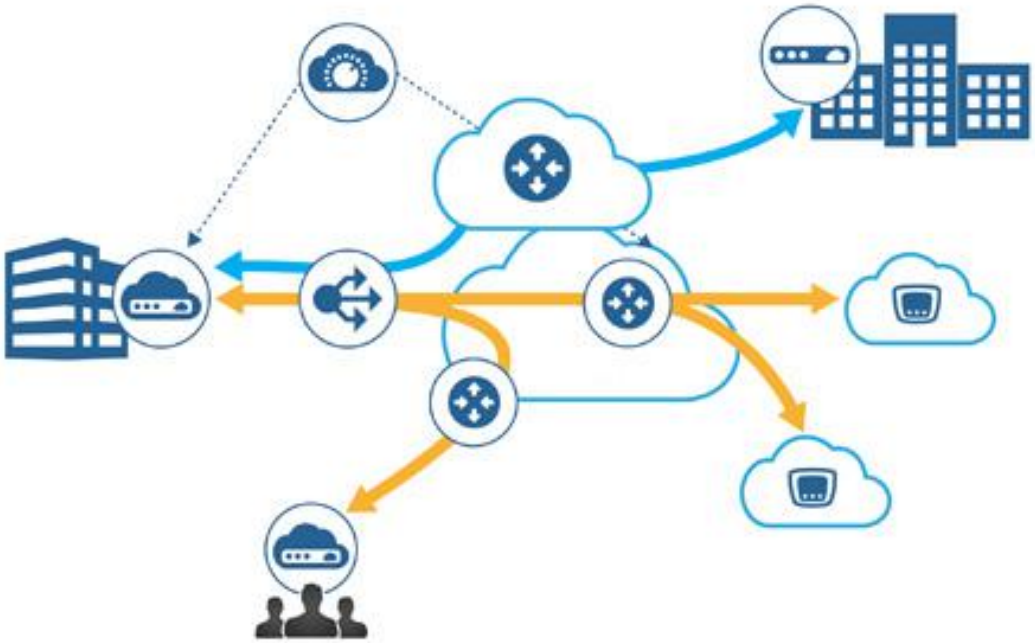
This book was created by :

Egi Fadli Soerachman



Solusi Panduan Untuk Routing Switching

Based on 200-125 CCNA R&S

Unofficial Cisco Books.

Contents

Kata Pengantar 7

Latar Belakang 8

Profile Penulis 9

Day 1 10

1. ***Pengetahuan Dasar Jaringan*** 10

Apa sih Network itu ? 10

Nah… Bagaimana sih, gambarannya pada Network (jaringan komputer) atau internet itu ? 10

Ada apa di dalam Internet ? 12

Tahukan kalian, bahwa proses komunikasi yang terjadi di Internet itu sangat panjang dan rumit ? 12

Disaat seperti apa kita membutuhkan Network ? 13

Apakah Network memudahkan aktifitas Manusia ? 15

2. ***Perkembangan Dunia Jaringan*** 19

3. ***LAN, MAN & WAN*** 23

Apa itu LAN ? 23

Apa itu WAN ? 25

LAN vs WAN 26

Apa sih MAN itu ? 28

4. ***Internetworking Devices*** 29

Apa sih Switch itu ? 30

≈ ***UnManaged Switch*** 31

≈ ***Managed Switch*** 32

Apa sih Hub itu ?.....33

Apa sih Router itu ?.....34

5. *Packet Tracer Simulation*.....**Error! Bookmark not defined.**

Day 2..... **Error! Bookmark not defined.**

6. *Network Protocols and Communications*.....42

7. *Network Access*.....44

8. *OSI Layer vs TCP IP*.....47

OSI Layer.....47

- *TCP / IP Models (Darpa)*.....54

9. *IPv4*.....66

Lalu, apa itu IPv4 ?.....67

Metode Pengiriman IPv4.....69

Day 3..... **Error! Bookmark not defined.**

10. *Subnetting*.....73

Apa sih Network ID itu ?.....73

Lalu apa sih Host ID itu ?.....73

Network ID vs Host ID.....74

IPv4 Class.....74

Binary.....76

Konversi dari IP ke Binary.....78

Lalu, apa sih Netmask itu ?.....78

Apa itu Classful ?.....79

Apa itu Classless ?.....79

11. Collision Domain & Broadcast Domain.....80

Menghitung Collision Domain.....82

Menghitung Broadcast Domain.....84

12. Basic Config.....87

Apa itu Cisco IOS ?.....88

IOS Startup Sequence.....90

Yuk… kita ngonfig.....90

Configuring Console.....92

13. Router Introduction.....94

14. Dynamic Routing Introduction.....96

Day 4.....98

15. Apa itu Switch.....98

Apa sih Switching itu ?.....101

16. Configuring Telnet.....102

17. Configuring SSH.....104

18. DHCP.....106

Yuk kita ngonfig.....107

19. Yuk… kita ngonfig.....**Error! Bookmark not defined.**

Static Routing Configuration.....109

Day 5.....111

20. Routing Information Protocol (RIP).....111

21. RIPv2.....115

Yuk … kita ngonfig.....116

22. VLAN 117

Ngonfig VLAN 119

23. Trunk 121

Apa itu Native VLAN ? 122

Filtering VLAN in Trunking 124

24. Dynamic Trunking Protocol 125

25. VLAN Trunking Protocol 127

Day 6 129

26. Spanning Tree Protocol 129

27. InterVLAN Routing 133

28. Port Security 135

29. Etherchannel 137

Day 7 140

30. OSPF 140

RIP vs OSPF 141

Perintah pada OSPF 142

OSPF Authentication 142

31. EIGRP 144

EIGRP Metric 144

Yuk kita ngonfig 145

32. Access-List 146

Yuk kita ngonfig 146

Day 8 148

33. Network Address Translation.....148

Static NAT..... 149

Dynamic NAT..... 150

Port Address Translation.....151

34. IPv6 Essence..... 153

Apa saja kelebihan, perubahan, dan fitur yang ada pada IPv6 ini ? berikut listnya :..... 154

Penutup.....163

Kata Pengantar

Puji syukur Alhamdulillah, penulis panjatkan kehadirat Allah S.W.T atas ridha dan rahmat-Nya yang dilimpahkan sehingga pada akhirnya penulis dapat menyusun dan menyelesaikan buku ini dengan baik. Dan juga saya ber-terima kasih banyak kepada Orang Tua dan Keluarga saya yang sudah mendidik saya semenjak lahir hingga besar sekarang, Guru-Guru saya semasa sekolah yang telah berjasa dan juga kepada para sahabat saya.

Jika ada **Saran, Kritik, Komentar & Review** tentang buku ini silahkan kontak melalui **egifadlisoerachman@gmail.com**

Latar Belakang

Buku ini dibuat khusus untuk digunakan disetiap training yang pengisi training tersebut adalah saya sendiri. Buku ini sebagai modul pegangan peserta di Training tersebut, yang dimana isi buku ini adalah terdiri dari beberapa kutipan Training dan juga beberapa bahan untuk Lab. Buku ini juga dapat dijadikan sebagai bahan Pembalajaran di rumah (diluar training), baik itu untuk mengulang pembelajaran yang pernah di pelajari di Training, ataupun untuk mengingatkannya kembali. Besar harapan penulis, dapat memberikan manfaat besar dan berguna untuk para pemegang buku ini.

Buku ini juga dapat digunakan sebagai bahan pembelajaran bagi yang ingin ujian 200-125 CCNA Routing & Switching. **Karena silabus materi buku ini dibuat 100% sesuai dengan exam topics 200-125 CCNA Routing & Switching Official Cisco.**

Referensi : https://learningnetwork.cisco.com/community/certifications/ccna/ccna-exam/exam-topics

Profile Penulis

Nama : Egi Fadli Soerachman

Panggilan : Egi

Latar Belakang : Seorang Pengajar dunia IT Networking. Sekarang ini berstatus sebagai Freelance Trainer berpengalaman di beberapa Perusahaan, Training Center, dan External Lecturer di sebuah Perguruan Tinggi milik swasta dan milik BUMN.

E-mail : egifadlisoerachman@gmail.com

Blog : egifadlisoerachman.wordpress.com

LinkedIn : www.linkedin.com/in/egifadlisoerachman

Network Fundamentals

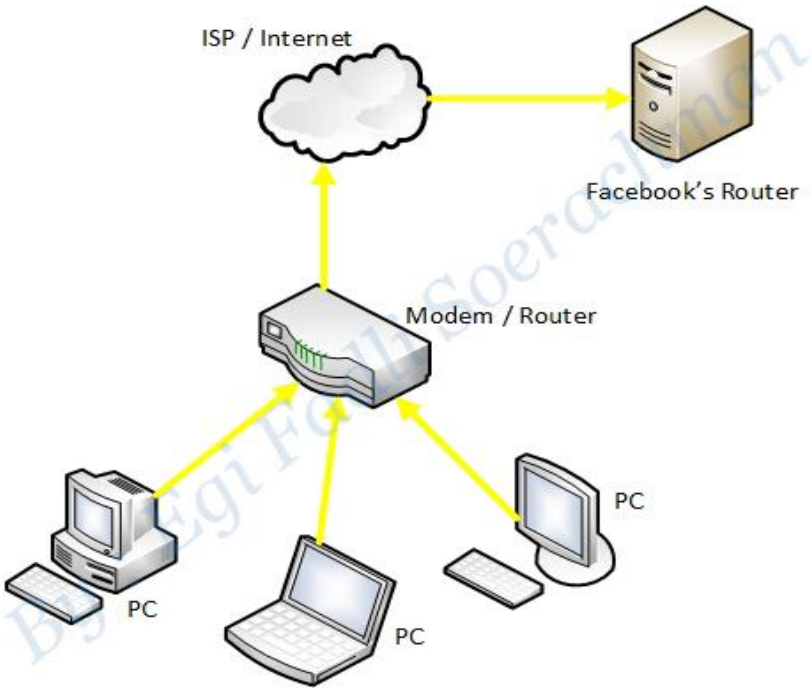
1. Pengetahuan Dasar Jaringan

Apa sih Network itu ?

Network atau Jaringan komputer, adalah sebuah kumpulan perangkat yang saling terhubung. Kata dalam " Perangkat " ini luas, bisa komputer, Router, Switch, Server, Printer, Smartphone dsb. Jaringan adalah, Kumpulan perangkat-perangkat yang saling berkomunikasi. Internet juga bisa dikatakan sebagai Jaringan, karena Internet itu terdiri dari Perangkat-perangkat yang saling terhubung atau berkomunikasi.

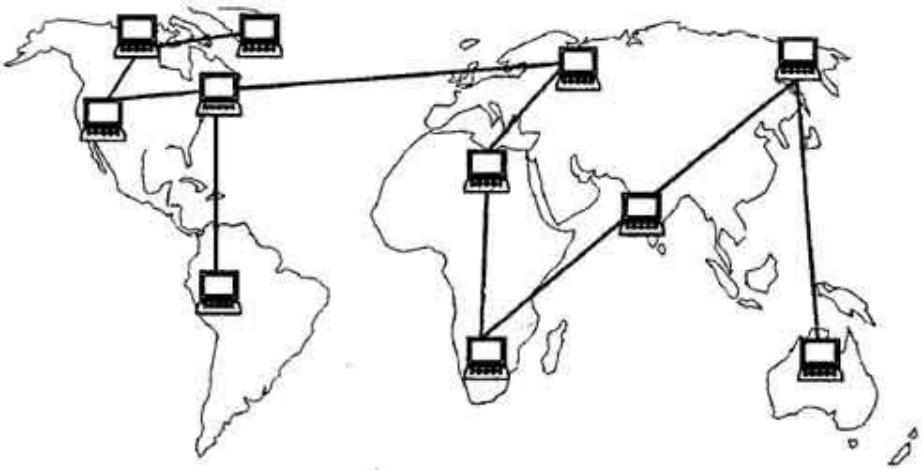
Nah… Bagaimana sih, gambarannya pada Network (jaringan komputer) atau internet itu ?

Pada umumnya , orang awam menggambarkan sebuah jaringan komputer atau Internet seperti berikut :



Gambar tersebut sudah benar jika dikatakan sebuah Jaringan, yaitu terdiri dari beberapa komputer yang saling terhubung, Modem sebagai perantara yang menghubungkan antara ke 3 PC tersebut dengan Internet. Namun gambar ini tidak bisa dikatakan sebagai gambaran Internet. Kenapa ? karena tepatnya gambar ini dikatakan sebagai LAN, bukan Internet.

Area pada Network terbagi menjadi 2 Jenis yang umum, yaitu LAN dan WAN. Apa itu LAN (Local Area Network) ? yaitu jaringan yang dalam lingkupnya terbatas, seperti di jaringan perkantoran, rumah, gedung, dsb. WAN (Wide Area Network) atau bisa juga disebut dengan Internet, yaitu jaringan yang lingkupnya tak terbatas, WAN terdiri dari jaringan kumpulan di benua Asia, Eropa, dll, yang cangkupannya adalah seluruh wilayah di dunia ini. WAN adalah jaringan yang lingkupnya sangat luas, seperti antar Negara, pulau, benua, dsb.



Wide area network

Ada apa di dalam Internet ?

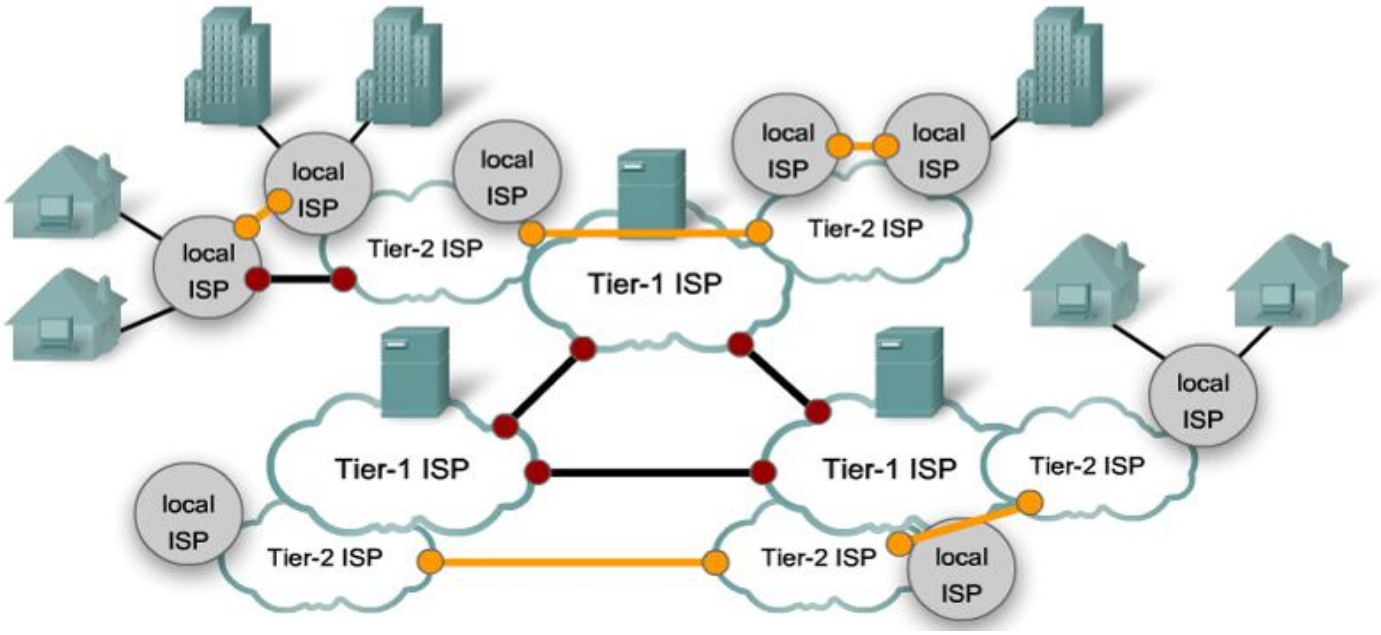
tentu di dalam internet adalah sebuah kumpulan jaringan-jaringan di seluruh dunia dan sebagian besar jaringan diwakili oleh sebuah ISP. *Lalu apa itu ISP* ? ISP (Internet Service Provider) adalah sebuah perusahaan yang menyediakan layanan jasa akses internet, contohnya seperti Telkom, Indosat, dll.

Tahukan kalian, bahwa proses komunikasi yang terjadi di Internet itu sangat panjang dan rumit ?

Orang-orang awam mengira sebuah proses komunikasi pada Internet itu simple. Ketika kalian membuka Web Browser, lalu mengetikan " www.facebook.com " maka prosesnya adalah dari PC menghubungi langsung ke Facebook, dengan perantaranya adalah ISP, dan ISP mengopernya ke Facebook. Maka Facebook pun merespon untuk memberikan webnya ke PC tersebut, dan di PC sudah tampil web halaman login Facebook. *Padahal Sesungguhnya, yang terjadi tak se-simple itu.* Kurang lebih seperti ini.

Internet Structure - A Network of Networks

Peer connections between networks at the same level provide direct connections, bypassing longer routes and preventing congestion on the backbone.



Internet adalah, sebuah kumpulan dari beberapa ISP yang saling kerja sama, dari yang satu dengan yang lainnya. Proses yang sebenarnya terjadi adalah, ketika PC tersebut me-*request* web dengan tujuan www.facebook.com, otomatis *request* tersebut diproses oleh ISP yang dipakai PC (semisal Telkom), ketika di proses oleh Telkom, ternyata rute nya adalah melalui ISP Indosat > ISP di Singapore > ISP di Amerika > Sampai di Facebook. Seperti gambar diatas, *Packet* yang berisikan *request* dari PC, ternyata melewati proses yang panjang, puluhan kali melewati sebuah ISP, melewati puluhan Negara, dan barulah sampai *packet request* tersebut ke Facebook.

Masih bingung ? ini sama halnya kita di Indonesia ingin mengirim surat ke Amerika, sudah pasti melewati beberapa Negara kan ? tidak langsung dari POS di Indonesia ke POS Amerika kan ? nah beginilah maksud tentang proses di dalam Internet.

Disaat seperti apa kita membutuhkan Network ?

Untuk menjawab pertanyaan ini sebenarnya sangat simple, karena hampir seluruhnya membutuhkan Jaringan Komputer, berikut contohnya :

- ***Yaitu, orang yang memiliki Handphone***. Kenapa ? bukankah handphone itu bisa berkomunikasi karena ada peran orang-orang Jaringan Komputer ? seperti yang kita ketahui, bahwa Handphone berkomunikasi tidak sekedar dari Handphone > Tower > Handphone lagi. Jika memang komunikasi handphone seperti menelpon, sms adalah murni dari Handphone lalu melalui Tower, lalu sampai ke handphone, **lalu bagaimana caranya bisa menelpon ke luar negri** ? suatu yang mustahil bukan ? pasti membutuhkan Tower yang sangat amat besar, yang dimana sinyalnya mencangkup minimal 2 negara, ini tentu tidak mungkin terjadi. Maka membutuhkanlah peran Jaringan Komputer, sebagai yang meng-handle hingga 100% komunikasi handphone. Maka dari itu, barangsiapa yang mempunyai handphone, maka ia secara otomatis berarti telah membutuhkan peran Network.
- ***Orang yang mempunyai Rekening Bank.*** Contoh, disaat kita mengambil uang di ATM, bukankah kita dapat mengambil uangnya dimanapun kita berada ? asalakan ATM tersebut men-support Bank yang kita gunakan. ***Bagaimana bisa ?*** tentu bisa, karena informasi keuangan kita, dan uang kita berada di pusat data Bank tersebut. Informasi uang yang berada di rekening kita, itu tidak berada di kartu ATM rekening yang kita gunakan. ***Kenapa*** ? karena jika kartunya hilang, maka hilanglah uang kita, namun nyatanya kehilangan kartu ATM, bukan berarti uang kita ikut hilang. Informasi uang di rekening kita, juga tidak berada di mesin ATM, ***kenapa ?*** karena kita dapat mengambilnya di mesin ATM dimanapun, itu artinya informasi uang kita tidak pada di ATM, kerusakan yang terjadi pada ATM tertentu, itu tidak mempengaruhi informasi keuangan kita, maka hal ini jelas bahwa ATM tidak menyimpan dan tidak mengetahui informasi keuangan rekening kita. ***Lalu siapa ?*** seperti yang telah saya sebutkan, yaitu yang mengetahui dan menyimpan informasi keuangan rekening kita adalah ada pada di Pusat Data Bank tersebut. ***Maka***, setiap kali kita mengambil uang di mesin ATM, karena mesin ATM tidak mengetahui

informasi uang kita, dan juga tidak menyimpan informasi keuangan kita, ***ia membutuhkan berkomunikasi dengan pusat data*** Bank yang kita gunakan, untuk menanyakan informasi keuangan rekening kita. Dari penjelasan ini sudah sangat jelas, bahwa per-Bankan peran utamanya ada pada komunikasi jaringan komputer, andai saja jaringan komputer pusat Banknya terputus, maka semua orang tidak bisa mengambil uang ataupun men-transfernya. Dari sini sudah sangat jelas, barang siapa yang mempunyai Rekening Bank, ataupun yang suka mengirimkan uang melalui bank, maka ia secara otomatis telah membutuhkan jaringan komputer.

- Dan masih sangat banyak lagi, contoh-contoh tentang kebutuhan kita terhadap jaringan komputer pada kehidupan sehari-hari.

Seiring dengan berkembangnya jaman, kebutuhan Manusia terhadap Jaringan Komputer semakin besar. Semakin lama, semakin besar. Seolah-olah hampir tidak ada manusia yang tidak membutuhkan Jaringan Komputer, bahkan tidak sedikit orang yang ***Merasa*** dirinya, hidupnya akan kesulitan jika tidak terhubung dengan Jaringan Komputer.

Padahal sesungguhnya seperti yang kita ketahui, bahwa manusia dapat hidup baik-baik saja, dapat hidup dengan lancar tanpa masalah, seandainya tidak ada Jaringan Komputer. Manusia tetap dapat menikmati hidupnya dengan baik. Namun karena seiring berkembangnya jaman, ***Seolah*** Jaringan Komputer itu mampu menghipnotis manusia-manusia, yang dimana diantaranya merasa hidupnya akan mengalami masalah besar jika tidak terhubung dengan Jaringan Komputer.

Apakah Network memudahkan aktifitas Manusia ?

Yap… betul sekali. Dengan kebaredaan Network atau Jaringan Komputer, banyak sekali aktifitas manusia menjadi lebih mudah, cepat, efektif, efisien, low cost, dsb, jika dibandingkan jaman sebelumnya yang tanpa ikut peran jaringan komputer. Berikut beberapa contohnya

- **E-Mail (Surat Menyurat)**

E-mail (Electronic Mail), yang jika kita terjemahkan menjadi bahasa Indonesia maka menjadi SurEl (Surat Elektronik). Konsep E-Mail pertama kali yang mengemukakan adalah Ray Tomlinson sekitar tahun 1971 akhir. E-Mail ini benar-benar jauh lebih banyak keuntungannya dibandingkan surat menyurat. Dimulai dari waktu, silahkan agan hitung, andai saja agan kirim surat ke Amerika, kira-kira membutuhkan berapa hari ? minggu ? bulan ? sangat lama bukan ? setau penulis, kurang lebih membutuhkan 3 bulan. Dengan adanya E-Mail yang dimana Surat yang berbentuk Elektronik tersebut dikirimkan melalui jalur Jaringan Komputer (Internet), hanya membutuhkan waktu kurang lebih 1 detik, sangat cepat, bahkan memungkinkan kurang dari 1 detik. Walaupun email tersebut kita kirimkan dari Indonesia, dengan tujuan ke Amerika. Bagaimana dengan biaya ? gratis bukan ? sepuas apapun kita mengirim E-Mail, tetap tidak bayar, alias gratisss.. tiss… 100% , bagaimana dengan surat menyurat di jaman sekarang ini yang dikirim dari Indonesia

dengan tujuan amerika ? biayanya antara ratusan ribu, sangat mahal bukan ? selain itu mudah sekali cara mengirim surat elektronik, tidak seperti surat menyurat pada umumnya yang dimana kita harus mendatangi kantor POS untuk mengirimkan surat tersebut, kini e-mail cukup di HP sudah bisa kirim e-mail sepuasnya.

- **Berkomunikasi**

Yaitu dengan adanya telpon menelpon menggunakan HandPhone. Jaman dulu, jika orang berkomunikasi yang letaknya berjauhan seperti antara Jakarta dengan Bandung, sesuatu yang merepotkan, menyita banyak waktu, membutuhkan biaya yang tidak sedikit, dsb. Dengan adanya fitur Call atau menelpon yang dimana kita dapat berkomunikasi dengan orang yang letaknya berjauhan, dengan biaya minim, waktu yang minim, dan tidak merepotkan.

- Dan masih banyak lagi contoh-contohnya yang ada pada kehidupan kita sehari-sehari di jaman sekarang ini.

Dijaman sekarang kita ini adalah, dimana jaman hampir segala sesuatu dicampuri peran Jaringan Komputer, contohnya bersosialisasi yang tadinya tidak ada peran Technology, kini dicampuri peran Technology tepatnya yaitu Jaringan Komputer, contohnya seperti Facebook yang disebut sebagai Sosial Media. Transportasi pun, bahkan kita ikut dicampuri peran Jaringan Komputer yang sangat erat, dimulai dari tiket pesawat, tiket kereta, yang tadinya ojek tidak ada peran technology, sehingga kini menjadi Ojek Online, sebagian besar

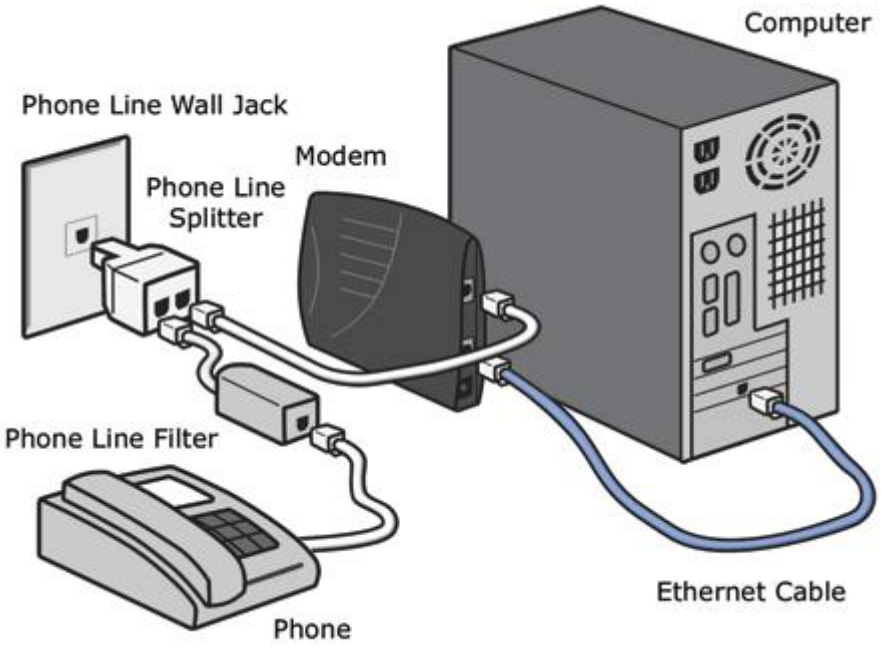
kehidupan kita benar-benar ikut dicampuri peran Jaringan Komputer. Belanja barang-barang yang dulu kita harus 😛 mendatangi tempat seperti mall, ruko, dll kini bisa melalui Online. Dikit-dikit online, apa-apa dibikin online, selamat datang di jaman, dimana di jaman ini hampir serba dikuasai oleh Jaringan Komputer

2. Perkembangan Dunia Jaringan

Pada Materi ini, kita membahas step by step Dunia Jaringan yang terjadi secara REAL pada kehidupan manusia, tapi pada Materi ini kita fokuskan yang terjadi pada Indonesia saja. Yuk kita coba-coba ingat yang terjadi pada Indonesia ini, tentu khususnya pada Perkembangan Dunia Jaringan Komputernya. Disini, kita mulai dari suatu masa yang dimana Internet sudah digunakan untuk masyarakat umum, bukan untuk kalangan tertentu.

Internet masuk ke Indonesia antara tahun 1988 atau sekitar tahun 1990an, namun penulis belum tau pasti tentang tepatnya tahun berapa Internet pertama kali masuk ke Indonesia, dimana pada masa ini kecepatan internet di jaman tersebut, dimulai dari kecepatan 1200 Bps, lalu 14.4 KBps, lalu 1.5 MB, hingga 2 MBps.

Antara tahun 1990an hingga 2000an, dimana adalah awal-awalnya Internet mulai digunakan masyarakat umum Indonesia, namun tentu penggunanya masih sedikit selesai, tahun 2000an keatas, pengguna Internet Masyarakat di Indonesia sudah mulai banyak jumlahnya.



Masih ingat gambar ini ? Yap… pada masa awal-awal Internet mulai nge-trend digunakan di Indonesia adalah, menggunakan jalur kabel telepon agar bisa Internetan. Seseorang jika ingin memasang Internet, maka ia harus mempunyai jalur kabel telepon di rumahnya terlebih dahulu. Ini adalah dimana masa-masa Handphone belum ada Web Browsernya, di jaman itu HandPhone belum bisa mengakses Internet. Di jaman ini, kita bisa mengakses internet ***hanya*** jika di depan komputer saja, jika kita keluar rumah, atau beraktifitas, maka kita dalam keadaan tidak terhubung dengan Internet. Dijaman ini, Internet masih mahal sekali, ribet, tidak fleksibel, kecepatannya benar-benar lambat, bahkan untuk mengakses halaman google aja memakan waktu yang tidak sebentar seperti sekarang. Di jaman ini, komputer masih berbentuk seperti ini :

Pada jaman itu, seseorang membutuhkan biaya investasi atau modal yang besar untuk dapat mengakses internet, seperti punya telepon, jalur kabel telepon, komputer, biaya bulanan listrik yang lumayan, meja komputer, dan masih banyak lagi. Dijaman itu, memang hanya orang-orang yang mempunyai finansial baik saja yang dapat mengakses Internet. Beda dengan jaman sekarang, yang dimana orang jika mengakses internet, sudah benar-benar low cost, bahkan tanpa modal sekalipun, yaitu seseorang cukup mendatangi warnet, maka ia sudah dapet mengakses sepuasnya dengan dibatasi waktu tertentu. Andai saja seseorang ingin meng-invest untuk dirinya agar bisa dapat mengakses internet, maka cukup membeli handphone seharga 350 - 500rban, kartu SIM Card, dan pulsa sekitar 50rban untuk membeli kuota. Maka ia sudah dapat terhubung dengan Internet, kapanpun, dimanapun, dan sedang apapun 😊 . Sekarang, Komputer sudah dapat disimpan didalam saku celana, maupun saku baju, ia dapat menyala tanpa harus mencolokkannya ke listrik, dapat dibawa kemana-mana, dapat digunakan dimana-dimana, sangat flexible.. yaitu Smartphone.

Yap.. kenapa SmartPhone ? apa bedanya Komputer dengan SmartPhone ? hampir gak ada bedanya…, sama-sama memiliki OS, sama-sama memiliki Processor, sama-sama memiliki RAM, sama-sama memiliki tempat penyimpanan Data, sama-sama bisa mengakses Internet, sama-sama bisa membuat document, iya kan ? hampir tidak ada bedanya.

Kini dijaman sekarang ini, seseorang yang ingin terhubung dengan Internet atau Jaringan Komputer itu sudah berubah drastis, menjadi sangat mudah, siapapun bisa mengaksesnya, biayanya rendah, dimanapun & kapanpun. Sangat jauh sekali dijaman 2000an keatas, dimasa internet baru-baru digunakan masyarakat Indonesia dimana pada masa itu harus lewat jalur kabel telepon, sekarang tidak butuh seribet itu, sangat simple, cukup beli SIM Card dapat dibeli dimanapun, beli Pulsa dapat dibeli dimanapun, tinggal dibelikan kuota dari Pulsa tersebut, maka orang itu sudah terhubung dengan Internet.

3. LAN, MAN & WAN

LAN yang merupakan singkatan dari Local Area Network, WAN yang merupakan singkatan dari Wide Area Network, keduanya adalah merupakan jenis dari Jaringan. Kedua jenis jaringan tersebut tentu berbeda dalam banyak hal, namun memiliki hal yang sama yaitu menghubungkan atau mengkoneksikan antara satu dengan yang lainnya. Jika LAN adalah menghubungkan perangkat 1 dengan yang lainnya, Maka WAN menghubungkan antara suatu Negara, dengan Negara yang lainnya.

Apa itu LAN ?

LAN adalah sebuah jaringan komputer yang memungkinkan 2 perangkat atau lebih yang dalam keadaan berdekatan, yang bertujuan untuk saling terhubung & berkomunikasi. LAN ini terdiri dari perangkat-perangkat yang ada pada keseharian manusia pada umumnya, diantaranya seperti Komputer, Laptop, Printer, SmartPhone, Modem, Router, Switch, Hub, dsb. Fungsi dari LAN ini adalah sebagaimana fungsi dari Jaringan Komputer, yaitu untuk memudahkan pekerjaan manusia, meminimalisir waktu yang terbuang, meminimalisir pengeluaran biaya, dsb, hanya saja dalam lingkup berdekatan.

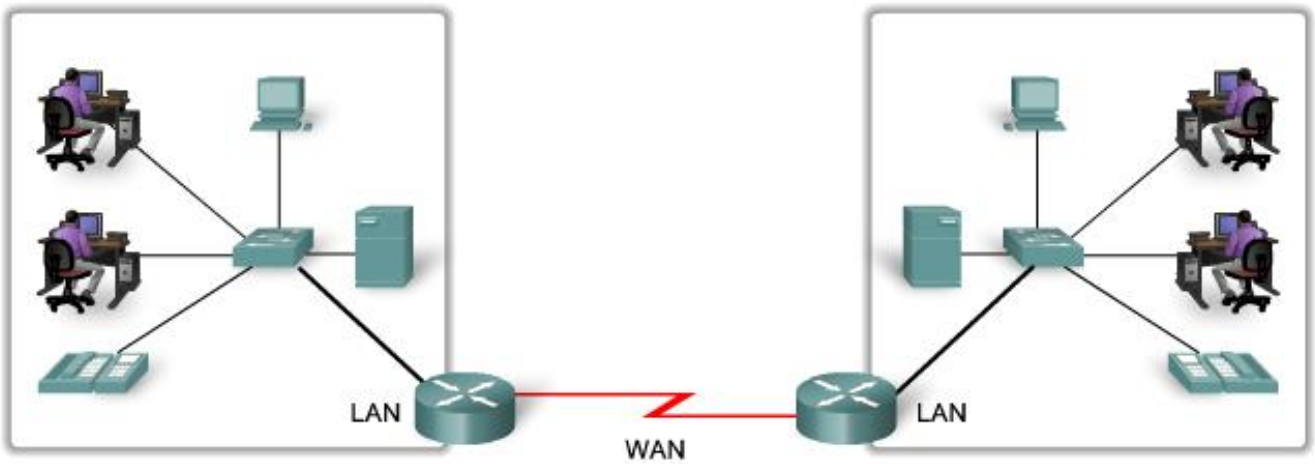
Contohnya seperti Jaringan LAN di Perkantoran yang berfungsi sebagai sarana untuk bertukar laporan, informasi, document atau data dari orang satu ke yang lainnya, yang dimana dengan adanya LAN ini dapat meminimalisir tenaga yang dibutuhkan, waktu, cost, dan masih banyak lagi keuntungan dengan adanya LAN pada kantor tersebut.

LAN ini dibangun menggunakan peralatan atau perangkat yang sederhana, yang mudah kita temui di banyak toko komputer pada umumnya, yaitu seperti Kabel UTP (Unshielded Twisted-Pair) untuk menghubungkan antara perangkat satu dengan yang lainnya, atau secara WLAN (Wireless Local Area Network) yang dimana di jaringan ini, dibangun menggunakan nirkabel, jaringan ini banyak kita temui seperti di café, restoran, dsb. Perangkatnya pun sederhana dan tergolong murah, perangkat yang kita gunakan tidak perlu High Technology & High Specs, yang dimana harganya sangat mahal. Contohnya perangkatnya seperti Hub, Switch, Modem, Router, kabel UTP yang terjangkau harga per meternya, yang memang perangkat tersebut khusus digunakan hanya untuk LAN saja. Dan WLAN, menggunakan Modem, Router, atau Access Point yang terdapat perangkat Antenna Wireless nya.

Apa itu WAN ?

WAN adalah sebuah jaringan komputer yang memungkinkan 2 perangkat atau lebih yang dalam keadaan tidak berdekatan atau berjauhan, yang bertujuan untuk saling terhubung & berkomunikasi. WAN ini dapat kita katakan sebagai Internet. Contohnya adalah seperti sebuah perusahaan multi nasional, yang dimana di perusahaan tersebut ada di Negara Indonesia dan Jepang. Komputer-komputer milik karyawan yang berada di kantor Indonesia, membutuhkan untuk saling terhubung, berkomunikasi, yang digunakan untuk

LANs separated by geographic distance are connected by a network known as a Wide Area Network (WAN).



mengirim document dengan komputer-komputer karyawan yang berada di kantor Jepang. Ini adalah salah satu tujuan, dan fungsi dari WAN.

