Free Ebook Edition

Mikrotik Security For Beginner's #1

Resep Cepat Mengamankan Router Mikrotik Anda Sedari Dini

Teddy Yuliswar, S.Kom (MTCNA, MTCTCE, MTCWE, MTCRE, MTCUME, MTCINE)
Primadonal, S.Kom (MTCNA, MTCTCE)

www.sahoobi.com

Mikrotik Security For Beginner's #1

Resep Cepat Mengamankan Router Mikrotik Anda Sedari Dini

Teddy Yuliswar, S.Kom **(MTCNA, MTCTCE, MTCWE, MTCRE, MTCUME, MTCINE)**
Primadonal, S.Kom **(MTCNA, MTCTCE)**

www.sahoobi.com | indonetworkers.com

Tentang Penyusun

Teddy Yuliswar adalah seorang Mikrotik Trainer dan Mikrotik Coordinator, mempunyai passion dalam Bisnis, Marketing dan Pelatihan. Telah berpengalaman dalam Support Jaringan Komputer selama lebih dari 8 tahun. Mempunyai sertifikat Mikrotik MTCNA, MTCTCE, MTCRE, MTCUME, MTCWE, MTCINE dan Sertifikat Mikrotik Trainer. Sekarang aktif menulis di blog indonetworkers.com

Primadonal adalah seorang System Administrator dan Freelance Teknikal Support Jaringan Komputer, mempunyai passion dalam Teori Konspirasi, Romansa, Keamanan Jaringan Komputer. Telah malang melintang dalam dunia IT selama lebih dari 15 tahun. Mempunyai sertifikat Mikrotik MTCNA, MTCTCE. Sekarang aktif menulis di blog www.sahoobi.com

Kata Pengantar

Terimakasih buat Anda, kawan-kawan peminat teknologi jaringan komputer khususnya teknologi Router Mikrotik di Indonesia, yang telah bersedia mendownload ebook sederhana ini.

Ebook sederhana ini, kami susun berdasarkan kumpulan artikel dari website Citraweb Nusa Infomedia Mikrotik Indonesia, dengan alamat http://www.mikrotik.co.id. Tulisan diwebsite tersebut kami baca dan analisa kemudian kami praktikkan dilab, beberapa warnet dan kantor. Banyak manfaat kami dapatkan setelah mempraktikkan tulisan dalam artikel tersebut. Sehingga berdasarkan tulisan tersebut kami beranikan diri untuk menyusun sebuah buku digital ringkas tentang **Mikrotik Security For Beginner's Bagian 1 - Resep Cepat Mengamankan Router Mikrotik Anda Sedari Dini**.

Ebook ini memang dikhususkan buat kawan-kawan yang tidak punya waktu banyak untuk menelusuri dan mencari artikel-artikel berkualitas yang beredar banyak di Internet, namun membutuhkan waktu yang singkat agar memahami dan menerapkan sedari dini cara mengamankan Router Mikrotik. Sebab sebagian besar kawan-kawan yang baru mengenal dan menggunakan Mikrotik RouterOS dan RouterBoard, banyak yang kurang memperhatikan tentang keamanan Router Mikrotik ini. Padahal isu tentang keamanan Router ini sangatlah penting.

Di antara para pembaca, pastilah banyak yang sudah lama jam terbangnya. Tentu, disana-sini masih ditemukan kekurangan. Dimohon masukannya sehingga Ebook ini kedepan semakin baik.

Akhirnya kami ucapkan selamat membaca dan praktik.

Salam hormat,

Teddy Yuliswar

Primadonal

Daftar Isi

1

Tentang Mikrotik

MikroTikls [dengan trade name MikroTik®] didirikan tahun 1995 bertujuan mengembangkan sistem ISP dengan wireless. MikroTikls saat ini telah mendukung sistem ISP dengan wireless untuk jalur data internet di banyak negara, antara lain Iraq, Kosovo, Sri Lanka, Ghana dan banyak negara lainnya.

Pengalaman dalam melakukan instalasi di Latvia menempa kami dengan kondisi serupa di negara-negara pecahan Uni Soviet dan negara berkembang lainnya. Berbagai pengembangan telah dilakukan hingga saat ini tersedia perangkat lunak sistem operasi router versi 2 yang menjamin kestabilan, kontrol, dan fleksibilitas pada berbagai media antar muka dan sistem routing dengan menggunakan komputer standart sebagai hardware. Perangkat lunak ini mendukung berbagai aplikasi ISP, mulai dari RADIUS modem pool, hingga sirkuit backbone dengan DS3.

