikan hanya ada satu jalur yang digunakan untuk melakukan transfer paket, dan memblok jalur yang dapat menyebabkan looping saat melakukan transfer paket



Gambar 4.3 Pengirian Data SPT

PC 1 mengirimkan paket ke PC 4. Namun, PC 4 tidak terdapat dalam Tabel MAC Address dari S2. Maka, S2 akan melakukan broadcast ke semua port yang terhubung sampai menemukan posisi PC4

4.2. Jenis-Jenis STP

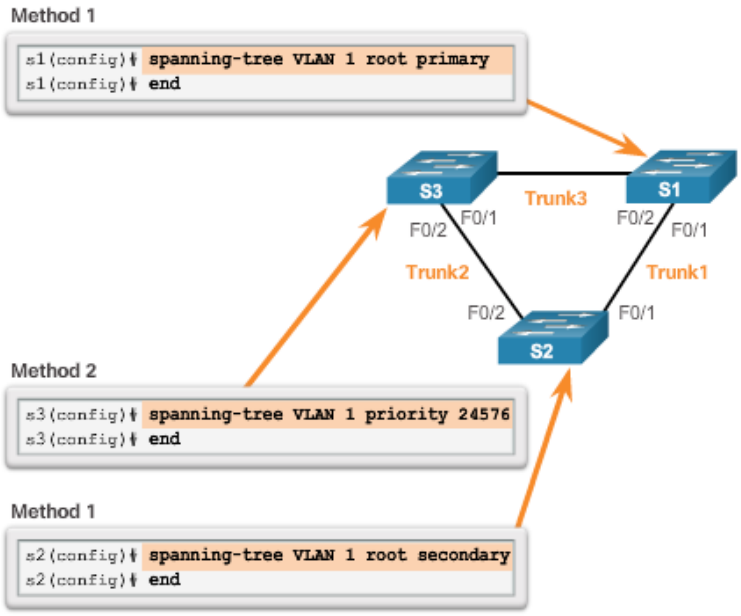
1. Open Standard

   STP (802.1D), Rapid STP (802.1W), Multiple Spanning Tree MST (802.1S)
2. Cisco Proprietary

   PVST (Per Vlan Spanning Tree), PVST+, Rapid PVST.

4.3. PVST+

Cisco PVST+ dikembangkan untuk menjalankan sebuah jalur yang independen dari IEEE 802.1D untuk setiap VLAN dalam jaringan, STP dan PVST+ menggunakan lima port state yang terdiri dari Blockir, Listening, Learning, Forwading dan Disabled.



Gambar 4.4 Konfirgurasi PSVT +

1. Metode Pertama

   Menggunakan vlan spanning-tree vlan-id root primary dan yang pertama yang akan dilalui.
2. Metode Kedua

   Menggunakan vlan spanning-tree vlan-id prioritas value sama dengan primary untuk mengutamakan akses kejalur tersebut.

4.4. PortFast dan BPDU Guard

Menggunakan perintah spanning-tree portfast untuk mengaktifkan PortFast pada port switch. Menggunakan perintah spanning-tree bpduguard enable untuk mengaktifkan BPDU guard pada port akses Layer 2.

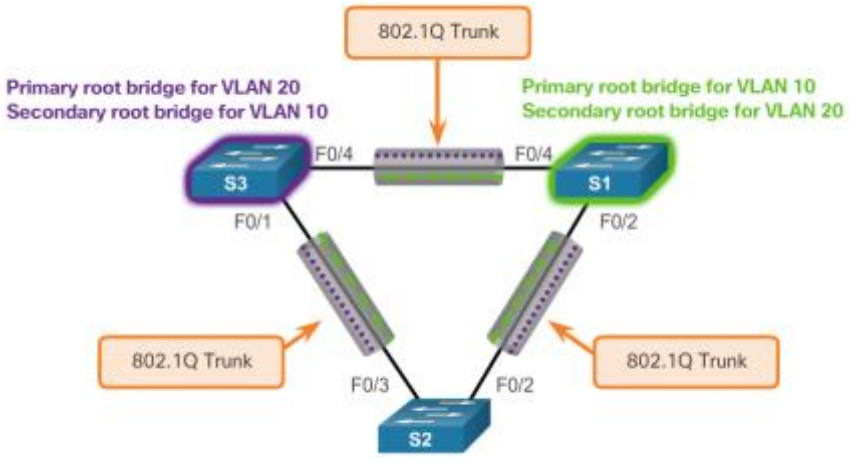
```
S2(config)# interface FastEthernet 0/11
S2(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to
a single host. Connecting hubs, concentrators, switches,
bridges, etc... to this interface  when portfast is enabled,
can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on FastEthernet0/11 but will only
 have effect when the interface is in a non-trunking mode.
S2(config-if)# spanning-tree bpduguard enable
S2(config-if)# end
```

Gambar 4.5 Konfirgurasi PortFast dan BPDU Guard

4.5. PVST dan Load Balancing

Dengan menggunakan mode PVST, dapat meminimalis terjadinya collision data saat pengiriman paket, Load Balancing dilakukan untuk melakukan backup jaringan dengan mempertimbangkan skala prioritasnya.

Tujuan dari PVST+ Load Balancing adalah untuk mengkonfigurasi dua ataupun lebih root bridges VLAN yang berbeda dengan menggunakan redundant link.



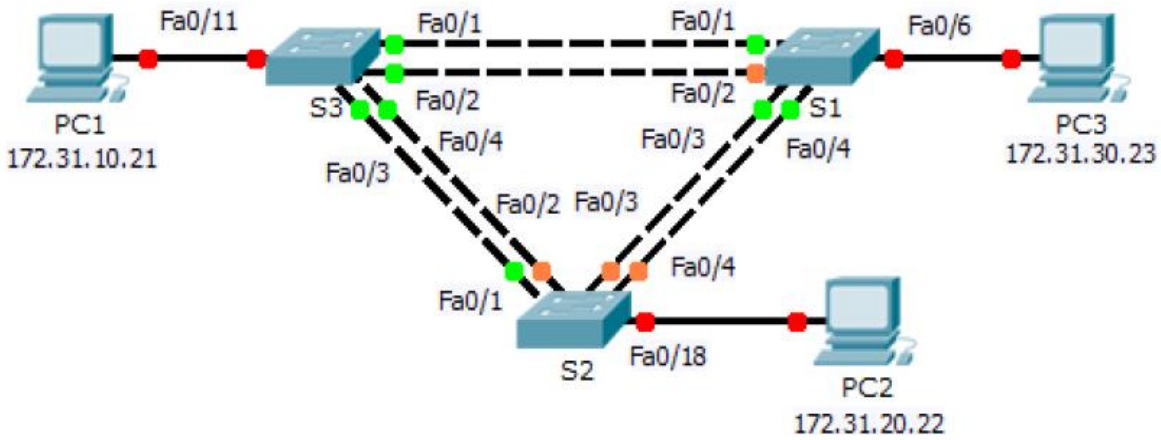
Gambar 4.6 PVST dan Load Balancing

```
S3(config)# spanning-tree vlan 20 root primary
S3(config)# spanning-tree vlan 10 root secondary
S3(config)#
```

```
S1(config)# spanning-tree vlan 10 root primary
S1(config)# spanning-tree vlan 20 root secondary
S1(config)#
```

S3 memberikan akses utama (prioritas) terhadap VLAN 20, Sedangkan, S1 memberikan akses utama (prioritas) terhadap VLAN 10

4.6. Skema dan Konfirgurasi PVST +



Gambar 4.7 Konfirgurasi PVST +

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.31.99.1	255.255.255.0	N/A
S2	VLAN 99	172.31.99.2	255.255.255.0	N/A
S3	VLAN 99	172.31.99.3	255.255.255.0	N/A
PC1	NIC	172.31.10.21	255.255.255.0	172.31.10.254
PC2	NIC	172.31.20.22	255.255.255.0	172.31.20.254
PC3	NIC	172.31.30.23	255.255.255.0	172.31.30.254

Gambar 4.8 Daftar IP

Switch Port Assignment Specifications

Ports	Assignments	Network
S1 F0/6	VLAN 30	172.17.30.0/24
S2 F0/18	VLAN 20	172.17.20.0/24
S3 F0/11	VLAN 10	172.17.10.0/24

Gambar 4.9 Akses VLAN

1. Memasuskan semua database VLAN pada semua Switch

```
S1(config)# vlan 10
S1(config-vlan)# vlan 20
S1(config-vlan)# vlan 30
S1(config-vlan)# vlan 40
S1(config-vlan)# vlan 50
S1(config-vlan)# vlan 60
S1(config-vlan)# vlan 70
S1(config-vlan)# vlan 80
S1(config-vlan)# vlan 99
```

2. Mengaktifkan mode access pada S1, S2, dan S3, dan mendaftarkan access vlan-vlan yang telah ditentukan

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 30
S1(config-if)# no shutdown