Dari gambar ini bisa kita lihat, bahwa WAN itu terdiri dari LAN. Diantaranya, hal ini bisa kita analogikan dengan cerita yang ada sebelumnya, yaitu perusahaan multi nasional yang berada di Indonesia dan di Jepang. Jaringan LAN kantor di Indonesia, terhubung dengan Jaringan LAN kantor yang di Jepang, melalui jalur WAN atau Internet. Hal ini membuktikan, bahwa WAN itu terdiri dari sebuah kumpulan LAN-LAN yang saling dapat terhubung dan dapat berkomunikasi.

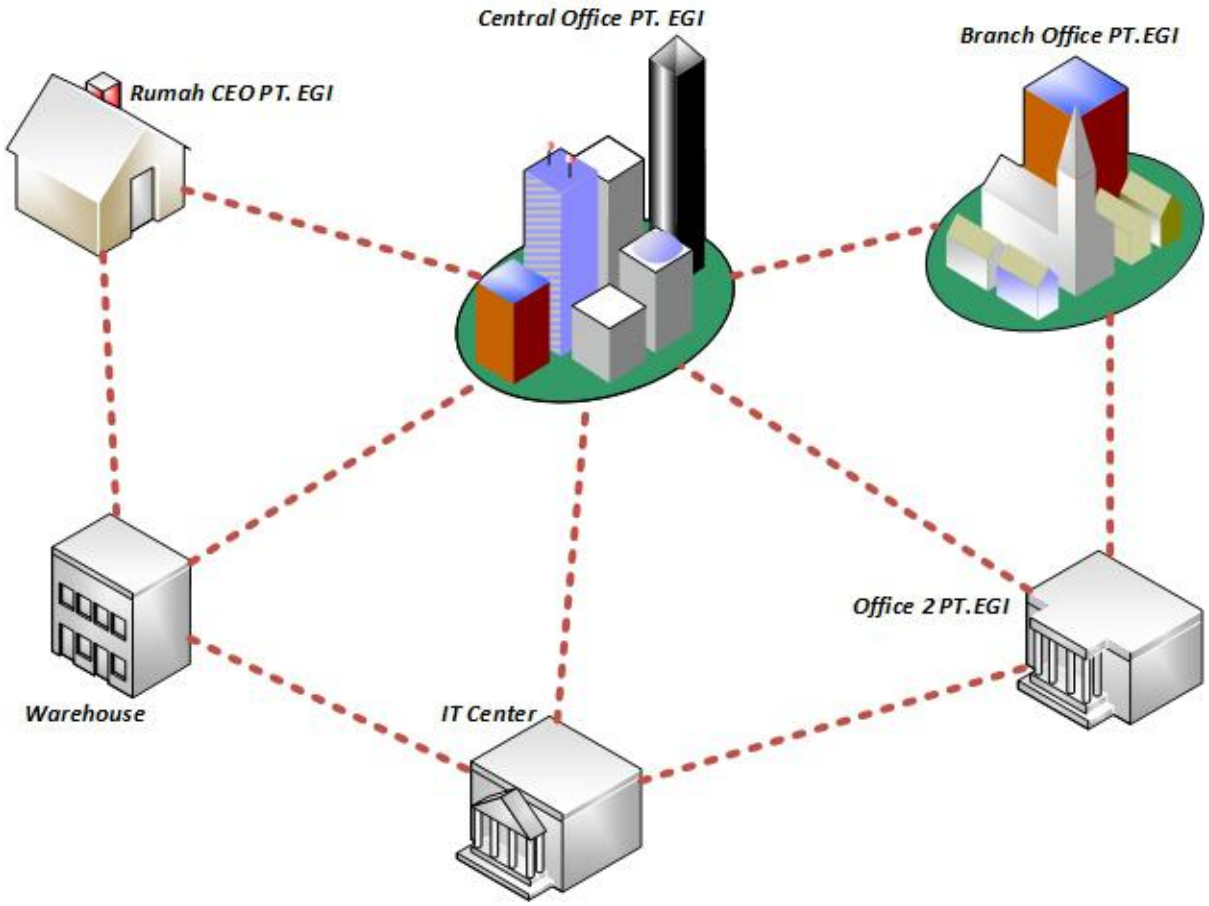
LAN vs WAN

Berikut tabel antara LAN vs WAN :

	LAN	WAN
Kemacetan Koneksi Yang Terjadi	Rendah	Tinggi
Biaya Perawatan	Mudah dan Murah	Sulit dan Mahal
Bandwidth	Bandwidth yang tersedia tinggi untuk melakukan transmisi	Bandwidth yang tersedia rendah untuk melakukan transmisi
Biaya Setup	Pada umumnya, untuk membangun LAN itu Mudah & Murah. Namun tergantung dari besar luasnya LAN yang ingin dibangun, semakin besar maka semakin sulit dan mahal	Jika sekedar ingin terhubung dengan WAN, maka sangat mudah dan murah. Namun jika ingin membangun WAN, maka sulit dan butuh biaya yang besar.
Hak Kepemilikan	Pada umumnya dikuasai, dimiliki dan dikelola oleh	WAN atau Internet tidak yang memiliki, tidak ada

	perorangan atau suatu organisasi.	yang menguasainya, dan tidak di kelola oleh siapa pun.
Area yang dapat dijangkau	Terbatas, hanya lokal saja. Seperti jaringan di rumah, kantor, dsb.	Tidak terbatas, dapat menjangkau jarak yang sangat jauh, seperti antara Indonesia – Amerika.
Kecepatan Koneksi	Cukup Tinggi, sekitar 1GBps (tergantung Port Interface yang digunakan, semisal Fast Ethernet maka 100MBps, Gigabit Ethernet maka 1GBps, dan Ethernet maka 10MBps	Rendah, berkisar 150MBps (Tergantung Port Interface yang digunakan)
Technology	Diantaranya adalah Ethernet, Token Ring, dsb.	Diantaranya adalah MPLS, ATM, Frame Relay, X.25, dsb.
Permasalahan yang terjadi	Kecil, dan tidak sulit menanganinya	Besar, dan sulit menanganinya
Komponen	L2 Operation Devices, L1 Operation Devices	L3 Operation Devices, L2 Operation Devices

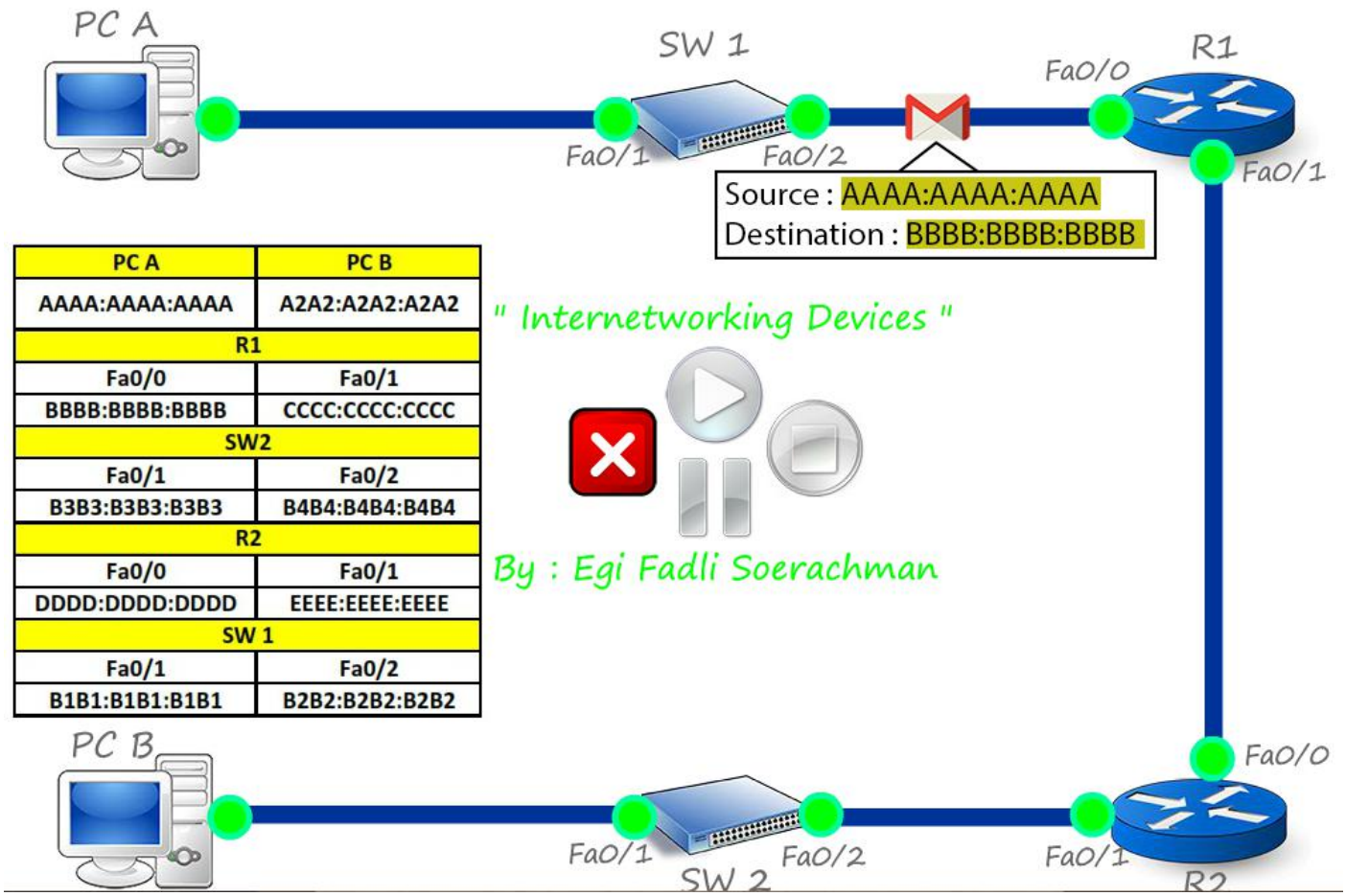
Apa sih MAN itu ?



MAN yang merupakan singkatan dari Metropolitan Area Network adalah sebuah Area Network yang mirip dengan LAN, tetapi jangkauannya mencakup perkotaan. Atau MAN adalah sebuah jaringan komputer yang lebih luas dari LAN namun lebih kecil dari WAN. Mekanisme cara kerja MAN ini mirip, sebagaimana cara kerja pada ISP (Internet Service Provider). MAN ini terbentuk dari beberapa gabungan Jaringan LAN yang saling terhubung, atau berkomunikasi (InterConnects).

Contohnya bisa kita lihat pada gambar diatas, disitu ada beberapa gedung yang terhubung. Dan pusat InterConnections tersebut adalah Central Office, ini menandakan bahwa Central Office adalah yang menyediakan layanan, kepada gedung-gedung atau rumah yang terhubung dengannya secara MAN. Dan pada gambar ini, semua gedung dan rumah tersebut adalah sama-sama milik PT.EGI.

4. Infrastructure Components



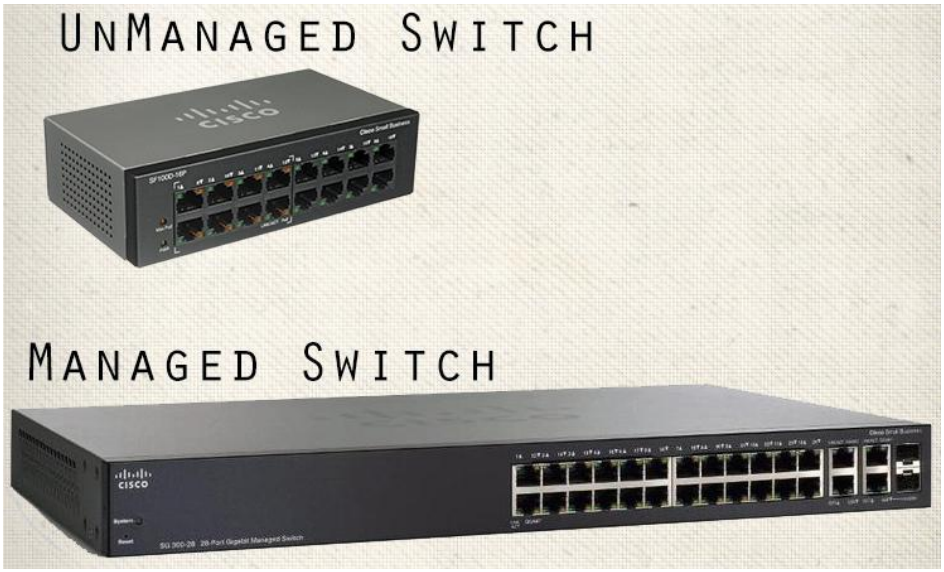
PC A	PC B
AAAA:AAAA:AAAA	A2A2:A2A2:A2A2
R1	
Fa0/0	Fa0/1
BBBB:BBBB:BBBB	CCCC:CCCC:CCCC
SW2	
Fa0/1	Fa0/2
B3B3:B3B3:B3B3	B4B4:B4B4:B4B4
R2	
Fa0/0	Fa0/1
DDDD:DDDD:DDDD	EEEE:EEEE:EEEE
SW 1	
Fa0/1	Fa0/2
B1B1:B1B1:B1B1	B2B2:B2B2:B2B2

Pada Internetworking Devices ini, kita berfokus kepada memahami tentang apa yang dilakukan antar perangkat di dalam jaringan atau memahami tentang komunikasi antar perangkat di jaringan. Contohnya seperti perangkat Hub, Switch, Router, dsb.

Apa sih Switch itu ?

Switch adalah sebuah perangkat sebagai yang menghubungkan perangkat-perangkat (contohnya seperti komputer, printer, dsb) yang bertujuan untuk membuat suatu jaringan, topologi, atau menghubungkan ke perangkat lainnya (LAN atau dalam Network yang sama). Atau bisa juga Switch disebut sebagai perantara yang menghubungkan perangkat satu, dengan perangkat yang lainnya dalam Network yang sama. Switch, ada juga yang menyebutankannya dengan nama lain, yaitu Intelligent Hubs.

Switch terbagi menjadi 2 jenis, yaitu UnManageable Switch dan Manageable Switch, atau ada yang menyebutkannya dengan UnManaged Switch dan Managed Switch.



≈ *UnManaged Switch*

Apa itu UnManaged Switch ? yaitu sebuah Switch yang dimana kita tidak dapat mengkonfigurasikannya / di setting. Switch pada jenis ini, yang kita lakukan hanyalah tinggal menyolokan Port dan tinggal menyalakannya. Tidak perlu penyesuaian apapun yang kita lakukan, atau simplenya adalah " Plug and Play ". Switch pada jenis ini, sering kita temukan dibanyak toko-toko asesoris komputer baik toko kecil hingga toko besar. Switch jenis ini, sangatlah mudah kita temukan di banyak toko. Merknya pun beragam, seperti TP-Link, D-Link, Cisco, Netgear, dsb. UnManaged Switch harganya tergolong murah untuk perangkat jaringan, yaitu berkisar kurang lebih 100 ribu – 1 Jutaan Rupiah. Switch jenis ini hanya kita temukan pada Jaringan berskala kecil hingga sedang saja. Seperti pada rumahan, SOHO, bisnis berskala kecil, dan yang pasti berada pada End User. Yang **Pasti** Switch jenis ini tidak akan harganya menyaingi atau lebih mahal dari Managed Switch. Switch ini tidak akan kita temui di jaringan berskala besar apalagi di jaringan raksasa, karena memang Switch ini tidak dirancang untuk Traffic yang besar. Sederhananya Switch ini **Hanya** kita temukan pada LAN tidak mungkin pada WAN. Switch jenis ini tidak menggunakan OS (Operating System), selayaknya Managed Switch dan juga tidak secanggih selayaknya Managed Switch.

≈ *Managed Switch*

Apa itu Managed Switch ? yaitu sebuah Switch yang dapat dikonfigurasikan atau di setting sesuai dengan kebutuhan kita maupun yang seperti kita inginkan. Switch ini juga bisa kita gunakan tanpa ada ubahan / setting / konfigurasi apapun, alias Plug and Play, tetapi jika ada Switch Manageable digunakan tanpa adanya konfigurasi sama sekali, maka Switch ini akan bekerja selayaknya UnManaged Switch. Switch jenis ini tidak mudah ditemukan pada Toko-toko komputer seperti biasanya. Switch jenis ini, harganya tergolong mahal hingga sangat mahal, yaitu berkisar kurang lebih dari 7 jutaan – hingga 400 jutaan. Pemain merknya adalah yaitu HP, Cisco, Force10 (dell), dll. Switch jenis ini bisa kita temukan jaringan berskala sedang hingga besar maupun raksasa. Switch ini bisa kita temukan pada, ISP, Jaringan Pusat Bank, Jaringan Perusahaan raksasa seperti Facebook, Google, dan tentunya bisnis yang berskala besar. Switch ini selayaknya komputer, ia memiliki OS (Operating System), RAM, Processors, Tempat penyimpanan data, dsb. Pada Switch ini memang jauh lebih canggih jika dibandingkan dengan UnManaged Switch. Namun meski begitu, orang yang mengoperasikannya atau mengkonfigurasinya yang profesinya disebut sebagai " Network Engineer ", tidak bisa sembarang orang dapat mengoperasikannya. Butuh banyak belajar tentang ilmu Switching, yang memang Switch jenis ini sudah seharusnya dioperasikan kepada ahlinya saja, tidak hanya itu, untuk menggunakan Jasa mereka, yang mempunyai keahlian dalam ilmu Switching, bayarannya pun tidak murah.

Apa sih Hub itu ?

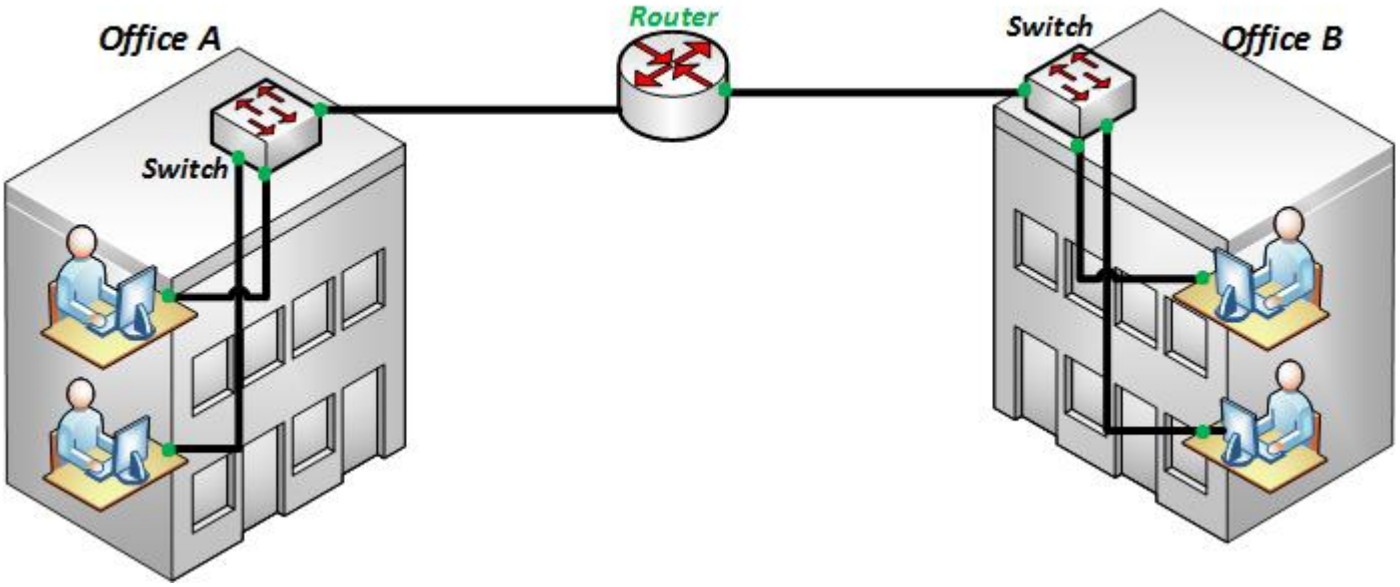
Apa sih Hub itu ? Hub mempunyai pengertian yang HAMPIR sama dengan Switch, yaitu sebagai perangkat yang menghubungkan perangkat yang satu, dengan yang lainnya. Atau Hub adalah penghubung perangkat pada segmen (*Baca : Network) yang sama pada LAN. Pada beberapa produk yang pernah penulis lihat, terdapat jenis produk yang dipasaran bernama " Switch-Hub " sesungguhnya produk itu bukanlah Switch, melainkan Hub. Hingga sekarang pun, penulis *belum mengetahui jawabannya dengan pasti,* mengapa pabrikan atau produsen menamakannya dengan " Switch-Hub ", padahal antara Switch dan Hub sangatlah berbeda, hampir tidak ada persamaannya. Ada yang mengatakan juga bahwa hub dikenal juga sebagai Repeater, karena diantara keduanya cara kerja dan konsepnya sangatlah mirip.

Yang membedakan antara Switch dan Hub adalah, Hub selalu mem-broadcast setiap Packet Data yang diterimanya. Karena Hub termasuk perangkat yang bodoh. Yang tidak dapat berpikir. Hub, hanya bekerja pada Layer 1. Hub tidak dapet mengenal MAC Address yang dapat digunakan Mapping Device seperti pada Switch.

Apa sih Router itu ?

Router adalah sebuah perangkat yang menghubungkan 2 jaringan berbeda atau lebih. Router dapat menentukan " Rute " yang akan dilalui oleh Paket Data tersebut, berdasarkan Routing Protocol yang digunakan. Router ini dapat kita temui baik itu pada jaringan kecil, sedang, besar, hingga raksasa. Dapat juga kita temui baik itu LAN maupun pada WAN. Contoh penggunaannya pada LAN adalah seperti berikut ini :

Bisa kita lihat pada gambar di atas, di situ terdapat 2 gedung kantor, yaitu Office A dan Office B. Antara kedua kantor itu posisinya dalam berdekatan. Karyawan yang berada di



Office A, ingin melakukan komunikasi secara audio dan Video dengan karyawan yang berada di Office B. Maka Router lah yang bertugas menghubungkan antara 2 jaringan yang berbeda

pada gedung-gedung tersebut, dan tugas switch adalah menghubungkan perangkat-perangkat yang ada di gedung tersebut.

Apa sih Firewall itu ?

Firewall ini, adalah sebuah perangkat keamanan jaringan yang bertugas memantau lalu lintas jaringan yang masuk dan keluar. Dan juga yang membuat keputusan apakah akan mengizinkan atau memblokir lalu lintas tertentu berdasarkan ***Rules*** yang diterapkan pada Firewall tersebut. **(Note : Rules = Sebuah aturan yang telah dibuat dan diatur oleh Security Engineer atau Network Security Engineer pada Firewall).* Firewall, pada umumnya dapat bekerja pada hampir semua layer, seperti layer 3, 4, 7, dsb (tergantung jenis firewallnya).

Firewall ini hampir yang selalu dijadikan *First Line* dalam pertahanan dari serangan-serangan di Jaringan. Konsep ini telah diterapkan lebih dari 25 tahun, hingga sekarang pun tidak berubah. Pada firewall kita juga bisa menerapkan *Trusted* dan *Untrusted Network*, yang dimana *Trusted Network* dapat memiliki akses jaringan yang bebas tanpa batas, sedangkan *Untrusted Network* memiliki akses jaringan yang sangat terbatas dan juga selalu di awasi.

Firewall ini, aslinya adalah sebuah hardware bukan software seperti yang ada pada Windows Desktop contohnya. Namun dijaman sekarang ini, sistem keamanan sudah dalam 3 bentuk. Yaitu Hardware, Software dan juga keduanya.

Firewall terdapat banyak jenisnya, berikut diantaranya :

Proxy Firewall

Proxy Firewall adalah sebuah perangkat yang digunakan sebagai gateway dari satu jaringan ke yang lain untuk pengaplikasian tertentu (bisa secara spesifik, sesuai yang diinginkan / dibutuhkan). Tentu, Proxy Firewall ini masuk sebagai kategori perangkat Network Security. Dan juga, jenis proxy firewall inilah yang paling powerfull diantara jenis Firewall yang lainnya.

Nah, apa saja yang bisa di proteksi oleh Proxy Firewall ini ? Proxy Firewall ini, sangat berurusan dengan proteksi pada Layer 7 *(melakukan filtering packet data pada Layer 7).* Contohnya adalah, seperti filtering pada protocol HTTP, FTP, dsb. Jenis keamanan ini dapat dipadukan dengan Proxy Servers yang berfungsi sebagai seperti *Content Caching*. Meski begitu, kekurangan sistem keamanan pada Proxy, dapat mengurangi perfoma pada *Throughput* dan juga tidak semua aplikasi yang berkomunikasi pada L7 support komunikasi yang diperantarai oleh Proxy, inilah kendalanya.

Proxy Firewall ini dikatakan powerfull, diantaranya karena dapat mencegah koneksi secara langsung dari luar *(Direct Connection).* Sehingga, dapat mencegah terjadinya serangan langsung dari outside network ke internal network. Analoginya, seperti ada paket datang yang ditunjukkan untuk big boss. Namun, sebelum paket itu sampai ke boss, diperiksa dulu oleh bagian security. Apakah paket tersebut aman ? Jika aman, maka akan dilanjutkan,

disampaikan ke boss. Jika tidak, maka akan di reject. Sehingga, mencegah terjadinya serangan langsung kepada big boss tersebut.

Proxy Firewall, juga dapat dipadukan dengan mesin Anti Virus untuk menangani permasalahan pada virus, threat, dsb. Sehingga pada client tidak memerlukan lagi mesin Anti Virus untuk memproteksi PCnya dari serangan yang berasal dari Network. Namun, ada juga Device Firewall yang didalamnya sudah terdapat mesin Anti Virus.

Apa sih Access Point itu ?

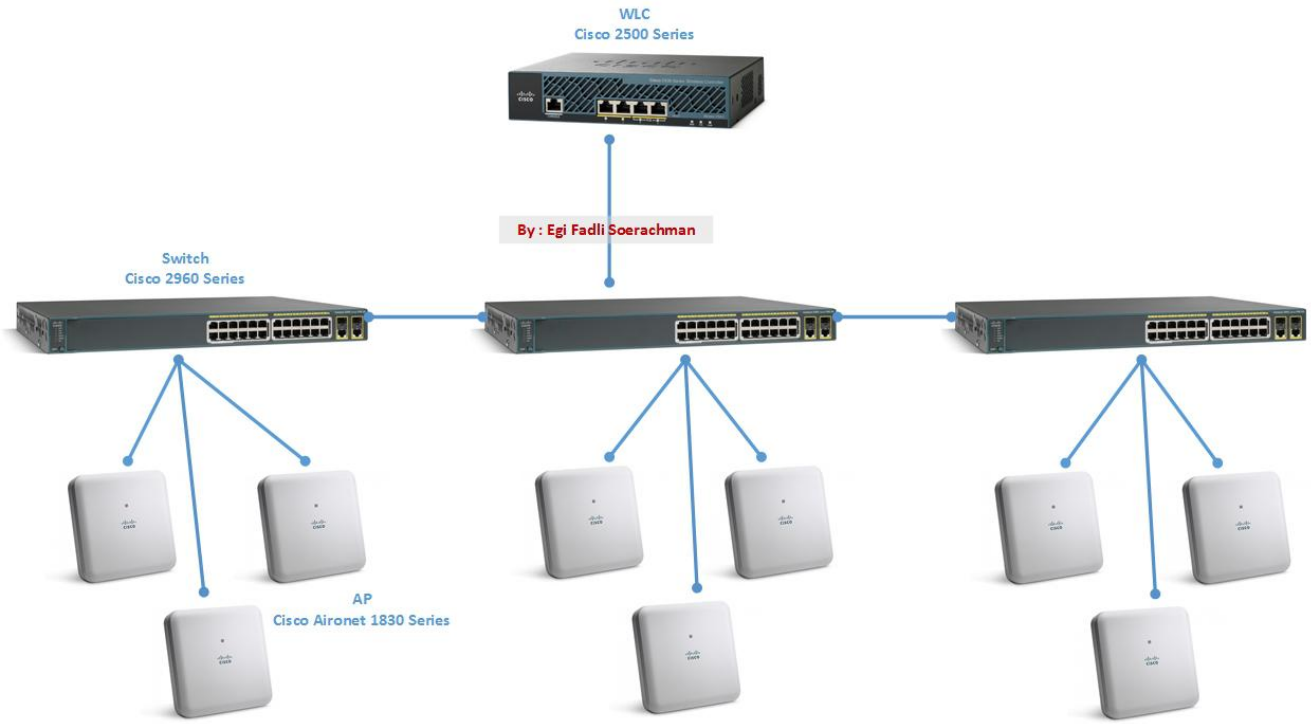
Yang harus bener-bener anda ingat adalah, bahwa Access Point bukanlah Router. Dan Router bukanlah Access Point. Antara Router dan Access Point sangatlah berbeda. Tentang definisi apa itu router ? kita sudah membaca di subbab sebelumnya. Lalu apa itu Wireless Access Point ? Access Point ini adalah sebuah perangkat yang berfungsi memancarkan sinyal WiFi. Access Point juga berfungsi sebagai *Transmitter* dan *Receiver* sinyal radio Wireless yang dipancarkannya. Jadi, sederhananya adalah Access Point itu pemancar sinyal WiFi.

Apakah ada, sebuah perangkat yang berfungsi memancarkan sinyal radio wifi namun sekaligus router ? Ada.. namun perangkat tersebut tidak bisa disebut sebagai Access Point. Bisa saja disebut sebagai router. Contohnya ? Yaitu HP Smartphone. Pada Smartphone jaman sekarang memiliki feature Hotspot. Yang berfungsi sharing koneksi, dari jalur data broadband di share melalui hotspot. Ini artinya, Smartphone tersebut berfungsi sebagai router karena telah menghubungkan 2 jaringan yang berbeda.

Apa itu Wireless Controllers ?

Wireless Controllers atau yang biasa disingkat dengan WLC, adalah sebuah perangkat yang me-*manage* Access Point dalam jumlah yang banyak. WLC juga sebagai pusatnya dalam hal *management* dan *configuration* Access Point. Misal, di sebuah perusahaan kita membangun jaringan wireless, dengan jumlah AP yang sangat banyak, yaitu 300 AP. Access Point sebanyak 300 itu, langsung pasang aja, langsung dihubungkan ke jaringan, tidak perlu kita config dan manage. Configuration dan Management, kita lakukan secara terpusat di WLC. Sangat memudahkan pekerjaan kita bukan ?

Bagaimana contoh topologinya ? berikut saya gambarin.



Ini adalah contoh sederhana pada topologi WLC yang digunakan di lapangan. Access Point, terhubung dengan Switch PoE, lalu Switch PoE tersebut terhubung dengan WLC. Dan tentu, semua itu menggunakan Cabling.

5. Network Protocols and Communications

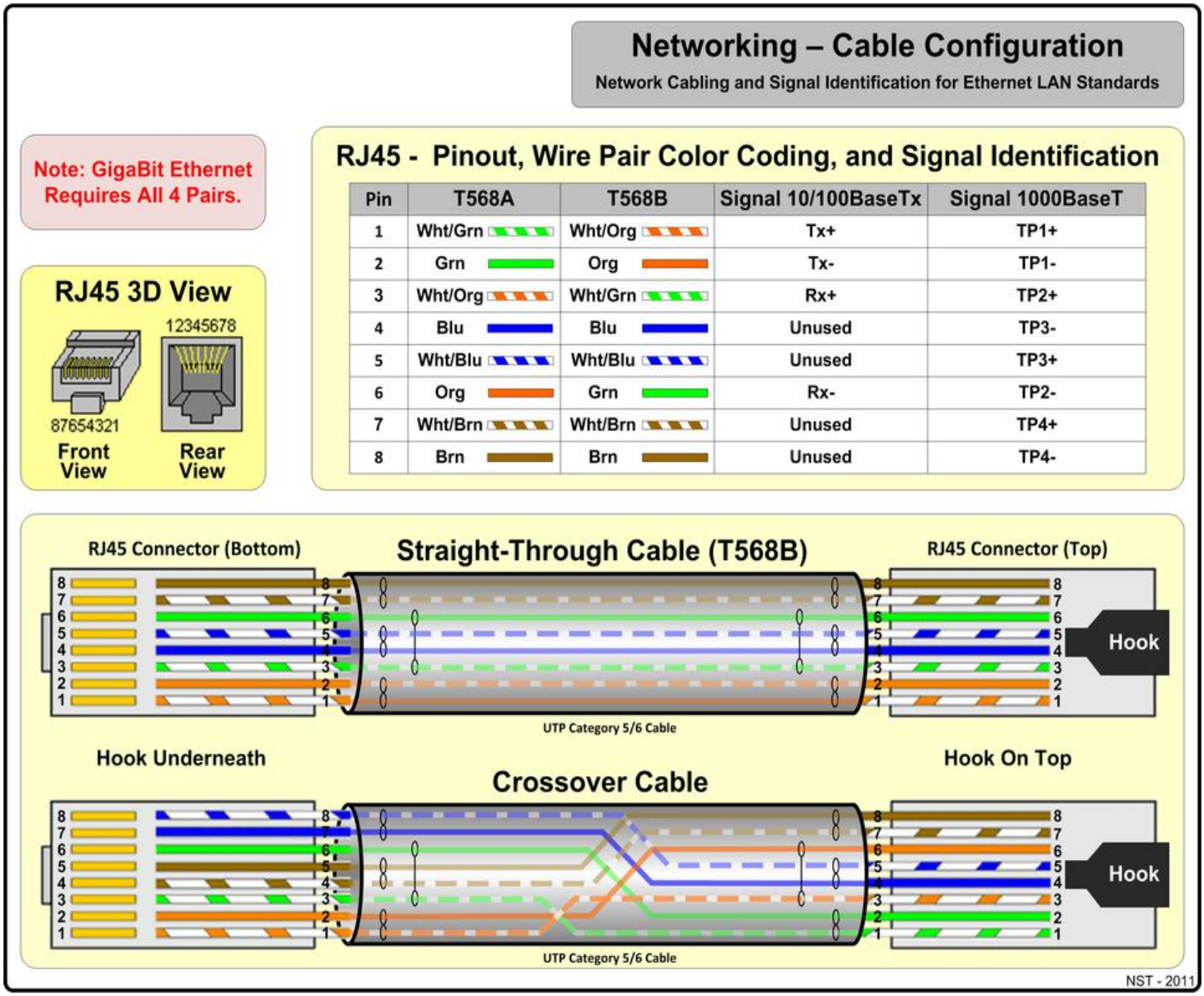
Apa itu Protocol ?

(Definisi ke 1) Protokol adalah sebuah kumpulan aturan dan pedoman untuk komunikasi data. Aturan yang ditetapkan / didefiniskan adalah untuk setiap langkah dan proses selama komunikasi antara dua atau lebih komputer. Apa tujuan dari aturan-aturan yang ada di protocol ? yaitu untuk keberhasilan, kelancaran, komunikasi pada data.

(Definisi ke 2) Protocol adalah sebuah kumpulan aturan yang memungkinkan dua perangkat untuk menghubungkan dan mengirimkan data satu sama lain. Protokol menentukan bagaimana data yang ditransmisikan antara perangkat komputasi melalui jaringan. Protocol dapat mendefinisikan masalah seperti error control dan metode data compression. Protokol menentukan berikut:

- jenis pengecekan error yang akan digunakan
- metode kompresi data (jika ada)
- bagaimana caranya tentang perangkat pengirim menunjukkan bahwa ia telah selesai mengirimkan pesannya dan bagaimana perangkat penerima menunjukkan bahwa ia telah menerima pesannya.

Contoh dari Protokol : TCP / IP (Transfer Control Protocol / Internet Protocol), HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), dan SMTP (Simple Mail Transfer Protocol), dan sebagainya.



6. Network Access

Gambar diatas adalah gambaran yang lengkap , tentang penjelasan T568A dan T568B pada kabel UTP (RJ45) Cross dan Straight dan juga fungsi di tiap nomor kabel tersebut, baik itu yang menggunakan jenis Port Interface Signal 10/100 Base Tx maupun Signal 1000 Base T.