MikroTik berlokasi di Riga, ibukota Latvia, dengan 50 orang karyawan. Mikrotik juga menjalankan sebuah ISP kecil, sebagai media percobaan untuk pengembangan routerOR software.

Wawancara dengan CTO Mikrotik Arnis Riekstins

Dalam dunia router, mesin yang berfungsi mengarahkan alamat di Internet, Cisco merupakan nama yang sudah tidak diragukan lagi. Tetapi di dunia lain, nama Mikrotik, yang berbentuk software, lumayan dikenal sebagai penyedia solusi murah untuk fungsi router, bahkan kita dapat membuat router sendiri dari komputer rumahan.

Untuk negara berkembang, solusi Mikrotik sangat membantu ISP atau perusahaan-perusahaan kecil yang ingin bergabung dengan Internet. Walaupun sudah banyak tersedia perangkat router mini sejenis NAT, dalam beberapa kondisi penggunaan komputer dan software Mikrotik merupakan solusi terbaik. Mikrotik adalah perusahaan kecil berkantor pusat di Latvia, bersebelahan dengan Rusia, pembentukannya diprakarsai oleh John Trully dan Arnis Riekstins. John Trully adalah orang Amerika yang berimigrasi ke Latvia dan berjumpa Arnis yang sarjana Fisika dan Mekanik di sekitar tahun 1995.

Tahun 1996 John dan Arnis mulai me-routing dunia (visi Mikrotik adalah me-routing seluruh dunia). Mulai dengan sistem Linux dan MS DOS yang dikombinasikan dengan teknologi Wireless LAN (W-LAN) Aeronet berkecepatan 2Mbps di Molcova, tetangga Latvia, baru kemudian melayani lima pelanggannya di Latvia. Ketika saya menanyakan berapa jumlah pelanggan yang dilayaninya saat ini, Arnis menyebut antara 10 sampai 20 pelanggan saja, karena ambisi mereka adalah

membuat satu peranti lunak router yang handal dan disebarkan ke seluruh dunia. Ini agak kontradiksi dengan informasi yang ada di web Mikrotik, bahwa mereka mempunyai 600 titik (pelanggan) wireless dan terbesar di dunia. Padahal dengan wireless di Jogja dan Bandung saja, kemungkinan besar mereka sudah kalah bersaing.

Prinsip dasar mereka bukan membuat Wireless ISP (WISP), tapi membuat program router yang handal dan dapat dijalankan di seluruh dunia. Latvia hanya merupakan "tempat eksperimen" John dan Arnis, karena saat ini mereka sudah membantu negara-negara lain termasuk Srilanka yang melayani sekitar empat ratusan pelanggannya.

Linux yang mereka gunakan pertama kali adalah Kernel 2.2 yang dikembangkan secara bersama-sama dengan bantuan 5 - 15 orang staf R&D Mikrotik yang sekarang menguasai dunia routing di negara-negara berkembang. Selain staf di lingkungan Mikrotik, menurut Arnis, mereka merekrut juga tenaga-tenaga lepas dan pihak ketiga yang dengan intensif mengembangkan Mikrotik secara maraton.

Ketika ditanya siapa saja pesaing Mikrotik, Arnis tersenyum dan enggan mengatakannya. Sewaktu saya simpulkan tidak ada pesaing, Arnis dengan sedikit tertawa menyebut satu nama yang memang sudah lumayan terkenal sebagai produsen perangkat keras khusus untuk teknologi W-LAN, yaitu Soekris dari Amerika. Tujuan utama mereka berdua adalah membangun software untuk routing, sementara kebutuhan akan perangkat keras juga terus berkembang, sehingga akhirnya mereka membuat berbagai macam perangkat keras yang berhubungan dengan software yang mereka kembangkan.

Semangat Mikrotik ini agak berbeda dari kebanyakan perusahaan sejenis di Amerika, karena mereka berkonsentrasi di pengembangan software lalu mencari solusi di hardware-nya dengan mengajak pihak ketiga untuk berkolaborasi. Dan kita dapat melihat ragam perangkat yang mereka tawarkan menjadi semakin banyak, mulai dari perangkat yang bekerja di frekwensi 2,4GHz dan 5,8GHz sampai ke interface dan antena.