S2(config)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if)# no shutdown

S3(config)# interface f0/11
S3(config-if)# switchport mode access
S3(config-if)# switchport access vlan 10
S3(config-if)# no shutdown
```

3. Mengaktifkan mode trunk native VLAN 99 pada S1, S2, dan S3

```
S1(config)# interface range f0/1-4
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport trunk native vlan 99

S2(config)# interface range f0/1-4
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# switchport trunk native vlan 99

S3(config)# interface range f0/1-4
S3(config-if-range)# switchport mode trunk
S3(config-if-range)# switchport trunk native vlan 99
```

4. Berikanlah IP Address terhadap VLAN 99 pada S1, S2 dan S3

```
S1(config)# interface vlan99
S1(config-if)# ip address 172.31.99.1 255.255.255.0
S2(config)# interface vlan99
S2(config-if)# ip address 172.31.99.2 255.255.255.0
S3(config)# interface vlan99
S3(config-if)# ip address 172.31.99.3 255.255.255.0
```

5. Konfigurasikanlah STP dan PVST+ Load Balancing. S1 prioritas VLAN 1, 10, 30, 50 dan 70. S2 secondary untuk semua VLAN. Sedangkan, S3 prioritas VLAN 20, 40, 60, 80 dan 99

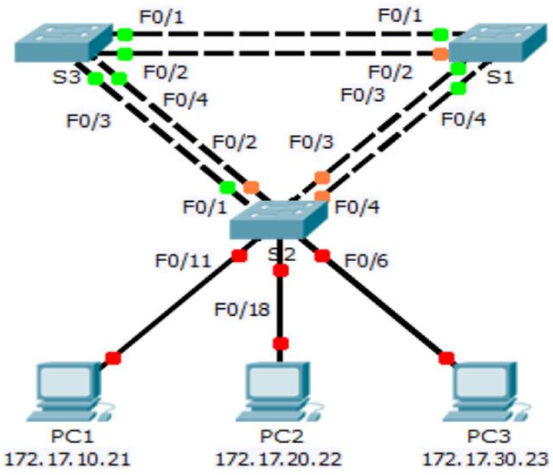
```
S1(config)# spanning-tree mode pvst
S1(config)# spanning-tree vlan 1,10,30,50,70 root primary

S2(config)# spanning-tree mode pvst
S2(config)# spanning-tree vlan 1,10,20,30,40,50,60,70,80,99 root secondary

S3(config)# spanning-tree mode pvst
S3(config)# spanning-tree vlan 20,40,60,80,99 root primary
```

6. Konfigurasikanlah Portfast dan BPDU Guard

```
S1(config)# interface f0/6
S1(config-if)# spanning-tree portfast
S1(config-if)# spanning-tree bpduguard enable

S2(config)# interface f0/18
S2(config-if)# spanning-tree portfast
S2(config-if)# spanning-tree bpduguard enable

S3(config)# interface f0/11
S3(config-if)# spanning-tree portfast
S3(config-if)# spanning-tree bpduguard enable
```

BAB V
STUDI KASUS

5.1. Perancangan Skema



Gambar 5.1 Perancangan Skema Rapid PSVT +

Pada skema tersebut buatlah sebuah Rapid PVST+ atau RPVST+, yang merupakan gabungan dari materi BAB 3 dan BAB 4 menggunakan VLAN dan Spanning Tree.

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	N/A
S2	VLAN 99	172.17.99.12	255.255.255.0	N/A
S3	VLAN 99	172.17.99.13	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.254
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.254
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.254

Gambar 5.2 IP address

Switch Port Assignment Specifications

Ports	Assignments	Network
S2 F0/6	VLAN 30	172.17.30.0/24
S2 F0/18	VLAN 20	172.17.20.0/24
S2 F0/11	VLAN 10	172.17.10.0/24

Gambar 5.3 Pembagian VLAN

Dalam aktivitas ini, akan mengonfigurasi VLAN dan trunk, Rapid Spanning Tree PVST +, jembatan root primer dan sekunder, dan memeriksa hasil konfigurasi. Anda juga akan mengoptimalkan jaringan dengan mengkonfigurasi PortFast, dan BPDU Guard pada port .

5.2. Confirgurasi VLAN

1. Aktifkan port pengguna pada S2 dalam mode akses

   Lihat diagram topologi untuk menentukan port switch mana pada S2 yang diaktifkan untuk akses perangkat pengguna akhir. Ketiga port ini akan dikonfigurasikan untuk mode akses dan diaktifkan dengan perintah no shutdown

```
S2(config)# interface range f0/6,f0/11,f0/18
S2(config-if-range)# switchport mode access
S2(config-fi-range)# no shutdown
```

2. Menggunakan perintah yang sesuai, buat VLAN 10, 20, 30, 40, 50, 60, 70, 80, dan 99 di semua Switch

```
S1(config)# vlan 10
S1(config-vlan)# vlan 20
S1(config-vlan)# vlan 30
S1(config-vlan)# vlan 40
S1(config-vlan)# vlan 50
S1(config-vlan)# vlan 60
S1(config-vlan)# vlan 70
S1(config-vlan)# vlan 80
S1(config-vlan)# vlan 99
```

```
S2(config)# vlan 10
S2(config-vlan)# vlan 20
S2(config-vlan)# vlan 30
S2(config-vlan)# vlan 40
S2(config-vlan)# vlan 50
S2(config-vlan)# vlan 60
S2(config-vlan)# vlan 70
S2(config-vlan)# vlan 80
S2(config-vlan)# vlan 99

S3(config)# vlan 10
S3(config-vlan)# vlan 20
S3(config-vlan)# vlan 30
S3(config-vlan)# vlan 40
S3(config-vlan)# vlan 50
S3(config-vlan)# vlan 60
S3(config-vlan)# vlan 70
S3(config-vlan)# vlan 80
S3(config-vlan)# vlan 99
```

3. Tetapkan VLAN untuk Melihat port.

   Penugasan port tercantum dalam tabel di awal aktivitas. Simpan konfigurasi Anda setelah menetapkan port switch ke VLAN.

```
S2(config)# interface f0/6
S2(config-if)# switchport access vlan 30
S2(config-if)# interface f0/11
S2(config-if)# switchport access vlan 10
S2(config-if)# interface f0/18
S2(config-if)# switchport access vlan 20
```

4. Verifikasi VLAN

   Gunakan perintah show vlan brief pada semua switch untuk memverifikasi bahwa semua VLAN terdaftar dalam tabel VLAN

5. Tetapkan Trunk ke VLAN Native 99.

   Gunakan perintah yang sesuai untuk mengkonfigurasi port F0 / 1 hingga F0 / 4 pada setiap switch sebagai port trunk dan tetapkan port trunk ini ke VLAN 99 asli.

```
S1(config)# interface range f0/1-4
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport trunk native vlan 99

S2(config)# interface range f0/1-4
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# switchport trunk native vlan 99

S3(config)# interface range f0/1-4
S3(config-if-range)# switchport mode trunk
S3(config-if-range)# switchport trunk native vlan 99
```

6. Konfigurasikan Interface manajemen pada ketiga switch dengan IP Address

```
S1(config)# interface vlan99
S1(config-if)# ip address 172.17.99.11 255.255.255.0

S2(config)# interface vlan99
S2(config-if)# ip address 172.17.99.12 255.255.255.0

S3(config)# interface vlan99
S3(config-if)# ip address 172.17.99.13 255.255.255.0
```

5.3. Konfigurasi Rapid Spanning Tree PVST + Load Balancing

Rapid Spanning Tree Protocol (RSTP; IEEE 802.1w) dapat dilihat sebagai evolusi dari standar 802.1D. Terminologi 802.1D terutama tetap sama. Sebagian besar parameter tidak berubah sehingga pengguna yang terbiasa dengan 802.1D dapat dengan cepat mengkonfigurasi protokol baru dengan nyaman. Dalam kebanyakan kasus, RSTP berkinerja lebih baik daripada ekstensi milik Cisco tanpa konfigurasi tambahan. 802.1w juga dapat kembali ke 802.1D untuk dapat beroperasi dengan jembatan lawas berdasarkan basis per-dasar

1. Configure STP mode

   Gunakan perintah mode spanning-tree untuk mengkonfigurasi Switch menggunakan PVST sebagai mode STP

```
S1(config)# spanning-tree mode rapid-pvst
S2(config)# spanning-tree mode rapid-pvst
S3(config)# spanning-tree mode rapid-pvst
```

2. Configure Rapid Spanning Tree PVST+ load balancing

   Konfigurasikan S1 untuk menjadi root utama untuk VLAN 1, 10, 30, 50, dan 70. Konfigurasikan S3 menjadi root utama untuk VLAN 20, 40, 60, 80, dan 99. Konfigurasikan S2 menjadi root sekunder untuk semua VLAN

```
S1(config)# spanning-tree vlan 1,10,30,50,70 root primary
S2(config)# spanning-tree vlan 1,10,20,30,40,50,60,70,80,99 root secondary
S3(config)# spanning-tree vlan 20,40,60,80,99 root primary
```

5.4. Configure PortFast and BPDU Guard

1. Configuring PortFast on S2

   PortFast menyebabkan sebuah port untuk memasuki kondisi penerusan segera dengan secara dramatis mengurangi waktu status mendengarkan dan belajar. PortFast meminimalkan waktu yang diperlukan server atau workstation untuk online. Konfigurasikan PortFast pada antarmuka S2 yang terhubung ke PC.