Pada gambar diatas terdapat pengertian tentang kegunaan atau fungsi dari warna kabel 1 – 8 yang digunakan untuk jalur Rx (Receiving) dan Tx (Transmitting) hanyalah 1, 2, 3, dan 6. Sedangkan pengertian + atau – adalah arus listrik seperti halnya pada baterai terdapat + dan – . Nah, Port Interface yang hanya menggunakan 1 , 2, 3 dan 6 adalah jenis Port Interface 10/100 Base Tx atau sederhananya adalah Interface Ethernet yang

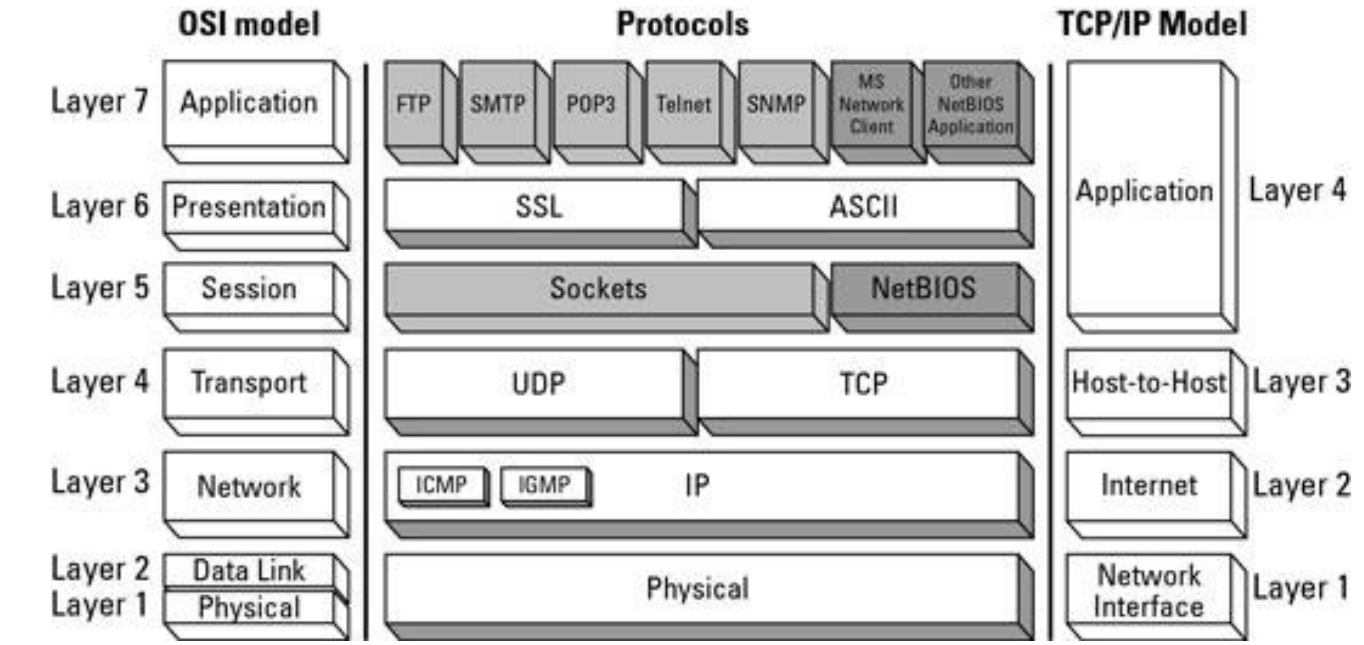
berkecapatan 10 Mbps dan 100 Mbps. Lalu apa kegunaan kabel yang bernomor 4 , 5, 7 dan 8 ? kabel ini tidak digunakan untuk komunikasi sebagai kabel bernomor 1, 2, 3 & 6, tapi digunakan untuk PoE , yaitu untuk mengaliri arus listrik (Power), seperti untuk menyalakan lampu kedap kedip pada interface, menyalakan perangkat, dsb. Tetapi meskipun kabel bagian 4, 5, 7 & 8 tidak digunakan untuk PoE maka statusnya akan " unused ", namum penulis menyarankan baiknya meskipun "unused" tetap dipasang, jadi dibiarkan tetap ada 8 kabel sebagaimana semestinya.

Dan pada Interface Gigabit Ethernet (1000BaseT) atau yang berkecepatan 1 Gbps / 1000 Mbps kabel dari 1 – 8 tersebut digunakan semua untuk jalur koneksi alias digunakan untuk komunikasi, tidak ada PoE atau yang digunakan untuk Power sebagaimana 10/100BaseTx. Tiap " TP (Twisted Pair) " atau tiap satu Tx Rx memiliki kecepatan 250Mbps sedangkan jumlah " TP " (Twisted Pair) atau Tx Rx tersebut memiliki 4. Maka kecepatannya adalah 250Mbps x 4 = 1 Gbps.

Berikut jenis-jenis kabel pada jaringan dan interfacenya :

Optical Terminations	Copper Terminations	GBICs
ST (Straight Tip)	RJ-45	1000Base-SX/LX
SC (Subscriber Connector)	RJ-11	1000Base-T
LC (Local Connector)	RJ-21 (25-pair)	Cisco GigaStack
MT-RJ	DE-9 (Female)	1000Base-SX/LX SFP
Wireless Antennas		
RP-TNC	DB-25 (Male)	1000Base-T SFP
RP-SMA	DB-60 (Male)	X2 (10Gig)

7. Compare OSI Layer vs TCP IP



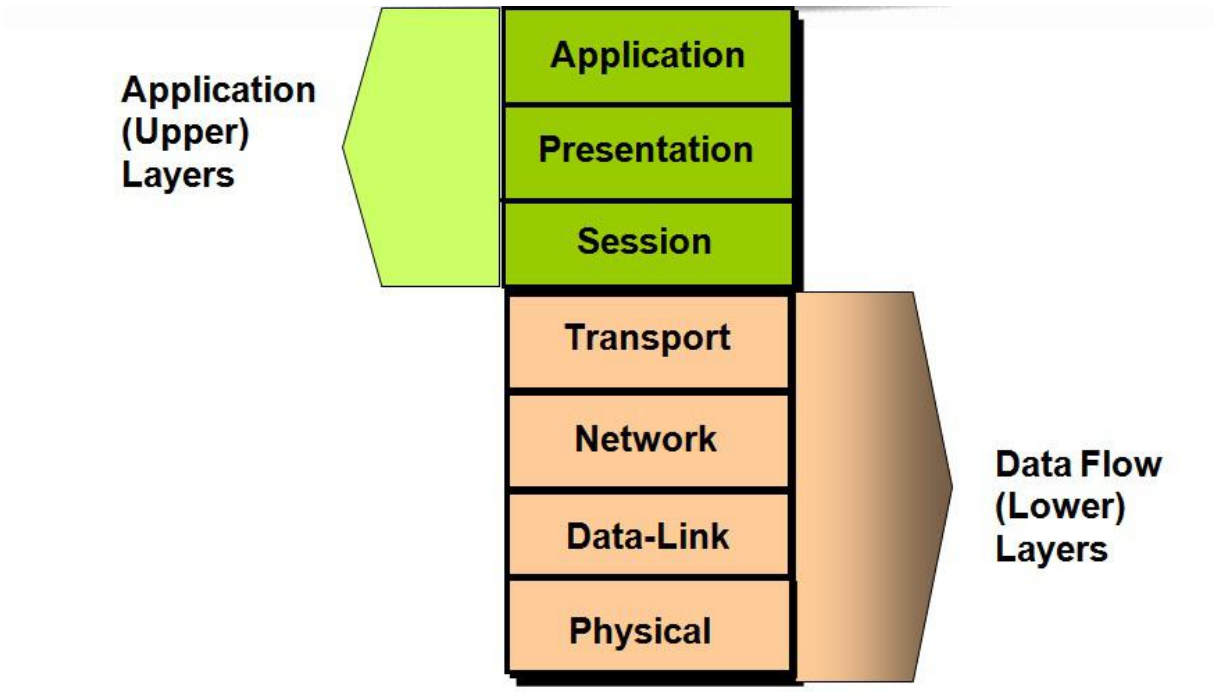
➢ *OSI Layer*

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP		GATEWAY	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP		Can be used on all layers	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card —— Switch —— NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch** **Bridge** **WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

Apa itu OSI Layer / OSI Model ? OSI kepanjangan dari Open System Interconnection, yaitu sebuah model konsep atau sebuah logika yang men-definisikan tentang kominikasi jaringan komputer. OSI digunakan oleh sebuah sistem terbuka (Open) untuk interkoneksi dan komunikasi dengan sistem yang lainnya.

Model ini terbagi menjadi 7 lapisan, yaitu Application, Presentation, Session, Transport, Network, Data-Link dan Physical yang dimana masing-masing lapisan tersebut mewakili sebuah kumpulan Konsep layanan (Conceptual of Services). OSI Model ini dapat mendeskripsikan tentang Komunikasi Packet Data Computer menggunakan Lapisan Protocol yang berbeda dengan efektif. OSI Layer ini terbagi menjadi dua Porsi yaitu Upper Layer dan Lower Layer.



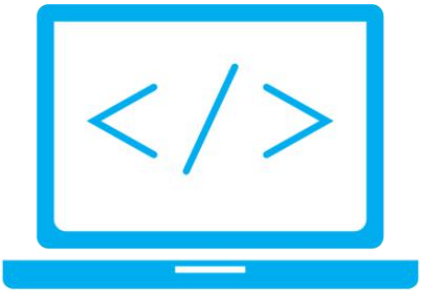
Open System Interconnection atau OSI. OSI diciptakan oleh International Organization for Standarization atau ISO. Dahulu sebelum OSI Layer ditetapkan, perangkat komunikasi tidak dapat saling berkomunikasi pada vendor yang berbeda. Contoh seperti perangkat komunikasi IBM, tidak dapat berkomunikasi dengan vendor lain, maka dari itu ISO membuat OSI sebagai standar komunikasi dalam jaringan komputer. OSI adalah kerangka

logika terstruktur bagaimana proses / menggambarkan komunikasi data berinteraksi melalui jaringan.

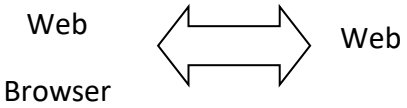
Cara singkat menghapal setiap lapisan OSI adalah dengan singkatan APeS Te eN DePe

- Lapisan Upper fokus di aplikasi pengguna dan bagaimana file di presentasikan di komputer.
- Lapisan Lower adalah intisari komunikasi data melalui jaringan, dan bagian ini menjadi perhatian utama oleh para Network Engineer untuk seorang yang berkutat di jaringan better focus di lower layer ini.

➢ *Layer 7 (Application)*



Lapisan Application. Pada Lapisan ini menjelaskan dimana Aplikasi pengguna berkomunikasi. Berikut penjelasan contohnya.



Web Browser adalah sebagai Aplikasi pengguna, berkomunikasi dengan web browser sebagai layanan jaringan. Selain itu pada lapisan ini menyediakan jasa untuk aplikasi pengguna dan bertanggung jawab atas pertukaran informasi antar program komputer, seperti email, server printer. Protokol yang berada didalam lapisan ini adalah HTTP, FTP, DNS, dll...

- *Layer 6 (Presentation)*

Pada lapisan ini untuk menerjemahkan data yang akan ditransmisikan oleh aplikasi kedalam format yang dapat di transmisikan melalui jaringan (atau yang dapat dimengerti oleh jaringan). Maksud dari menerjemahkan adalah sama seperti hal mengkonversi. Pada jaringan pun punya definisi yang mirip, yaitu paket data dari lapisan Application dirubah formatnya dengan tujuan agar bisa diteruskan melalui jaringan. Protokol yang berada di dalam lapisan ini seperti Windows NT, VNC, MPEG dll. Jadi, bisa dibilang ini adalah Layernya para Programmer. Dan di layer ini punya nama lain, yaitu Syntax Layer.

- *Layer 5 (Session)*

Pada lapisan ini bertanggung jawab sebagai membuat koneksi, memelihara, menjaga, menghancurkan koneksi, selain itu di lapisan ini juga terjadinya resolusi nama. Protokol yang berjalan pada lapisan ini adalah NetBIOS, dll …

Pada layer ini, berbicara tentang komunikasi antara end user application.

- *Layer 4 (Transport)*

Pada lapisan ini bertugas memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu pada lapisan ini juga membuat sebuah tanda bahwa paket diterima dengan sukses, dan mentransmisikan ulang terhadap paket-paket yang hilang di tengah jalan. Protokol yang jalan pada lapisan ini adalah TCP & UDP.

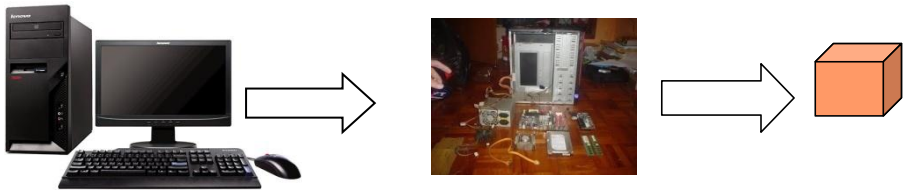
Lalu apa maksudnya memecah data ke dalam paket data serta memberi nomor urut ? Maksud disini adalah sama ibaratnya kita ingin mengirimkan sebuah komputer lengkap dengan monitor, speaker, CPU, dll …

lalu apakah kita akan mengirim Komputer tersebut secara utuh ? Tidak kan ?

Nah, nama lapisannya aja ' Transportasi ', di lapisan ini juga bertugas menjaga kualitas dan kehandalan komunikasi / koneksi, agar bisa mengirim komputer tersebut , maka dibongkar menjadi bagian kecil yang mudah di bawa dan dibungkus di tempat yang aman, monitor di bongkar bagian kakinya, lalu dikemas demi menjaga layar agar tetap utuh tanpa rusak, CPU, Keyboard, Speaker, dll, lalu diberi tulisan pada pembungkus agar tidak tertukar

Setelah di bungkus baru deh bisa dikirim lewat expedisi atau dibawa sendiri, ketika sampai di tujuan, baru deh dibuka bungkus tadi dan dirakit ulang.Nah berikut gambarannya.

Proses pengiriman pada LapisanTransport



Pada lapisan ini Protocol Data Unit (PDU) disebut dengan Segment

- *Layer 3 (Network)*

Pada lapisan ini mendefinisikan alamat-alamat IP, membuat header pada paket, dan kemudian melakukan routing melalui internetworking dengan menggunakan router atau switch layer 3. Jadi pada lapisan ini, paket yang sudah dikemas di lapisan transport tadi, di beri alamat-alamat, rules terbaik, dan *header* pada lapisan ini. Protokol yang berjalan pada lapisan ini IP, ICMP, RIP, EIGRP, OSPF, ISIS, dll ...

Pada lapisan ini PDU-nya disebut Packet

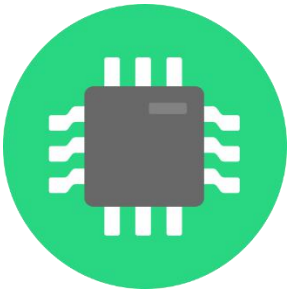
- *Layer 2 (Data Link)*

Pada lapisan ini berfungsi menentukan bagaimana bit-bit dikelompokan menjadi format disebut sebagai ' frame '. Pada lapisan ini juga bertanggung jawab koreksi kesalahan, flow control, pengalamatan perangkat keras (MAC Address) dan menentukan bagaimana perangkat-perangkat jaringan seperti bridge dan switch berkerja. Protokol yang berjalan pada lapisan ini adalah PPP, PPTP, VLAN, Token Ring, dll

Pada lapisan ini, sangat berkaitan dengan Physical. Seperti halnya me-manage Physical, mengatur bagaimana pada Lapisan Physical berkomunikasi, men-definisikan Physical.

Pada lapisan ini PDU-nya disebut Frame

- *Layer 1 (Physical)*



Lapisan ini adalah lapisan dasar, berkaitan dengan data mentah dalam bentuk sinyal-sinyal listrik. Data bit dikirim sebagai 1 dan 0. Pada lapisan ini selalu berhubungan dengan hardware seperti NIC Card, media pengkabelan atau radio (nirkabel), bekerja, media transmisi jaringan (seperti RJ 45, fiber optic, dll), metode persinyalan (sinyal 0 dan 1, atau pada sinyal nirkabel), sinkronisasi bit (mengirim, menerima sinyal 0 dan 1 / Binary) dan sebagainya …

Hub berada di layer ini karena yang sifatnya selalu broadcast

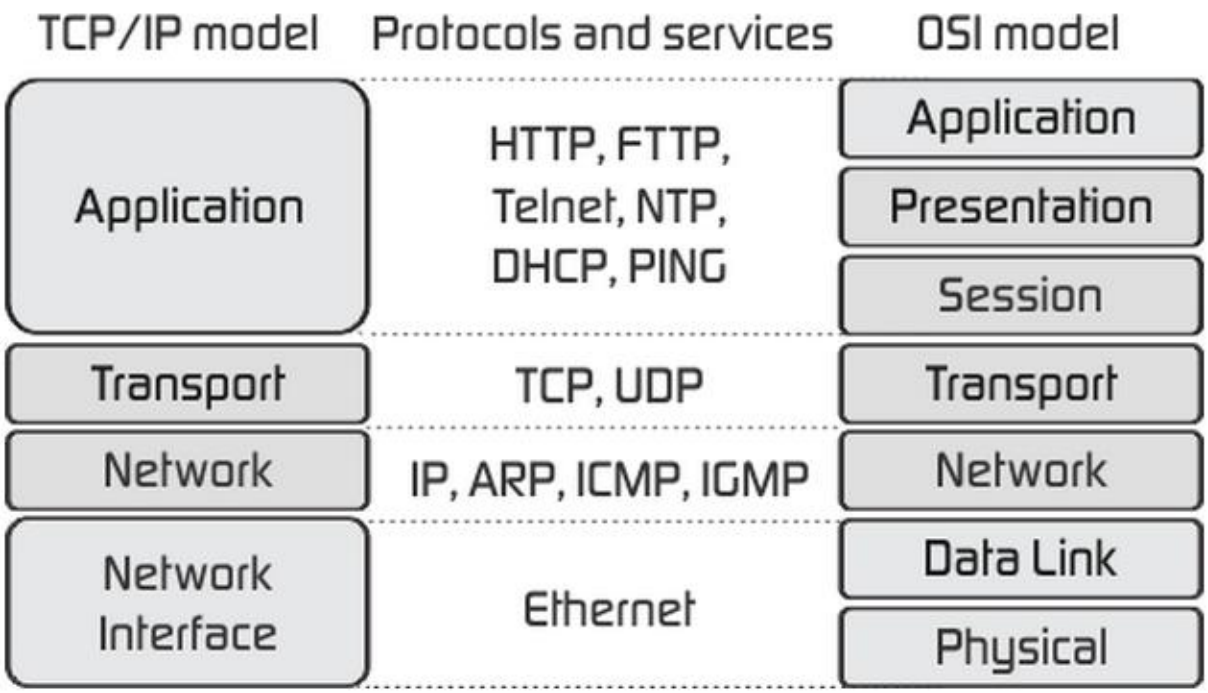
- *Apa itu PDU ?*

PDU (Protocol Data Unit) adalah sebuah istilah pada OSI yang digunakan dalam hal komunikasi data yang mengacu pada sebuah kumpulan informasi ditambahkan atau dihapusnya pada lapisan tersebut. Setiap lapisan pada OSI menggunakan PDU untuk komunikasi dan bertukar informasi yang hanya dapat dibaca oleh lapisan-lapisan pada perangkat penerima hingga lapisan teratas.

PDU pada layer 1 adalah bit, layer 2 adalah frame, layer 3 adalah Packet, Layer 4 adalah segment dan Layar 5 keatas adalah Data.

Didalam PDU memiliki 4 hal yaitu: the destination service access point, source service access point, control field and information field.

- *TCP / IP Models (Darpa)*



TCP / IP ini, seperti halnya OSI Layer, yaitu sebuah standar atau yang mengatur komunikasi data sebuah komputer. TCP/IP atau *Transmission Control Protocol/Internet Protocol* adalah model jaringan yang digunakan untuk komunikasi data dalam proses tukar-menukar informasi(paket data) di internet. TCP / IP ini menggunakan modelnya referensi dari DARPA Model. Seorang Network Engineer sudah seharusnya memahami tentang TCP / IP ini, karena lebih simple yang hanya terdiri dari 4 Lapis, dan lebih sesuai yang dibutuhkan oleh para Network Engineer.

TCP / IP ini, dikembangkan oleh ARPANET dan ARPANET lah yang membuat Internet. Jadi TCP / IP ini lebih mengarah ke Internet. TCP / IP ini terdiri dari 4 Lapis / Layer yaitu Application, Transport, Network, Network Interface.

Berikut penjelasannya tiap lapisan TCP / IP :

- *Layer 4 (Application)*

Pada layer ini,bertanggung jawab untuk menyediakan akses / service kepada aplikasi terhadap layanan jaringan TCP/IP. Protocol-protocol yang beroperasi di Layer ini seperti : HTTP, FTP , POP3, SMTP, DHCP, DNS, dll

Dalam beberapa implementasi stack protokol, seperti halnya Microsoft TCP/IP, protokol-protokol lapisan aplikasi berinteraksi dengan menggunakan antarmuka Windows Sockets (Winsock) atau NetBIOS over TCP/IP (NetBT)

- *Layer 3 (Transport)*

Pada lapisan ini berfungsi untuk membuat komunikasi menggunakan sesi koneksi yang bersifat connection-oriented atau broadcast yang bersifatconnectionless. Pada lapisan ini, punya pengertian yang sama dengan Layer 4 Transport pada 7 OSI Layer.

Lapisan ini adalah, lapisan yang berususan dengan TCP dan UDP.

- *Layer 2 (Network)*

Pada lapisan ini, bertanggung jawab untuk melakukan pemetaan (routing) dan enkapsulasi paket-paket data jaringan menjadi paket-paket IP. Protocol yang berjalan di lapisan ini adalah IP, ARP, ICMP, IGMP.

- *Layer 1 (Network Interface)*

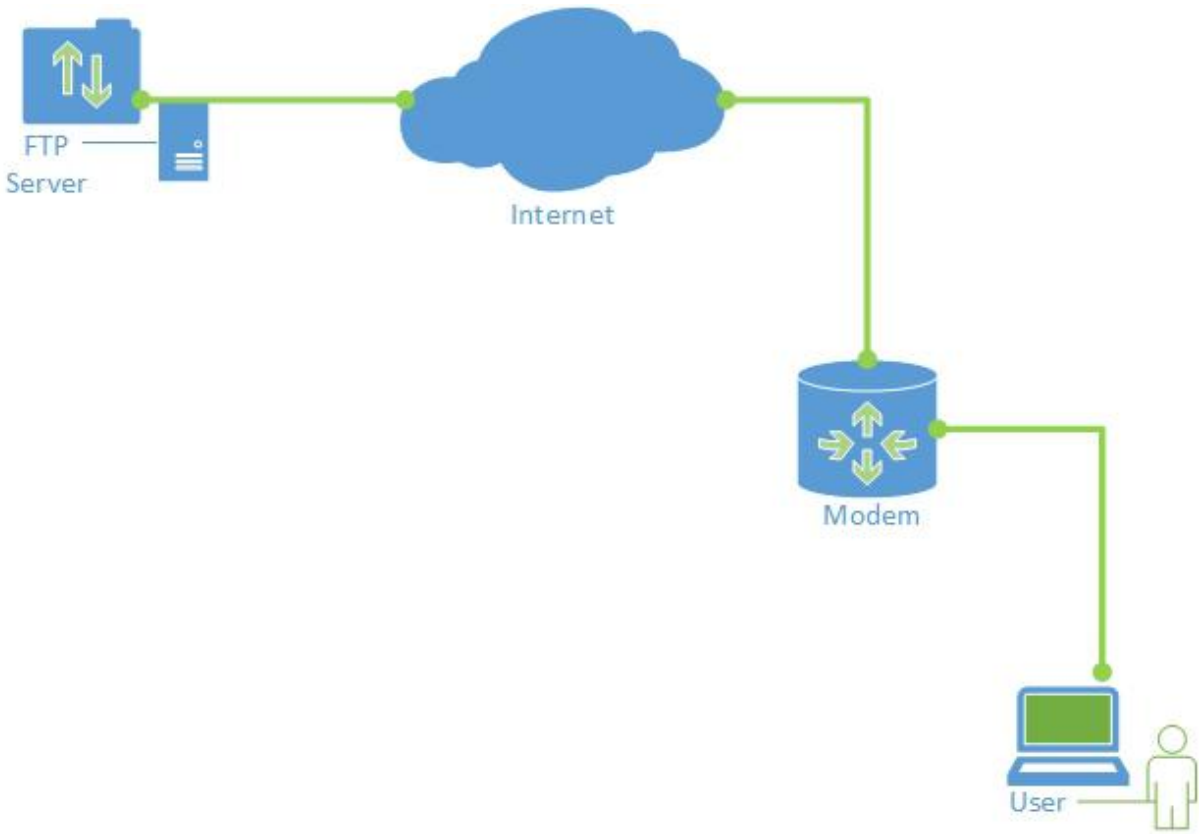
Pada lapisan ini, berurusan dengan interface fisik, bertanggung jawab untuk meletakkan frame-frame jaringan di atas media jaringan yang digunakan.

➢ *Lebih Mendalam Tentang TCP*

Transport Control Protocol

Pada Transport Control Protocol, dapat kita analogikan dengan pengiriman paket seperti di jasa eskpedisi. Pada TCP, ia memiliki karakter melacak setiap *packet data* yang dirikirim. Seperti yang kita ketahui, sistem komunikasi pada dunia jaringan tidak mengirimkan *packet data* secara utuh, melainkan *Packet Data* tersebut dipecah-pecah sesuai dengan settingan yang telah kita tentukan (atau default). Dan customer (penerima *Packet Data)* ia dapat memeriksa secara online untuk melihat urutan pengiriman & keadaan pengiriman *packet data* tersebut.

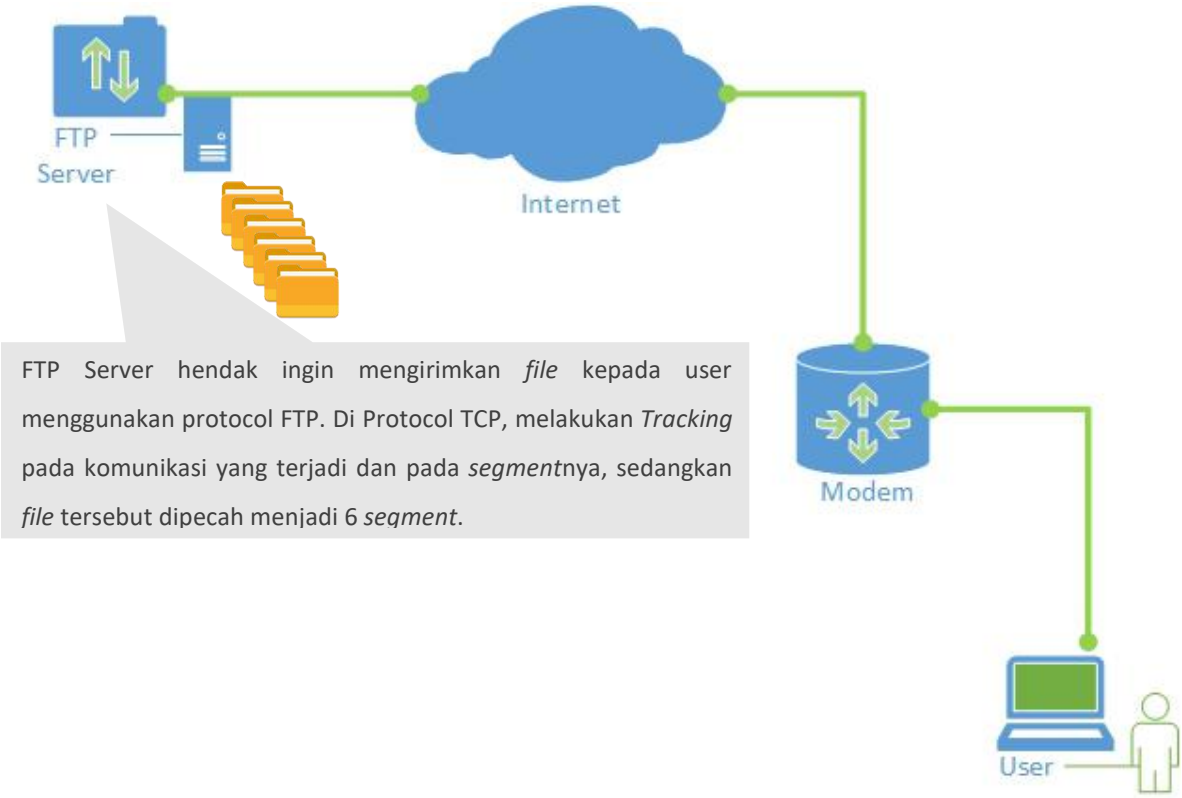
Berikut saya gambarkan, karateristik komunikasi pada TCP.



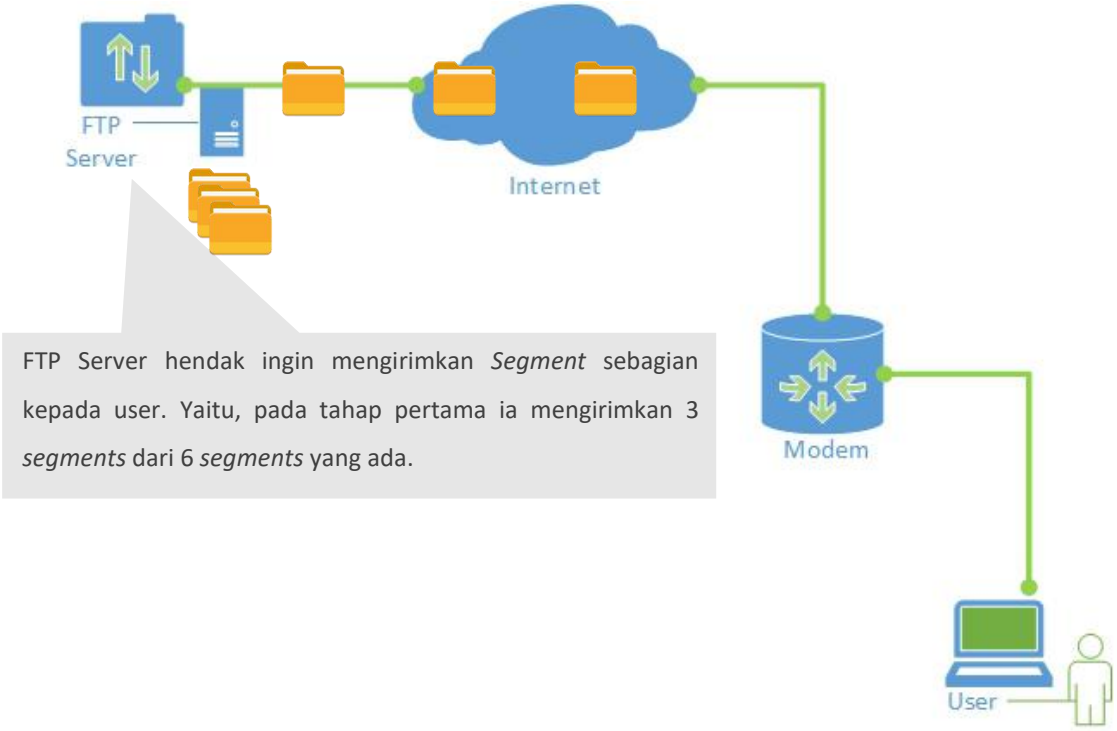
Diatas adalah contoh topologi yang saya buat dengan sederhana. Disini terdapat User yang memiliki koneksi ke internet. User tersebut, sedang mendownload sebuah file

menggunakan Protocol FTP yang berjalan pada TCP. Seperti apa proses komunikasinya antara User dan Server dengan menggunakan protocol TCP ? yuk… kita simak..

1. Karakter TCP ketika ingin mengirimkan *Data* tersebut, maka ia akan memecahnya menjadi beberapa bagian. Seperti kita ketahui, sistem komunikasi pada jaringan, tidak akan mengirimkan data secara utuh. Melainkan dipecah-pecah menjadi beberapa bagian kecil. Seperti mendownload file 1GB, maka tidak mungkin Server mengirimkan file tersebut secara utuh. Misal dipecah menjadi beberapa *packet data* sebesar 10kb. Maka dari itu, muncullah Speed dalam hal men-download *(seberapa cepat, ia menerima pecahan-pecahan data tersebut)*, dan juga rentang waktu dari mulai pertama kali men-download hingga selesai *(waktu yang dibutuhkan, untuk mengumpulan pecahan-pecahan data tersebut hingga lengkap)*. Bagaikan ingin mengirimkan buah jeruk seberat 1 ton, tidak mungkin kita mengirimkannya secara utuh 1 ton, tanpa dipecah menjadi bagian-bagian yang ringan, lebih kecil, dan yang dapat mudah diterima & dikirim. Semisal, dipecah menjadi kumpulan jeruk seberat 10kg *(analogi).*
2. Simak gambar berikut ini. FTP Server, hendak ingin mengirimkan sebuah file. Ternyata, file tersebut dipecah-pecah menjadi 6 *segment.* Pada karakter TCP, ia akan men-*Tracking* setiap *segment* yang dikirimnya dan juga pada komunikasi antara FTP Server dengan User. **tracking = melacak, segment = packet data*

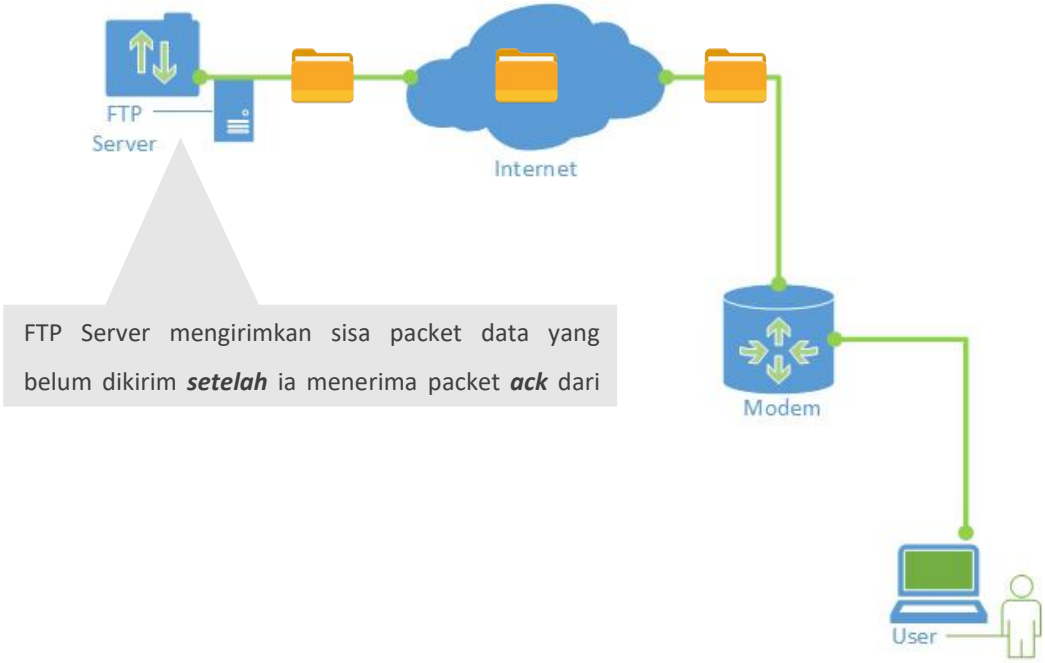


3. Kemudian setelah itu, karakter TCP pada *segment-segment* tersebut tidak dikirim secara sekaligus, melainkan sebagian-sebagian. Semisal adalah pada tahap pertama, ternyata hanya dikirimkan adalah 3 *segments*. **simak gambar berikut dibawah ini.*



4. Ketika user telah menerima sebagian *segment* tersebut yang berjumlah 3, maka ia akan mengirimkan packet data *acknowledgement,* yang berisikan, untuk memberi tau kepada server, bahwa ia telah menerima 3 *segment* yang dikirimkan oleh server tersebut.

5. Ketika FTP Server telah menerima *ack* dari User, maka ia akan melanjutkan sisa packet data yang belum dikirimkan.



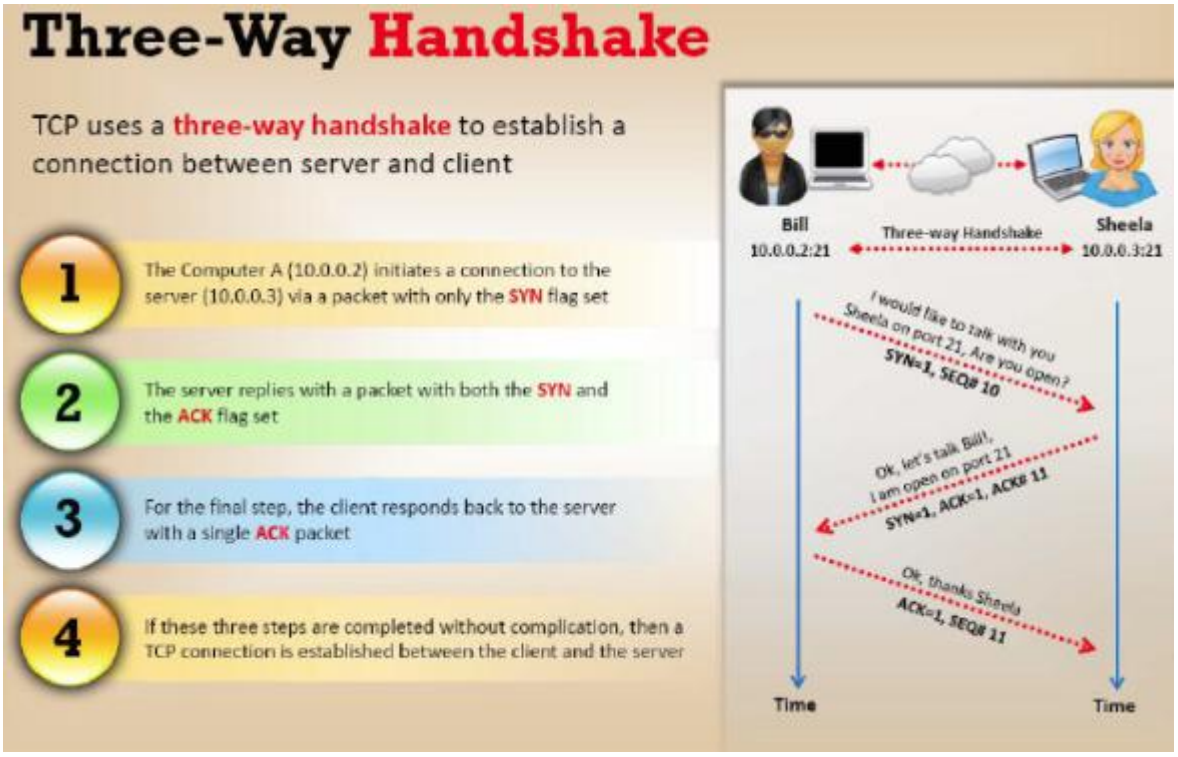
Ok, what is three way handshake ?