Keahlian Mikrotik sebetulnya di perangkat lunak routernya, karena terlihat mereka berjualan perangkat W-LAN dengan antena omni yang sangat tidak dianjurkan pemakaiannya di dunia W-LAN, karena sangat sensitif terhadap gangguan dan interferensi. Walaupun punya tujuan yang sangat jelas, yaitu mendistribusikan sinyal ke segala arah sehingga merupakan solusi murah.

Kepopuleran Mikrotik menyebar juga ke Indonesia. Pertama kali masuk tahun 2001 ke Jogja melalui Citraweb oleh Valens Riyadi dan kawan-kawan, lalu meluas menjadi satu solusi murah untuk membangun ISP, terutama yang berbasis W-LAN. Kebetulan sekali, Jogja merupakan salah satu kota di Indonesia yang populasi pemakaian W-LAN-nya terbesar kalau

dibandingkan luas daerahnya.

Keberhasilan Mikrotik me-routing dunia merupakan satu contoh, bahwa kita semua mampu membantu calon pemakai Internet untuk masuk ke dunia maya, terutama membantu membangun infrastrukturnya.

Michael Sunggiardi

Mengenal Mikrotik dengan PC Router

Installasi PC Router

Mikrotik tidak hanya tersedia dalam produk hardware, namun juga menyediakan produk software dalam bentuk Operating System yang mana dapat diinstall di PC . Salah satu nilai lebih ketika kita memilih PC router, kita bisa upgrade spesifikasi PC sesuai kebutuhan jaringan kita. Misal ketika processor sudah dirasa terlalu terbebani, kita bisa upgrade ke processor dengan kemampuan yang lebih tinggi. Sedangkan kekurangan dari PC router salah satunya RAM yang maksimal hanya 2 GB, juga konsumsi power yang cukup besar, dibandingkan dengan RouterBoard yang hanya membutuhkan konsumsi power yang relatif kecil.

Sebelum mambahas lebih jauh, perlu diketahui terlebih dahulu apa itu PC Router. PC Router merupakan sebuah PC yang sudah disiapkan untuk dijadikan sebagai Router. PC ini tidak akan digunakan untuk kebutuhan komputer pada umumnya, namun akan difungsikan untuk menjalankan service dalam jaringan.

Jika kita sudah menyiapkan PC yang nantinya khusus dijadikan sebagai PC Router, selanjutnya yang perlu dilakukan adalah menginstall PC tersebut dengan Mikrotik OS. Langkah installasi Mikrotik OS :

Download CD Image Mikrotik OS dalam format ISO. Anda bisa download disini.

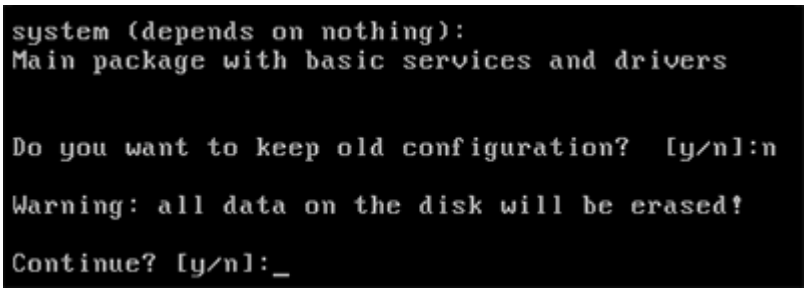
Burn file ISO ke dalam CD menggunakan aplikasi CD Burner, seperti Nero misalnya.

Jika CD Mikrotik OS sudah siap, set BIOS PC Router booting via CD ROM dan masukkan CD Mikrotik OS kedalam CD ROM.