```
S2(config)# interface range f0/6 , f0/11 , f0/18
S2(config-if-range)# spanning-tree portfast
```

2. Configuring BPDU Guard on S2

   Peningkatan STP PortFast BPDU Guard memungkinkan perancang jaringan untuk menegakkan batas domain STP dan menjaga topologi aktif dapat diprediksi. Perangkat di belakang port yang mengaktifkan STP PortFast tidak dapat memengaruhi topologi STP. Pada penerimaan BPDU, operasi BPDU Guard menonaktifkan port yang telah dikonfigurasikan PortFast. BPDU Guard mentransisikan port ke status err-disable, dan sebuah pesan muncul di konsol. Konfigurasikan BPDU Guard pada antarmuka S2 yang terhubung ke PC

```
S2(config)# interface range f0/6 , f0/11 , f0/18
S2(config-if-range)# spanning-tree bpduguard enable
```

BAB VI
ETHERCHANNEL DAN HSRP

6.1. Pengertian EtherChannel

EtherChannel adalah teknik untuk menggabungkan dua atau lebih Interface fisik Fast Ethernet atau Gigabit Ethernet untuk membuat satu tautan ethernet logis dalam rangka meningkatkan kemampuan bandwidth dan menciptakan ketahanan dan kapasitas link. EtherChannel juga dapat diartikan sebagai suatu teknologi trunking yang digunakan oleh switch C10 Konfrensi Nasional Teknologi Informasi dan Aplikasinya Palembang, 13 September 2014 Cisco catalyst untuk menggabungkan beberapa physical port menjadi satu jalur logika dalam satu buah port group, dan jika salah satu port atau jalur rusak maka port group akan tetap bekerja menggunakan jalur atau port yang lain (Amin, 2014).

6.2. Fungsi EtherChannel

EtherChannel memiliki beberapa fungsi dalam jaringan komputer yang dapat mempermudah network administrator dalam mengelola jaringan, anara lain :

1. Membuat link cadangan apabila terjadi disconnected yang diakibatkan oleh putusnya kabel (link) yang menghubungkan host ke host yang lain.
2. Menggabungkan kecepatan pengiriman data dengan cara menggabungkan beberapa fisik port sampai dengan 800 Mbps untuk fastethernet dan 8 Gb untuk gigabyte ethernet.
3. Dengan menggabungkan beberapa port ethernet maka etherchannel dapat digunakan sebagai load balancing.

6.3. Jenis EtherChannel

Dalam penggunaannya etherchannel memiliki dua jenis jenis yang berbeda yang masing masing jenis memiliki fungsi yang berbeda yaitu :

1. Port Aggregation Protocol (PAgP)

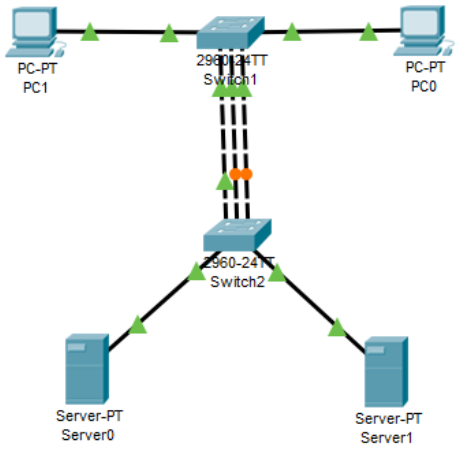
   Protocol proprietary Cisco, digunakan untuk membuat EtherChannel otomatis. Ketika PAgP di set, PAgP packet akan dikirim ke media dan mendeteksi konfigurasi dikedua belah pihak (typically switch) dan memastikan bahwa kedua belah pihak port (FastEthernet atau yg lain) kompatible untuk di jadikan EtherChannel jika dibutuhkan. PAgP packet dikirim tiap 30 detik.

2. Link Aggregation Control Protocol (LACP)

   merupakan protokol yang digunakan untuk melakukan negosiasi pembentukan EtherChannel dengan switch non-Channel.

6.4. Konfigurasi EtherChannel

Untuk membuat etherchannel LACP dan PAGP buatlah topologi dibawah ini :



Gambar 6.1 Topologi EtherChannel

6.4.1. Konfigurasi PAgP

Dengan menggunakan topologi diatas lakukan beberapa langkah langkah berikut ini. Pertama Untuk modenya kita gunakan mode **"desirable".**Serta konfigurasi port-channel 1 menjadi mode trunk. Konfigurasi pada switch 1 sebagai berikut.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int range fa0/1-3
Switch(config-if-range)#channel-group 1 mode desirable
Switch(config-if-range)#exit
Switch(config)#int port-channel 1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

Langkah yang sama juda diterapkan untuk switch 2

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int range fa0/1-3
Switch(config-if-range)#channel-group 1 mode desirable
Switch(config-if-range)#exit
Switch(config)#int port-channel 1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

protokolnya menjadi PaGP seperti berikut.

```
Ports in the Port-channel:

Index   Load   Port     EC state      No of bits
------+------+------+------------------+-----------
  0     00     Fa0/1    Desirable-Sl     0
  0     00     Fa0/2    Desirable-Sl     0
  0     00     Fa0/3    Desirable-Sl     0
Time since last port bundled:  00d:00h:01m:04s    Fa0/3
Switch#
```

Gambar 6.2 Cek Port EtherChanel PAgP

6.4.2. Konfigurasi LACP

Pada switch 1 lakukan konfigurasi untuk mengaktifkan EtherChannel dengan menggabungkan port ethernet 1 sampai 3 seperti dibawah ini. Kemudian aktifkan mode trunk pada port tersebut.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int range fa0/1-3
Switch(config-if-range)#channel-group 1 mode active
Switch(config-if-range)#ex
Switch(config)#int port-channel 1
Switch(config-if)#switchport mode trunk
Switch(config-if)#ex
Switch(config)#
```

lakukan hal sama pada switch 2 dan pilih port mana yang akan digabungkan. Port yang dipilih tidak harus sama dengan port pada switch 1.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int range fa0/1-3
Switch(config-if-range)#channel-group 1 mode active
Switch(config-if-range)#ex
Switch(config)#int port-channel 1
Switch(config-if)#switchport mode trunk
Switch(config-if)#ex
Switch(config)#
```

Kemudian cek port-channelnya dengan perintah “show etherchannel port-channel” maka setiap interfacenya akan berubah menjadi type active, dan protokolnya akan menjadi LACP.

```
Ports in the Port-channel:

Index   Load   Port     EC state      No of bits
------+------+--------+-----------+----------
  0     00     Fa0/3    Active         0
  0     00     Fa0/1    Active         0
  0     00     Fa0/2    Active         0
Time since last port bundled:  00d:00h:04m:06s    Fa0/2
Switch#
Switch#
Switch#
Switch#
```

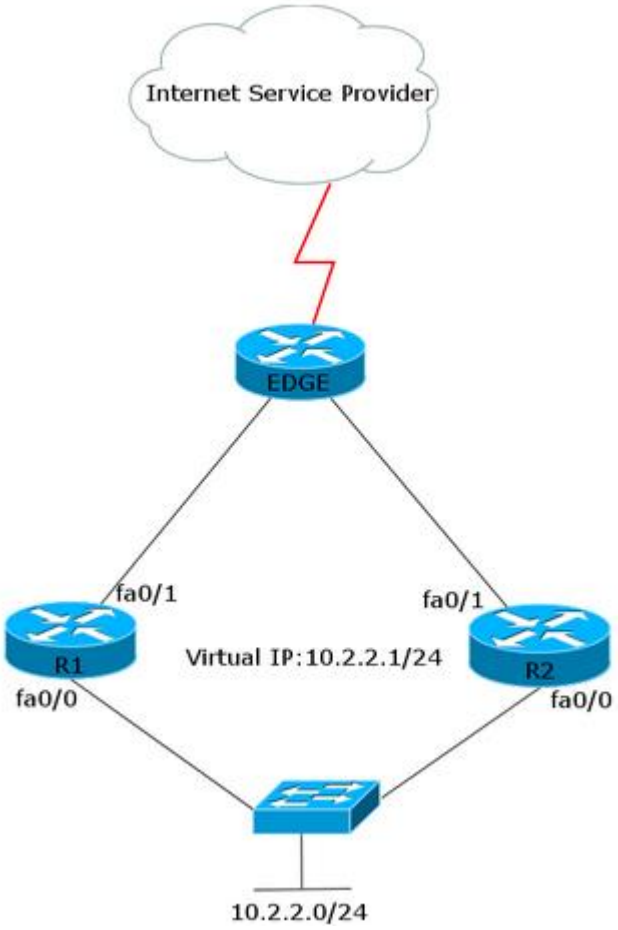
Gambar 6.3 Cek Port EtherChanel LACP

6.5. First Hop Redundancy Protocol (FHRP)

First Hop Redundancy Protocol adalah layanan Internet dengan availability dan reliability yang tinggi, pada jaringan dapat digunakan lebih dari satu gateway atau redundansi. Sehingga bila terjadi down pada salah satu gateway, gateway yang lain dapat mengambil tugas dari gateway yang down tadi. Penggunaan lebih dari satu gateway ini dapat dimanfaatkan pada jaringan lapisan core, distribution, dan access. Pada lapisan core dan distribution dapat dimanfaatkan protokol routing untuk redundansinya. Pada lapisan akses, penggunaan lebih dari satu gateway(Naqvi, Hertiana, & Negara, 2015).

First Hop Redundancy Protocol (FHRP) adalah kumpulan protokol yang bisa digunakan untuk membuat router yang ada dalam jaringan LAN akan mengambil alih secara otomatis jika router utama yang digunakan sebagai gateway gagal bekerja (Dzulfiqar Anwar, Vidya Yovita, & Mayas ari, 2015).

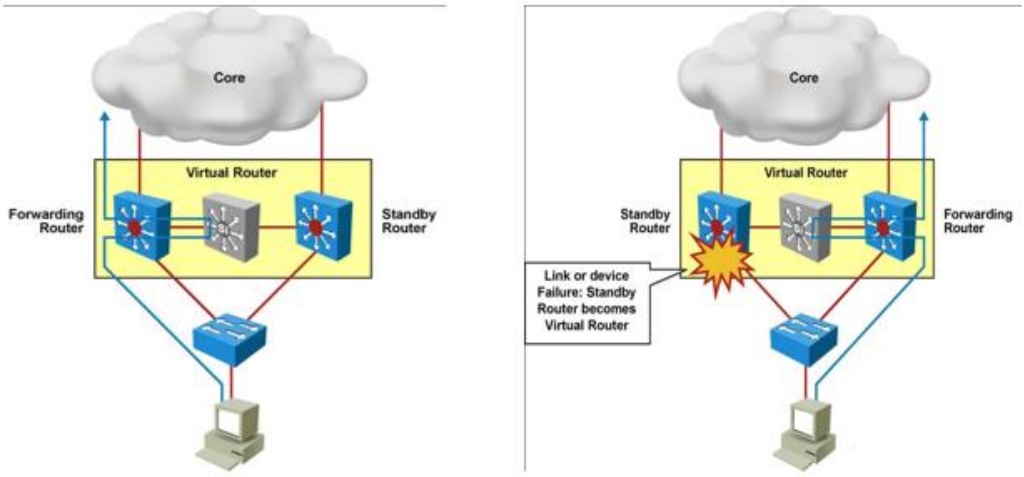
First-hop redundancy merupakan sebuah mekanisme untuk menjadikan salah satu router sebagai default gateway saat terdapat dua atau lebih gateway pada jaringan yang menggunakan teknologi layer 2 seperti Ethernet, yang biasanya dijadikan mekanisme network redundancy di distribution network dan access network, dan diaplikasikan di data-center network maupun kampus network. Selain itu jika terjadi down pada router maupun link yang menuju ke gateway tersebut, gateway dapat dialihkan ke gateway lainnya. Protokol ini tidak menambahkan kemampuan routing. Terdapat beberapa protokol first-hop redundancy yang digunakan pada jaringan saat ini: Proxy Address Resolution Protocol dan Virtual Router Redundancy Protcol dibuat oleh Internet Engineering Task Force; Hot Standby Router Protocol dan Gateway Load Balancing Protocol yang dipatenkan Cisco; Common Address Router Protocol yang merupakan bagian dari Berkeley Software Distribution.



Gambar 6.4 Topologi First Hop Redundancy Protocol

6.6. Hot Standby Router Protocol (HSRP)

HSRP (Hot Standby Router Protocol) merupakan teknologi yang akan digunakan dalam menangani permasalahan yang ada di perusahan saat ini dimana akan ada satu jalur backup apabila terjadi gangguan pada perangkat dan juga adanya pembagian beban sehingga kinerja jaringan tidak terlalu berat (Li & Hu, 2010). HSRP juga merupakan protokol redundancy standar Cisco yang menetapkan sebuah standby router dan active router yang saling mengirimkan paket hello setiap 3s dan secara otomatis standby router dapat mengambil alih tugas active router yang mengalami gagal link (Amanda Yudiani, Munadi, & Vidya Yovita, 2013).

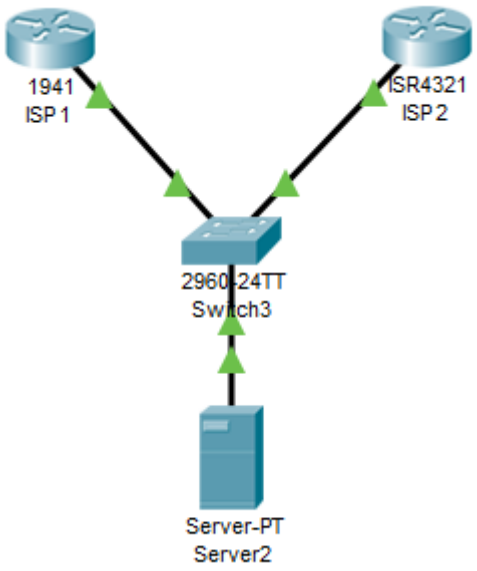


Gambar 6.5 Hot Standby Router Protocol

Ketika router master mengalami kegagalan, maka router standby akan membackup dan beralih fungsi menjadi router master (active).

6.7. Konfigurasi Hot Standby Router Protocol

Buatlah topologi dibaw ini dengan menggunakan packet tracer. Topologi yang dibuat menggunakan dua router untuk masing masing ISP. Salah satu isp akan kita buat prioritas utama untuk jalur pengiriman data dan router lainnya menjadi jalur cadangan ketika jalur putus.



Gambar 6.6 topologi Hot Standby Router Protocol

Untuk konfigurasi pada topologi diatas lakukan langkah berikut ini. Pada router ISP 1 Buat prioritas. Prioritas yang lebih kecil akan diutamakan

```
RouterA(config)# interface G 0/1
RouterA(config-if)# ip address 10.1.1.2 255.255.255.0
RouterA(config-if)# standby 10 ip 10.1.1.1
RouterA(config-if)# standby 10 priority 110
RouterA(config-if)# standby 10 preempt
```

Pada router dua lakukan hal yang sama akan tetapi pada router tersebut tidak kita berikan prioritas.default prioritas adalah 100. Maka router ini menjadi jalur prioritas utama.