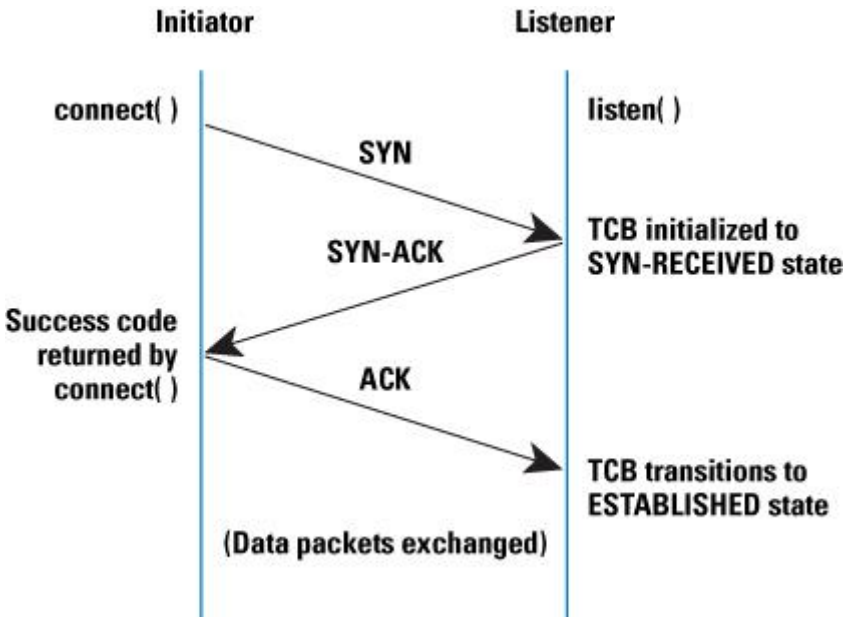
The three way handshake is a method used in a TCP/IP network to create a connection between 2 devices. It is a three-step method that requires both the 2 devices to exchange SYN (synchronization) and ACK (acknowledgment) packets before actual data communication begins.

For what ?

If we are talking about the Three Way Handshake, that's means we talking about Transmission Control Protocol. The function of Three Way Hanshake is for supporting TCP feature like guaranteed free loss packet, wrong sequence, corrupted packets, and etc.

ok…, now i will explain about the three way handshake with full explanation.





The Three Way Handshake is be like (Analogy) Online Shopping. For example, the first things we do before buy something, is asking the seller. Example :

Buyer : Hello… I want to buy New Asus ROG Notebook GL552VX. Do you still have the stock? ***SYN***

Seller : Yes, stocks are still there … I will prepare the package for you… ***SYN + ACK***

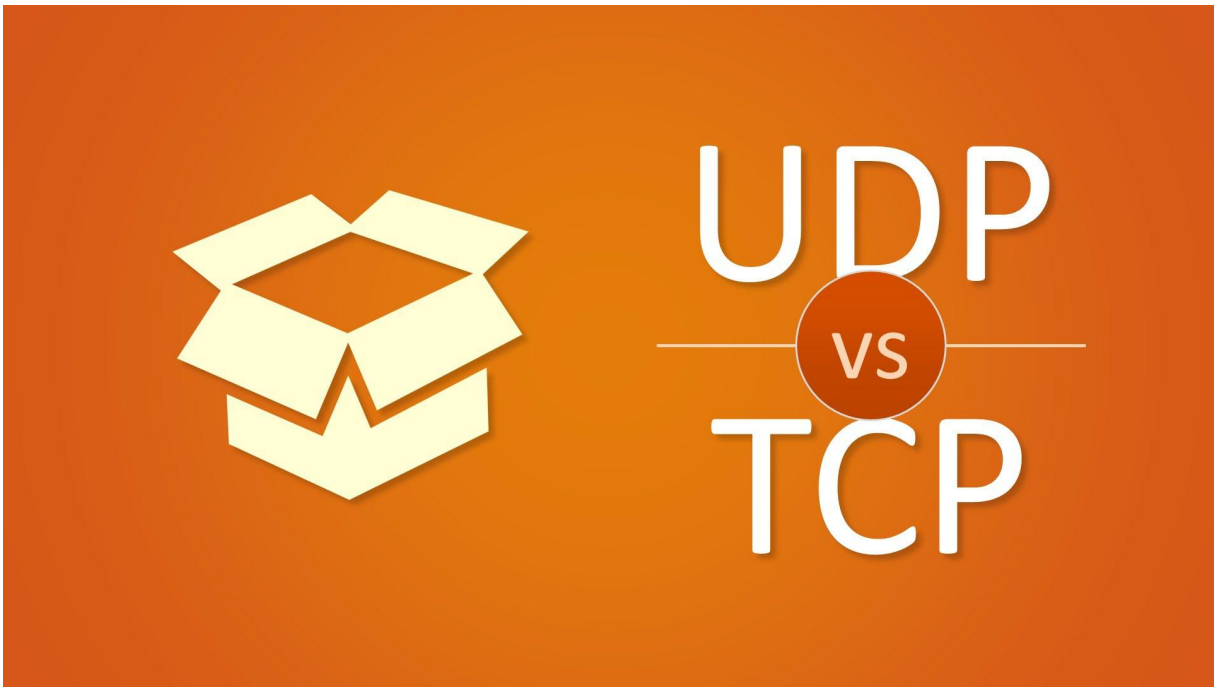
Buyer : Ok, thanks man … ***ACK***

After that conversation, the package has begun shipped to the buyer. The Question is " ***Why the TCP is need Three Way Handshake, but UDP not ?*** "

Remember, the UDP is Simple & Lightweight Protocol. If UDP use Three Way Handshake Feature, then it will become not simple. " ***Not UDP, if not simple.*** " TCP needed Three Way Handshake, is for Matching Connections between Server & Client, Accurate Flow Control, Congestion Control, and much more, more than 50% of TCP Feature needed Three Way Handshake for their Feature.

TCP, before Sending Real Packet data, they're preparing for the feature like flow control, error detection, and etc. The all feature in TCP is relate to each other, like Between Three Way Handshake and Flow Control, Three Way Handshake

- *TCP vs UDP*



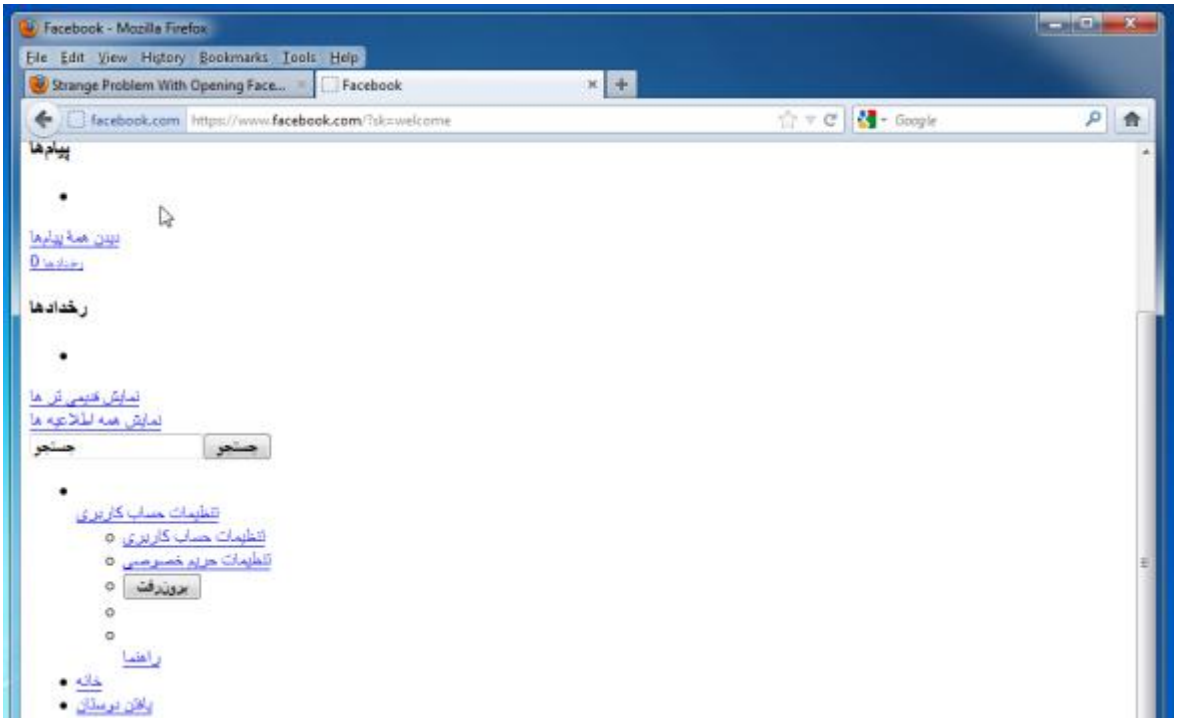
TCP dan UDP adalah sebuah jenis Protocol yang cukup terkenal, yang berada di *Layer Transport* baik itu pada model OSI ataupun pada model TCP/IP. Kedua jenis protocol tersebut sama-sama memastikan *packet data* yang dikirimkan terbebaskan dari terjadinya error (kesalahan dalam pengiriman paket data), seperti dalam kesalahan urutan packet data, dan dari hilangnya packet data maupun terjadinya packet data duplikasi. Kunci perbedaan

pada kedua tersebut adalah pada TCP memiliki services yang lebih luas dibandingkan UDP. Dan tidak hanya itu, TCP lebih kompleks dibandingkan UDP.

Secara garis besar, perbedaannya adalah :

- TCP cukup lambat, namun dapat dihandalkan
- UDP cukup cepat, namun tidak dapat dihandalkan

Disaat apa, kita menggunakan TCP yang tepat ?



TCP akan sangat tepat, jika digunakan untuk seperti *Web Access*, *E-Mail*, men-*download file* ataupun meng-*upload file*, dan sebagainya yang sejenis. Mengapa ? karena kalau disaat kita mengakses web dari 100 packet data yang dikirimkan, ternyata diantara 100 tersebut ada 10 packet data yang rusak atau hilang, maka tampilan web tersebut akan rusak *(bisa dilihat pada contohnya seperti gambar di atas)*.

Sama seperti halnya dalam men-download. Ketika ada packet data yang sampai ke tujuan ada yang rusak, maka file yang kita download akan error dan tidak bisa di buka oleh aplikasi / sistem operasi, dan akhirnya kita sia-sia belaka mendownload file tersebut. Mengapa ? karena tidak bisa kita gunakan file tersebut, misal kita men-download game dengan format *.exe* sebesar 4GB, lalu file tersebut error, maka kita harus men-downloadnya ulang dari awal lagi jika ingin menjalankan file dengan normal.

Pada intinya, TCP digunakan pada akses yang cukup fatal atau sangat penting terhadap komunikasi paket-paket data tersebut. Seperti halnya dalam men-download / upload, jika kehilangan beberapa paket data, maka file / data tersebut akan error *(data yang sensitive, yang tidak boleh terjadi kesalahan).*

Lalu bagaimana dengan UDP ?

UDP memang tidak menjamin pengiriman paket data sebaik TCP, meski begitu, UDP lebih cepat dari TCP. UDP akan sangat tepat jika digunakan pada *Real Time Application*. Seperti Live Stream, Audio Stream, Live Radio (Jalur Internet), Video Conference, Game Online, dan sebagainya yang sejenis. Jenis komunikasi aplikasi seperti ini sangat cocok menggunakan UDP, karena memang tidak membutuhkan keutuhan paket data seperti ada beberapa paket data yang hilang, dan tidak terjadinya masalah ketika ada paket data error. Ia mengutamakan kecepatan. Mengapa ? Kok bisa begitu ?

Wokeh…, jadi begini… Layanan yang biasa digunakan UDP, adalah layanan yang mengutamakan kelancaran dan kecepatan. Seperti main game online. Komunikasi antara player-player dengan server, tidak membutuhkan keutuhan packet data seperti di TCP.

Layanan yang menggunakan UDP, seperti game online, tidak dapat menunggu paket data yang hilang, untuk di re-transmission. Services yang berjalan secara real-time, waktu terus berjalan, jika terjadi packet data yang hilang / rusak, maka services akan tetap lanjut teruss… Seolah-olah semua berjalan dengan lancar & baik. Itulah yang dibutuhkan layanan seperti main game online, live stream, dll….

Apa jadinya kalau pakai TCP ? wah… yang pasti akan banyak kekacauan yang terjadi…, yang pertama load processor akan sangat tinggi, bandwidth boros, akan banyak terjadi buffering, dan kekacauan yang lainnya. Dan juga, mustahil aplikasinya dapat menunggu packet di transmisikan ulang. Jika pada waktu 12:52:30 terjadi loss packet, dan waktu sekarang adalah 12:52:33, maka aplikasi tidak dapat di-*pause (buffering)* sebagaimana *video content* pada *youtube. Real Time Apllication* itu harus tetap berjalan terus sebagaimana waktu yang berjalan terus, tidak boleh berhenti.

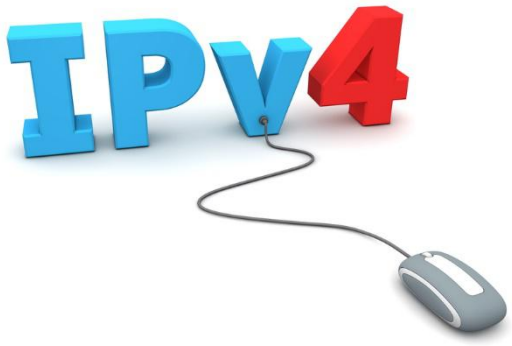
8. IPv4

Apa itu IP ? IP yang merupakan singkatan dari Internet Protocol, adalah sebuah alamat yang digunakan untuk berkomunikasi antar Perangkat, seperti komputer, smartphone, laptop, router, server, dsb. Diantaranya fungsi IP adalah sebagai Pengalamatan, Komunikasi & Identitas. IP juga bisa disebut sebagai deretan nomor unik yang digunakan oleh komputer, smartphone, server,dsb untuk berkomunikasi. " Unik " berarti, antara satu dengan yang lain tidak akan ada yang sama. IP tidak akan terjadi ada yang sama, karena IP merupakan sebuah alamat. Setiap alamat pasti berbeda-beda, begitu juga dengan IP.

Apa yang terjadi jika terdapat IP yang sama ? yang terjadi adalah, komputer tersebut tidak akan bisa berkomunikasi, terjadi kegagalan koneksi pada jaringan alias Disconnect. Karena Packet Data akan bingung alamat yang ditujunya, terdapat dua komputer memiliki alamat yang sama.

Contoh IP yang paling banyak dikenal orang adalah " 192.168.1.1 "

Lalu, apa itu IPv4 ?



IPv4 adalah singkatan dari IP version 4, adalah IP yang umumnya kita gunakan sekarang ini. IPv4 ini adalah IP yang pertama digunakan pada masyarakat umum secara luas. IPv4 ini terdiri 32-bit , dengan contoh format seperti berikut ini : " ***xxxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx*** " yang dimana ***x*** adalah bilangan binary. Setiap octet (titik), terdiri dari 8 bit, maka 8 x 4 = 32 bit. IPv4 ini berjumlah 4.294.967.296 , dari jumlah 4 milyar tersebut adalah tidak semua IP dapat digunakan. IP yang tidak dapat digunakan tersebut, disebut dengan " IP Reserve " atau " IP Reservation ". Sebenarnya IP tersebut bukan tak dapat digunakan, melainkan tak dapat digunakan untuk masyarakat umum. Ada beberapa IP Reservation yang memang di alokasikan untuk kepentingan tertentu seperti " Private Network " yang dapat kita gunakan bebas pada Jaringan LAN, dan begitu juga dengan yang lainnya. Berikut tabel IP Reservation :

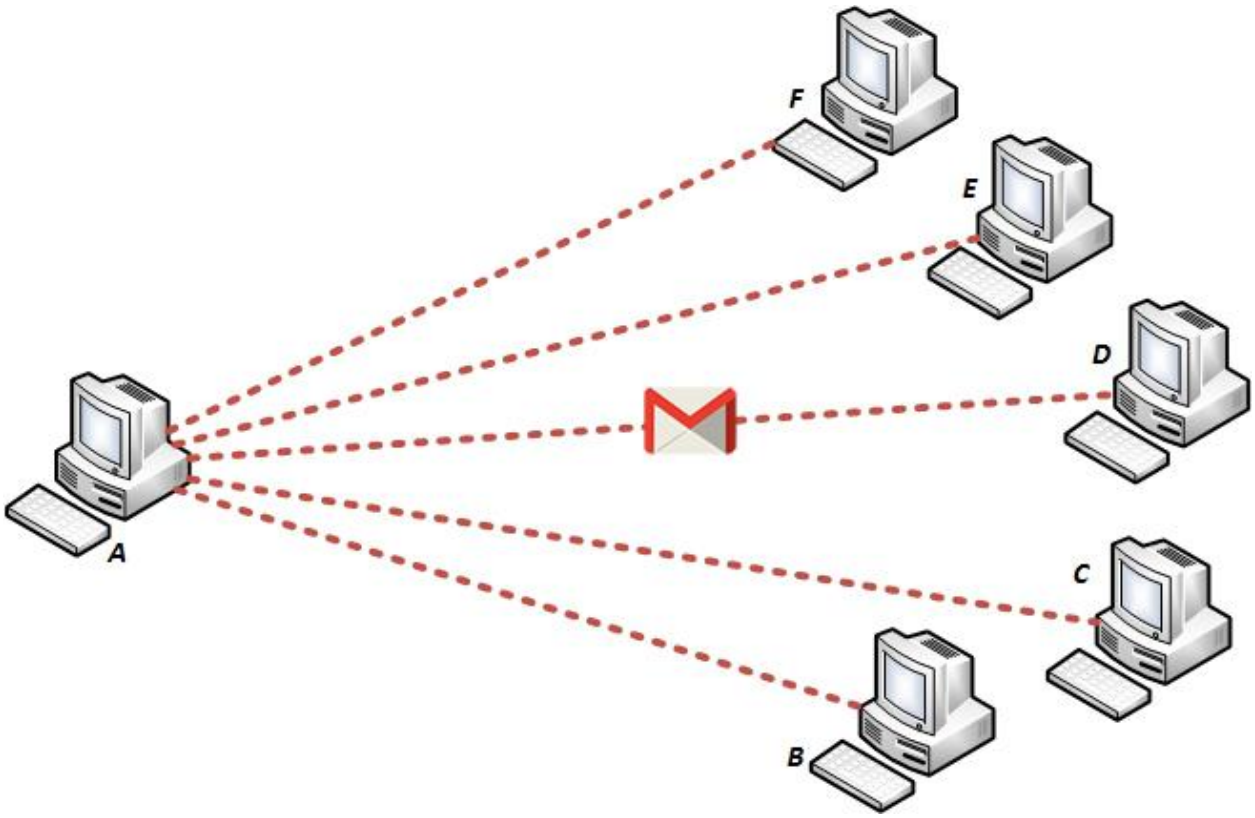
Range	Description	Reference
0.0.0.0/8	Current network (only valid as source address)	RFC 6890
10.0.0.0/8	Private network	RFC 1918
100.64.0.0/10	Shared Address Space	RFC 6598
127.0.0.0/8	Loopback	RFC 6890
169.254.0.0/16	Link-local	RFC 3927
172.16.0.0/12	Private network	RFC 1918
192.0.0.0/24	IETF Protocol Assignments	RFC 6890

192.0.2.0/24	TEST-NET-1, documentation and examples	RFC 5737
192.88.99.0/24	IPv6 to IPv4 relay	RFC 3068
192.168.0.0/16	Private network	RFC 1918
198.18.0.0/15	Network benchmark tests	RFC 2544
198.51.100.0/24	TEST-NET-2, documentation and examples	RFC 5737
203.0.113.0/24	TEST-NET-3, documentation and examples	RFC 5737
224.0.0.0/4	IP multicast (former Class D network)	RFC 5771
240.0.0.0/4	Reserved (former Class E network)	RFC 1700
255.255.255.255	Broadcast	RFC 919

Metode Pengiriman IPv4

Berikut adalah topologi, yang akan menjadi sebuah gambaran proses pengiriman IPv4. Pada materi ini, proses metode pengiriman IPv4 ini ada 3, yaitu Unicast, Multicast, Broadcast.

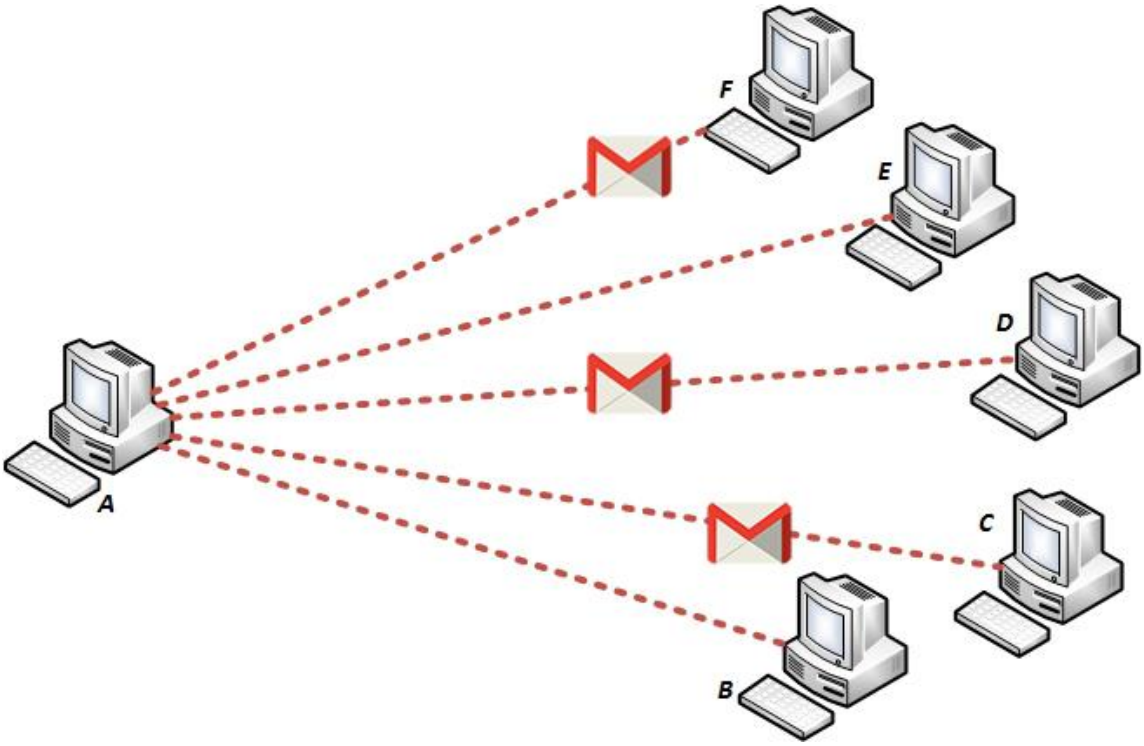
Unicast



Unicast adalah salah satu metode pengiriman komunikasi pada IPv4, yang konsepnya adalah " point to point " atau " one to one " alias paket yang dikirimkan itu hanya dari source ke destination. Jadi Unicast ini yang menerima dan mengirim paket hanyalah mesin ke mesin, alias " satu ". Pada konsep ini analoginya seperti dengan 6 orang yang saling kenal sedang berkumpul, ada 2 orang yang sedang berbicara " hanya berdua saja " yaitu " A " dan " D ". Tanpa 4 orang tersebut mendengarkan (B, C, E & F) , ataupun ikut berbicara dengan 2 orang tesebut. Hal ini sama dengan topologi diatas. Ketika si " A " berbicara, maka yang mendengarkan ucapan A tersebut adalah hanya D , dan begitupun sebaliknya.

Unicast ini biasa digunakan pada Protocol : HTTP, FTP, SMTP, Telnet, DNS, dsb.

Multicast

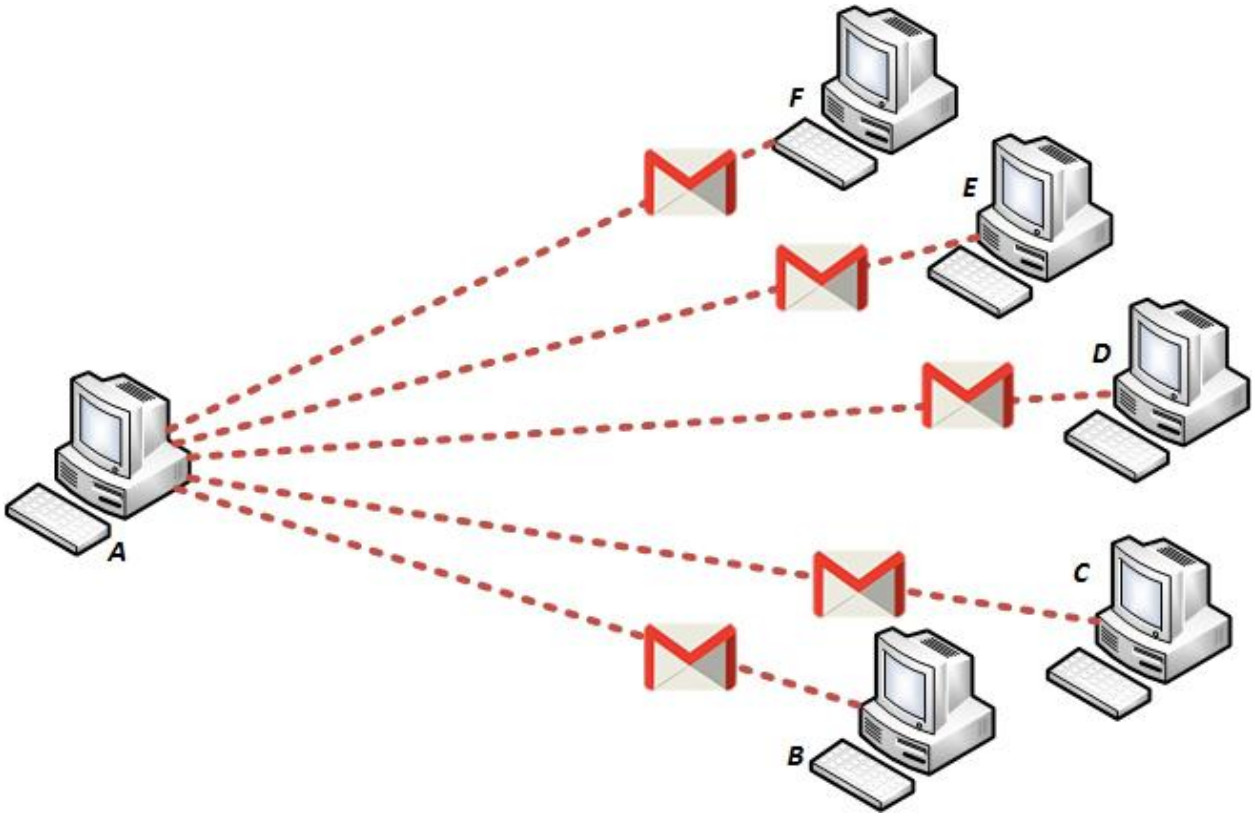


Multicast adalah salah satu metode pengiriman komunikasi pada IPv4, yang memiliki konsep " one to many " yang di desain agar diproses oleh satu atau beberapa node dalam segmen jaringan yang sama atau berbeda. Atau bisa juga dibilang satu paket kepada banyak penerima. Multicast ini menggunakan IP yaitu 224.0.0.0 – 239.255.255.255 . Pada hal ini bisa dianalogikan seperti 6 orang yang sedang berkumpul, dan ada 4 orang yang sedang mengobrol, Yaitu A, C, D & F sedangkan B & E tidak ikut dalam pembicaraan orang tersebut. Konsepnya seperti ini, yaitu A berbicara kepada 3 orang tersebut, dan C, D & F hanyalah mendengarkannya dan bisa juga sebaliknya (contoh : **D** berbicara kepada C, A & F) hal ini sama halnya dengan pelatih pemain bola sedang melakukan pembicaraan kepada timnya, sedangkan timnya hanyalah mendengarkan ucapan dari pelatih. Dan yang mendengarkan hanyalah " Timnya " baik itu supporter maupun tim lawan tidak akan mendengarkan ucapan apalagi ikut dalam pembicaraan. Jadi Komputer A mengirimkan paket, yang dimana paket tersebut akan diterima oleh hanya host / komputer yang mengadakan koneksi multicast (para penerima paket).

Multicast berjalan pada protocol yang seperti “ Live Streaming “ , IPTV, live TV Streaming, Radio Online, dsb. Yang dimana multicast tidak bisa di “ pause “, contohnya jika ada film bola sedang Live Streaming dan sudah di pertengahan pertandingan, maka jika ada yang ikut gabung proses multicast tersebut dalam menonton juga ikut dimulai dari pertengahan pertandingan, bukan dari awal pertandingan dan tidak bisa di “ pause “.

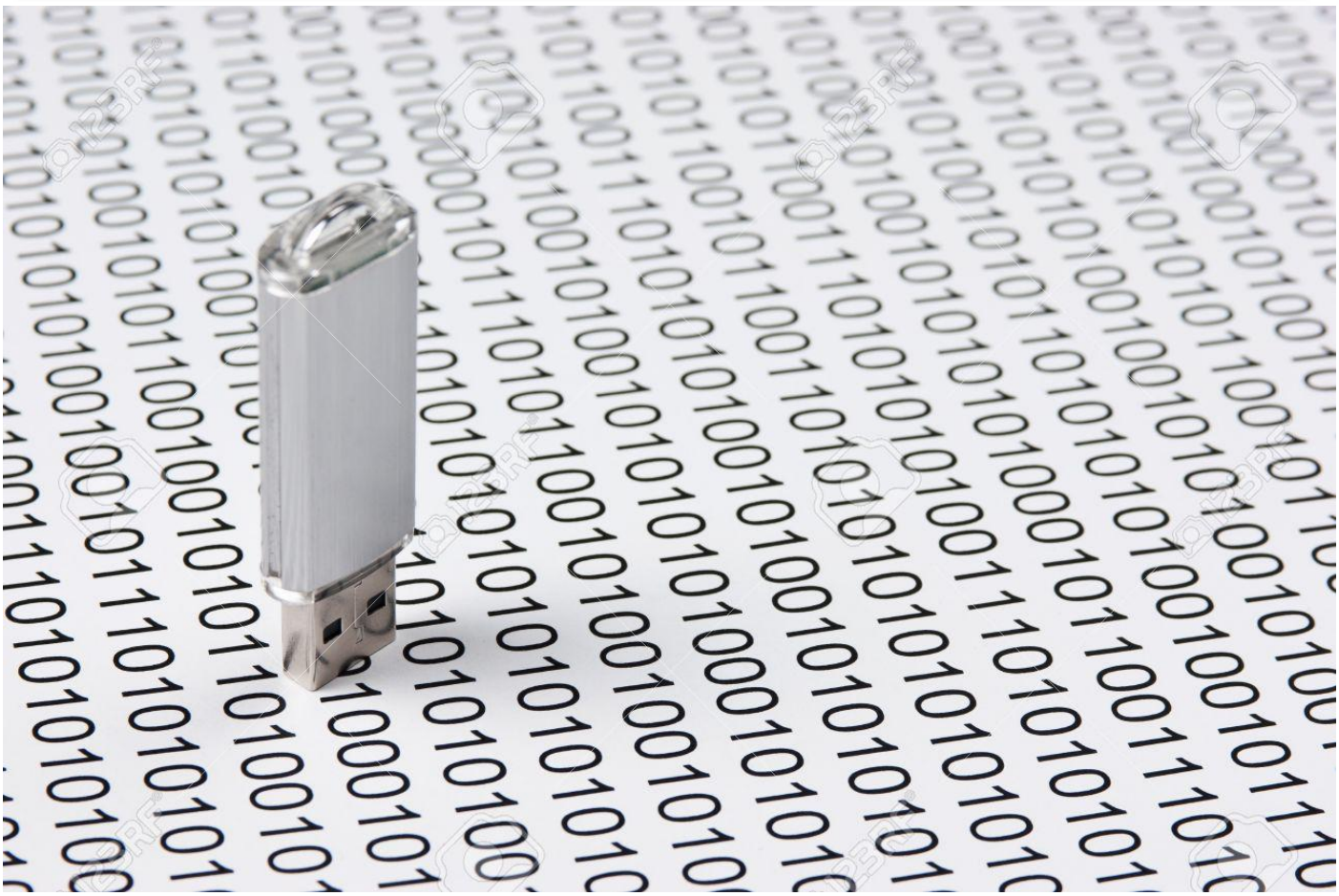
Multicast biasa digunakan untuk komunikasi routing protocol untuk mencari jalur tercepat.

Broadcast



Broadcast adalah salah satu metode pengiriman komunikasi pada IPv4, yang memiliki konsep “ one to everyone “ merupakan alamat IPv4 yang didesain agar diproses oleh setiap node IP dalam segmen jaringan yang sama. Jika sebuah komputer hendak mengirimkan paket data Broadcast, maka semua “ node “ atau setiap komputer yang aktif dalam satu segmen akan menerima paket tersebut dan memprosesnya. Hal ini bisa dianalogikan sebagai, seorang presiden sedang berpidato dengan dihadapan banyak orang,

maka presiden pun mengucapkan pidatonya, dan “ semua “ para hadirin pun akan mendengarkan pidato presiden tersebut. Atau juga bisa dianalogikan sebagai ceramah pada hari jum’at di Shalat Jum’at , ustadz yang berceramah kepada semua jama’ah, dan jama’ah pun mendengarkannya. Sama halnya dengan topologi diatas, ketika komputer A mengirimkan paket Broadcast, maka semua komputer / node yang satu segmen dengannya akan menerima paket tersebut.



9. Subnetting

Pada subnetting kali ini, kita fokus kepada IPv4 saja. Pada IPv4 terbagi menjadi dua bagian, yaitu Network ID (atau dapat disingkat menjadi NetID) dan Host ID.

Apa sih Network ID itu ?

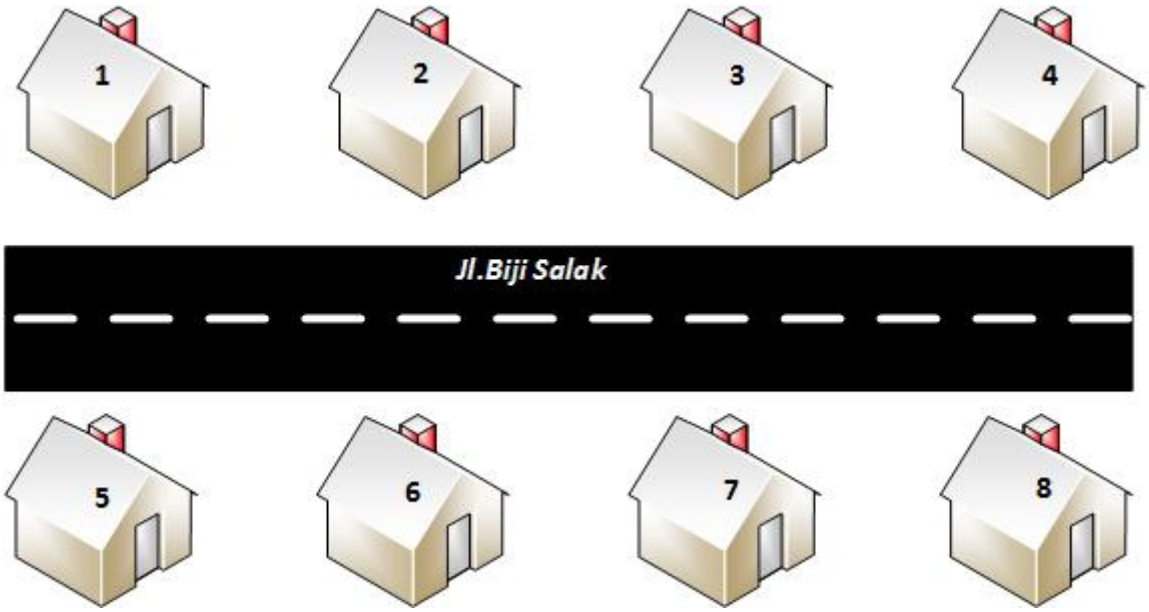
Network ID yang merupakan singkatan dari Network Identifier, merupakan sebuah bagian dari alamat IP, yang mengidentitaskan alamat Jaringan. Mengapa ? karena guna untuk membedakan jaringan yang satu, dengan jaringan yang lainnya. Network ID ini bisa dianalogikan dengan banyak hal yang ada pada kehidupan kita. Contohnya nama Jalan pada perumahan.

Lalu apa sih Host ID itu ?

Host ID yang merupakan singkatan dari Host Identifier adalah sebuah bagian dari alamat IP, yang mengidentitaskan alamat perangkat. Host ID ini juga bisa kita analogikan

dengan banyak hal yang ada pada kehidupan kita. Contohnya adalah nomor rumah yang ada pada perumahan.

Network ID vs Host ID



Dari gambar tersebut kita bisa lihat, bahwa terdapat 8 rumah yang masing-masing memiliki nomor, dan sebuah jalan yang bernama " Jl. Biji Salak ". Setiap rumah alamatnya tertulis dengan penulisan " Jl. Biji Salak no.1 " , " Jl. Biji Salak no.2 ", dan seterusnya. Ini berarti " Jl. Biji Salak " mewakili ke 8 rumah tersebut, inilah yang dimaksud dengan Network ID. Singkatnya, fungsi Network ID mengidentitaskan alamat jaringan, dan jaringan adalah yang mewakili perangkat-perangkat yang ada di dalam jaringan tersebut.