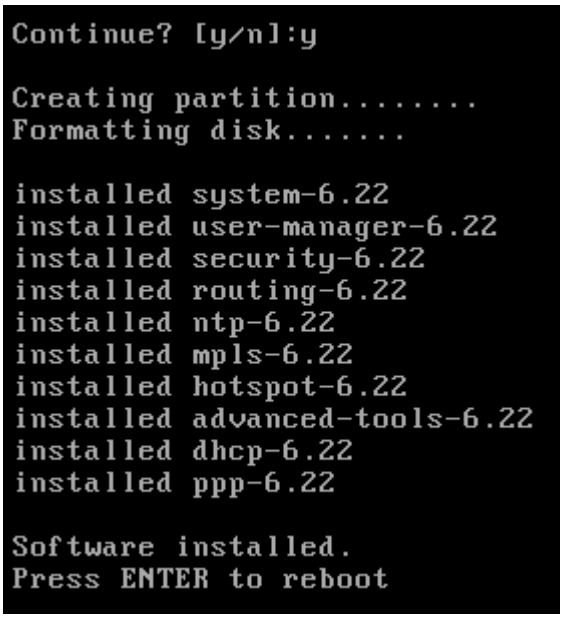
Jika PC Router berhasil booting via akan muncul tampilan seperti berikut :

Disini kita diminta untuk memilih paket Mikrotik OS yang akan diinstall. Minimal paket "System". Gunakan tombol arah panah pada keyboard untuk memilih, dan tekan tombol spasi untuk select paket. Jika sudah yakin, tekan tombol "i" pada keyboard.

Akan muncul beberapa pertanyaan, sepeti apakah akan menyimpan konfigurasi yang sudah ada ?, karena kita install fresh maka ketik "n". Akan muncul juga peringatan bahwa semua hardisk akan di format. jadi Mikrotik OS tidak dapat dibuat doal booting, atau lebih dari satu OS dalam PC Router. Mikrotik akan menformat dan menggunakan semua resource hardisk yang ada.



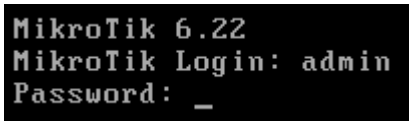
Ketik "y" pada pertanyaan Continue ? jika Anda sudah yakin. PC akan memulai proses installasi Mikrotik OS.



Jika proses install sudah selesai, tekan ENTER untuk restart dan kembalikan setting booting pada BIOS melalui hardisk.

Lisensi Trial

Setelah proses installasi selesai, tampilan pertama yang akan mucul adalah halaman login router Mikrotik. Secara default username administrator mikrotik adalah "admin" tanpa tanda kutip, dengan password dikosongkan.



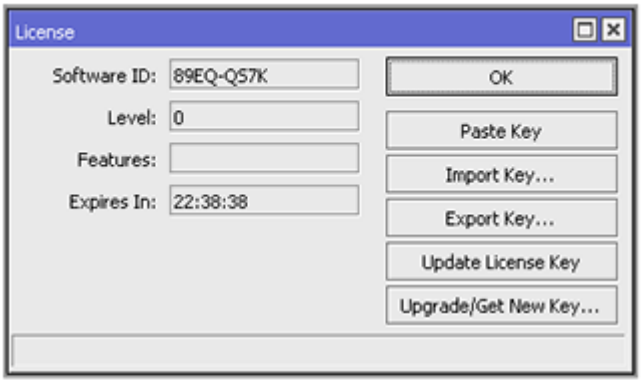
By default setelah Anda install Mikrotik OS pada PC, Anda sudah bisa menggunakan Mikrotik dengan lisensi level 0 (trial). Dimana kita bisa menggunakan semua fitur mikrotik namun dibatasi selama 24 jam. Pembatasan waktu ini bersifat akumulasi, artinya jika baru 2 jam dinyalakan lalu dimatikan, masih bisa digunakan walaupun 2 hari kemudian selama akumulasi waktu aktif mikrotik belum mencapai 24 jam.

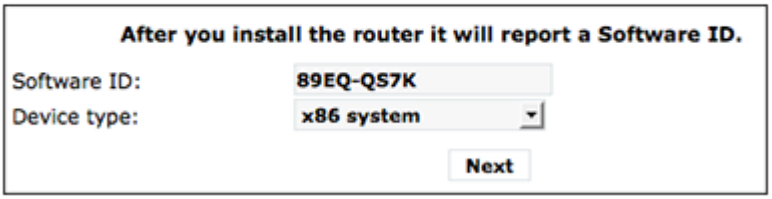
Lisensi Demo

Bagaimana jika kita ingin menggunakan mikrotik lebih dari 24 jam ?, jangan khawatir ternyata mikrotik juga menyediakan level 1 (demo) yang tentu saja bisa didapatkan secara gratis. Level 1 tidak memiliki batasan waktu dan dapat digunakan selama hardware router masih normal.