```
RouterA(config)# interface G 0/1
RouterA(config-if)# ip address 11.11.11.2 255.255.255.0
RouterA(config-if)# standby 10 ip 11.11.11.1
RouterA(config-if)# standby 10 preempt
```

BAB VII
ROUTING DYNAMIC

7.1. Pengertian Routing Dinamis

Routing merupakan sebuah proses untuk meneruskan paket-paket jaringan dari suatu jaringan ke jaringan lainnya sehingga menjadi rute tertentu (Hasanah & Mubarakah, 2014). Secara umum jenis protokol routing terdapat 2 macam yaitu routing statik, dan routing dinamis (Masykur, 2016). Routing dinamis merupakan routing yang mempelajari sendiri rute terbaik mana yang dipilih untuk ditempuh untuk meneruskan paket dari sebuah network ke network lainnya (Hasanah & Mubarakah, 2014).

Ada beberapa jenis routing dinamis yang banyak digunakan diantaranya Routing Information Protocol (RIP) (Hasanah & Mubarakah, 2014), Open Shortest Path First (OSPF) (Rahmawati, Shaleh, & Winarno, 2011), Border Gateway Protocol (BGP) (Lestari, Andrian, & Susanti, 2011), Interior Gateway Routing Protocol (IGRP) (Masykur, 2016), dan Enhanced Interior Gateway Routing Protocol (EIGRP) (Yolanda, Pramono, & Purnomo, n.d.). Berbagai macam jenis routing tersebut memiliki kelebihan dan kekurangannya masing-masing yang mana tidaklah sempurna (Masykur, 2016) oleh karena itu terkadang traffic perlu ditentukan dan diprediksi secara manual.

7.2. Jenis Routing Dinamis

Pada penggunaannya routing dinamis memiliki beberapa cara dalam mengirimkan data pada jaringan. Yaitu :

1. Link-State

   link state adalah metode routing yang menitik beratkan pada perhitungan metric cost. pada metode ini router akan menggunakan algoritma Dijkstra's untuk menghitung route terbaik dalam setiap tujuannya. Router yang menggunakan teknik link state artinya tiap router akan mengumpulkan informasi tentang interface, bandwidth, roundtrip dan sebagainya. Kemudian antar router akan saling menukar informasi, nilai yang paling efisien yang akan diambil sebagai jalur dan di masukkan ke dalam tabel routing seperti OSPF. informasi LSA tersebut akan diatur sedemikian rupa hingga membentu suatu jalur routing dengan menggunakan agoritma pengambilan keputusan SPF (Shortest Path First) (Rifiani et al., 2011).

2. Distance Vector

   Distance vector adalah sebuah algoritma routing yang menginformasikan banyaknya hop jaringan yang dituju dengan menitik beratkan pada jarak dan arah. Sebuah distance vector protocol menginformasikan banyaknya hop ke jaringan tujuan (the distance) dan arahnya dimana sebuah paket dapat mencapai jaringan tujuan (the vector) Algoritma distance vector juga dikenal sebagai algoritma Bellman-Ford (Rifiani et al., 2011). Setiap router akan mengirimkan routing table ke router terdekat tanpa mengetahui topologi atau bagaimana mereka terkoneksi. distance vector tidak mampu melihat topologi yang ada dibelakang network terdekatnya. kekurangan dari distance vector ini adalah Update tabel routing dikirim setiap 30 detik yang bisa menyebabkan CPU load dalam router itu tinggi. Routing yang menggunakan distance vector adalah RIP, EIGRP dan BGP.

7.3. EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) adalah protocol dengan optimalisasi untuk meminimalkan ketidak stabilan routing yang terjadi setelah perubahan topologi, serta penggunaaan dan pengolahan daya bandwith pada router EIGRP menggunakan algoritma Difusssing Update Algorithm (DUAL) untuk mencari jalur terbaik. Eigrp Juga dapat didefinisikan sebagain routing protocol yang menggunakan formula berbasis bandwidth dan delay untuk menghitung metric yang sesuai untuk menentukan rute (Musril, 2017).

7.4. Fitur EIGRP

EIGRP memiliki beberapa fitur yang tidak dimiliki oleh distance vector routing protocol lainnya, seperti:

1. Neighbor discovery/recovery mechanism

   teknologi ini memungkinkan router untuk dapat mengenali setiap neighbor pada network yang terhubung langsung secara dinamik. Router juga harus mengetahui jika ada salah satu neighbor yang mengalami kegagalan dan tidak dapat dijangkau lagi (unreachable). Proses ini dapat diwujudkan dengan pengiriman paket hello yang kecil secara periodik. Selama router menerima paket hello dari router neighbor, maka router akan mengasumsikan bahwa router neighbor berfungsi dengan normal dan keduanya dapat bertukar informasi routing.

2. RTP

   Bertanggung jawab atas pengiriman paket-paket kepada neighbor yang terjamin dan terurut. RTP mendukung transmisi campuran antara paket multicast dan unicast. Untuk tujuan efisiensi, hanya paket EIGRP tertentu yang dikirim menggunakan teknologi RTP.

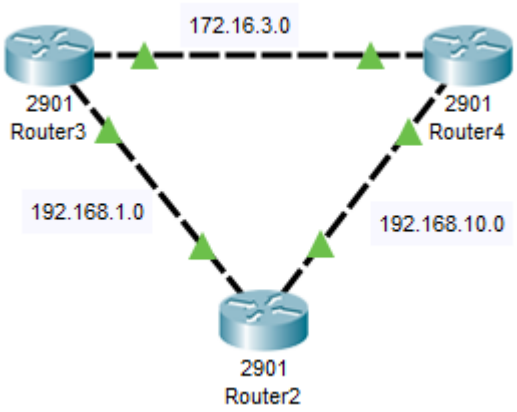
3. DUAL finite state machine

   mewujudkan proses penentuan untuk semua komputasi route. DUAL melacak semua route yang di advertise oleh setiap neighbor dan menggunakan metric untuk menentukan jalur paling effisien dan bebas looping ke semua network tujuan.

4. Protocol-dependent modules (PDM)

   bertanggung jawab untuk keperluan layer network protokol-protokol tertentu. EIGRP mendukung IP, AppleTalk, dan Novell NetWare; setiap protokol tersebut telah disediakan module EIGRP nya masing-masing dan satu sama lain beroperasi secara independent. Module IP-EIGRP misalnya, bertanggung jawab untuk pengiriman dan penerimaan paket-paket EIGRP yang telah di enkapsulasi dalam IP.

7.5. Konfigurasi EIGRP



Gambar 7.1 topologi EIGRP

Konfigurasi EIGRP dilakukan pada setiap router dengan perintah yang sama. Perintah tersebut hanya memasukan alamat network pada router itu sendiri. Ketika sudah dilakukan maka router router tersebut akan mengirimkan alamat tersebut kepada router router tetangganya.