Lalu pada Host ID, berfungsi sebagai alamat rumah-rumah tersebut.

IPv4 Class

Pada IP Address IPv4 ini, memiliki 5 kelas, yaitu A, B, C, D dan E

- ***Kelas A***

Kelas A, memiliki IP dari (octet pertamanya) 0 – 127 yaitu : 0.0.0.0 – 127.0.0.0.

Pada kelas A diberikan untuk jaringan skala besar. 8 bit pertama (oktet pertama) adalah untuk porsi network, dan 24 Bit (3 oktet terakhir) adalah untuk porsi host. Pada kelas A memiliki network 128 & host sebanyak 16.777.216. Berikut rumusnya :

IP address = zxxxxxxx.yyyyyyyy.yyyyyyyy.yyyyyyyy

x=network

y=host

z=class

network = 2^7 = 128

Host = 2^24 = 16.777.216

- ***Kelas B***

Kelas B, memiliki IP di octet pertamanya 128 – 191 yaitu : 128.0.0.0 – 191.0.0.0

Pada kelas B dikhususkan untuk jaringan skala menengah hingga skala besar. 16 Bit pertama (2 oktet pertama) adalah untuk porsi network dan 16 bit (2 oktet terakhir) berikutnya adalah untuk porsi host. Pada kelas B memiliki network sebanyak 16.384 dan host sebanyak 65.536 memiliki skala jaringan lebih kecil dari kelas A, namun dapat membuat jaringan lebih banyak dari kelas A.

IP address = zzxxxxxx.xxxxxxxx.yyyyyyyy.yyyyyyyy

x=network

y=host

z=class

network = 2^14 = 16.384

Host = 2^16 = 65.536

- ***Kelas C***

Kelas C, memiliki IP di octet pertamanya 192 – 223 yaitu : 192.0.0.0 – 223.0.0.0

Pada IP kelas C digunakan untuk jaringan berskala kecil. 24 bit pertama (3 oktet pertama) adalah porsi network dan 8 bit (1 oktet terakhir) berikutnya adalah porsi host. Pada kelas C memiliki Network sebanyak 2.097.152 dan Host sebanyak 256 memiliki skala yang kecil, tapi dapat membuat jaringan yang jumlahnya lebih banyak.

IP address = zzzxxxxx.xxxxxxxx.xxxxxxxx.yyyyyyyy

x=network

y=host

network = 2^21 = 2.097.152

host = 2^8 = 256

- ***Kelas D***

Kelas D, memiliki IP di octet pertamanya 224 – 239 yaitu : 224.0.0.0 – 239.0.0.0. Pada IP kelas D disediakan hanya untuk alamat-alamat IP multicast seperti diperlukan untuk routing protocol (RIP, EIGRP, OSPF), namun berbeda dengan tiga kelas di atas. Di kelas ini tidak digunakan untuk komunikasi antar perangkat selayaknya kelas A, B & C.

- ***Kelas E***

Kelas E, memiliki IP dari 240 – 255 yaitu : 240.0.0.0 – 255.0.0.0. Pada IP kelas E disediakan sebagai alamat yang bersifat "eksperimental". Di kelas ini juga tidak digunakan untuk komunikasi antar perangkat sebagaimana kelas A, B & C.

Binary

Binary atau biner, bilangan biner ini pada umumnya orang menyebutkan digunakan sebagai bahasa komunikasi antara komputer ke komputer lainnya (bahasa mesin). Bilangan

biner adalah sebuah system penulisan angka dengan menggunakan dua symbol yaitu 0 dan 1. Bilangan biner ini adalah dasarnya semua system bilangan berbasis digital.

Dari bilangan biner, dapat mengkonversinya ke bilangan Oktal atau Hexadesimal. Sistem ini juga dapat kita sebut dengan istilah bit, atau Binary Digit. Pengelompokan biner dalam komputer selalu berjumlah 8, dengan istilah 1 Byte. Dalam istilah komputer, 1 Byte = 8 bit. Berikut perhitungan Binary ke desimalnya …

Binary	Decimal
0	0
01	1
10	2
11	3
100	4
101	5
110	6
111	7

Bingung ya ? Jadi begini rumusnya

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Cara menghitungnya rumus diatas dari yang paling kiri dulu hingga ke kanan

Yuk kita coba latihan dulu. yaitu mengkonversi dari ***7*** ke ***Binary*** :

Pangkat	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Nilai	128	64	32	16	8	4	2	1
Hasil Binary	0	0	0	0	0	***1***	***1***	***1***

Kenapa seperti ini ? coba dilihat tabelnya kembali. Disitu hasil binary yang bernilai 1 adalah 4 + 2 + 1 jika dijumlahkan maka hasilnya adalah 7. Maka cara penulisannya adalah " 00000111 " atau 0 dapat dihapus karena BERADA DIPOSISI PALING KIRI dan TIDAK DIAPIT OLEH 1 maka bisa disingkat menjadi " 111 ".

Yuk kita coba latihan lagi, yaitu mengkonversi dari ***192*** ke ***Binary*** :

Pangkat	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

Nilai	128	64	32	16	8	4	2	1
Hasil Binary	***1***	***1***	0	0	0	0	0	0

Lihat pada tabel hasil binary, disitu hasil binary yang bernilai 1 nya adalah 128 + 64 maka hasilnya adalah 192. Maka penulisannya adalah “11000000“ angka 0 tidak dapat dihapus karena berada di posisi paling kanan.

Nah bagaimana dengan ***168*** ?

Pangkat	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Nilai	128	64	32	16	8	4	2	1
Hasil Binary	***1***	0	***1***	0	***1***	0	0	0

Pada hasil binary yang bernilai 1 adalah 128 + 32 + 8 maka hasilnya adalah 168. Maka penulisannya adalah “10101000 “ angka 0 tidak dapat dihapus karena berada di posisi paling kanan & karena di apit oleh angka 1.

Konversi dari IP ke Binary

Contoh IP yang paling sering diketahui oleh orang awam adalah “ 192.168.1.1 “. Nah sekarang kita latihan menggunakan contoh IP tersebut, kebetulan kita sudah menghitung 192 dan 168, sekarang yang kita lakukan hanyalah mengalokasikan 192.168.1.1 ke dalam bentuk binary. Berikut saya buatkan dalam bentuk tabel :

IP	**192**	**168**	**1**	**1**
Binary	11000000	10101000	00000001	00000001

Ketika kita mempelajari tentang IP, maka sudah tidak asing lagi dengan istilah “ Netmask “

Lalu, apa sih Netmask itu ?

Netmask adalah sebuah istilah yang digunakan untuk menentukan jumlah host yang dapat ditampung di dalam jaringan tersebut. Netmask tak hanya sekedar menentukan jumlah host, melainkan dapat juga menentukan alamat Broadcast, alamat Network ID, dan kelas IP tersebut seperti kelas, A atau B atau C.

Netmask pada kelas A adalah “ 255.0.0.0 “, kelas B “ 255.255.0.0 “ dan kelas C “ 255.255.255.0 “ nah .. yang umumnya biasa kita pakai sehari-hari pada jaringan LAN adalah kelas C dengan Netmask “ 255.255.255.0 “. Netmask ini, merupakan binary yang bernilai ***1*** tidak boleh diapit oleh nilai ***0*** seperti ***11110100.11111111.11111111.00000000*** ataupun ***11111111.00000100.00000000.00000000*** .

Pada istilah Netmask, terdapat juga istilah yang disebut dengan Classfull dan Class.

Apa itu Classful ?

Classful Address adalah Pengalamat Jaringan dalam hal SubnetMask (atau bisa juga dikatakan Netmask) yang bernilai default, dalam arti tidak di Subnet. Classful ini adalah netmask,yang Binarynya bernilai 1 dalam kelipatan 8. Classfull ini, ada juga yang menyebutkan sebagai defaultnya netmask (sesuai kelasnya).

Kelas	Binary	Netmask
A	11111111.00000000.00000000.00000000	255.0.0.0
B	11111111.11111111.00000000.00000000	255.255.0.0
C	11111111.11111111.11111111.00000000	255.255.255.0

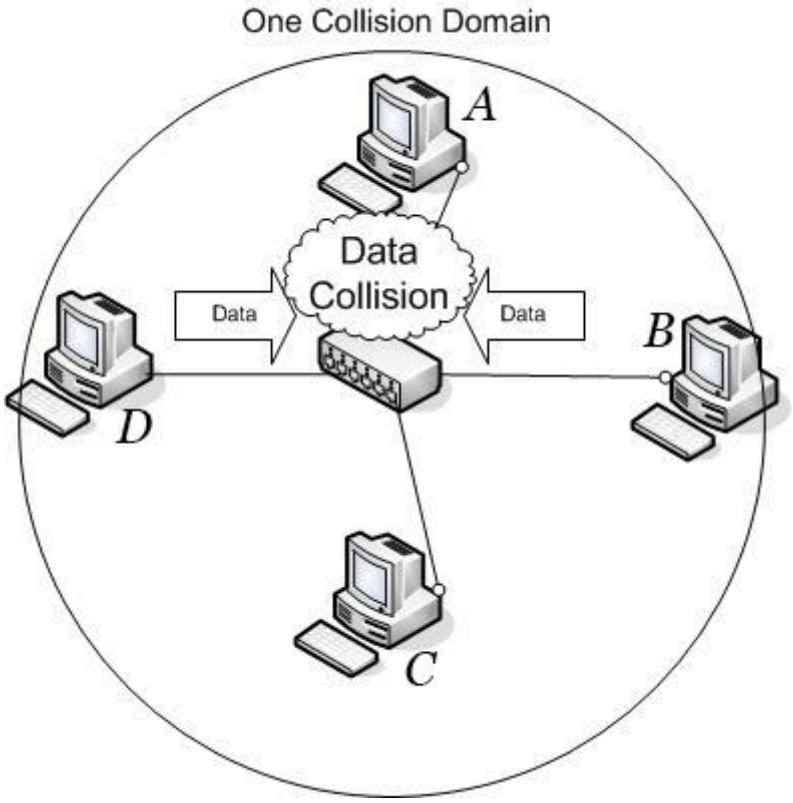
Apa itu Classless ?

Classless Address adalah Pengalamatan Jaringan dalam hal SubnetMask yang bernilai selain default, dalam arti telah di subnet. Classless ini adalah bisa juga dibilang kebalikan dari Classful. Classless ini adalah netmask yang binary bernilai 1 nya tidak berjumlah 8. Berikut contohnya :

Kelas	Binary	Netmask
C (telah di Subnet)	11111111.11111111.11111111.11000000	255.255.255.192
B (telah di Subnet)	11111111.11111111.10000000.00000000	255.255.128.0
A (telah di Subnet)	11111111.11100000.00000000.00000000	255.224.0.0

10.Collision Domain & Broadcast Domain

Apa sih Collision Domain itu ? Collision Domain adalah sebuah istilah yang menggambarkan tentang kemungkinan terjadinya tabrakan pada jaringan.



Collision Domain adalah sebuah Frame di jaringan yang dapat bertabrakan dengan satu sama lain, terjadi tabrakan karena 1 jalur yang digunakan untuk mengirim dan menerima frame.

- ***Gambaran tetang collision domain***

Coba kita lihat gambar sebelumnya, disitu terlihat komputer " D " dan " B " mengirimkan sebuah data ke komputer " A " secara bersamaan. Nah …, karena perangkat yang menghubungkan ke-4 komputer tersebut adalah " Hub " maka , terjadilah " Collision " diantara packet data tersebut (dari Komputer " B " & " D "). Mengapa bisa terjadi bertabrakan ?

Hal ini bisa terjadi, karena Hub selalu Mem-Flooding (mengirim ke semua port kecuali port asal) frame yang akan diterima dan dikirimkannya, karena ada dua frame yang masuk secara bersamaan. Yuk kita coba ingat lagi tentang hub.

Cara Kerja Hub, yaitu ketika ada frame yang masuk pada hub, lalu hub akan mengirimkan frame tersebut ke seluruh komputer yang terhubung dengan Hub. Kecuali ke komputer yang mengirim paket tersebut. Nah …, paket yang dikirimkan tersebut diulang-ulang walaupun framenye dah diterima oleh komputer tujuannya. Lalu bagaimana jika ada computer lain yang ingin melakukan pengiriman juga ? Nah …, hal ini lah .., yang menyebabkan " Collision " karena ada 2 komputer atau lebih yang mengirimkan frame secara bersamaan.

Dan hal ini terjadi hanya pada Hub dan Jaringan di WiFi aja. Namun pada Switch dan Router jarang ditemukan terjadinya collision. Karena WiFi dan Hub memilik jalur pengiriman dan penerimaan hanya memiliki 1 jalur saja.

Rumus collision domain & broadcast domain :

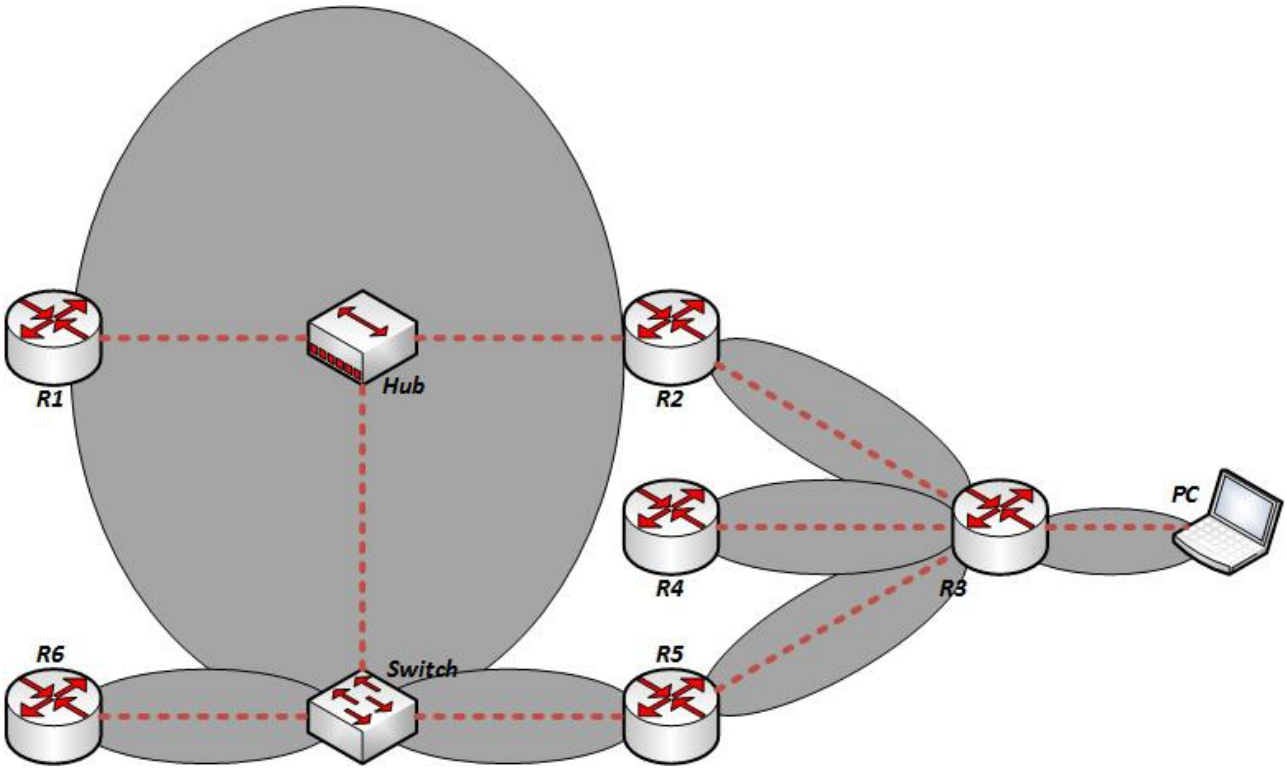
Perangkat	**Rumus Collision Domain**
Hub	Seluruh port 1 CD
Switch	Tiap Port yang aktif 1 CD
Router	Tiap Port yang aktif 1 CD

*Note: semakin banyaknya jumlah CD, maka dari segi Efektif atau Efisiensi pada Jaringan tersebut semakin baik. Yang artinya, terjadinya Collision semakin kecil kemungkinan bahkan tak mungkin terjadi.

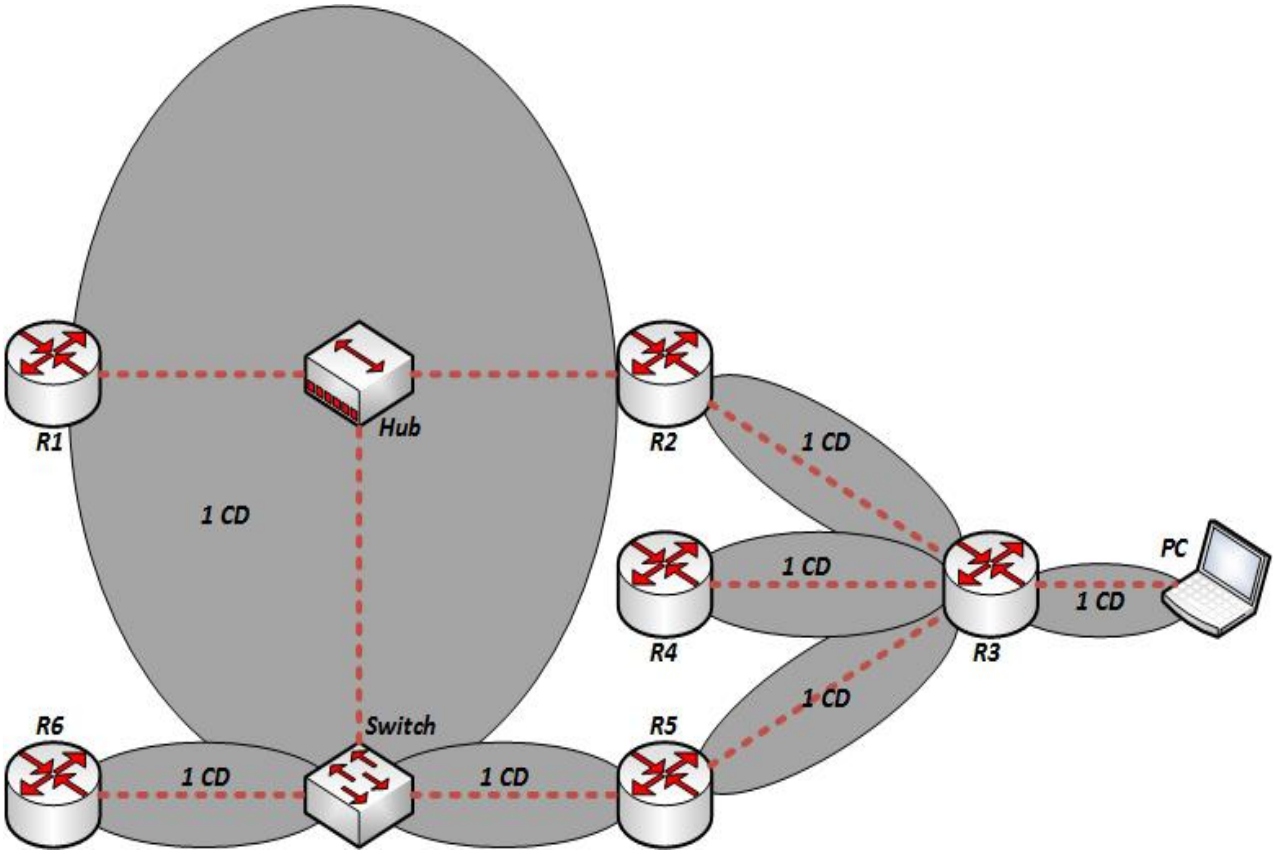
Apa itu broadcast domain?

Broadcast domain adalah sebuah istilah yang dimana mengetahui tentang perangkat yang mana saja, yang menerima packet data broadcast yang berasar dari segmen jaringan yang sama.

Menghitung Collision Domain



Di gambar topologi tersebut, Collision Domainnya adalah sebanyak 7 CD (Collision Domain) kemungkinan yang akan terjadi. Berikut cara menghitungnya :



Silahkan lihat gambar diatas ini, terlihat ada sebuah Line dari R1 ke R2 melalui Hub dan Hub ke Switch. Sebelum kita menghitung, perhatikan rumusnya.Wokeh … kita mulai dari LINE paling atas dan dari kiri.

- Router 1 » Hub = 1 CD
- Hub » Router 2 = 1 CD
- Router 2 » Router 3 = 1 CD
- Router 3 » PC = 1 CD
- Router 3 » Router 4 = 1 CD
- Router 3 » Router 5 = 1 CD
- Router 5 » Switch = 1 CD
- Switch » Hub = 1 CD
- Switch » Router 6 = 1 CD

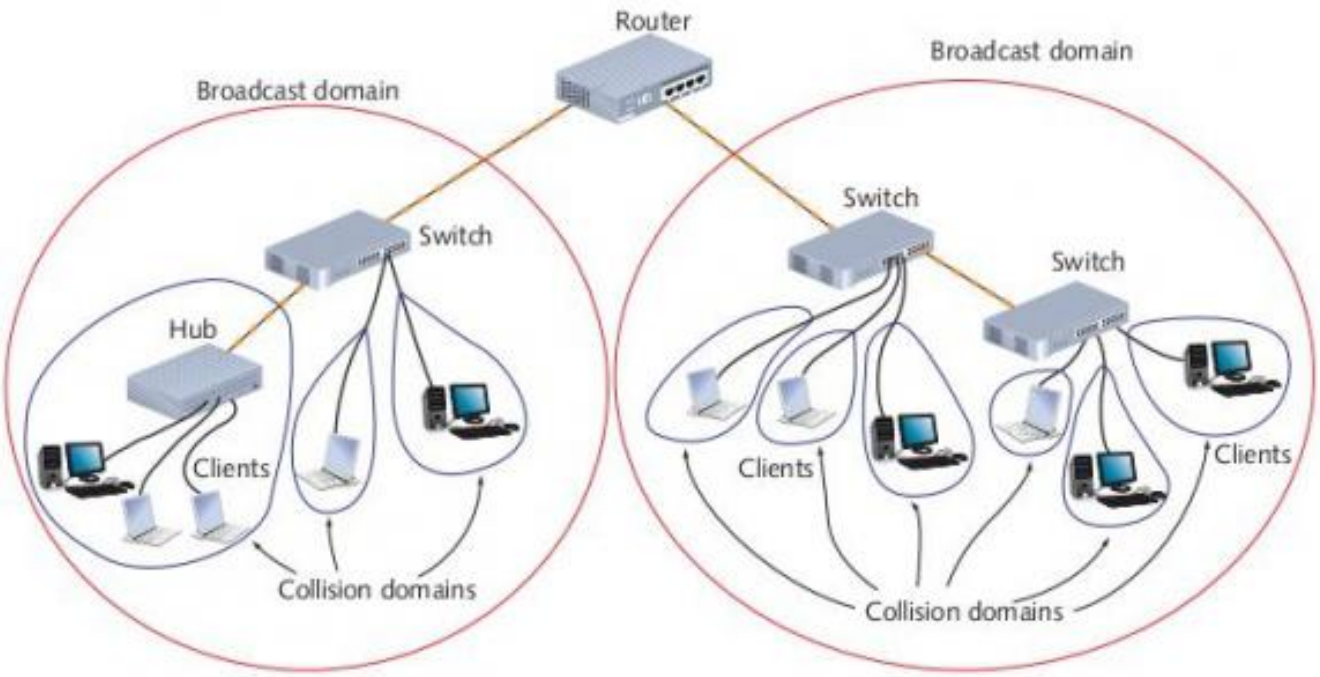
*Note : Maka ke 3 CD tersebut akan menjadi 1 CD. Sesuai dengan rumusnya yaitu

Hub = Seluruh Port 1 CD

Mengapa hasilnya 7 ?

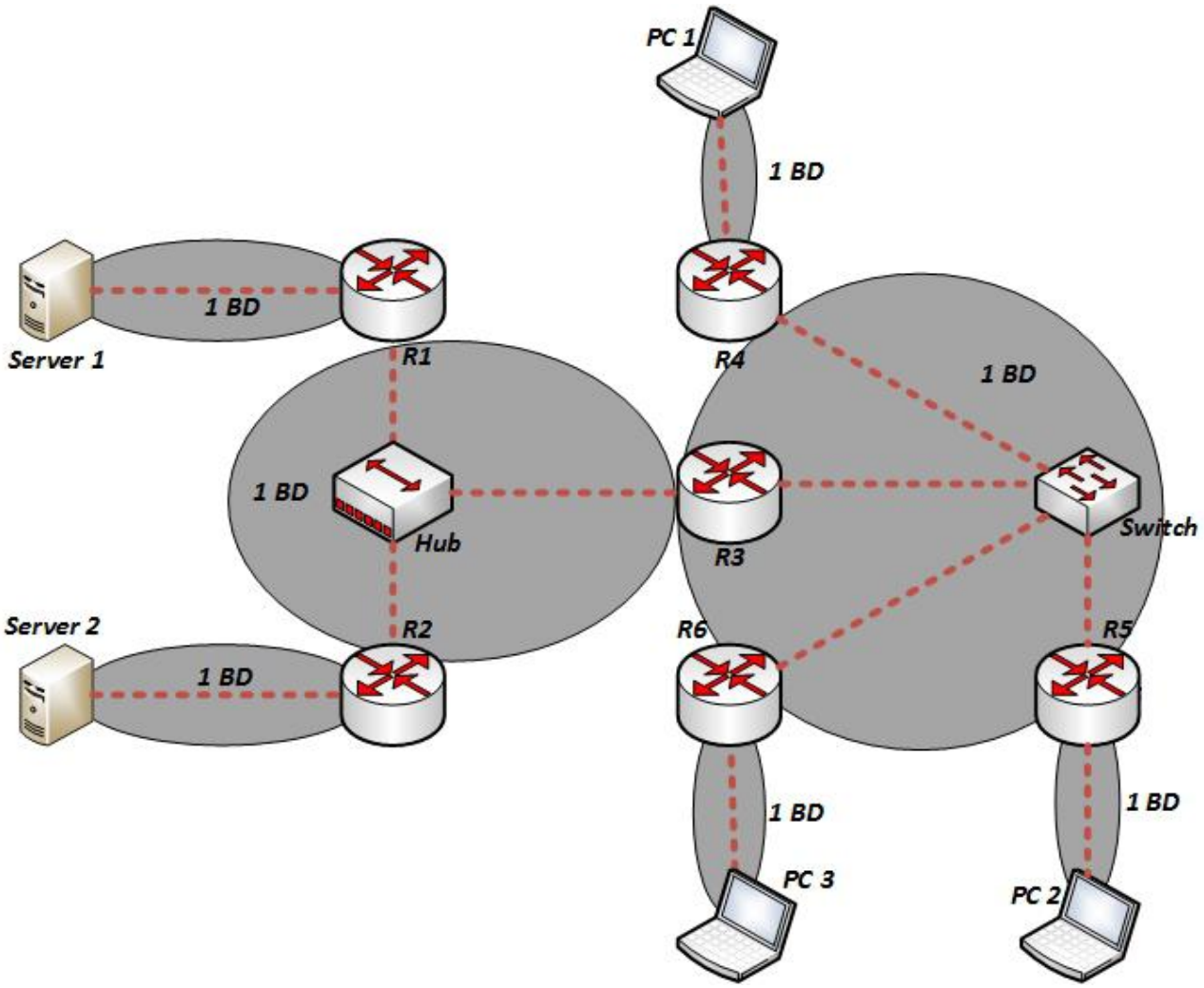
Karena setiap perangkat yang terhubung dengan Hub, maka akan menjadi 1 CD sesuai dengan rumusnya.

Menghitung Broadcast Domain



*Note: Semakin besar Nilai BD, maka dari segi efektif dan efisien semakin baik pada jaringan tersebut. Dan 1 BD adalah 1 Segmen. (1 BD = 1 Segmen, 2 BD = 2 Segmen yang berbeda)

Perangkat	Rumus Broadcast Domain
Router	Tiap Port yang aktif 1 BD
Switch	Seluruh Port 1 BD
Hub	Seluruh Port 1 BD



Kita coba perhatikan topologi diatas, mari kita hitung menggunakan rumusnya. Seperti biasa, kita mulai dari line paling atas dan dari kiri terlebih dahulu. Terlihat dimulai dari Line Server 1 » R1 adalah 1 BD. Mari kita kupas satu-satu :

- Server 1 » R1 = 1 BD
- R1 » Hub = 1 BD
- Hub » R2 = 1 BD
- Server 2 » R2 = 1 BD
- Hub »R3 = 1 BD
- R3 » Switch = 1 BD
- Switch » R4 = 1 BD
- R4 » PC 1 = 1 BD
- Switch » R5 = 1 BD
- R5 » PC 2 = 1 BD
- Switch » R6 = 1 BD
- R6 » PC 3 = 1 BD

*Note: Maka ke 3 BD tersebut, akan menjadi 1 BD. Sesuai dengan rumusnya, yaitu

Hub = seluruh port 1 BD

*Note: Maka ke 4 BD tersebut akan menjadi 1 BD. Sesuai dengan rumusnya, yaitu

Switch = seluruh port 1 BD

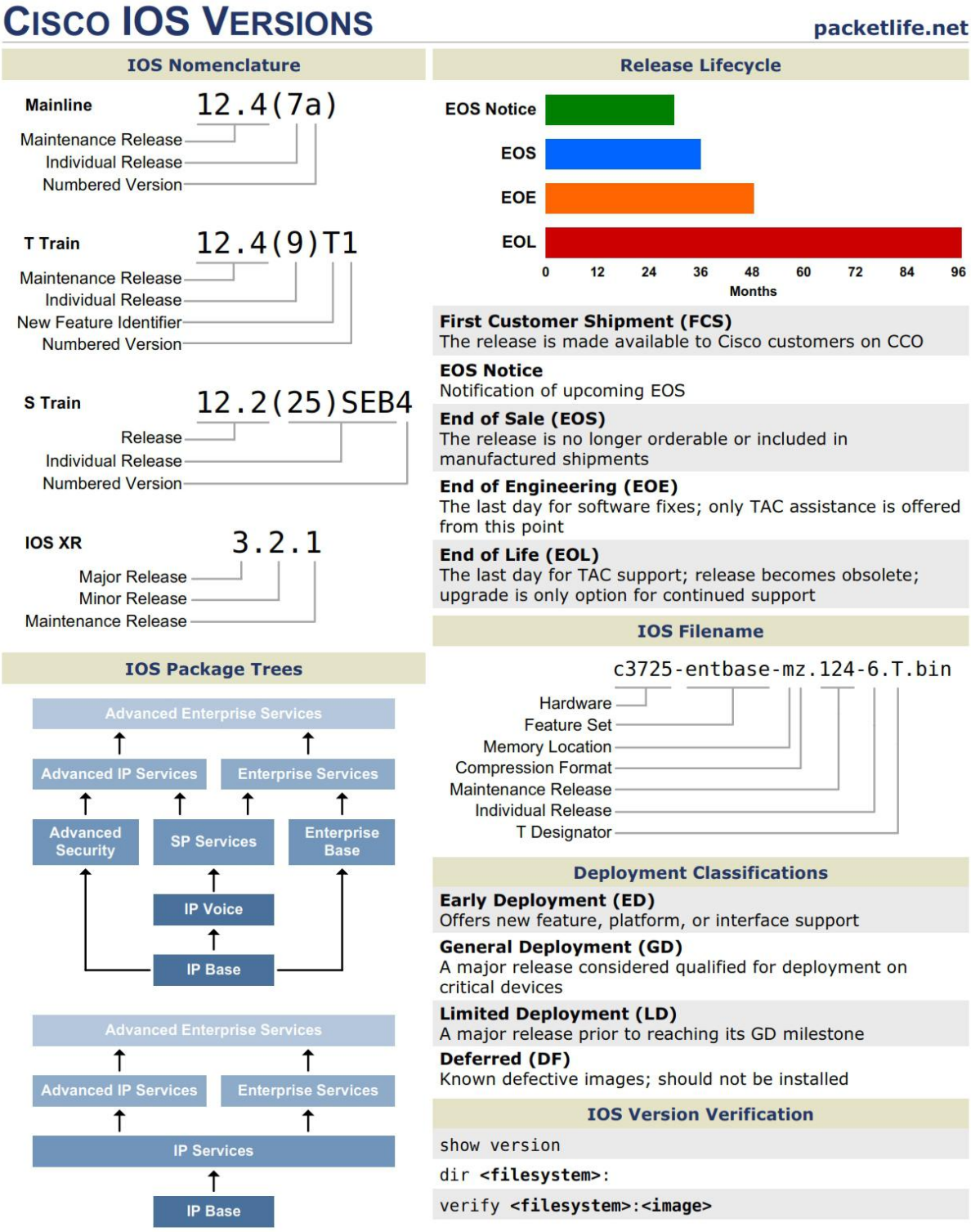
Jika kita hitung, maka hasilnya adalah 7 BD. Cara menghitungnya sama seperti di CD. Dan sesuaikan juga rumusnya, yaitu setiap perangkat yang " **Line** " nya mengarah ke perangkat Hub / Switch, maka line itu akan menjadi 1 BD.

*Note: Khusus untuk perangkat Switch Manageble, jika perangkat Switch tersebut memiliki VLAN, maka VLAN Tersebut dapat memecah Broadcast Domain. Contoh : Di Switch 1 terdapat VLAN Sebanyak 1 maka BD pada Switch itu adalah 1. Di Switch 2 terdapat VLAN sebanyak 3, maka BD Pada Switch 2 adalah sebanyak 3.Dan Di Switch 3 terdapat VLAN Sebanyak 17 maka BD nya juga sebanyak 17. Banyaknya VLAN tersebut adalah, Jumlah VLAN yang tentunya dengan VLAN ID yang berbeda-beda.

11. Basic Config

Sebelum kita memulai mengkonfigurasi baik itu Cisco Router ataupun Cisco Switch, maka terlebih dahulu kita harus mengenal tentang OS yang digunakan oleh Cisco Router dan Cisco Switch yaitu IOS (Internetworking Operating System). Namun dahulu Cisco Switch menggunakan OS yang bernama " CatOS (Catalyst OS), dan sekarang nama OS nya sudah diganti menjadi seperti Cisco Router, yaitu IOS. Berikut bebebrapa keterangannya :

IOS Nomenclature	
Mainline	Versi ter-stabil yang dapat digunakan untuk kebutuhan Operasional
T Train	T adalah singkatan dari Technology, versi seperti " Beta ", yang dimana versi ini merupakan terdapat fitur-fitur baru.
S Train	S adalah singkatan dari Service Provider, seperti namanya, yang dimana IOS ini lebih cocok jika digunakan untuk ISP atau telco
IOS XR	Versi ini digunakan oleh perangkat yang hanya digunakan di ISP & Telco. IOS yang digunakan perangkat ini berbeda dari yang biasanya, karena sanggup mengelola proses traffic yang sangat tinggi.



Apa itu Cisco IOS ?

Cisco IOS yang merupakan singkatan dari Internetwork Operating System adalah sebuah sistem operasi yang digunakan oleh Router & Switch Cisco. Nah untuk Switch, dulu

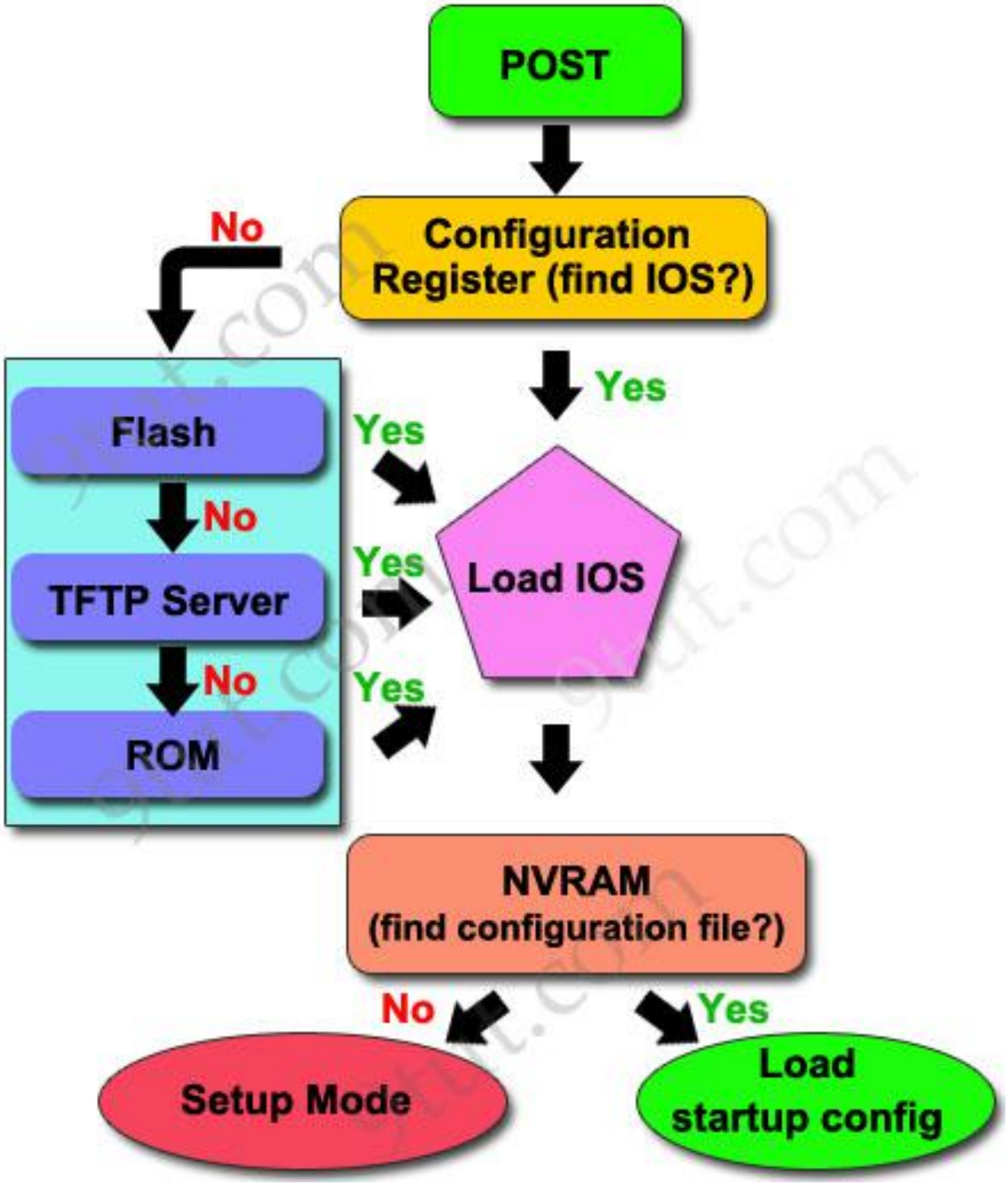
Sistem Operasinya bernama *CatOS (Catalyst OS).* IOS ini memiliki sifat Proprietary. IOS adalah sebuah paket Software dari kumpulan-kumpulan seperti : Routing, Switching, Internetworking, telecommunication, security dan masih banyak beberapa yang lainnya, yang dijadikan sebagai feature di Router dan Switch tersebut.