Akan tetapi ada beberapa batasan pada fitur tertentu, misal fitur firewall dan queue yang dibatasi maksimal 1 rule. Untuk mendapatkan lisesi level 1, kita harus memiliki account di Mikrotik.com

Pada halaman account setelah login, akan ada opsi “Make Demo Key”. Jika kita klik kita akan diminta memasukkan soft-id router. Soft-id bisa kita lihat melalui menu System License. Setelah soft-id router kita tambahkan, klik next dan kita akan mendapatkan lisensi demo.

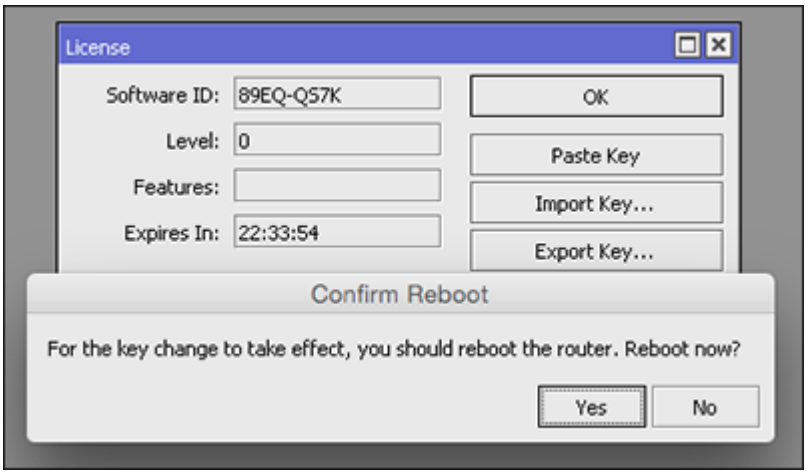




Akan muncul halaman baru yang menampilkan informasi key lisensi level demo yang digenerate berdasarkan soft-id router.

	Soft ID	Key
☑	89EQ-QS7K *(root)*	-----BEGIN MIKROTIK SOFTWARE KEY----- QjeeahafBQoT7Rrb2ZGo8rjKVJzsOx/hDuxDPsI1a8d7 2oodlQV9iujZw614cuSaLpe2v3MQ7XOAsloGlNRyJA== -----END MIKROTIK SOFTWARE KEY-----

Select dan copy kode lisensi mulai dari tanda "--" awal sampai akhir, dan masukkan kedalam router dengan cara klik tombol Paste Key di menu System --> License. Router akan restart, dan setelah kembali up, cek di menu System -->License.

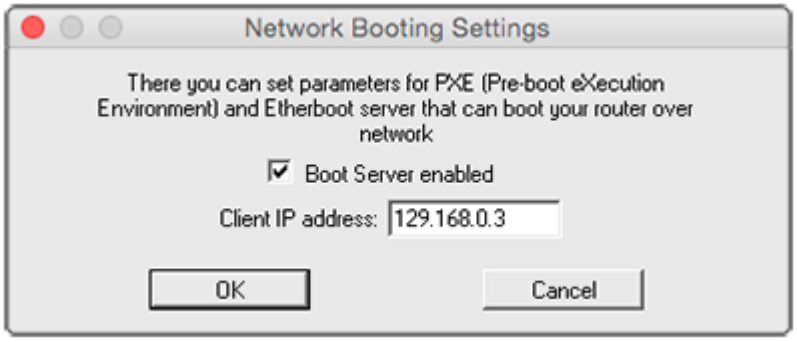


Selesai reboot, kita sudah mendapatkan lisensi level 1 untuk bisa bermain dengan mikrotik lebih lama. Jika sudah cocok dan yakin untuk menggunakan PC Router Mikrotik, jangan lupa upgrade ke lisensi 4, 5, atau 6 supaya bisa menggunakan feature Mikrotik dengan optimal.

Install Ulang

Jika PC router mengalami permasalahan seperti lupa password, router gagal booting, atau OS Mikrotik corrupt maka tidak ada cara lain selain install ulang PC router. Ada catatan khusus bahwa Jangan Install Ulang PC Router Menggunakan CD. Hal ini dapat mengakibatkan hilangnya lisensi. Dan lisensi yang hilang karena proses installasi menggunakan CD tidak akan mendapatkan garansi. Cara install ulang PC router yang aman adalah dengan Netinstall. Software ini dapat di-download di download-area mikrotik.co.id. Syarat PC router yang dapat di netinstall harus bisa booting via ethernet.