```
R2(config)#router eigrp 1
R2(config-router)#network 192.168.10.0
R2(config-router)#network 192.168.1.0
R2(config-router)#no auto-summary
```

7.6. OSPF

OSPF merupakan protokol routing link state dan digunakan untuk menghubungkan router-router yang berada dalam satu Autonomous System (AS) sehingga protokol routing ini termasuk juga kedalam kategori Interior Gateway Protocol (IGP). Ospf juga merupakan Intra – Domain Internet Routing Protocol yang paling sering dipergunakan (Utomo & Purnama). Open Shortest Path First (OSPF) merupakan pengembangan dari routing protocol sebelumnya yaitu routing internet protocol (RIP) yang dibangun oleh Internet Enginering Task Force (IETF) pada tahun 1980(Kurniawan & Rahmad, n.d.). Routing OSPF menggunakan algoritma shorted path atau biasa disebut jalur terpendek dalam rangka membangun dan menghitung jalur terpendek ke semua jalur tujuan yang dikenal dengan istilah Algoritma Djikstra (Novendra, Arta, & Siswanto, 2010).

7.7. Kelebihan dan Kekurangan OSPF

Setiap routing memiliki kelebihan dan kekurangan dari segi fungsi dan kegunaannya. Berikut ini kelebihan dan kekurangan routing ospf :

Kelebihan dari OSPF:

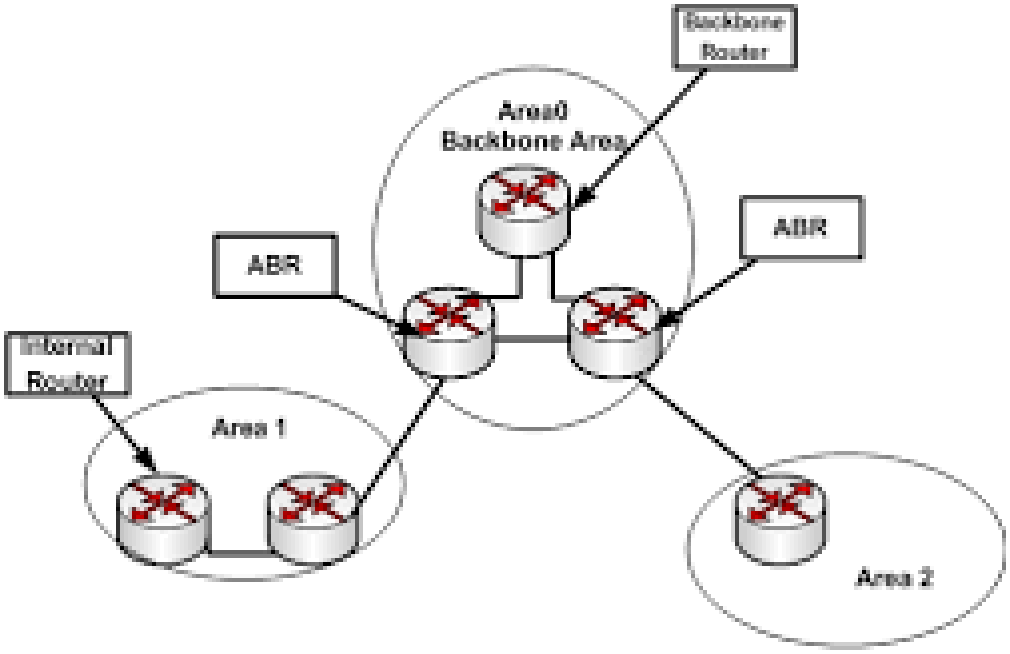
1. Tidak menghasilkan routing loop
2. Mendukung penggunaan beberapa metrik sekaligus
3. Dapat menghasilkan banyak jalur ke sebuah tujuan
4. Membagi jaringan yang besar menjadi beberapa area
5. Waktu yang diperlukan untuk konvergen lebih cepat

Kekurangan dari OSPF:

1. Membutuhkan basis data yang besar
2. Lebih rumit

7.8. Jenis OSPF

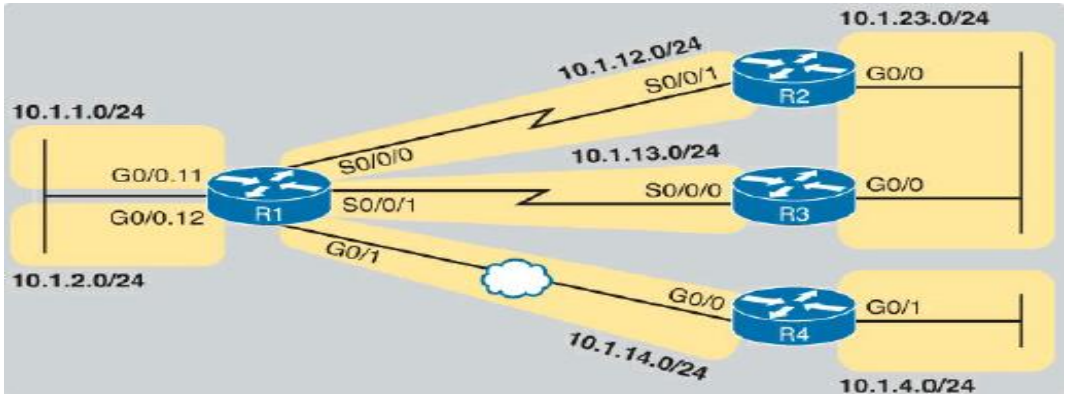
Ospf terdiri dari dua jenis berdasarkan cakupan wilayahnya. Ospf yang berada dalam satu area atau yang disebut area backbone dan ospf yang berbeda area tapi tetap terhubung ke area backbone.



Gambar 7.2 topologi OSPF

7.7.1 Single-area OSPF

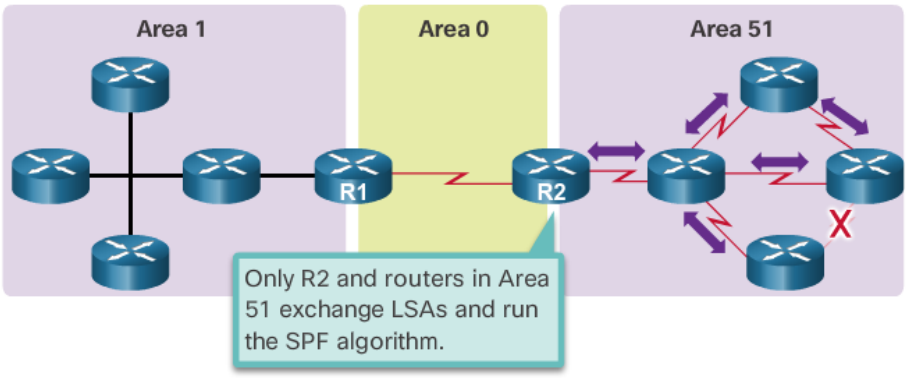
Pada single area router router yang terkoneksi menggunakan ospf ini berada dalam satu area backbone.fungsi single area ini adalah untuk dapat mengontrol informasi routing yang dikirimkan oleh router tetangga dalam satu area.



Gambar 7.3 OSPF Single Area

7.7.2 Multi-area OSPF

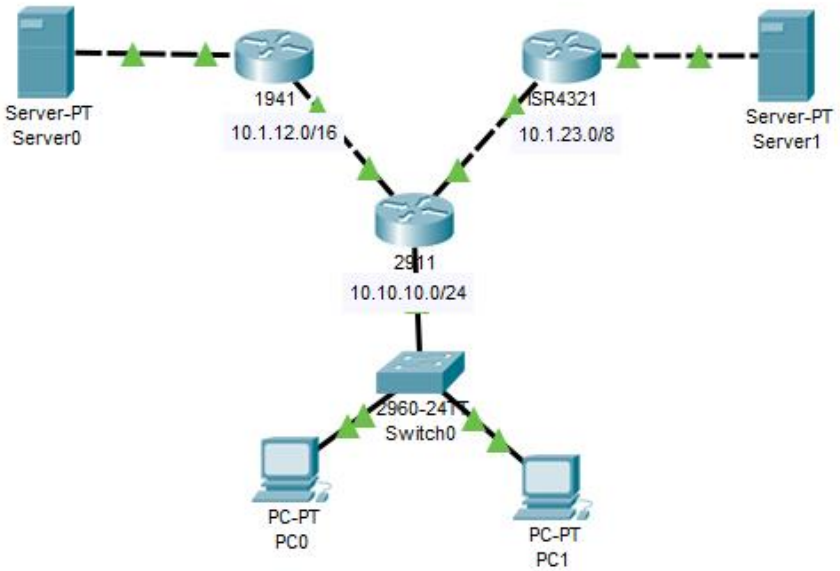
Pada multi area router router yang terkoneksi menggunakan ospf ini berada pada area yang terpisah baik itu wilayah atau negara. Fungsi dari ospf ini adalah untuk dapat bertukar informasi antar tetangga yang berada pada luar area tetapi dalam satu Autonomus system agar dapat dikontrol oleh area backbone



Gambar 7.4 OSPF Multi Area

7.9.Konfigurasi Single-area OSPF

Untuk mengaktifkan ospf pada router cisco dapat menggunakan perintah “router ospf process_id”. Process_id merupakan angka 1 sampai dengan 65.535. buatlah tpologi seperti dibawah ini.



Gambar 7.5 Topologi OSPF Single Area

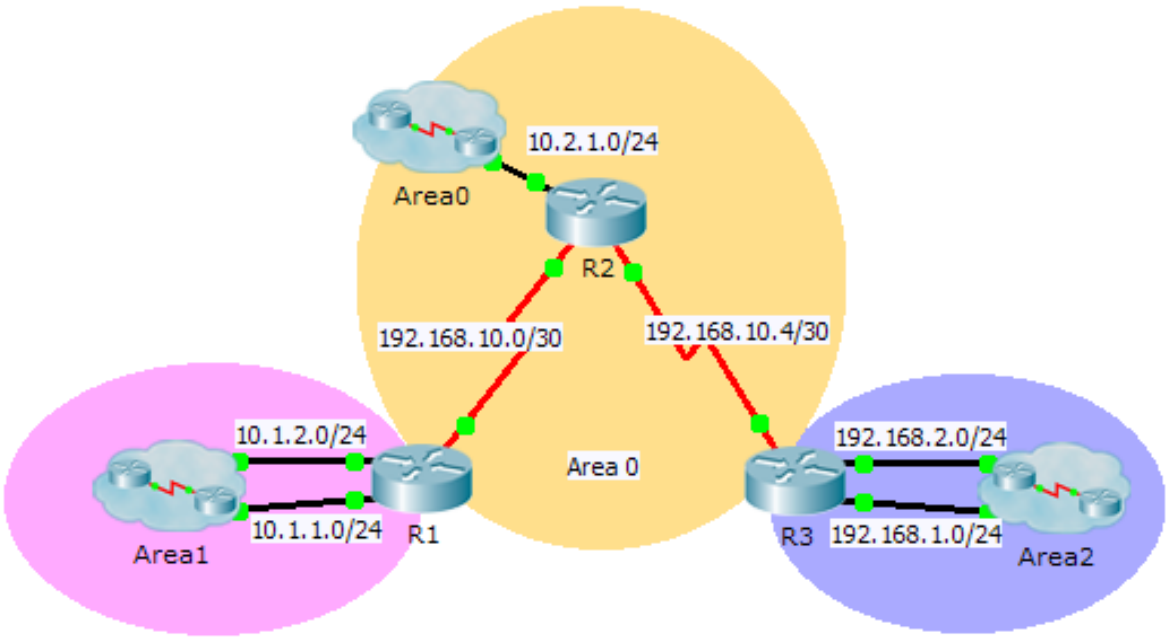
```
R2911(config)#router ospf 10
R291 (config-router)#router-id 1.1.1.1
R291 (config-router)#network 10.1.0.0 0.0.255.255 area 0
R291 (config-router)#network 10.0.0.0 0.255.255.255 area 0
R291(config-router)#network 10.1.23.0 0.0.0.255 area 0
R291 (config-router)#passive-int g0/0
```

Konfigurasi diatas dapat dilakukan oleh setiap router hanya mengganti alamat setiap network pada router tersebut. Untuk setiap network address diikuti oleh wildcard mask. Kemudian karena single area maka kita memasukan semua network kedalam area 0.

7.10. Konfigurasi Multi-area OSPF OSPF

OSPF dibuat dan dirancang untuk melayani jaringan lokal berskala besar. Semakin membesarnya area jaringan yang dilayaninya akan semakin banyak informasi yang saling dipertukarkan.

Ketika sebuah jaringan semakin membesar, routing protokol OSPF tidak efektif lagi jika dijalankan dengan hanya menggunakan satu area saja. Seperti yang telah Anda ketahui, OSPF merupakan routing protokol berjenis Link State. Ciri-ciri dari routing Multiarea OSPF ini adalah menggunakan beberapa area atau minimal 2 area dalam implementasinya



Gambar 7.6 Topologi OSPF Multi Area

```
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 10.1.1.0 0.0.0.255 area 1
R1(config-router)#network 10.1.2.0 0.0.0.255 area 1
R1(config-router)#network 192.168.10.0 0.0.0.3 area 0
```

Pada router ini masukan dua area yaitu area 1 untuk network 10.1.1.0/24 dan 10.1.2.0/24 dan area 0 untuk network 192.168.10.0/30

```
R2(config)# router ospf 1
R2(config-router)# router-id 2.2.2.2
R2(config-router)# network 10.2.1.0 0.0.0.255 area 0
R2(config-router)# network 192.168.10.0 0.0.0.3 area 0
R2(config-router)# network 192.168.10.4 0.0.0.3 area 0
```

Pada router 3 masukan router id 3.3.3.3 dan dua area yaitu area 2 dan area 0. Untuk process idnya disamakan.