Berikut beberapa *Commands Mode* pada IOS.

- User EXEC mode
- Privileged EXEC mode
- Global Configuration mode
- ROM Monitor mode
- Setup Mode
- Dan lebih dari 100 *Commands Mode* dan sub mode yang ada di IOS

Inti, dari fungsi Cisco IOS adalah memungkinkan komunikasi data antar jaringan / node.

IOS Startup Sequence



Yuk… kita ngonfig

- User Mode & Privilege Mode

Router>

Router> enable

Router#

- ***Global Config Mode***

Router# configure terminal

Router(config)#

atau

Router# conf t

Router(config)#

- ***Merubah hostname***

Router(config)# hostname <nama>

Contoh

Router(config)# Egi_INDO

Egi_INDO(config)#

- ***Saving Configuration***

Egi_INDO(config)# do write

Atau

Egi_INDO(config)# do wr

Atau

Egi_INDO# write

Atau

Egi_INDO# copy running-config startup-config

- ***Daftar perintah Show Command***

Command	Display
#show version	➢ Untuk melihat versi IOS ➢ Informasi hardware, RAM, dsb.
#show running-config	➢ Melihat konfigurasi yang sedang berjalan & digunakan.
#show startup-config **Atau** **#show config**	➢ Konfigurasi yang telah tersimpan pada NVRAM

#show flash	➢ Melihat ukuran file konfigurasi ➢ Storage Memory ➢ Informasi IOS Image Files yang disimpan
#show history	➢ Melihat history perintah yang telah kita ketik

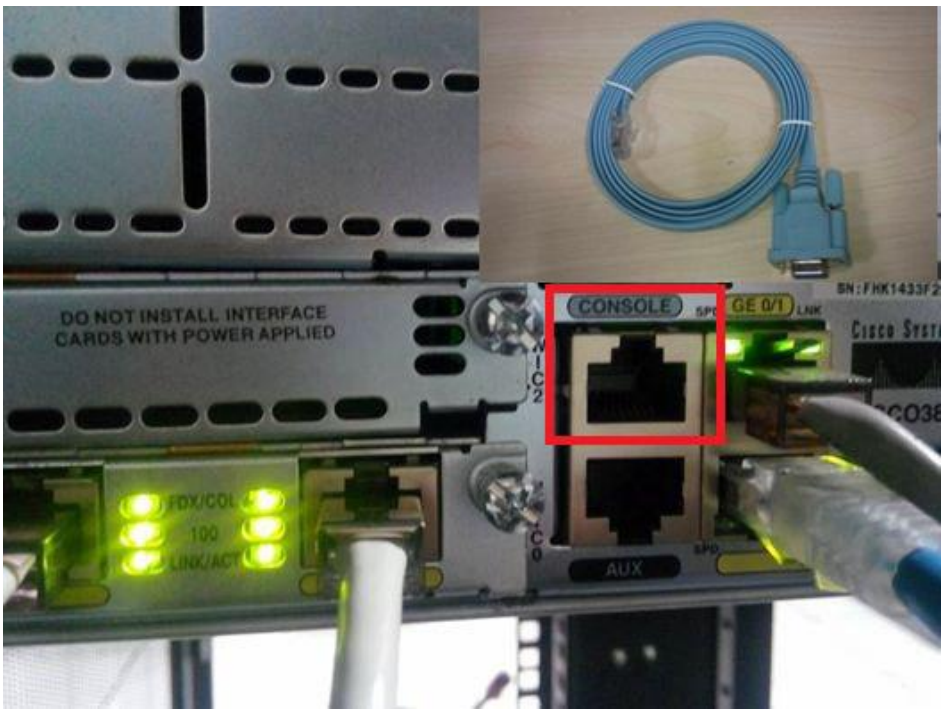
➢ ***Disable DNS lookup yang bertujuan untuk mencegah translasi perintah yang salah ketik.***

Egi_INDO(config)# no ip domain-lookup

➢ ***Pasang proteksi password pada privileged mode***

Egi_INDO(config)# enable secret tes1234

Configuring Console



Console adalah sebuah Port, yang dimana untuk dapat mengoprek, mensetting, ngonfig Router / Switch tersebut. Untuk masuk ke IOS, terdapat 3 cara yaitu melalui Console, Telnet dan SSH. Telnet dan SSH adalah secara jarak jauh, sedangkan Console adalah berada di tempat, dimana Router / Switch itu berada.

➢ ***Pasang proteksi password pada console (Low Protection)***

```
Egi_INDO(config)# line console 0
Egi_INDO(config-line)# password egi1234
Egi_INDO(config-line)# login
```

- ***Pasang proteksi pada Console (High Protection)***

```
Egi_INDO(config)# username egifadli secret 1234
Egi_INDO(config)# line con 0
Egi_INDO(config-line)# login local
Egi_INDO(config-line)# exit
```

- ***Banner, untuk menulis sebuah deskripsi pada Router / Switch ketika memasuki IOSnya***

```
Egi_INDO(config)# banner login # jomblo dilarang masuk #
```

12.Router Introduction

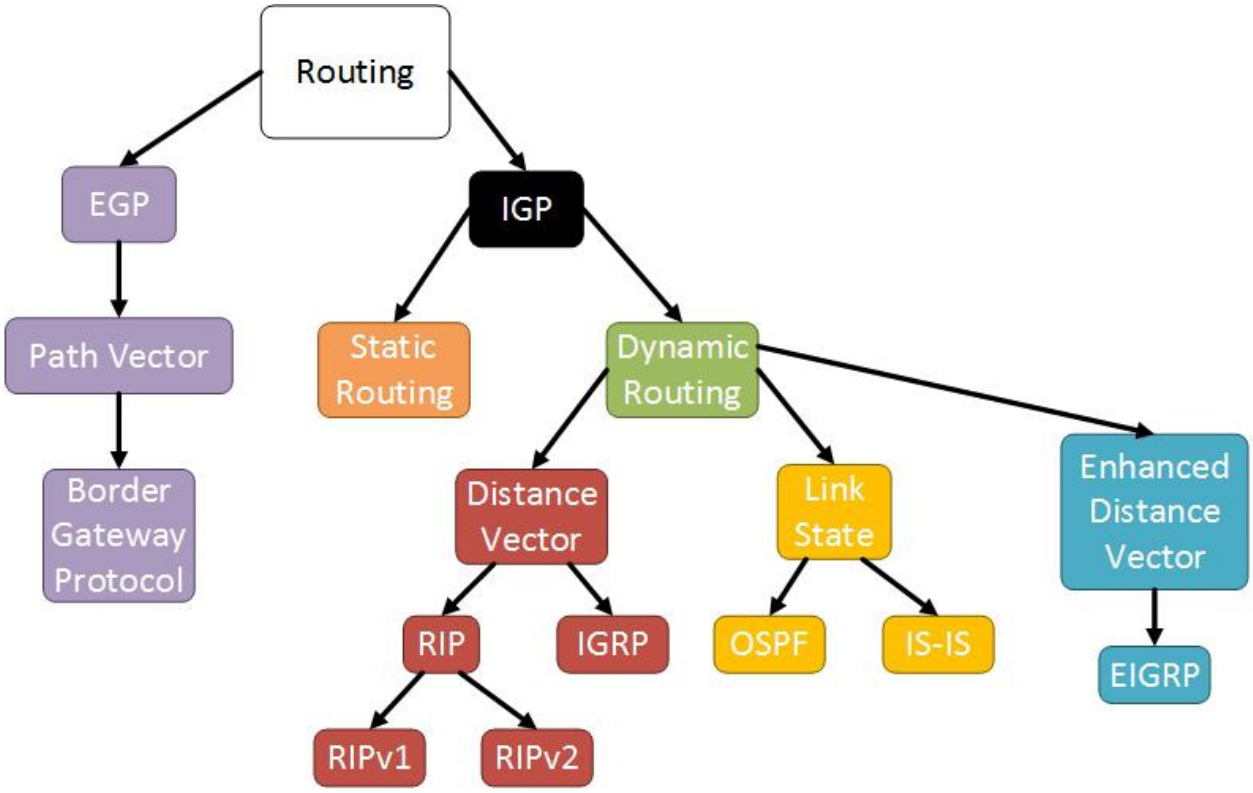
Router adalah sebuah perangkat yang berfungsi untuk menghubungkan 2 jaringan yang berbeda atau lebih. Atau Router juga dapat dikatakan sebagai perangkat yang berjasa agar suatu jaringan dapat berkomunikasi dengan jaringan yang lainnya. Router ini adalah perangkat utama di dalam jaringan, dimana ialah yang menghubungkan jaringan yang satu, dengan jaringan yang lainnya. Semisal, jaringan perusahaan A terhubung dengan jaringan perusahaan B, ketika Router ini bermasalah atau bahkan mati, maka hubungan koneksi antara Perusahaan A dan B tersebut bermasalah, hal ini memang bisa kita atasi dengan jalur Backup, namun tetap saja perangkat yang digunakan adalah Router. Ini menandakan perangkat Router ini sangat penting di dalam jaringan. Router ini bekerja pada layer 1, 2 & 3. Dan intinya ada pada Layer 3.

Router melakukan sebuah proses yang disebut dengan Routing. Apa itu Routing ? yaitu sebuah proses formarding packet data yang menuju ke jaringan yang lainnya, dengan memilih jalur terbaik dari routing table. Routing inilah yang berjasa jaringan kita bisa berkomunikasi dengan jaringan yang lainnya.

Apa itu routing table ? yaitu routing table adalah sebuah kumpulan-kumpulan jalur terbaik (berdasarkan Routing Protocol) untuk setiap Network Destination alias jaringan yang ingin dituju. Routing table ini digunakan untuk menentukan “ akan kemanakah ? “ atau “ melalui manakah ? “ packet data tersebut dikirim.

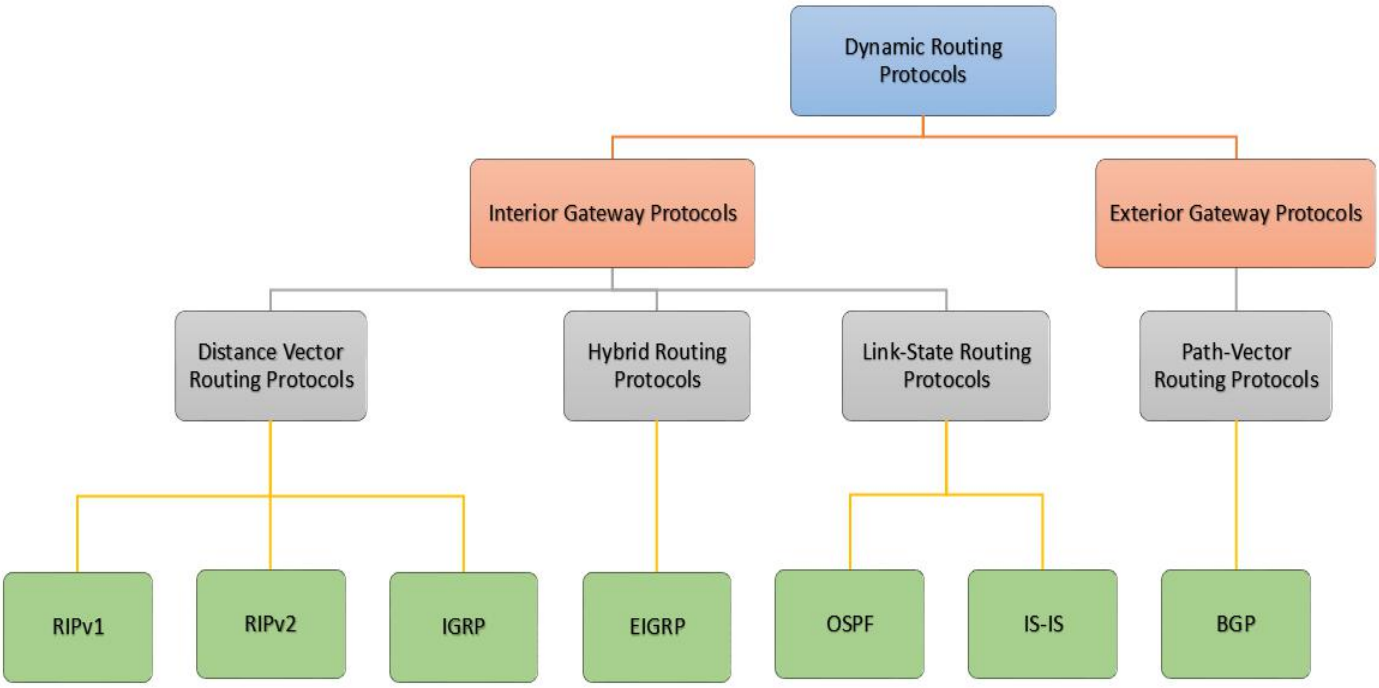
Perintah untuk melihat routing table :

Router# show ip route



Jenis routing umumnya terbagi dua, yaitu static routing dan Dynamic Routing. Apa itu Static Routing ? Simplenya, static routing adalah sebuah mekanisme routing yang menggunakan alogirtma secara manual, alias sang Admin nya lah yang menentukan dan membuat algoritma tersebut. Tentu yang dimaksud disini adalah algoritma dalam hal mencari jalur terbaik.

Lalu apa itu dynamic routing ? untuk dynamic routing nanti akan kita bahas di materi yang terpisah. Materi khusus membahas dynamic routing.



13. Dynamic Routing Introduction

Apa itu Dynamic Routing ? Dynamic Routing adalah sebuah tehnik (teknologi) dalam jaringan yang membuat data routing menjadi optimal. Mengapa ? karena tidak seperti static routing, dynamic routing memiliki fitur yang dimana agar router dapat memilih jalur terbaik sesuai yang diinginkan dengan secara real-time.

Tidak hanya itu, pada Dynamic Routing itu jauh lebih mudah dikonfigurasi dari pada Static Routing. Dynamic Routing berjalan diatas protocol, sedangkan Static Routing adalah sebuah mekanisme. Tapi seperti yang kita ketahui, bahwa hampir segala sesuatu selalu memiliki kekurangan dan kelebihan. Kekurangan Dynamic Routing ini mengkonsumsi Processor dan RAM lebih besar dari pada Static. Dan tak hanya itu, Dynamic Routing tingkat keamanannya lebih rendah daripada Static Routing.

Yuk … kita coba ingat tulisan sebelumnya pada Router Introduction. ***Bagaimana caranya Router memilih jalur terbaik dari Routing Table ?*** jawabannya yaitu dari nilai ***Administrative Distance.***

Apa itu Administrative Distance ?

Administrative Distance adalah sebuah nilai yang dimana digunakan oleh Router untuk memilih jalur terbaik ketika terdapat dua atau lebih rute dengan destination network yang sama dan dari routing protocol yang berbeda.

Berikut tabel Nilai Administrative Distancenya :

Routing Technique	Preference
Connected Interface	0
Static Route	1
EIGRP Summary Route	5
EBGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
ISIS	115
RIP	120
EGP	140
ODR	160
External EIGRP	170
Internal BGP	200
Unknown	255

Semakin kecil nilai tersebut, maka itulah yang semakin terpilih oleh Router.

Day 4

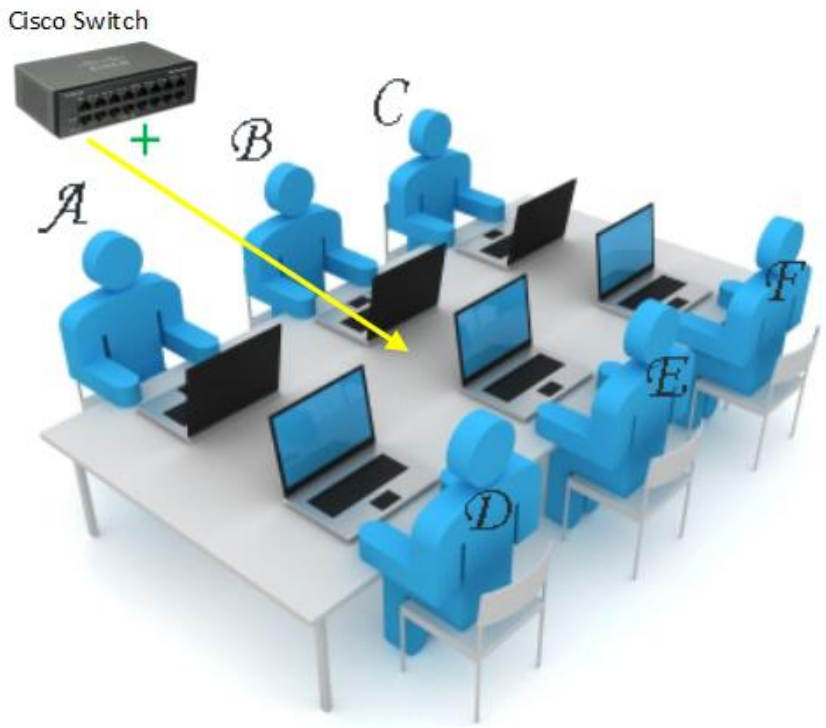
14.Apa itu Switch

Bagaimana dengan contoh " SEDERHANA ", kapan ketika saya membutuhkan

Switch ?

Silahkan anda lihat gambar tersebut, disitu terdapat 6 orang yang masing-masing memiliki Laptop di dalam meja yang sama. Nah… ke 6 orang tersebut ingin melakukan berbagi Transfer file dari yang satu ke yang lainnya, seperti mengirim document, file, data, dan sebagainya. **Semisal,** bagaimana caranya si **A** mengirim document sebesar 2 GB tanpa

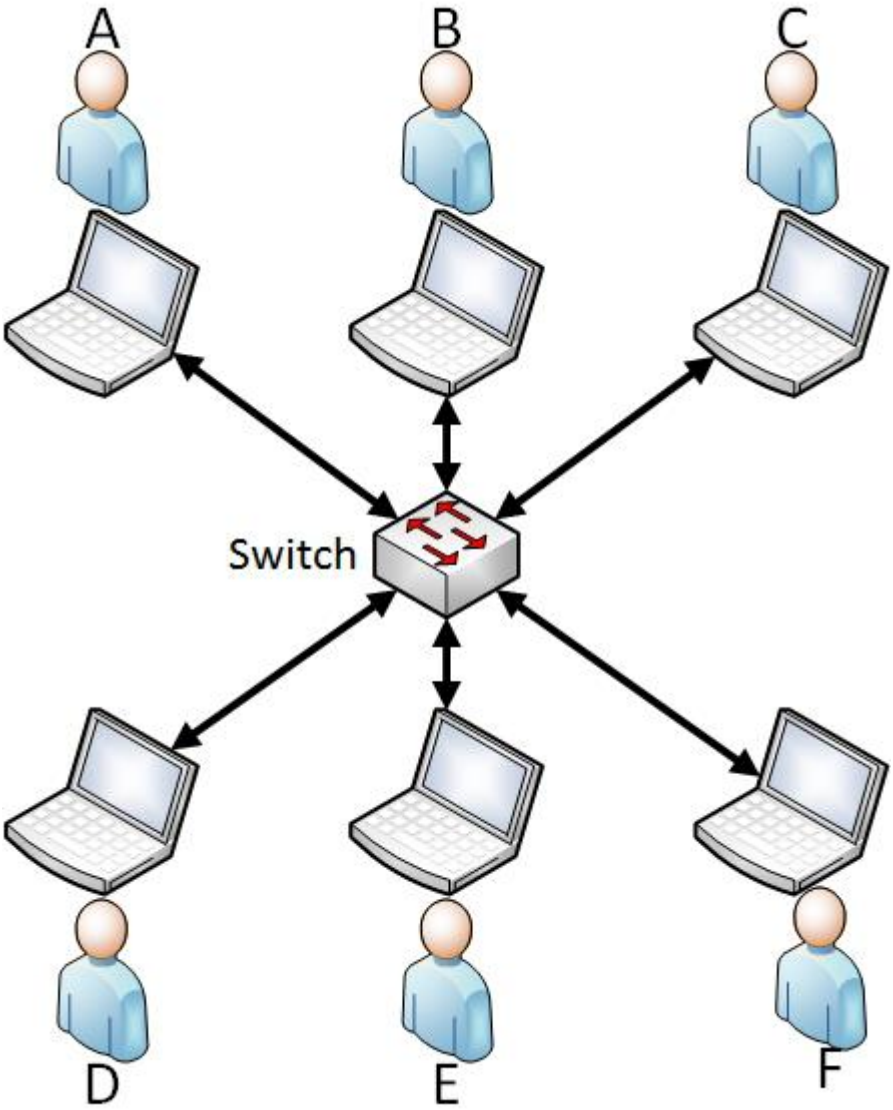
membutuhkan waktu yang lama ke si **E, D dan C** ? Jawabannya untuk orang awam mungkin bisa dengan cara, si **A** mempunyai flashdisk yang berkapasitas lebih besar dari 2 GB, lalu menaruh Documentnya ke dalam Flashdisk, dan membagikannya ke si **E, D dan C.** Namun, bukankah cara seperti itu membutuhkan waktu yang lama ? bukankah cara tersebut tidak bisa ditransfer secara bersamaan ? jika si **E** sedang meng-copy document dari Flashdisk si **A,** maka si **D dan C** sedang menunggu flashdisk tersebut. Ahh… itumah



cara lama bro.., jadi cara yang tepat untuk sharing file yang besar adalah :

Kita bangun atau membuat jaringan yang terdiri dari 6 laptop tersebut. Caranya pun sangat mudah. Yaitu kita gunakan Switch yang bertugas untuk menghubungkan ke 6 laptop tersebut. Dengan begini, maka komunikasi maupun sharing files pun dapat dilakukan secara bersamaan. Ketika si **A** berbagi file Document yang sebesar 2GB, Maka dengan begini si **E, C dan D** dapat mendownloadnya atau mengambilnya secara bersamaan, tanpa harus ganti-gantian atau menunggu giliran. Bahkan Speednya pun tergolong sangat cepat, untuk kecepatan Ethernet rata-rata adalah 10 sampai 100MBps alias 100MB per detik. Sehingga dalam 1 sampai 3 menit pun sudah selesai ter-download

document 2GB tersebut oleh si **E, D dan C**. Bukankah cara seperti sangat efisien ? yap betul sekali…



Berikut gambaran topologinya :

Jadi… dari penjelasan di atas, agan sudah paham kan ? kapan kita membutuhkan atau menggunakan Switch ? Yap… yaitu ketika kita ingin menghubungkan perangkat yang satu, dengan perangkat yang lainnya dalam jaringan yang sama. Yaitu ketika kita dari 6 laptop tersebut ingin berkomunikasi dalam jaringan yang sama. Maka

dari itu silahkan agan perhatikan pada gambar awal, disitu terdapat 6 orang ataupun 6 laptop tersebut berada dalam meja yang sama, ini menggambarkan bahwa mereka sebenarnya berada di dalam LAN yang sama ataupun Jaringan yang sama.

Apa sih Switching itu ?

Switching adalah sebuah Proses yang dilakukan oleh perangkat jaringan, yang mengarahkan sinyal (Layer 1) atau sebuah element data yang menuju ke perangkat (Hardware) tertentu. Switching ini juga bisa disebut sebagai sebuah technology. (Proses Switching ada pada L1 & L2)

Pada CCNA kali ini, materi Switching kita fokus membahas tentang cara kerja, cara berkomunikasi pada Cisco Switch. Sebenarnya antara Cisco Switch dengan Switch Brand yang lainnya tidaklah berbeda, sama-sama memiliki konsep yang sama.

15.Configuring Telnet

Apa itu Telnet ? telnet adalah sebuah *User Command* dan dibangun dengan dasar TCP / IP, yang digunakan sebagai *Access* untuk me-*Remote Computer* atau sebuah perangkat yang terhubung dengan sebuah jaringan. Melalui Telnet, seorang Administrator atau User dapat mengakses dan mengontrol (me-remote) komputer atau perangkat tersebut dari jarak jauh.

Seperti contoh, kita bekerja sebagai staff IT di sebuah perusahaan yang berada di bandung. Di waktu itu, kita sedang berada di Jakarta, dan mendapatkan telepon dari orang kantor, bahwa ada komputer yang terjadi error, dan komputer itu harus segera dibetulkan dari masalahnya. Dikasus seperti ini, tidak mungkin rasanya kita harus ke Bandung dengan segera, nah kasus seperti inilah disaat yang tepat untuk menggunakan Telnet. Tinggal kita remote komputer yang di bandung tersebut dari Jakarta.

Info lebih lengkap :

https://egifadlisoerachman.wordpress.com/2014/08/11/konfigurasi-telnet-cisco/

Wokeh, sekarang saatnya Lab.

1. ***Config IP pada Router***

```
Router> en
Router# conf t
Router(config)# int fa0/0
Router(config-if)# ip add 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
```

2. ***Config Telnet Pada Router***

```
Router(config-if)# exit
Router(config)# enable secret egi
Router(config)# username egifadli secret CCIE
Router(config)# line vty 0 4
Router(config-line)# login local
```

16. Configuring SSH

Apa itu SSH ? SSH merupakan singkatan dari Secure Shell, ssh ini sama halnya seperti Telnet, lalu apa bedanya ? bedanya pada SSH memiliki jalur koneksi yang aman, antara jalur dari user yang me-remote dan komputer yang sedang diremote. Kenapa SSH dikatakan lebih aman dari pada Telnet ? karena pada SSH, setiap informasi pada Data yang berlalu lalang di jalur tersebut, telah ter-enkripsi, sehingga user yang iseng (Hacker) akan kesulitan membaca informasi pada Data yang berlalu lalang tersebut. Beda dengan Telnet, sedangkan Telnet tidak ter-enkripsi sama sekali alias ClearText, sehingga user yang awam ketika melakukan iseng membaca informasi packet data yang berlalu lalang, bisa langsung dibaca isi informasi tersebut. Nah hal seperti inilah yang berujung menjadi bahaya, karena tak ada lagi ke-rahasian informasi tersebut.

Informasi lebih lanjut : https://egifadlisoerachman.wordpress.com/2014/08/14/ssh-pada-switch-cisco/

Untuk lab, kita melanjutkan topologi sebelumnya.

Config SSH

```
Router(config)# host R1
R1(config)# ip domain-name egi.com
```

```
R1(config)# crypto key generate rsa
The name for the keys will be: R1.egi.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 512
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
```

Tugas : silahkan konfig, agar si Router menerima di Remote melalui jalur SSH dan Telnet.

17.DHCP

Apa itu DHCP ? DHCP merupakan singkatan dari Dynamic Host Configuration Protocol, yaitu sebuah network management protocol yang digunakan untuk meminjamkan IP kepada setiap node yang baru memasuki jaringan secara dinamis. DHCP ini memungkinkan sebuah node dapat terkonfigurasi secara otomatis, sehingga dapat menghindari perlunya administrator jaringan untuk men-setting IP.

DHCP melakukan hal berikut :

- Mengelola IP terhadap semua nodes baik itu dalam hal menambahkannya ke jaringan ataupun mengusir dari jaringan tersebut.
- Maintains IP address yang unik dari host-host tersebut menggunakan DHCP server
- Mengirimkan sebuah permintaan IP kepada DHCP server setiap kali sebuah client/node, yang dimana telah dikonfigurasikan sebagai DHCP Client agar dapat terkoneksi dengan network. Dan server me-responnya dengan menyediakan sebuah IP address kepada client/node.

Referensi Dynamic Host Configuration Protocol terdapat pada di RFC 2131.

Yuk kita ngonfig

- ***Switch sebagai DHCP Server***

Switch dapat kita jadikan sebagai DHCP Server, yaitu melalui jalur VLAN.

Berikut perintahnya :

```
Switch(config)# ip dhcp pool <Nama Pool DHCPnya>
Switch(dhcp-config)# network <Network Address> <Netmask>
Switch(dhcp-config)# dns-server <IP Address>
Switch(dhcp-config)# default-router <IP Gateway>
```

Contoh konfigurasi :

```
Switch(config)# ip dhcp pool VLAN10
Switch(dhcp-config)# network 10.10.10.0    255.255.255.0
Switch(dhcp-config)# dns-server 10.10.10.10
Switch(dhcp-config)# default-router 10.10.10.1
```

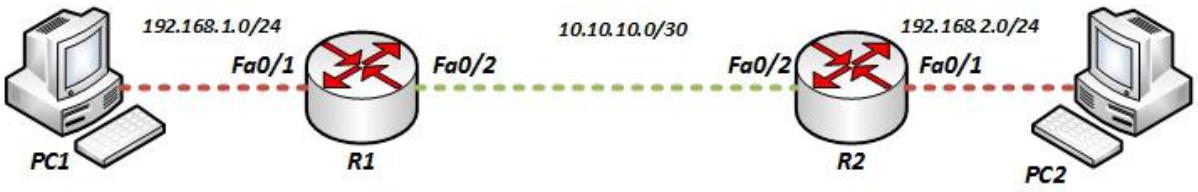
Jika ada IP yang tidak boleh untuk diberikan oleh DHCP Server ke Client, berikut perintahnya :

```
Switch(config)# ip dhcp excluded-address <Low IP> <High IP>
```

Berikut contohnya :

```
Switch(config)# ip dhcp excluded-address 10.10.10.1   10.10.10.10
```

18.Static Routing



Untuk mengkonfig static route ada 3 cara. Yaitu exit interface, next-hop ip dan Exit interface + next hop ip (hanya dapat dilakukan pada Real Devices atau Emulasi), pada pembahasan kali ini kita tidak membahas pada cara ke 3. Yaitu cara next-hop ip + exit interface.

- ***Exit Interface***

  Sesuai namanya, Static Route dengan metode ini, me-routing packet data berdasarkan interface yang sesuai pada tabel routing (Destination Network). Berikut perintahnya :

  Router(config)# ip route <destination network> <netmask destination network> <interface>

  Contoh pada kasus gambar di lembar sebelumnya, R1 ingin me-routing ke jaringan R2 yang **192.168.2.0/24** menggunakan static route. Berikut perintahnya :

  R1(config)# ip route 192.168.2.0 255.255.255.0 fa0/2

- ***Next-Hop IP***

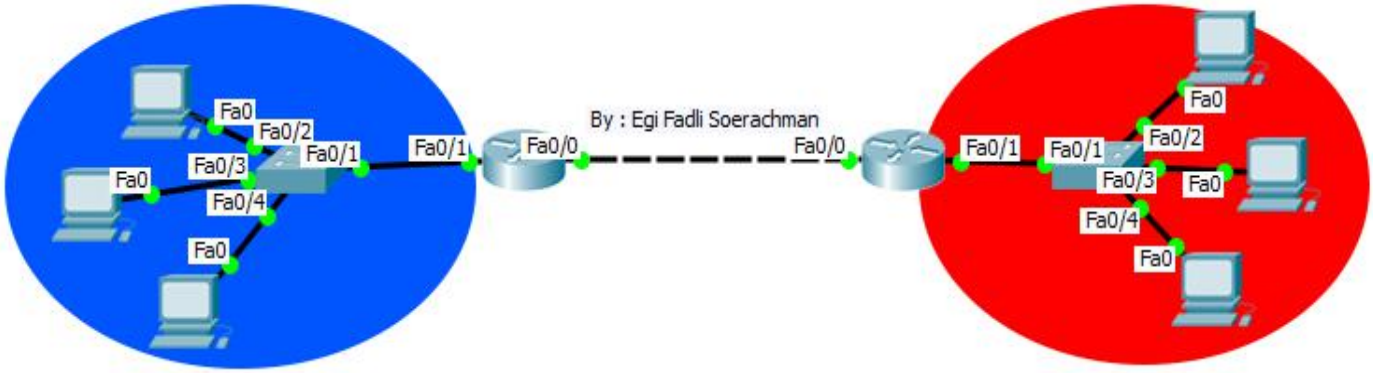
  Static Route dengan metode ini, me-routing packet data berdasarkan alamat IP Router Tetangga, yang dimana router tersebut terhubung dengan Destination Network yang ingin dituju. Hop ini bisa kita artikan sebagai Router Tetangga atau Router yang berperan sebagai perantara. Yaitu perantara yang menghubungkan antara jaringan kita dengan jaringan destination network yang ingin dituju.

  Berikut perintahnya :

  Router(config)# ip route <destination network> <netmask destination network> <interface>

  Contoh pada kasus gambar di lembar sebelumnya, R1 ingin me-routing ke jaringan R2 yang **192.168.2.0/24** menggunakan static route. Berikut perintahnya :

```
R1(config)# ip route 192.168.2.0 255.255.255.0 fa0/2
```



Static Routing Configuration

Bisa kita lihat, di dalam topologi ini ada dua area, yaitu area biru dan area merah.

Area biru memiliki network 192.168.1.0/24 dan merah 192.168.2.0/24. Nah bagaimana cara menghubungkan kedua jaringan ini agar saling bisa berkomunikasi ? berikut langkahnya.

*Di Router yang area biru, bernama R1 sedangkan area merah dengan hostname R2.

- ***R1 (Interface : Assign IP Configuration + Up Link)***

```
R1(config)# interface fa0/0
R1(config-if)# ip address 192.168.100.1 255.255.255.248
R1(config-if)# no shutdown
R1(config-if)# interface fa0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
```

- ***R2 (Interface : Assign IP Configuration + Up Link)***

```
R2(config)# interface fa0/0
R2(config-if)# ip address 192.168.100.2 255.255.255.248
```

```
R2(config-if)# no shutdown
R2(config-if)# interface fa0/1
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)# no shutdown
```

Routing Configuration

- ***IP Next Hop***

Berikut format perintahnya, **# ip route <Destination Prefix> <Destination Prefix Mask> <Forwarding Router's Address>**

```
R1(config)# ip route 192.168.2.0 255.255.255.0 192.168.100.2
R2(config)# ip route 192.168.1.0 255.255.255.0 192.168.100.1
```

- ***Exit Interface***

Berikut format perintahnya, **# ip route <Destination Prefix> <Destination Prefix Mask> <Exit Interface>**

```
R1(config)# ip route 192.168.2.0 255.255.255.0 fa0/0
R2(config)# ip route 192.168.1.0 255.255.255.0 fa0/0
```

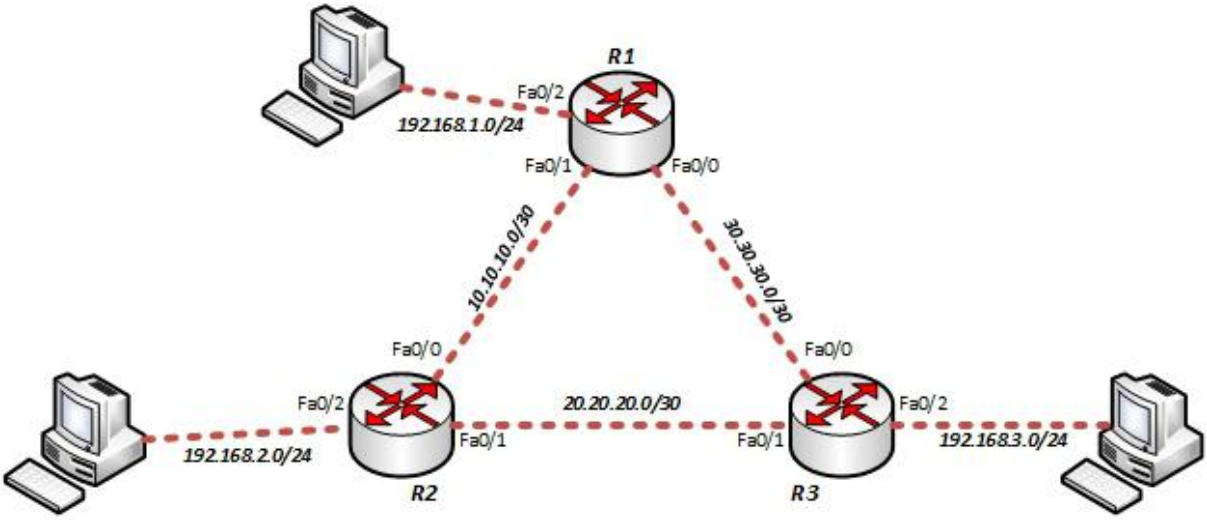
Tugas : hapus perintah IP Route yang sebelumnya, lalu diganti dengan IP Route yang menggunakan IP Next Hop dan Exit Interface sekaligus.