Koneksikan PC router dengan komputer/laptop Anda via kabel LAN. Setting ip address static di komputer. Download kemudian jalankan progran Netinstall di komputer Anda. Klik tombol Netbooting pada program netinstall, centang opsi "Boot Server Enabled", kemudian isi parameter "Client IP Address" dengan IP address yang satu subnet dengn ip static di komputer Anda. Misal jika komputer NAda menggunakan IP address 192.168.0.2, Anda bisa isi parameter client ip address dengan IP address 192.168.0.3.

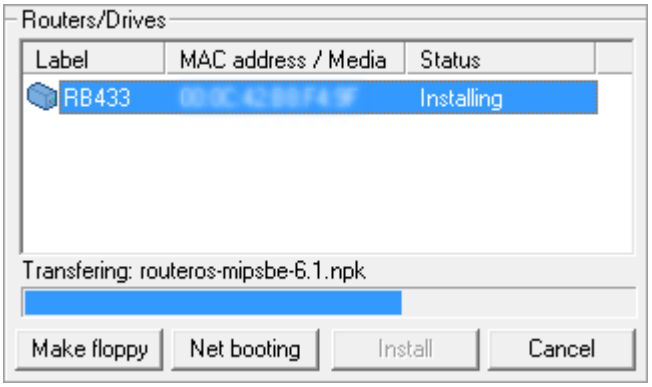


Lepas hardisk secondary jika ada, kemudian set Boot PC Anda menggunakan boot-rom mainboard (diconfigure dari BIOS) atau boot-disk buatan Netinstall, biarkan proses booting berjalan sendiri sampai selesai.

Setelah booting selesai akan muncul item baru (mac address PC router) dalam program Netinstall item tersebut adalah router yang berhasil booting dan siap untuk di install ulang.

Pilih source paket RouterOS yang Anda miliki dengan tombol 'Browse'. Paket RouterOS juga dapat didownload di download-area mikrotik.co.id atau di www.routeros.co.id. Untuk PC router, pastikan Anda download paket x86.npk.

Select mac address router kemudian klik tombol 'Install' untuk melakukan install ulang, tunggu sampai proses selesai dan restart atau reboot router Anda setelah ada perintah dari Netinstall. Jangan men-select "D:/" atau letter drive lain, karena jika Anda select netinstall justru akan menginstall RouterOS di hardisk komputer Anda.



Setelah proses instalasi di Netinstall selesai, tombol yang sebelumnya memiliki label install akan berubah menjadi "Reboot". Klik tombol tersebut, maka PC router akan restart, dan jangan lupa kembalikan boot device menjadi hardisk dimana RouterOS disimpan.

Membuat Jaringan

SEBUAH sistem jaringan, baik itu skala kecil maupun skala besar, memerlukan sebuah perangkat yang disebut sebagai router (baca: rowter). Perangkat router ini menentukan titik jaringan berikutnya di mana sebuah paket data dikirim ke jalur-jalur jaringan yang dituju.

Sebuah perangkat router umumnya terhubung sedikitnya ke dua jaringan, dalam konfigurasi dua buah LAN (Local Area Network) dengan WAN (Wide Area Network, seperti akses pita lebar broadband) atau sebuah LAN dengan jaringan penyedia akses internet (Internet Service Provider, ISP). Sebuah router biasanya terletak pada sebuah gateway, tempat di mana dua atau lebih jaringan terkoneksi satu sama lainnya.

Ada banyak router yang tersedia di pasaran yang dijual dengan harga yang bervariasi, tergantung dari kebutuhan sebuah jaringan. Untuk penggunaan akses broadband yang dikombinasi dengan penggunaan fasilitas nirkabel berupa Access Point, umumnya perangkat ini sudah dilengkapi dengan sebuah fasilitas router yang sudah lumayan lengkap.

Namun, untuk sebuah usaha kecil menengah dengan kebutuhan beberapa jasa jaringan seperti e-mail, web server, dan sejenisnya untuk menggunakan beberapa alamat protokol internet (IP address), perangkat router yang tersedia akan menjadi sangat mahal. Apalagi, kalau IP address yang digunakan hanya dalam jumlah yang terbatas, maka penggunaan perangkat keras router bermerek menjadi terlalu mahal.