```
R3(config)# router ospf 1
R3(config-router)# router-id 3.3.3.3
R3(config-router)# network 192.168.2.0 0.0.0.255 area 2
R3(config-router)# network 192.168.1.0 0.0.0.255 area 2
R3(config-router)# network 192.168.10.4 0.0.0.3 area 0
```

BAB VIII
STUDI KASUS

8.1. Kasus Routing

Perusahaan XYZ memiliki 3 kantor Cabang. Pada kantor **cabang 1** memiliki 14 komputer yang terhubung menggunakan kabel serta terdapat 5 Laptop yang terhubung menggunakan media Wireless. Sedangkan pada kantor **cabang 2**, memiliki 20 komputer yang terhubung menggunakan kabel. Dan kantor **cabang 3** memiliki 10 komputer.

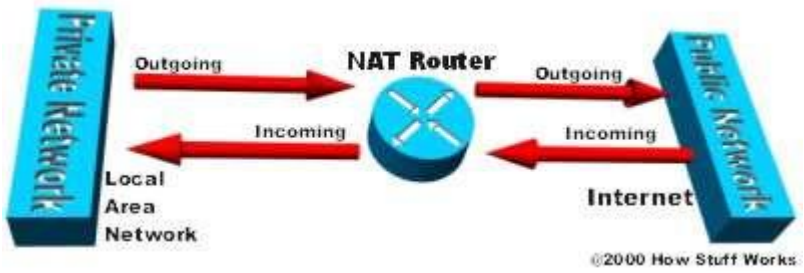
Anda sebagai seorang Network Administrator diminta untuk melakukan konfigurasi terhadap ketiga kantor cabang tersebut dengan ketentuan, sebagai berikut:

1. Melakukan konfiguarsi IP Address dengan menggunakan Subnetting pada perangkat Komputer dan Laptop yang terhubung. **Tidak dianjurkan menggunakan /24**,
2. Berikan IP Address dengan menggunakan **subnetting /30** terhadap interface yang terhubung secara langsung dari **router ke router**,
3. Terapkan konfigurasi Routing Dynamic,
4. Serta pastikan seluruh Client di Kantor Cabang 1, kantor cabang 2 dan kantor cabang 3 dapat saling terkoneksi dengan baik
5. Setelah jaringan berjalan sesuai dengan fungsinya, upload dokumentasi pembuatan jaringan kedalam blog

BAB IX
NETWORK ADDRESS TRANSLATION

9.1. Pengertian NAT

Network Address Translation merupakan suatu metode dimana IP address dipetakan dari satu grup ke grup lainnya secara transparan bagi sisi penerima (Kurniawan & Rahmad, n.d.). Network Address Translation (NAT) adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet menggunakan satu alamat IP (Riadi, 2011). NAT merupakan teknologi yang memungkinkan IP Private dapat membagi koneksi akses internet jaringan yang didesain untuk menyederhanakan IP address, dan berperan juga untuk melindungi jaringan dan kemudahan serta fleksibilitas dalam administrasi jaringan. Banyaknya penggunaan metode ini disebabkan karena ketersediaan alamat IP Address yang terbatas. NAT berlaku sebagai penerjemah antara dua jaringan (Taringan, 2009).



Gambar 9.1 Router NAT

NAT bekerja dengan jalan mengkonversikan IP address ke satu atau lebih IP address lain. IP address dikonversi adalah IP address yang diberikan untuk tiap mesin dalam jaringan internal. IP address yang menjadi hasil konversi terletak di luar jaringan internal tersebut dan merupakan IP address legal yang valid (Husaini, 2008).

9.2. Jenis NAT

Dua Tipe NAT Dua tipe NAT adalah Statik dan Dinamik yang keduanya dapat digunakan secara terpisah maupun bersamaan.

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

a. NAT dengan Pool (kelompok) 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.

b. NAT Overload Sejumlah IP lokal/internal dapat ditranslasikan ke satu alamat IP global/internet. Hal ini sangat menghemat penggunakan alokasi IP global dari ISP. Pemakaian bersama satu alamat IP ini menggunakan metoda port multiplexing, atau perubahan port ke outbound packet yang disebut juga dengan metode Network Address Port Translation (NAPT).

9.3. Translasi NAT

Berdasarkan cara translasinya NAT dibagi menjadi 3 bagian, yaitu:

1. Cone NAT

   Mentranslasikan alamat dan port internal dari host yang berada di belakang perangkat NAT ke sebuah alamat dan port eksternal, jadi semua trafik yang erasal dari alamat di luar perangkat NAT akan dapat diteruskan ke host yang berada di belakang NAT(Novendra, Arta, & Siswanto, 2010)..

2. Restricted NAT

   Mentranslasikan alamat dan port internal dari host yang berada di belakang perangkat NAT ke suatu alamat dan port eksternal. Alamat tujuan dari paket yang dikirim oleh host yang berada di belakang perangkat NAT akan disimpan dalam tabel NAT. Trafik yang berasal dari alamat di luar perangkat NAT hanya akan diteruskan apabila alamat tersebut terdapat di dalam tabel NAT (Novendra, Arta, & Siswanto, 2010).

3. Port Restricted Cone NAT

   Tipe ini menambah larangan dalam penerimaan paket yang dikirim oleh host di jaringan eksternal. Restricted Cone NAT hanya mengamati host jaringan luar, akan tetapi Port Restricted Cone NAT juga mengamati port yang digunakan untuk dapat melalui NAT, paket yang dikirimkan oleh host dari jaringan luar tidak hanya harus dikirim dari host yang menjadi tujuan komunikasi yang dimulai oleh host internal, tetapi juga harus dikirim melalui port yang menjadi tujuan komunikasi, jika tidak maka semua paket akan ditolak (Novendra, Arta, & Siswanto, 2010).

9.4 . Jenis NAT

NAT merupakan perpindahan suatu alamat IP ke alamat IP lain. Ada dua macam dari NAT, yaitu:

1. DNAT (Destination Network Address Translation)

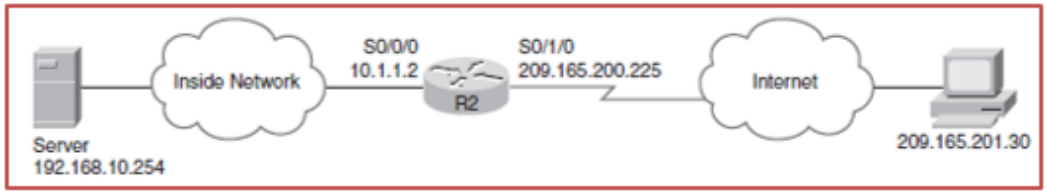
   Digunakan untuk meneruskan paket dari IP Public melalui firewall ke dalam suatu Host

2. **SNAT (Source Network Address Translation)**

   Dipergunakan untuk merubah source address dari suatu paket data. Sebagai contoh penggunaannya pada Gateway Internet.

9.5. Konfigurasi Static NAT

Buat topologi seperti berikut ini untuk mengkonfigurasi static NAT. berikan router dua ip address yang dapat terkoneksi ke internet.

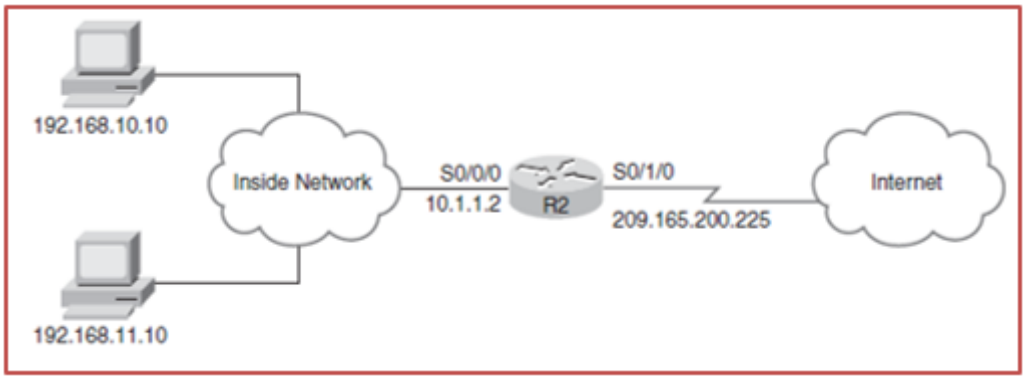


Gambar 9.2 Topologi Static Nat