Day 5

19.Routing Information Protocol (RIP)

RIP yang merupakan singkatan dari Routing Information Protocol adalah sebuah Dynamic Routing yang digunakan untuk mencari jalur terbaik dari source menuju destination melalui jaringan berdasarkan Routing Metric / Hop Count Algorithm (Distance Vector). RIP adalah Routing Protocol yang sudah berumur cukup tua yakni sudah ada sejak tahun 1988 dan hingga sekarang belum dikembangkan lagi oleh Developer bahkan sudah tidak dikembangkan.

Jumlah hop countnya terbatas, yaitu hanya 15 saja. RIP tidak men-support jika hop count lebih dari 15.



Routing Information Protocol Configuration

- ***R1 (Interface Configuration)***

```
R1(config)# interface fa0/1
R1(config-if)# ip address 10.10.10.2  255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# interface fa0/0
R1(config-if)# ip address 30.30.30.1  255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# interface fa0/2
```

```
R1(config-if)# ip address 192.168.1.1  255.255.255.0
R1(config-if)# no shutdown
```

- ***R2 (Interface Configuration)***

```
R2(config)# interface fa0/1
R2(config-if)# ip address 20.20.20.1  255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# interface fa0/0
R2(config-if)# ip address 10.10.10.1  255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# interface fa0/2
R2(config-if)# ip address 192.168.2.1  255.255.255.0
R2(config-if)# no shutdown
```

- ***R3 (Interface Configuration)***

```
R3(config)# interface fa0/1
R3(config-if)# ip address 20.20.20.2  255.255.255.252
R3(config-if)# no shutdown
R3(config-if)# interface fa0/0
R3(config-if)# ip address 30.30.30.2  255.255.255.252
R3(config-if)# no shutdown
R3(config-if)# interface fa0/2
R3(config-if)# ip address 192.168.3.1  255.255.255.0
R3(config-if)# no shutdown
```

- ***R1***

```
R1(config)# router rip
R1(config-router)# network 10.10.10.0
R1(config-router)# network 30.30.30.0
R1(config-router)# network 192.168.1.0
```

- ***R2***

```
R2(config)# router rip
```

```
R2(config-router)# network 10.10.10.0
R2(config-router)# network 20.20.20.0
R2(config-router)# network 192.168.2.0
```

- ***R3***

```
R3(config)# router rip
R3(config-router)# network 20.20.20.0
R3(config-router)# network 30.30.30.0
R3(config-router)# network 192.168.3.0
```

- ***Troubleshooting***

```
Router# show ip route
```

20.RIPv2

Apa itu RIPv2 ? RIPv2 adalah hasil pengembangan & penyempurnaan versi sebelumnya yakni RIPv1. RIPv2 ini dikembangkan pada tahun 1993 dan terakhir kali dikembangkan adalah pada tahun 1998. Apa saja perbedaan RIPv1 dan RIPv2 ? berikut tabelnya :

RIPv1	RIPv2
RIPv1 is a Distance-Vector Routing protocol.	RIPv2 is a Hybrid Routing Protocol. A Hybrid Routing Protocol is basically a Distance-Vector protocol which some characteristics of Link State routing protocols.
RIPv1 is a Classful routing protocol. Classful routing protocols support only the networks which are not subnetted. Classful routing protocols do not send subnet mask information with their routing updates. In other words, if you have a subnetted network in your RIPv1 routing domain, RIPv1 will announce that network to other as unsubnetted network.	RIPv2 is classless routing, which allows us to use subnetted networks also. RIPv2 has the option for sending network mask in the update to allow classless routing.
RIPv1 does not support VLSM (Variable Length Subnet Masking).	RIPv2 support VLSM (Variable Length Subnet Masking).
RIPv1 support maximum metric (hop count) value of 15. Any router farther than 15 hops away is considered as unreachable.	RIPv2 support maximum metric (hop count) value of 15. Any router farther than 15 hops away is considered as unreachable.
RIPv1 send routing updates periodically	RIPv2 routing updates are sent as Multicast

every 30 seconds as broadcasts using destination IP address as limited broadcast IP adddress 255.255.255.255. Since the updates are sent using the destination IP address of limited broadcast IP adddress 255.255.255.255, every router need to process the routing update messages (whether they are running RIPv1 or not).	traffic at destination multicast address of 224.0.0.9. Multicast updates reduce the network traffic. The Multicast routing updates also helps in reducing routing update message processing overhead in routers which are not running RIPv2. Only the routers running RIPv2 join to the multicast group 224.0.0.9. Other routers which are not running RIPv2 can simply filter the routing update packet at Layer 2.
RIPv1 does not support authentication of update messages (plain-text or MD5).	RIPv2 support authentication of RIPv2 update messages (plain-text or MD5). Authentication helps in confirming that the updates are coming from authorized sources.

Yuk … kita ngonfig

Topologinya kita lanjutkan yang tadi, yang kita lakukan hanyalah merubahnya menjadi versi 2.

- ***R1***

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# no auto-summary
```

- ***R2***

```
R2(config)# router rip
R2(config-router)# version 2
R2(config-router)# no auto-summary
```

- ***R3***

```
R3(config)# router rip
R3(config-router)# version 2
R3(config-router)# no auto-summary
```

- ***Troubleshooting***

```
Router# show ip route
Router# show ip protocols
```

21. VLAN

Apa itu VLAN ? VLAN adalah singkatan dari Virtual LAN. Yap sesuai namanya, yaitu memecah LAN yang ada, menjadi Virtual LAN. Pada VLAN, memecah segmentasi dari segi Layer 2, sedangkan memecah segmentasi dari layer 3 adalah dengan Subnetting.

Jaringan VLAN ini, pasti anda temui baik itu jaringan kecil ataupun yang besar, baik itu traffic yang low hingga high, JIKA dijaringan tersebut menggunakan Switch Manageable. Pada dasarnya, banyak jaringan yang menggunakan Switch Manageable, karena ingin memanfaatkan VLAN & Trunk, dua teknologi inilah yang paling diincar dari penggunaan Switch Manageable.

Apa saja benefit jaringan yang menggunakan VLAN ?

- Security
- Cost Reduction
- Higher Perfomance
- Broadcast Storm Mitigation
- Improved IT Staff Efficiency
- Simpler Project or Application Management

VLAN Configuration

Untuk menconfig VLAN pada Switch, ada 3 cara yaitu melalui Mode Privileged, Global Config, Interface.

Privileged Configuration

Switch# vlan database

% Warning: It is recommended to configure VLAN from config mode, as VLAN database mode is being deprecated. Please consult user documentation for configuring VTP/VLAN in config mode.

Switch# vlan 10 name egi

VLAN 10 added:

Name: egi

Global Config Configuration

Switch(config)# vlan 20

Switch(config-vlan)# name ozan

Interface Configuration

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 30

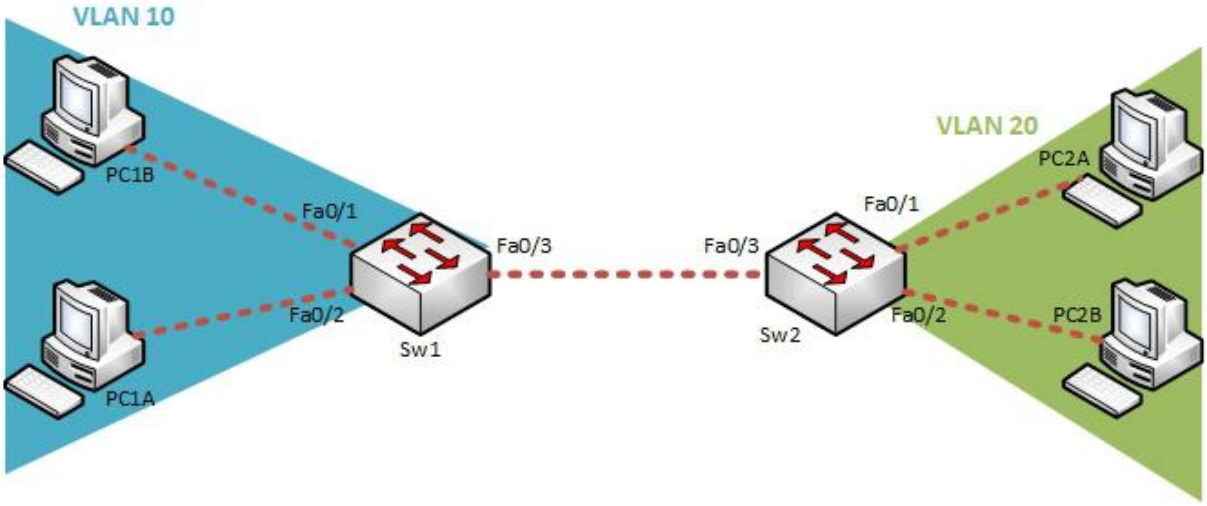
% Access VLAN does not exist. Creating vlan 30

Check VLAN Configuration

Switch# show vlan brief

VLAN	*Name*	*Status*	*Ports*
1	*default*	*Active*	*Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7,Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig0/1, Gig0/2*
10	*egi*	*active*	
20	*ozan*	*active*	
30	*VLAN0030*	*active*	*Fa0/1*
1002	*fddi-default*	*active*	
1003	*token-ring-default*	*active*	
1004	*fddinet-default*	*active*	
1005	*trnet-default*	*active*	

Ngonfig VLAN



- ***Sw1 (membuat VLAN)***

Sw1(config)# vlan 10

Sw1(config-vlan)# name dosen

- ***Sw2 (Membuat VLAN)***

Sw2(config)# vlan 20

Sw2(config-vlan)# name mahasiswa

- ***Sw1 (Assign VLAN ke Port Interface)***

Sw1(config)# int fa0/1

Sw1(config-if)# Switchport mode access

Sw1(config-if)# switchport access vlan 10

Sw1(config-if)# int fa0/2

Sw1(config-if)# switchport mode access

Sw1(config-if)# switchport access vlan 10

- ***Sw2 (Assign VLAN ke Port Interface)***

Sw2(config)# int ra fa0/1 – 2

Sw2(config-if-range)# switchport mode access

Sw2(config-if-range)# switchport access vlan 20

- ***Verifikasi VLAN Status***

Sw1(config)# do show vlan brief

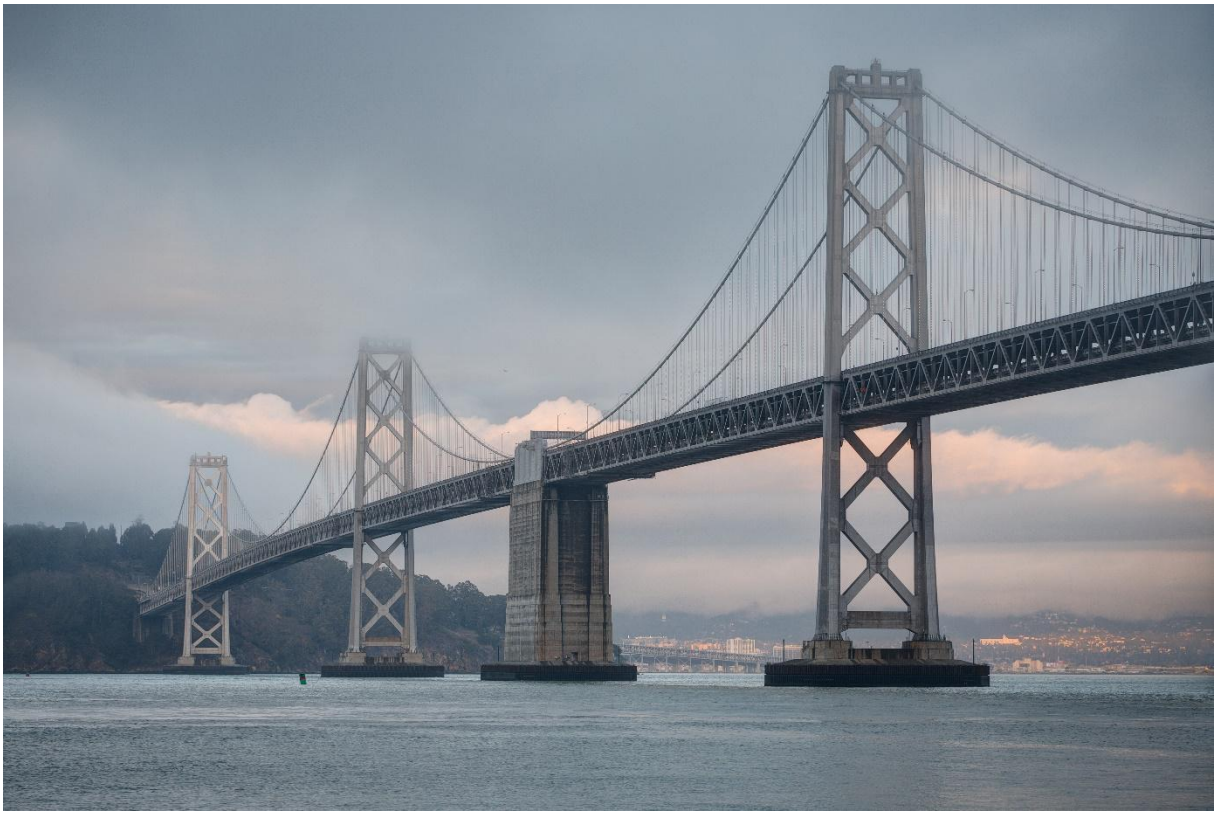
VLAN	*Name*	*Status*	*Ports*
1	*default*	*Active*	*Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7,Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig0/1, Gig0/2*
10	***dosen***	*active*	***Fa0/1, Fa0/2***
1002	*fddi-default*	*active*	
1003	*token-ring-default*	*active*	
1004	*fddinet-default*	*active*	
1005	*trnet-default*	*active*	

Sw2# sh vla bri

VLAN	*Name*	*Status*	*Ports*
1	*default*	*Active*	*Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7,Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig0/1, Gig0/2*
20	***mahasiswa***	*active*	***Fa0/1, Fa0/2***
1002	*fddi-default*	*active*	
1003	*token-ring-default*	*active*	
1004	*fddinet-default*	*active*	

1005	*trnet-default*	*active*	

22.Trunk



Apa itu Trunk ? Trunk berfungsi sebagai menjembatani VLAN. Sehingga pada Link tersebut bisa dilewati banyak VLAN.

Trunk Configuration

Switch(config-if)# switchport mode trunk

Checking / Verification Trunk

Switch# show interface trunk

Port	*Mode*	*Encapsulation*	*Status*	*Native vlan*
Fa0/1	*on*	*802.1q*	*trunking*	*1*

Port	*Vlans allowed on trunk*
Fa0/1	*1-1005*
Port	*Vlans allowed and active in management domain*
Fa0/1	*1*
Port	*Vlans in spanning tree forwarding state and not pruned*
Fa0/1	*1*

Apa itu Native VLAN ?

Native VLAN adalah VLAN yang tidak di " Tag " atau UnTagged, alias yang tidak dimodifikasi packet datanya oleh Switch.

Native VLAN Configuration

Switch(config-if)# switchport trunk native vlan 15

Untuk melakukan checking Native VLAN, yaitu sama dengan menggunakan *" **Switch#** show interface trunk ".* Atau bisa juga dengan melalui show interface <interface> switchport, pada contoh ini saya menggunakan interface FastEthernet 0/1

Switch# show interface fa0/1 switchport

Name: Fa0/1

Switchport: Enabled

Administrative Mode: trunk

Operational Mode: trunk

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: On

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: 15 (Inactive)

Voice VLAN: none

Administrative private-vlan host-association: none

Administrative private-vlan mapping: none

Administrative private-vlan trunk native VLAN: none

Administrative private-vlan trunk encapsulation: dot1q

Administrative private-vlan trunk normal VLANs: none

Administrative private-vlan trunk private VLANs: none

Operational private-vlan: none

Trunking VLANs Enabled: ALL

Pruning VLANs Enabled: 2-1001

Capture Mode Disabled

Capture VLANs Allowed: ALL

Protected: false

Appliance trust: none

Jika dikedua interfaces diantara kedua switch tersebut, salah satunya Native VLAN belum disesuaikan, maka akan muncul pesan error seperti berikut " *%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with Switch FastEthernet0/1 (15).* " kenapa bisa terjadi error ? hal ini disebabkan karena *Native VLAN* digunakan sebagai sarana komunikasi untuk protocol seperti CDP, VTP, DTP dan STP. Jika dikedua interface diantara kedua switch tersebut terjadi perbedaan *Native VLAN,* maka sudah pasti terjadi konflik, dengan penyebab ketidak cocokan *Native VLAN* tersebut.

Tugas : cari tau mengapa pada *Trunking Native Mode,* terdapat tulisan *(inactive),* dan temukan solusi & penyebabnya !

Filtering VLAN in Trunking

Switch(config-if)# switchport trunk allowed vlan 10, 20, 30

Silahkan lakukan verifikasi, melalui *" Show interface trunk "*. Jika ingin menambahkan, maka berikut perintahnya

Switch(config-if)# switchport trunk allowed vlan add 15

23. Dynamic Trunking Protocol

Apa itu Dynamic Trunking Protocol ?

Dynamic Trunking Protocol (DTP) adalah sebuah Trunking Protocol (Cisco proprietary), yang digunakan untuk menegosiasi trunk diantara perangkat Cisco Switches. Yang dimaksud negosiasi disini adalah status Switchport mode pada interface tersebut, akan menjadi Access ? atau Trunk ?

Pada Dynamic Trunking Protocol, terbagi menjadi 2 yaitu Dynamic Desirable dan Dynamic Auto.

- ***Dynamic Desirable***

  Dynamic Desirable ini sifatnya " Mengajak " atau " Nembak Duluan ", kepada Port Interface lawannya untuk menjadi Trunk. Bisa dibilang juga bahwa, Port Interface

yang statusnya Dynamic Desirable ini menginginkan untuk menjadi ***Trunk*** namun tidak menolak juga jika menjadi ***Access***.

Berikut perintah confignya :

Switch(config)# interface fa0/1

Switch(config-if)# switchport mode dynamic desirable

- ***Dynamic Auto***

  Dynamic Auto ini sifatnya " Menunggu diajak " atau " menunggu ditembak ", terhadap Port Interface lawannya untuk menjadi Trunk. Bisa dibilang juga bahwa, Port Interface yang statusnya Dynamic Auto ini menginginkan untuk menjadi ***Trunk***, mengapa ? karena ia menunggu Port Interface lawannya untuk mengajaknya menjadi ***Trunk***. Namun tidak menolak juga jika menjadi ***Access***.

  Berikut perintah confignya :

  Switch(config-if)# switchport mode dynamic auto

Berikut adalah tabel dari DTP :

	Access	**Trunk**	**Dynamic Auto**	**Dynamic Desirable**
Access	Access	Disconnected	Access	Access
Trunk	Disconnected	Trunk	Trunk	Trunk
Dynamic Auto	Access	Trunk	Access	Trunk
Dynamic Desirable	Access	Trunk	Trunk	Trunk

24. VLAN Trunking Protocol

VLAN Trunking Protocol (VTP) adalah sebuah Protocol (Cisco Propietary) yang digunakan oleh Cisco Switch, untuk menyebarkan Definisi (Informasi) VLAN kepada seluruh perangkat Switch di dalam Jaringan (LAN). Definisi yang disebarkan berguna untuk " Auto Configuration ", sehingga memudahkan NE. Selain itu VTP ini juga bisa meningkatkan Management pada perangkat-perangkat tersebut. Atau ada juga yang menyebutkannya bahwa VTP ini untuk meng-advertise kan informasi konfigurasi Database VLAN.

VTP terdapat 3 mode, yaitu Client, Server dan Transparent.

- ***VTP Mode Client***

  VTP Mode Client ini adalah seperti namanya, yaitu sebuah Switch yang bersifat sebagai Client DTP. Switch dengan mode ini, ia hanya menerima, men-singkronkan VLAN Database sesuai Informasi yang ia terima dari Server, lalu menyebarkannya kembali. VTP Mode ini tidak dapat membuat VLAN, merubah, dan menghapus.

Perintah Konfigurasinya :

Switch(config)# vtp mode client

- ***VTP Mode Server***

VTP Mode Server ini adalah seperti namanya, yaitu sebuah Switch yang bersifat sebagai Server DTP. Switch dengan mode ini, ia dapat menerima, men-singkronkan VLAN Database sesuai Informasi yang ia terima dari Server yang memiliki nilai " Revision " nya lebih tinggi, lalu menyebarkannya kembali. VTP Mode ini adalah yang dapat membuat VLAN, merubah, dan menghapus.

Setiap Switch, sudah secara default menggunakan mode server

Perintah Konfigurasinya :

Switch(config)# vtp mode Server

- ***VTP Mode Transparent***

VTP Mode Transparent ini adalah seperti namanya, yaitu sebuah Switch yang bersifat sebagai Transparent DTP. Switch dengan mode ini, ia hanya mem-forwardnya kembali informasi yang ia terima ke switch yang lain, ia tidak men-singkronkan VLAN Database yang di terimanya. VTP Mode ini dapat membuat VLAN, merubah, dan menghapus, namun Database VLAN tersebut digunakan hanya untuk dirinya saja.

Perintah Konfigurasinya :

Switch(config)# vtp mode transparent

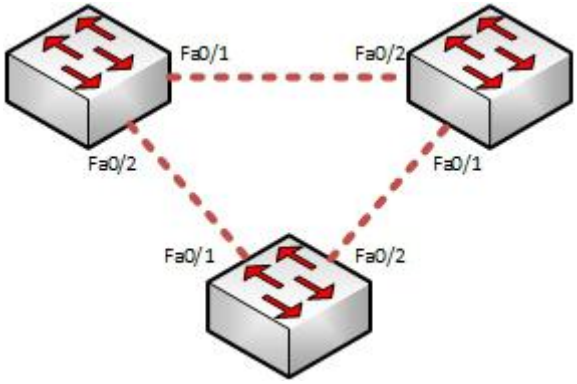
Day 6

25.Spanning Tree Protocol

Apa itu Spanning Tree Protocol (STP) ? Spanning Tree adalah sebuah protocol dalam hal link management yang bertujuan untuk mencegah terjadinya looping atau Frame Loop Forever atau broadcast storm. Terjadinya looping pada jaringan adalah sebuah bencana yang dimana banyak menimbulkan hal-hal yang tidak di inginkan seperti jaringan menjadi " Sibuk Sendiri ", kinerja perangkat menjadi berat, bahkan jaringan menjadi down.

Dengan STP ini, salah satu port atau lebih (tergantung topologi) yang akan menjadi blocking sehingga hanya satu link yang digunakan agar tidak terjadinya loop.

Berikut labnya :



Silahkan buat topologi seperti di gambar. Pada lab kita kali ini lebih ke menghitung terjadinya " Port Interface mana yang statusnya akan menjadi Blocking ? ". Berikut rumusnya :

- Root Bridge

1. Untuk menjadi Root Bridge yang pertama dilihat adalah nilai Prioritynya, yang terpilih adalah yang terkecil. Nilai defaultnya adalah 32768. Dan perubahan nilai Priority haruslah kelipatan 4096
2. Jika nilai Priority sama, maka yang dilihat selanjutnya adalah MAC Address terkecil.

- ***Root Port***

Setiap Port Interface yang berhadapan langsung dengan Root Bridge, maka ia adalah Root Port. Namun hal ini dilihat dari nilai Costnya, semakin kecil nilai cost maka Interface tersebut yang semakin terpilih.

Link Speed	Cost
10 GBps	2
1 GBps	4
100 MBps	19
10 MBps	100

- ***Designated Port***

Setiap Port Interfacenya Root Bridge adalah Designated Port, untuk selain Root Bridge, maka dilihat dari nilai Cost, jika sama maka MAC Address.

Perintah / Command :

- ***Untuk melihat MAC Address***

```
Switch# show version

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

ROM: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE
SOFTWARE (fc4)

System returned to ROM by power-on

Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of
memory.

24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 000C.CFE4.D382
Motherboard assembly number     : 73-9832-06
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC103248MJ
Power supply serial number      : DCA102133JA
Model revision number           : B0
Motherboard revision number     : C0
Model number                    : WS-C2960-24TT
System serial number            : FOC1033Z1EY
Top Assembly Part Number        : 800-26671-02
Top Assembly Revision Number    : B0
Version ID                      : V02
CLEI Code Number                : COM3K00BRA
Hardware Board Revision Number  : 0x01


Switch   Ports  Model              SW Version          SW Image
------   -----  -----              ----------          ----------
*   1     26    WS-C2960-24TT      12.2                C2960-LANBASE-M

Configuration register is 0xF
```

- ***Perintah untuk melihat status STP***

```
Switch# show spanning-tree
```

```
VLAN0001
 Spanning tree enabled protocol ieee
 Root ID    Priority    32769
          Address     0001.4282.284D
          Cost        19
          Port        1(FastEthernet0/1)
          Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

 Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
          Address     000C.CFE4.D382
          Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
          Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
```

- ***Contoh perintah untuk merubah nilai Priority***

```
Switch(config)# spanning-tree vlan 1 priority 28672
```

Atau

```
Switch(config)# spanning-tree vlan 1 priority 0
```

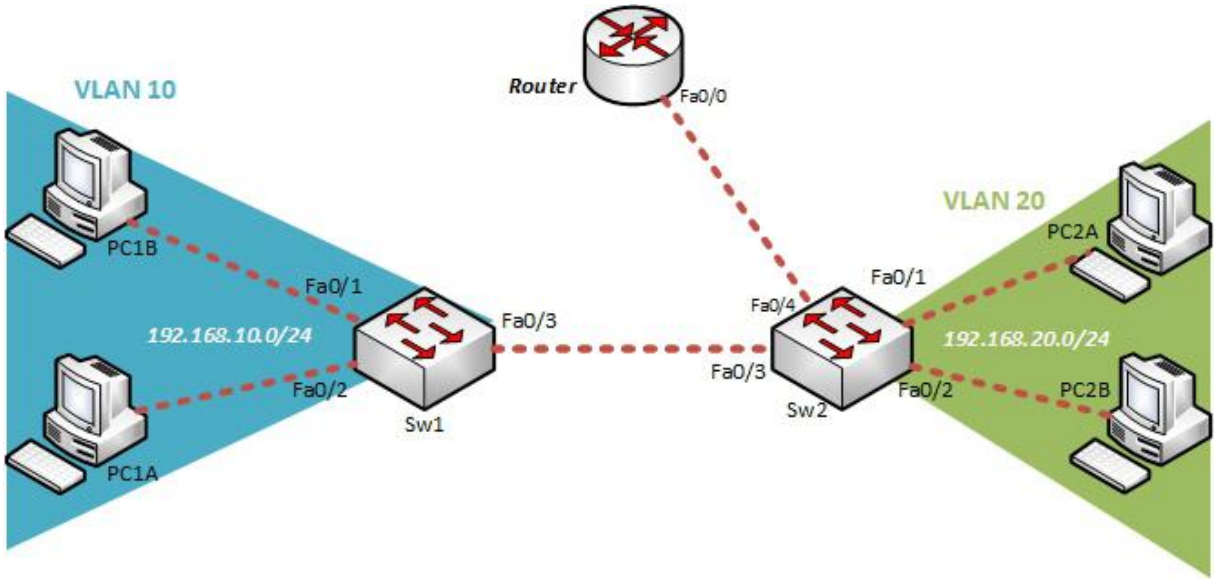
- ***Perintah untuk melihat status Root Bridge***

```
Switch# show spanning-tree

VLAN0001
 Spanning tree enabled protocol ieee
 Root ID    Priority    32769
          Address     0001.4282.284D
          This bridge is the root
          Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

 Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
          Address     0001.4282.284D
          Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
          Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p
```

26.InterVLAN Routing

Apa itu InterVLAN Routing ? InterVLAN Routing ini adalah sebuah Routing L3 yang me-Routingkan VLAN. Karena VLAN yang berbeda tidak dapat saling berkomunikasi, maka agar ia dapat berkomunikasi membutuhkan peran " Gateway ". Sedangkan peran Gateway ini ada pada router. InterVLAN Routing dapat menggunakan routing apa saja, baik itu directly connected, static route, OSPF, dsb.

InterVLAN Configuration



Contoh, kita ingin meroutingkan 2 VLAN, yaitu VLAN 10 dan VLAN 20. Dengan Network masing-masing 192.168.10.0/24 dan 192.168.20.0/24.

```
Router(config)# interface fa0/0
Router(config-if)# no shutdown
Router(config-if)# interface fa0/0.10
Router(config-subif)# encapsulation dot1q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config-subif)# interface fa0/0.20
Router(config-subif)# encapsulation dot1q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
```

****Note :*** jangan lupa untuk menjadikan trunk link pada switch yang berhadapan langsung dengan Router.

27.Port Security

Port Security adalah sebuah mekanisme yang digunakan untuk mengamankan port interface Switch menggunakan MAC Address dari perangkat liar yang tidak dijinkan pada Port Interface tersebut. Pada mekanisme Port Interface ini dapat mencegah terjadinya MAC Flooding dan Spoofing Attack

Pada Port Security, Violation Mode ada 3, yaitu :

- Protect

  Data yang masuk ke Port Interface yang menggunakan Violation Protect, data tersebut dibiarkan, atau diabaikan, atau dengan tidak mengirimkannya kembali.

  Perintah :

  Switch(config-if)# switchport mode access

  Switch(config-if)# switchport port-security

  Switch(config-if)# switchport port-security mac-address sticky

  Switch(config-if)# switchport port-security violation **protect**

- Restrict

  Pada Restrict ini Seperti Protect, yaitu Data yang masuk ke Port Interface yang menggunakan Violation Protect, data tersebut dibiarkan, atau diabaikan, atau dengan tidak mengirimkannya kembali. Hanya saja ia mengirimkan notifikasi dengan SNMP.

  Perintah :

  Switch(config-if)# switchport mode access

  Switch(config-if)# switchport port-security

  Switch(config-if)# switchport port-security mac-address sticky

  Switch(config-if)# switchport port-security violation restrict

- ***Shutdown***

  Pada Shutdown ini ketika terjadi pelanggaran maka ia akan mematikan port interface tersebut. Untuk menyalakannya kembali dengan cara manual, yaitu dengan perintah mematikan, lalu menyalakan port interface tersebut.

  Perintah :

  Switch(config-if)# switchport mode access

  Switch(config-if)# switchport port-security

  Switch(config-if)# switchport port-security mac-address sticky

  Switch(config-if)# switchport port-security violation protect

- ***Perintah melihat status Port Security***

  Switch# show port-security

28.Etherchannel

Apa itu Etherchannel ? Etherchannel atau ada yang menyebutkannya dengan Link Aggregation adalah sebuah teknologi yang memungkinkan menggabungkan beberapa link untuk dijadikan satu link logical. Tujuan dari etherchannel ini untuk meningkatkan kecepatan pada jalur link tersebut. Semisal link / interface nya menggunakan tipe 100 Base Tx yang berkecapatan 100MBps, lalu terdapat 2 link yang sama dan ingin menggabungkannya menjadi satu dengan etherchannel maka Kecepatannya adalah 100MBps x2 = 200MBps.

Kita dapat mengkonfigurasikan etherchannel dengan 3 cara. Yaitu PAgP, LACP dan ON.

- ***PAgP (Port Aggregation Protocol)***

  PAgP ini adalah sebuah protocol cisco proprietary. PAgP memiliki keunggulan kepada kecepatan link yang dihasilkan dibandingkan yang lainnya. PAgP terbagi

menjadi 2 mode yaitu Desirable dan Auto. Definisi Desirable dan auto sama seperti yang ada pada DTP.

Perintah Desirable :

```
Switch(config-if-range)# channel-protocol pagp
Switch(config-if-range)# channel-group 1 mode desirable
```

Perintah Auto :

```
Switch(config-if-range)# channel-protocol pagp
Switch(config-if-range)# channel-group 1 mode auto
```

- ***LACP (Link Aggregation Control Protocol)***

LACP ini adalah protocol yang sifatnya open. LACP ini lebih memiliki keunggulan yang lebih banyak dibandingkan PAgP. Diantaranya dapat mencegah terjadi Loop Pada Switch ketika terjadi Misconfiguration. Pintar dalam hal beradaptasi (penyesuaian kondisi pada link). Dan kebanyakan orang lebih memilih menggunakan LACP karena beberapa keunggulannya dan yang terpenting adalah sifatnya yang open. LACP juga terbagi menjadi 2 mode yaitu Active dan Passive. Hal ini memiliki definisi yang sama dengan Desirable dan Auto.

Perintah Active :

```
Switch(config-if-range)# channel-protocol lacp
Switch(config-if-range)# channel-group 1 mode active
```

Perintah Passive :

```
Switch(config-if-range)# channel-protocol lacp
Switch(config-if-range)# channel-group 1 mode passive
```

- ***ON***

ON ini adalah bukan sebuah protocol selayaknya LACP ataupun PAgP. ON ini juga tidak melakukan negosiasi melainkan sebuah mekanisme. ON ini juga bisa dikatakan sebagai Static Link Aggregation atau Static Etherchannel.

Perintah :

```
Switch(config-if-range)# channel-group 1 mode on
```

- ***Troubleshooting***

```
Switch# show etherchannel summary
```

Atau

```
Switch# show etherchannel port-channel
```

Atau

```
Switch# show interface port-channel 1
```

Day 7

29.OSPF

Open Shortest Path First (OSPF) adalah sebuah link state routing protocol (LSRP) yang menggunakan Shortest Path First (SPF) network communication algorithm (Dijkstra's algorithm) untuk mengkalkulasi Jalur Koneksi tersingkat diantara perangkat yang dikenali.

Cara kerja OSPF mencari jalur terbaik adalah dengan melalui hitungan bandwidth. Semakin besar nilai Bandwidth, maka jalur tersebut lah yang semakin terpilih. Apa saja kelebihan OSPF dibandingkan RIP ? berikut listnya :

RIP vs OSPF

Features	RIP		OSPF
	Version 1	Version 2	
Algorithm	Bellman-Ford		Dijkstra
Path Selection	Hop based		Shortest Path
Routing	Classful	Classless	Classless
Transmission	Broadcast	Multicast	Multicast
Administrative Distance	120		*110*
Hop Count Limitation	15		No Limitation
Authentication	No	MD5	MD5
Protocol	UDP		IP
Convergence Time	RIP>OSPF		

Kelebihan OSPF :

- Loop Free
- Konvergensi lebih cepat dibandingkan RIP
- Tidak ada batasan jumlah HOP
- Open Standard
- Minim atau bahkan tidak melakukan update routing (jika tidak ada perubahan)
- Hierarchical Network dengan menggunakan Area

Kekurangan OPSF :

- High Resource CPU & RAM
- Diharuskannya kompleks men-design dan mengimplementasikannya

Metric Calculation :

Cost : 10^8 / Bandwitdth Interface Out (dalam Bit)

Perintah (Tshoot) :

Router# show interface <name interface>

Router# show ip route <destination networks>

Perintah pada OSPF

Router(config)# router OSPF <Proccess ID> *(Meng-aktifkan OSPF Routing)*

Router(config-router)# network <Network Address> <Wildcard Address> area <ID> *(memasukan Network Address kedalam Routing)*

Router# show ip ospf *(melihat Status pada OSPF)*

Router# show ip ospf database *(melihat database OSPF)*

Router# show ip ospf neighbor *(melihat Neighbor table)*

OSPF Authentication

Pada OSPF terdapat fitur untuk security, yaitu authentication. Authentication dapat dilakukan dengan 2 cara, yaitu melalui interface atau melalui area OSPF. Sebelum melakukan konfigurasi Authentication, pastikan didalam topologi tersebut sudah run dengan baik pada interface, ip dan OSPF nya. Dan yang sekarang kita gunakan adalah menggunakan Interface saja.

- ***R1***

R1(config)# interface fa0/1

R1(config)# ip ospf authentication message-digest

R1(config)# ip ospf message-digest-key 1 md5 EGI

- ***R2***

R2(config)# interface fa0/1

R2(config)# ip ospf authentication message-digest

R2(config)# ip ospf message-digest-key 1 md5 EGI

- ***Verification***

  R1# show ip ospf interface fa0/1 *(lakukan pada R2 juga)*

30.EIGRP

EIGRP merupakan singkatan dari Enhanced Interior Gateway Routing Protocol yaitu sebuah advanced distance vector routing protocol yang diciptakan oleh Cisco. Cisco memperkenalkan EIGRP karena Dunia Jaringan membutuhkan sebuah protocol dengan faster converging abilities, route selection and calculation and the ability to record information from neighboring devices.

EIGRP menggunakan algoritma yang disebut dengan DUAL yang merupakan singkatan dari Diffusing Update Algorithm. DUAL menghitung atau mengkalkulasi routing berdasarkan Bandwidth, Delay, Load dan Reliability. Seperti apakah itu ? berikut penjelasannya :

EIGRP Metric

Semakin besar nilai Bandwitdth, maka itulah yang semakin dipilih. Semakin kecil nilai Delay, maka itulah yang semakin terpilih. Semakin kecil nilai Load, maka itulah yang semakin

EIGRP Composite Metric

Default Composite Formula:
metric = **[K1*bandwidth + K3*delay]**

Complete Composite Formula:
metric = **[K1*bandwidth + (K2*bandwidth)/(256 - load) + K3*delay] * [K5/(reliability + K4)]**
(Not used if "K" values are 0)

Default values:
K1 (bandwidth) = 1
K2 (load) = 0
K3 (delay) = 1
K4 (reliability) = 0
K5 (reliability) = 0

"K" values can be changed with the `metric weights` command.