Dana terbatas

Salah satu kemungkinan adalah membuat sendiri apa yang disebut PC router, menggunakan komputer sederhana dan murah dan memiliki dua perangkat Ethernet masing-masing digunakan untuk jaringan lokal dan lainnya untuk akses ke jaringan WAN (terhubung ke ISP). Perangkat PC router ini kemudian diisi dengan sebuah perangkat lunak router buatan Mikrotik (www.mikrotik.com) dengan membayar lisensi sekitar 45 dollar AS.

Perangkat lunak router Mikrotik memiliki seluruh fasilitas routing yang dibutuhkan, mampu mengendalikan jaringan kerja yang kompleks. Penggunaan dan pemasangannya sederhana, cukup dengan pelatihan sebentar saja, sebuah UKM mampu menggunakan fasilitas router ini tanpa harus memiliki departemen teknologi informasi sendiri.

Fitur PC router Mikrotik ini mencakup load balancing untuk membagi beban akses jaringan, fasilitas tunneling untuk membuat akses aman VPN (Virtual Provate Network), bandwith management untuk mengatur berbagai protokol dan port, serta memiliki kemampuan untuk dikombinasikan dengan jaringan nirkabel.

Miktrotik juga menyediakan fasilitas firewall untuk melindungi akses dari berbagai ancaman yang

tersebar di internet. Mereka yang memiliki dana terbatas tapi menginginkan akses jaringan di dalam dan luar yang aman, mudah digunakan, murah, dan tangguh, menggunakan Mikrotik adalah pilihan yang menarik. (rlp)

Unjuk Gigi Router Rakitan

Jaringan data dan internet adalah kumpulan dari jutaan komputer dan alat-alat digital lain yang bersambungan. Beberapa komputer akan membentuk jaringan kecil dan berhubungan dengan jaringan kecil lainnya. Sebuah komputer yang terkoneksi ke jaringan dapat berkomunikasi dengan komputer lainnya berkat adanya router yang berfungsi mengatur aliran data dari satu jaringan ke jaringan lainnya.

Sebagian orang beranggapan bahwa router yang baik hanyalah router yang bermerek. Padahal, router sebenarnya juga bisa dibuat dengan menggunakan komputer, dan menginstal perangkat lunak yang sesuai. Salah satu perangkat lunak yang bisa difungsikan menjadi sebuah router adalah Mikrotik (http://www.mikrotik.com).

Mikrotik mulai dibuat di Latvia pada tahun 1996. Versi-versi awal Mikrotik dibuat untuk digunakan pada sistem pengoperasian DOS. Sejak versi 2, Mikrotik kemudian menggunakan kernel Linux dalam aplikasinya. Tahun 2003 Mikrotik kemudian juga memproduksi perangkat keras berbentuk motherboard mini yang didesain untuk digunakan sebagai perangkat wireless, yang dinamai routerboard.

Sebagai perangkat lunak router, cukup banyak fungsi yang bisa dilakukan dengan Mikrotik, mulai dari quality of services (pengaturan bandwidth), firewall, hotspot gateway, web proxy, dns cache, hingga penggunaan virtual private network (VPT). Fasilitas pemantauan seperti watchdog dan netwatch juga tersedia. Salah satu keunggulan lainnya adalah adanya aplikasi pengaturan yang tidak lagi hanya berbasis teks, tetapi juga berbasis grafis.

Kebolehan sistem operasi Mikrotik ini banyak terlihat pada acara Mikrotik User Meeting yang diselenggarakan tanggal 19-20 Januari lalu di Praha, Ceko. Sebanyak 175 peserta dari berbagai belahan dunia ikut hadir.

Routerboard

Salah satu produk terbaru Mikrotik adalah Routerboard 532 (RB532), motherboard kecil (14 x 14 cm) didesain sebagai motherboard perangkat wireless. Perangkat RB532 menggunakan media penyimpanan onboard 64 MB dan RAM 64 MB, memiliki 2 slot minipci dan 3 port ethernet 10/100 mbps.

Untuk menjadikan perangkat ini sebagai perangkat wireless, kita memasangkan kartu antarmuka wireless yang berbentuk minipci (biasanya banyak digunakan juga pada laptop). Fasilitas power over ethernet pun sudah tersedia sehingga kita tidak perlu mengulur kabel listrik jika menggunakan perangkat ini di tempat-tempat yang sulit seperti di menara. Cukup dengan menggunakan kabel ethernet saja.