```
R2(config)#ip nat inside source static 192.168.10.254 209.165.200.254
R2(config)#interface serial0/0/0
R2(config-if)#ip nat inside
R2(config-if)#interface serial 0/1/0
R2(config-if)#ip nat outside
```

9.6. Konfigurasi Dynamic NAT

Masukan kelompok alamat IP kedalam access list. Router(config)#ip nat inside source list access-list-number pool name. Spesifikasikan inside dan outside interfaceRouter(config)#interface type number. Router(config-if)#ip nat inside. Router(config-if)#ip nat inside.



Gambar 9.3 Dynamic NAT

```
R2(config)#ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask
255.255.255.224
R2(config)#access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)#ip nat inside source list 1 pool NAT-POOL1
R2(config)#interface serial 0/0/0
R2(config-if)#ip nat inside
R2(config-if)#interface serial s0/1/0
R2(config-if)#ip nat outside
```

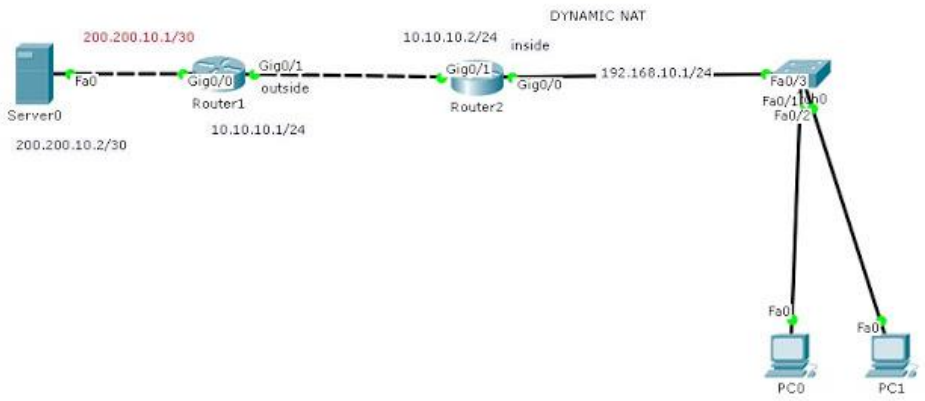
Inside Global, yaitu IP Address yang menjadi penerjemah dari IP Private 192.168.10.5.

Inside Local, yaitu IP Address yang digunakan sebagai client pada PC0.

Outside Local, yaitu IP Address yang sudah sobat PING tadi, dalam artian yaitu IP Address yang dilakukan dari jaringan Lokal.

Outside Global, yaitu IP Address yang menjadi tujuannya.

9.7. Konfigurasi Dynamic NAT Overloading



Gambar 9.4 Nat Overloading

Buat topologi diatas dengan ketentuan sebagai berikut :

Router1 : Gig0/0 = 200.200.10.1/30
Gig0/1 = 10.10.10.1/24

Router2 : Gig0/0 = 192.168.10.1/24
Gig0/1 = 10.10.10.2/24

Server : 200.200.10.2/30

PC0 : 192.168.10.2/24

PC1 : 192.168.10.3/24

Konfigurasi pada router 1 dengan perintah dibawah ini

```
Router1>enable
Router1#conf ter
Router1(config)#int
Router1(config)#interface gi
Router1(config)#interface gigabitEthernet 0/0
Router1(config-if)#ip ad
Router1(config-if)#ip address 200.200.10.1 255.255.255.252
Router1(config-if)#no sh
Router1>enable
Router1#conf ter
Router1(config)#int
Router1(config)#interface gi
Router1(config)#interface gigabitEthernet 0/1
Router1(config-if)#ip ad
Router1(config-if)#ip address 10.10.10.1 255.255.255.0
Router1(config-if)#no sh
Router1(config-if)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
Router(config)#
```

Default route adalah sebuah rute yang dianggap cocok dengan semua IP address tujuan ditulis dengan 0.0.0.0/0. Dengan default route ketika IP address destination(tujuan) dari sebuah paket tidak ditemukan dalam tabel routing, maka router akan menggunakan default route untuk mem-forward paket tersebut.

```
Router2(config)#int
Router2(config)#interface gi 0/0
Router2(config-if)#ip na
Router2(config-if)#ip nat ins
Router2(config-if)#ip nat inside
Router2(config-if)#exit
Router2(config)#interface gig 0/1
Router2(config-if)#ip na
Router2(config-if)#ip nat outs
Router2(config-if)#ip nat outside
Router2(config-if)#ex
Router2(config)#ac
Router2(config)#access-list 1 per
Router2(config)#access-list 1 permit 192.168.10.0 0.0.0.255
Router2(config)#ip na
Router2(config)#ip nat poo
Router2(config)#ip nat pool poolR2 10.10.10.10 10.10.10.50 net
Router2(config)#ip nat pool poolR2 10.10.10.10 10.10.10.50 netmask
255.255.255.0
Router2(config)#ip na
Router2(config)#ip nat ins
Router2(config)#ip nat inside sour
Router2(config)#ip nat inside source lis
Router2(config)#ip nat inside source list 1 pool poolR2
Router2(config)#
```

```
Router>en
Router#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip na
Router(config)#ip nat ins
Router(config)#ip nat inside sour
Router(config)#ip nat inside source lis
Router(config)#ip nat inside source list 1 pool poolR2 overl
Router(config)#ip nat inside source list 1 pool poolR2 overload
Router(config)#
```

DAFTAR PUSTAKA

Amanda Yudiani, R., Munadi, R., & Vidya Yovita, L. (2013). Implementasi Dan Analisis Virtual Router Redundancy Protocol (Vrrp) Dan Hot Standby Router Protocol (Hsrp). Retrieved from www.tcpdf.org

Amin, Z. (2014). Simulasi Dan Perancangan Keamanan Autentikasi Jaringan Hirarki Link Aggregation Control Protocol (Lacp) Berbasis Router Cisco (Studi, *3*(September), 138–144.

Dzulfiqar Anwar, N., Vidya Yovita, L., & Mayas ari, R. (2015). Implementasi Dan Analisa Performansi Redundancy Pada Jaringan Multicast Dengan Metode Protocol Independent Multicast Implementation and Performance Analysis of Redundancy on Multicast Network Using Protocol Independent Multicast Sparse Mode, *2*(3), 7159–7166.

Kurniawan, H., & Rahmad, I. F. (n.d.). Analisa interkoneksi, 129–141.

Li, G. F., & Hu, G. D. (2010). Mineralization information extraction using ASTER image. *2010 International Conference on Multimedia Technology, ICMT 2010*, *2*(1), 75–82. https://doi.org/10.1109/ICMULT.2010.5631046

Maulana, A., Harafani, H., & Setiawan, A. (2018). Konsep Dan Perancangan Routing Eigrp , Ripv2 Dan Ospf, *15*(2), 234–243.

Musril, H. A. (2017). ANALISIS UNJUK KERJA RIPv2 DAN EIGRP DALAM DYNAMIC ROUTING PROTOCOL. *Jurnal Elektro Dan Telekomunikasi Terapan*, *2*(2), 116–124. https://doi.org/10.25124/jett.v2i2.99

Naqvi, H. A., Hertiana, S. N., & Negara, R. M. (2015). SIMULASI DAN ANALISIS SISTEM GATEWAY TERDISTRIBUSI UNTUK FIRST-HOP REDUNDANCY DAN LOAD BALANCING, *30*(6), 2729–2736. https://doi.org/10.3969/j.issn.1002-5006.2015.06.006

Novendra, Y., Arta, Y., & Siswanto, A. (2010). Analisis Perbandingan Kinerja Keuangan, *2*(2), 97–106.

Riadi, I. (2011). Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik. *JUSI, Universitas Ahmad Dahlan Yogyakarta*, *1*(1), 71–80.

Rifiani, V., Hadi, M. Z. S., Darwito, H. A., Politeknik, M., Negeri, E., & Telekomunikasi, J. T. (2011). ANALISA PERBANDINGAN METODE ROUTING DISTANCE, 2– 7.

Srisuresh, P., dan Egevang, K. Traditional IP Network Address Translator (Traditional NAT). RFC 3022. Januari 2001.

Utomo, P., & Purnama, B. E. (2012). Pengembangan Jaringan Komputer Universitas Surakarta Berdasarkan Perbandingan Protokol Routing Information Protokol (RIP) Dan Protokol Open Shortest Path First (OSPF) Prawido Utomo, Bambang Eka Purnama ABSTRAKSI. IJNS, 1(November), 8–25