```
Router(config-router)#metric weights tos k1 k2 k3 k4 k5
```

terpilih. Semakin besar nilai reliability maka itulah yang semakin terpilih.

Yuk kita ngonfig

Format Perintah :

Router(config)# router eigrp <autonomous system number>

Router(config-router)# network <Network address> <wildcard>

Router(config-router)# no auto-summary

Contoh Perintah :

Router(config)# router eigrp 10

Router(config)# network 10.10.10.0 0.0.0.3

Router(config-router)# no auto-summary

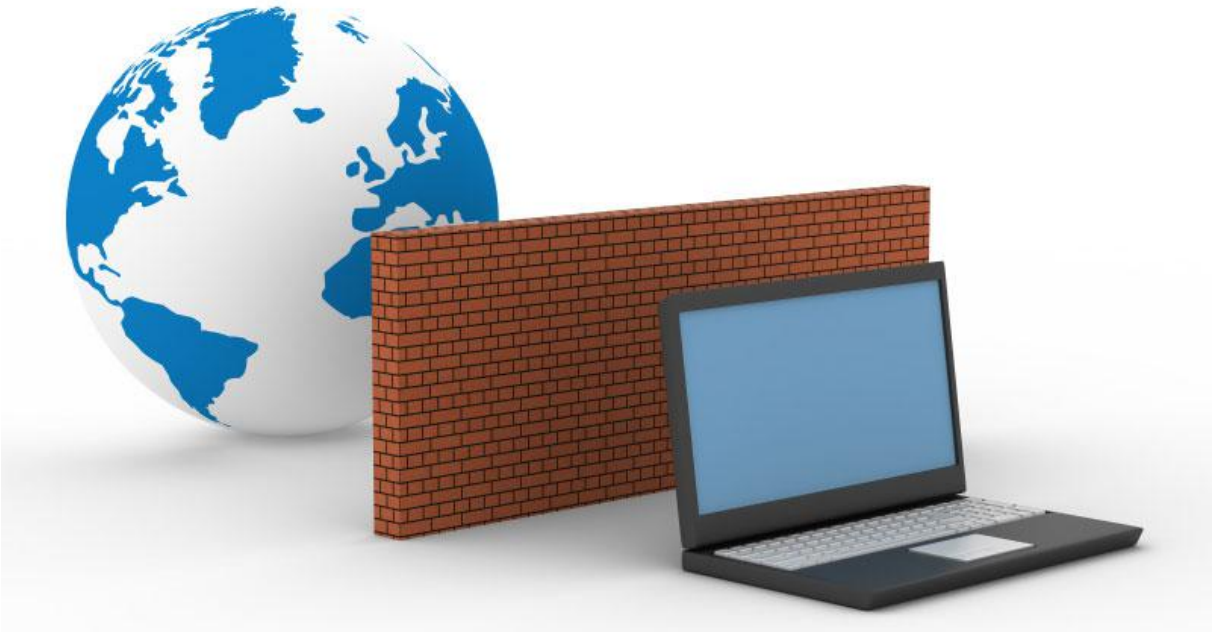
Format perintah Tshoot :

Router# show ip route

Router# show ip eigrp neighbors

Router# show ip eigrp topology

31. Access-List



Apa itu Access List ? Access list yang biasa disingkat dengan ACL, adalah sebuah fitur security yang disediakan oleh Cisco IOS untuk mem-filtering packet data. Atau dalam bahasa inggrisnya adalah " is a list of permissions attached to an object ".

Access-list terbagi menjadi 2 jenis, yaitu ACL Standard dan ACL Extended. ACL Standard adalah digunakan untuk memfilter berdasarkan Source IP. ACL Standard bernomor dari 1 hingga 99.

ACL Extended adalah giunakan untuk memfilter berdasarkan IP, Port dan Protocol. ACL Exteded bernomor 100 hingga 199.

Yuk kita ngonfig

- ***ACL Standard***

  DENY

  Router(config)# access-list <ACL Number> deny host <IP Address> (untuk men-deny satu IP)

  Router(config)# access-list <ACL Number> deny any (untuk men-deny seluruh traffic)

Router(config)# access-list <ACL Number> deny <Network Address> <Wildcard> (untuk men-deny IP tertentu yang lebih 1)

PERMIT

Router(config)# access-list <ACL Number> permit host <IP Address> (untuk men-permit satu IP)

Router(config)# access-list <ACL Number> permit any (untuk men-permit seluruh traffic)

Router(config)# access-list <ACL Number> permit <Network Address> <Wildcard> (untuk men-permit IP tertentu yang lebih 1)

- ***ACL Extended***

Router(config)# access-list <ACL Number> deny <Protocol> <Source IP> <Destination IP>

Router(config)# access-list <ACL Number> permit <Protocol> <Source IP> <Destination IP>

- ***REMARK***

Router(config)# access-list <ACL Number> remark <Comment> (untuk memberi Comment pada ACL Number tertentu>

Day 8

32. Network Address Translation

Apa itu Network Address Translation ? Network Address Translation yang biasa disingkat dengan NAT, adalah sebuah fungsi yang ada pada Router, yang dapat membuat banyak IP Private terkoneksi dengan jaringan Public menggunakan single IP Public yang sama. Dikarenakan tersediaan jumlah IPv4 Public terbatas, dan pengguna Internet terus bertambah, maka tentu hal ini butuh solusi. Yaitu NAT, yang dapat mengatasi secara efektif terhadap masalah tersebut.

Diantaranya kegunaan menggunakan NAT adalah meng-hemat IP, fleksibel, security lebih aman, dsb. Dan kerugiannya adalah terdapat delay ketika proses switching, dan terdapat beberapa hal yang tidak dapat berjalan jika menggunakan NAT.

NAT Pada Cisco terbagi menjadi 3, yaitu Static NAT, Dynamic NAT dan PAT.

Pada NAT terdapat istilah Inside Local Address, Outside Local Address, Inside Global Address dan Outside Global Address. Berikut penjelasannya ?

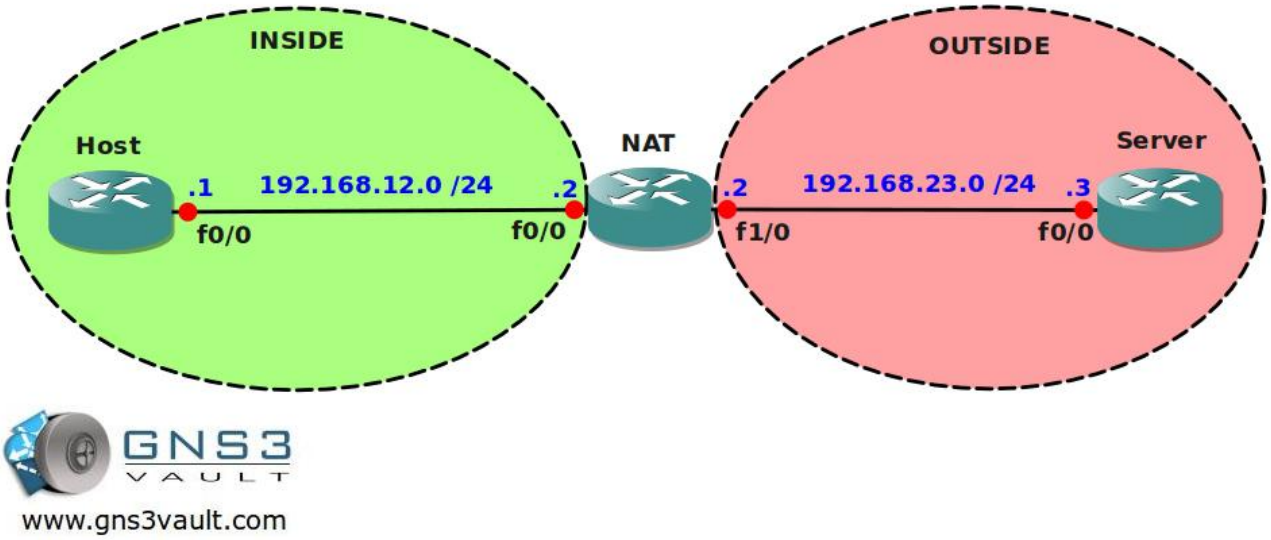
Inside Local Address : Source IP Address sebelum translasi *(IP Private)*

Outside Local Address : Destination IP Address sebelum translasi *(IP Private)*

Inside Global Address : Inside IP Host sesudah translasi *(IP Public)*

Outside Global Address : Outside Destination IP Host sesudah translasi *(IP Public)*

Static NAT



Apa itu Static NAT ? Static adalah one-to-one mapping dari private IP address menjadi public IP address. Static NAT ini berguna ketika sebuah perangkat jaringan yang berada di dalam Private IP Network, untuk dapat diakses dari internet.

Yuk kita ngonfig

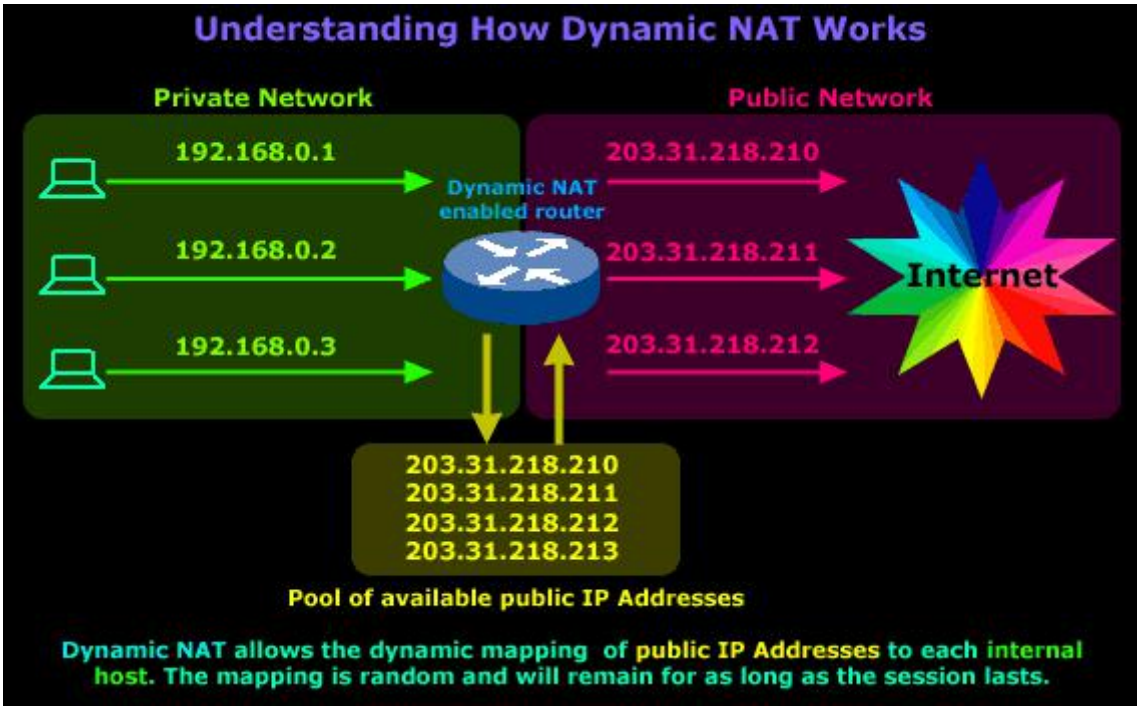
Format perintah :

Router(config)# ip nat inside source static <Inside Local IP Address> <Inside Global IP Address>

Jika sudah membuat NAT, maka selanjutnya adalah kita menentukan Inside atau Outside pada interface tersebut.

Router(config-if)# ip nat <Inside atau Outside>

Dynamic NAT



Apa itu Dynamic NAT ? Dynamic NAT ini adalah NAT yang memiliki konsep Many-to-many. Dynamic NAT ini fungsinya sama yaitu memetakan Private IP Address menjadi Public IP address, hanya saja konsepnya berbeda yaitu ia memetakan beberapa Private IP Address menjadi sebuah kumpulan Public IP addresses yang disebut sebagai NAT pool.

Yuk.. kita ngonfig

Router(config)# ip access list standard <Nama ACL>

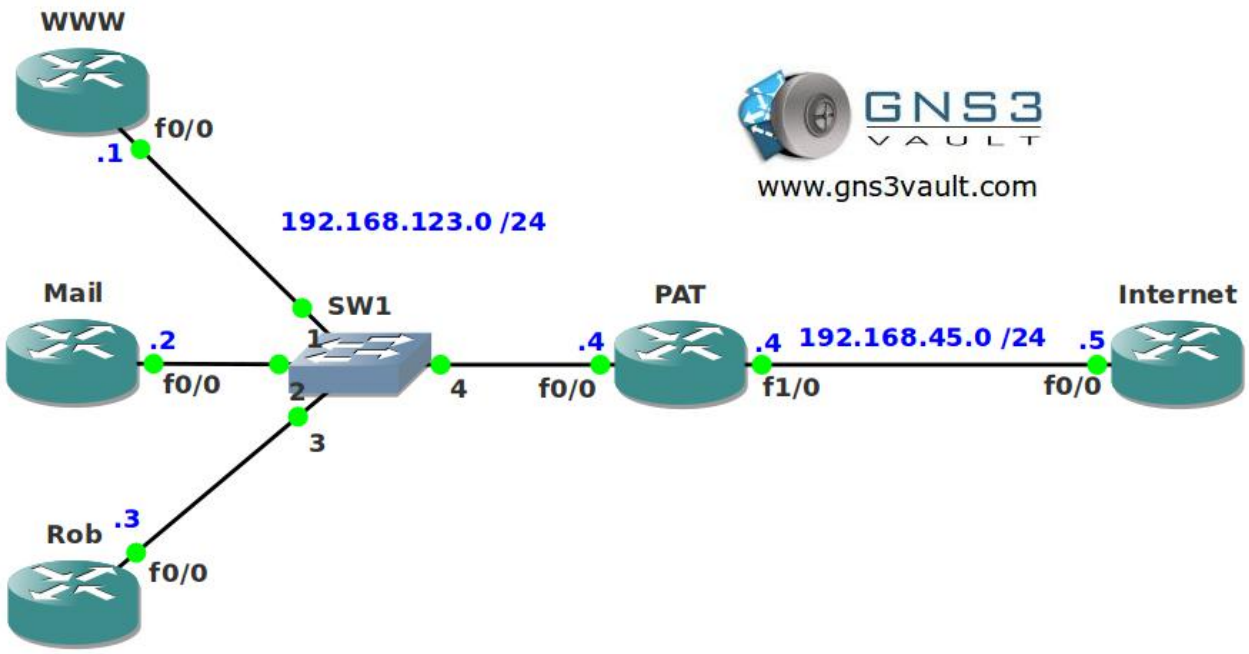
Router(config-std-nacl)# permit host <IP Address> *(untuk single IP Address)*

Router(config-std-nacl)# permit <network> <wildcard> *(untuk sebuah kumpulan IP Address)*

Router(config-std-nacl)# ip nat pool <Nama Pool> <Start Public IP Address> <End Public IP Address> netmask <Netmask Address>

Router(config)# ip nat inside source list <Nama ACL> pool <Nama Pool>

Port Address Translation



Port Address Translation atau yang biasa disingkat dengan PAT adalah salah satu jenis dari Dynamic NAT yang dimana dapat memetakan multiple private IP addresses menjadi single public IP address dengan menggunakan technology yang disebut sebagaiPort Address Translation. PAT memiliki konsep many-to-one, Dan NAT jenis ini adalah yang paling banyak digunakan diseluruh dunia.

Yuk… kita ngonfig

Router(config)# ip access list standard <Nama ACL>

Router(config-std-nacl)# permit host <IP Address> *(untuk single IP Address)*

Router(config-std-nacl)# permit <network> <wildcard> *(untuk sebuah kumpulan IP Address)*

Router(config-std-nacl)# ip nat pool <Nama Pool> <Start Public IP Address> <End Public IP Address> netmask <Netmask Address>

Router(config)# ip nat inside source list <Nama ACL> pool <Nama Pool>

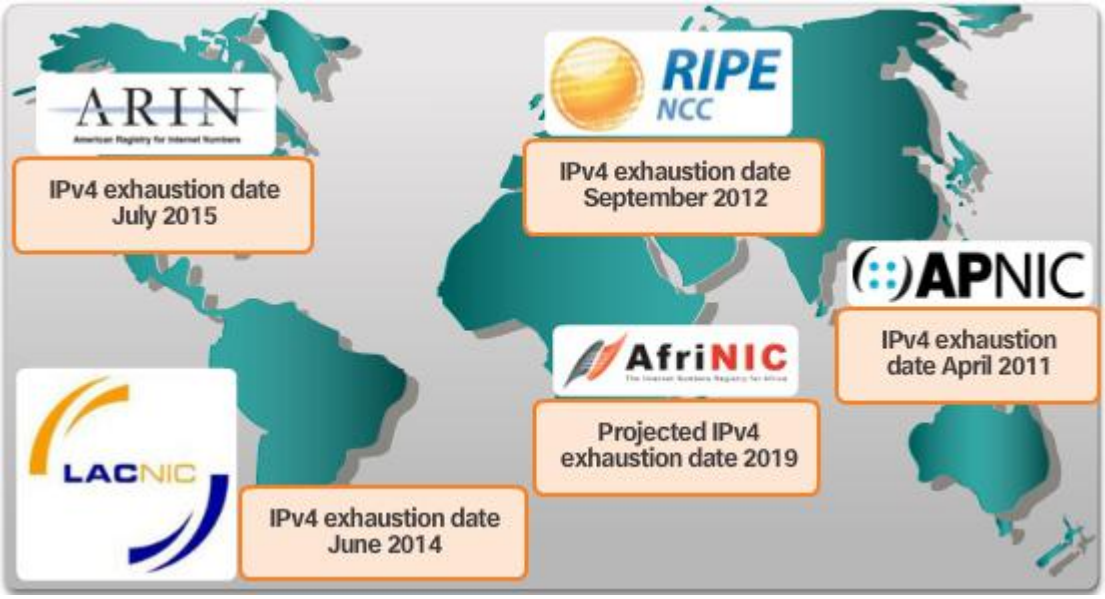
33.IPv6

IPv6 yang merupakan singkatan dari Internet Protocol versi 6 adalah versi hasil dari pengembangan sebelumnya yaitu versi 4. IPv6 adalah generasi baru yang akan menggantikan versi sebelumnya, yaitu versi 4. IPv6 ini bisa dikatakan versi penyempurnaan dari versi sebelumnya. IPv6 ini dikembangkan oleh Internet Engineering Task Force (IETF).

IPv6 ini jauh lebih banyak jumlah bit nya jika dibandingkan dengan IPv4, yaitu 128-bit. Berikut contohnya : " ***xxxxxxxxxxxxxxxx: xxxxxxxxxxxxxxxx: xxxxxxxxxxxxxxxx: xxxxxxxxxxxxxxxx: xxxxxxxxxxxxxxxx: xxxxxxxxxxxxxxxx: xxxxxxxxxxxxxxxx.*** "(Setiap titik, disebut dengan Quartets). Inilah tujuan utama IPv6 diciptakan, yaitu jumlah bit nya lebih banyak, sehingga IP yang dapat digunakan oleh masyarakat umum jauh lebih banyak dari versi sebelumnya, kurang lebih yaitu berjumlah berkisar : " ***340.282.366.920.938.463.463.374.607.431.768.211.456*** ". Sangat banyak sekali bukan ?

Seperti yang kita ketahui, sekarang ini, semakin lama semakin banyak pengguna Internet di setiap sudut dunia. Maka, semakin banyak IP yang dibutuhkan. Semakin hari, semakin terus bertambah. Itupun baru user, belum server, router, firewall yang itu semua butuh IP. Pada 15 April 2011 sudah terjadi kehabisan IPv4 pada Asia-Pacific, dan sekarang ini adalah tahun 2017, bisa dibayangkan betapa pesatnya perkembangan Internet di dunia ini.

IPv6 ini digunakan sebagai IP Address untuk menggantikan IPv4 yang telah kehabisan. Dengan besarnya IPv6 space 2^{128} dibandingkan dengan IPv4 space 2^{32} diharapkan mampu memenuhi kebutuhan IP di dunia ini dalam jangka waktu yang lama. Dari sini telah kita lihat, mau tidak mau, kita sudah harus siap untuk mempelajari dan meng-implementasikan IPv6. Berikut info di tiap bagian dunia yang kehabisan IPv4.



Apa saja kelebihan, perubahan, dan fitur yang ada pada IPv6 ini ? berikut listnya :

- IPv6 terdiri dari 128 bit, jumlah bit yang sangat panjang sehingga memiliki jumlah yang banyak
- Tidak ada lagi NAT (Network Address Translation)
- Auto-configuration
- Tidak ada lagi private address collisions
- Perfoma multicast routing yang lebih baik
- Format Header yang lebih sederhana
- Routing yang lebih efisien (karena lebih simple)
- Menggunakan Flow Label field untuk mengidentifikasikan packet flow dalam hal QoS handling oleh router.
- Built-in authentication and privacy support
- Flexible options and extensions

- Easier administration (tidak lagi menggunakan DHCP)
- Dan masih banyak lagi.

Hexadecimal to binary

IPv6 menggunakan format Hexadecimal, berkat penggunaan penulisan format Hexadecimal inilah menjadi berjumlah sangat banyak, dari pada IPv4 yang menggunakan format Decimal. Contoh IPv6 adalah semisal " 2021:0000:110E:0000:0000:02E0:126A:1000 " yang dimana terdiri dari 32 Bilangan Hexadecimal. Nah sekarang kita terjemahkan menjadi Binary step by step.

Berikut tabel Hexadecimal ke Binary beserta nilai Decimalnya :

Nilai Decimal	Hexadecimal	Binary
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Nah sekarang kita coba mentranslasikan " 110E " menjadi Binary.

Hexadecimal	110E			
	1	1	0	E
Binary	0001	0001	0000	1110

Disini terlihat setiap 1 bilangan Hexadecimal, bernilai 4 Bit. Sedangkan jumlah bilangan Hexadecimal pada IPv6 adalah 32, maka 32 x 4 = 128 Bit. Yuk kita coba mentranslasikan " 2021 " menjadi Binary.

Hexadecimal	2201			
	2	2	0	1
Binary	0010	0010	0000	0001

Mudah bukan ? nah sekarang kita menterjemahkan seluruhnya pada " 2021:0000:110E:0000:0000:02E0:126A:1000 " menjadi Binary.

Hexadecimal	2201			
	2	2	0	1
Binary	0010	0010	0000	0001
Hexadecimal	0000			
	0	0	0	0
Binary	0000	0000	0000	0000
Hexadecimal	110E			
	1	1	0	E
Binary	0001	0001	0000	1110
Hexadecimal	0000			
	0	0	0	0
Binary	0000	0000	0000	0000
Hexadecimal	0000			
	0	0	0	0
Binary	0000	0000	0000	0000
Hexadecimal	02E0			
	0	2	E	0
Binary	0000	0010	1110	0000
Hexadecimal	126A			
	1	2	6	A
Binary	0001	0010	0110	1010
Hexadecimal	1000			
	1	0	0	0
Binary	0001	0000	0000	0000

Nah… selesai sudah, sekarang tinggal kita tulis deh kumpulan binarynya.

IPv6	2021 : 0000 : 110E : 0000 : 0000 : 02E0 : 126A : 1000
Binary	0010000000100001 : 0000000000000000 : 0001000100001110 : 0000000000000000 : 0000000000000000 : 0000001011100000 : 0001001001101010 : 0001000000000000

Hasilnya adalah ***" 0010000000100001 : 0000000000000000 : 0001000100001110 : 0000000000000000 : 0000000000000000 : 0000001011100000 : 0001001001101010 : 0001000000000000 "***.

Mempersingkat dengan Menghilangkan nilai 0

Format penulisan IPv6 dapat kita permudah, dengan cara menghilangkan nilai 0 yang ada di kiri. Contoh nilai " 02E0 " bisa disingkat menjadi " 2E0 ", sedangkan nilai " 1000 " tidak bisa menjadi " 1 ", tetap harus ditulisnya 0 nya, karena berada di kanan. Begitu juga pada nilai " 0000 " bisa menjadi " 0 ". Yuk… kita singkat nilai 0 pada " 2021 : 0000 : 110E : 0000 : 0000 : 02E0 : 126A : 1000 ".

IPv6 sebelum disingkat	**2021 : 0000 : 110E : 0000 : 0000 : 02E0 : 126A : 1000**
IPv6 sesudah disingkat	2021 : 0 : 110E : 0 : 0 : 2E0 :126A :1000

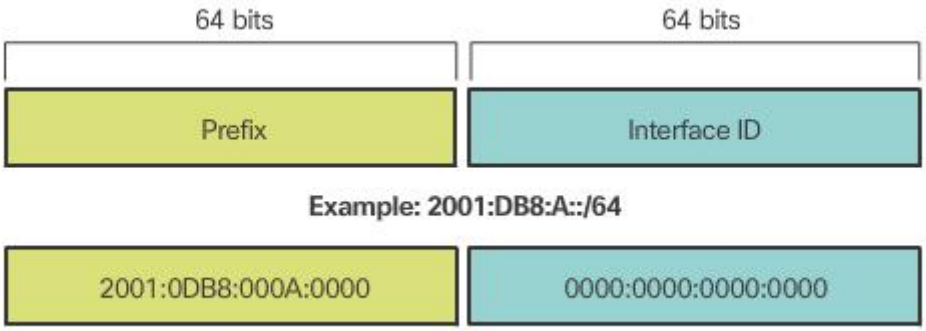
Mensederhanakan IPv6

Format penulisan IPv6 dapat kita persingkat lagi, dengan cara deretan yang bernilai 0 lebih dari 1 dapat kita ganti dengan dobel titik dua. Contoh :

IPv6 sebelum disederhanakan	**2021 : 0 : 110E : 0 : 0 : 2E0 :126A :1000**
IPv6 sesudah disederhanakan	2021 : 0 : 110E :: 2E0 : 126A : 1000

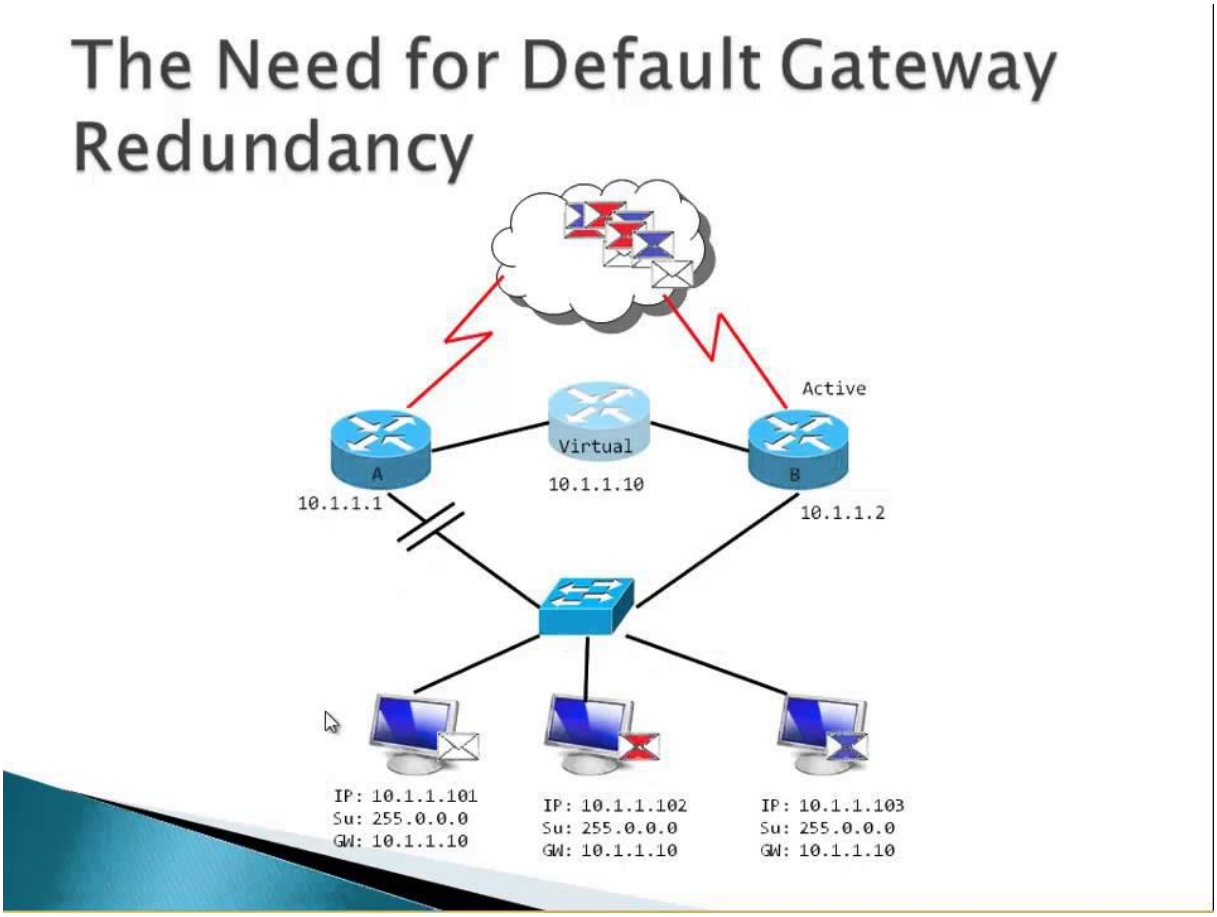
Disitu terlihat " : 0 : 0 : " bisa menjadi " :: ". Namun pen-sederhanaan ini, tidak dapat kita lakukan 2 tempat, hanya dapat dilakukan pada 1 tempat.

IPv6 Prefix



IPv6 juga seperti IPv4 ada yang disebut dengan Network ID atau Net ID dan ada juga Host ID, namun di IPv6 namanya Interface ID. Jika pada IPv4 ada yang disebut dengan Netmask, di IPv6 disebut dengan Prefix. Hanya saja pada IPv6 tidak ada Netmask seperti pada IPv4 yang penulisannya seperti 255.255.255.0. Jika kita hendak meng-konfigurasi pada

perangkat dengan menggunakan IPv4, maka kita mengkonfigurasi IP beserta netmasknya. Contohnya pada Router Cisco " ***Router(config-if)#*** *ip address 192.168.1.1 255.255.255.0* ", sedangkan pada IPv6 menggunan prefix (seperti slash notation) untuk menentukan Network ID dan Interface ID. Contohnya konfigurasi IPv6 pada Router Cisco " ***Router(config-if)#*** *ipv6 address 128A::1/64* ".


The Need for Default Gateway Redundancy
Active
Virtual
A
B
10.1.1.1
10.1.1.10
10.1.1.2
IP: 10.1.1.101
Su: 255.0.0.0
GW: 10.1.1.10
IP: 10.1.1.102
Su: 255.0.0.0
GW: 10.1.1.10
IP: 10.1.1.103
Su: 255.0.0.0
GW: 10.1.1.10

Pada dunia jaringan terdapat sebuah permasalahan, yaitu setiap perangkat dapat terhubung dengan Internet berkat adanya Gateway. Nah.., jika gateway tersebut terdapat masalah yang seperti mati atau down, error, atau bahkan terputus dari jaringan, maka terjadilah sebuah kekacauan, yang dimana setiap perangkat sudah tidak dapat lagi terhubung dengan internet, alias tidak bisa internetan.

Untuk mengatasi masalah tersebut, solusinya adalah menggunakan Gateway Redudancy. Yang dimana, terdapat 2 gateway yang sama-sama terhubung dengan Internet yang sama. Jadi ketika ke-2 gateway tesebut dalam keadaan Up, kita hanya menggunakan salah satu gateway tersebut, semisal yang kiri. Ketika gateway yang kiri terdapat masalah, maka jalur tersebut akan secara otomatis pindah ke gateway yang kanan tanpa perlu ada peran Administrator Jaringan.

Pada dunia Jaringan khususnya pada Cisco, Gateway Redudancy sendiri terdapat sebuah istilah yaitu FHRP. Lalu apa itu FHRP ? FHRP yang merupakan singkatan dari First Hop Redudancy Protocol adalah sebuah Protocol yang dapat memungkinkan mencegah terjadinya kegagalan koneksi pada Gateway, dengan cara seperti yang dijelaskan sebelumnya. Pada kali ini Protocol yang kita bahas adalah HSRP, HSRP ini adalah bagian dari FHRP, dibuat oleh Cisco dan bersifat Cisco Propietary.

Di dalam HSRP, ada beberapa istilah terminology, berikut diantaranya :

- Active Router

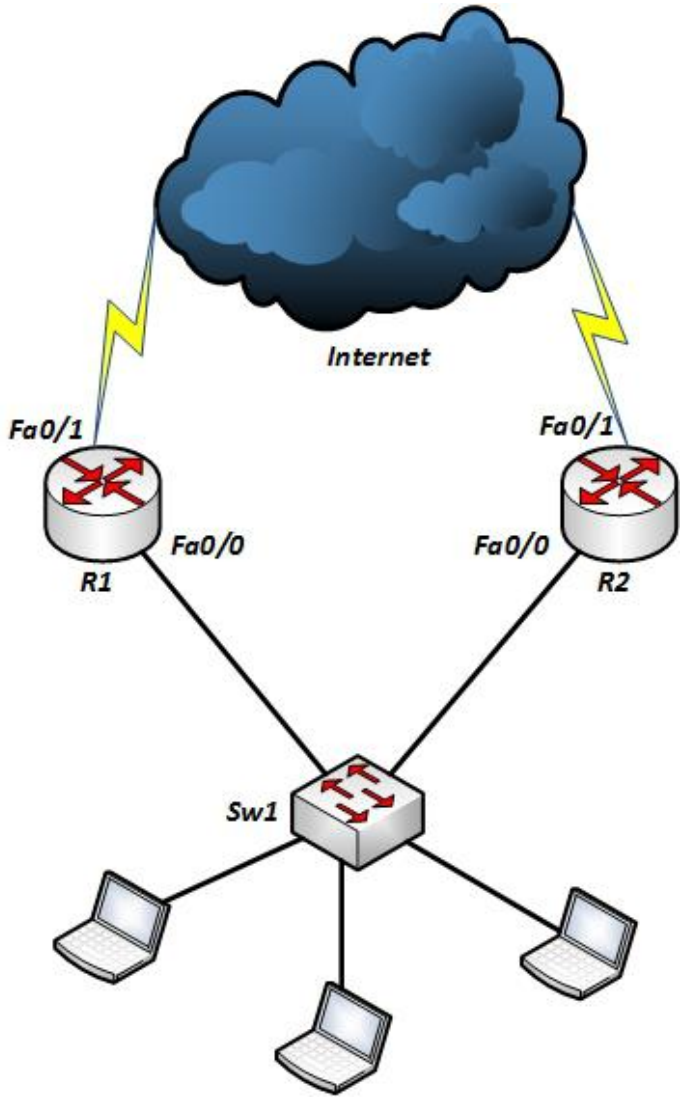
  Router yang digunakan lalu lalang Traffic
- Standby Router

  Yang dimaksud Standby Router adalah Router Backup
- Standby Group

  Standby Group adalah Group HSRP yang isinya terdapat Router Active dan Router yang Standby. Dan untuk Standby Group ini seolah-olah 2 Router menjadi 1 Virtual Router. Karena Router Active dan Router Standby dijadikan satu group, maka ada sebuah Router Virtual yang dimana hasil fusion Router-Router tersebut, dan yang mempunyai IP

virtual (tak hanya itu, bahkan MAC Address Virtual). Virtual MAC nya adalah 0000.0C9F.FXXX atau 0000.0C07.ACXX

Yuk… kita konfig



Pada kali ini, kita Virtual IP (Gateway)nya adalah " 192.168.1.254 ". Dan yang terakhir, jangan lupa buat Rute untuk menuju ke Internet.

R1 (Interface Configuration)

```
R1(config)#  interface fa0/0
R1(config-if)# ip add 192.168.1.1 255.255.255.0
R1(config-if)# no sh
R1(config-if)# interface fa0/1
```

```
R1(config-if)# ip add 10.10.10.1 255.255.255.248
R1(config-if)# no sh
R1(config-if)# ip route 0.0.0.0 0.0.0.0 fa0/1
```

R2 (Interface Configuration)

```
R2(config)#  interface fa0/0
R2(config-if)# ip add 192.168.1.2 255.255.255.0
R2(config-if)# no sh
R2(config-if)# interface fa0/1
R2(config-if)# ip add 10.10.10.2 255.255.255.248
R2(config-if)# no sh
R2(config-if)# ip route 0.0.0.0 0.0.0.0 fa0/1
```

R1 (HSRP Configuration)

```
R1(config)# interface fa0/0
R1(config-if)# standby 1 ip 192.168.1.254
R1(config-if)# standby 1 priority 10
R1(config-if)# standby 1 preempt
```

R2 (HSRP Configuration)

```
R2(config)# interface fa0/0
R2(config-if)# standby 1 ip 192.168.1.254
R2(config-if)# standby 1 priority 7
R2(config-if)# standby 1 preempt
```

Checking Configruation Command

```
Router# show standby
```

Atau

```
Router# show standby brief
```

Penutup

Alhamdulillah … selesai sudah kita membahas tentang CCNA Routing & Switching , namun saya akui, untuk belajar di dalam bidang dunia IT memanglah sangat luas. Saya akui, buku yang saya tulis belumlah sempurna seperti yang diharapkan, kami masih butuh masukan dari agan-agan sekalian semua agar buku ini semakin sempurna dan berguna untuk semua pencinta Networking.

Dari buku ini, saya sangat berharap bisa berguna dan bermanfaat untuk agan-agan sekalian.

Amiin …