Dalam uji coba yang dilakukan untuk mengukur kemampuan kinerja motherboard RB532 ini, dipasang dua komputer Pentium IV yang dihubungkan satu sama lain melalui port ethernet dari RB532 ini. Tes ini dilakukan lebih dari tiga jam, dan didapatkan kemampuan link yang cukup stabil dan besar, yaitu (akumulatif kirim dan terima) 189 mbps.

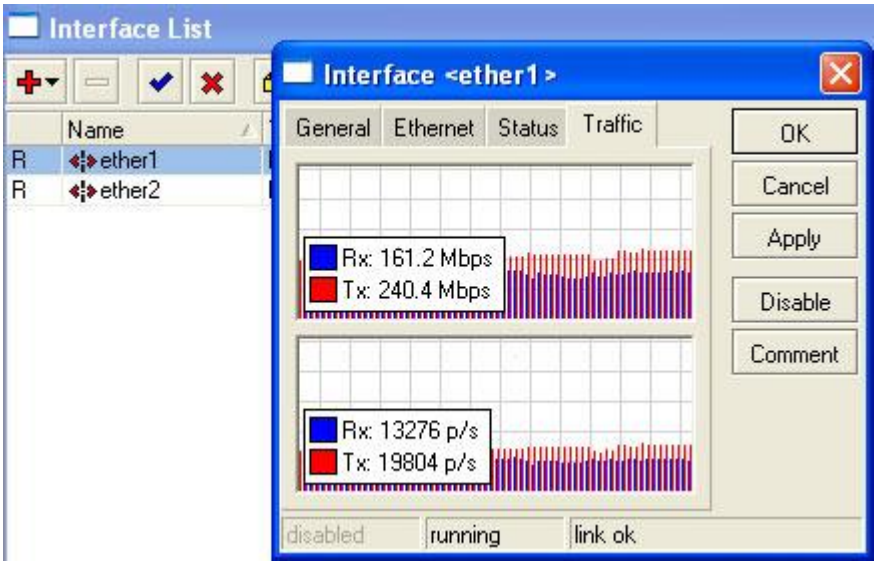
Selain RB532, saat ini Mikrotik juga dalam tahap akhir memproduksi motherboard Routerboard 112. Motherboard ini didesain lebih kecil dan sederhana daripada RB532 sehingga bisa dipasarkan dengan harga relatif lebih murah.

Wireless 350 mbps

Salah satu fungsi yang didemonstrasikan dan sangat diminati adalah kemampuan wireless dengan dual nstream yang digabungkan dengan sistem multigateway routing. Dual nstream

adalah kemampuan sebuah perangkat wireless yang dapat menggunakan dua antarmuka jaringan sekaligus sehingga lebarnya pita yang bisa digunakan juga menjadi dua kali lipat dibandingkan hanya menggunakan satu antarmuka.

Kemampuan bisa dilipatgandakan lagi menggunakan teknik multigateway routing, yaitu kemampuan routing untuk membagi trafik yang melaluinya ke beberapa gateway secara acak. Pada demonstrasi di Praha ini digunakan empat perangkat wireless sehingga secara keseluruhan terdapat delapan sambungan wireless. Gabungan keseluruhan teknologi ini secara total mampu menciptakan media wireless dari satu titik ke titik lainnya sebesar 350 mbps.



Penggunaan perangkat lunak dan perangkat keras Mikrotik sudah cukup meluas di beberapa belahan dunia. Di Denmark, router Mikrotik digunakan untuk pengaturan RT/RW-net yang sampai saat ini telah memiliki 2.000 pengguna. Di Belanda, jaringan wireless Mikrotik ini digunakan juga secara internal sebagai media jaringan kamera keamanan (video surveillance).

Meskipun tidak gratis, perangkat lunak Mikrotik ini bisa didapatkan dengan membayar lisensi seharga 45 dollar AS. Dengan membayar lisensi ini, pengguna juga mendapatkan hak untuk melakukan upgrade versi secara gratis selama satu tahun. Setelah itu, router akan tetap bisa digunakan, tetapi tidak bisa di-upgrade ke versi yang lebih baru, kecuali kalau pengguna memperpanjang lisensinya.

Secara umum, Mikrotik memang memiliki cukup banyak fasilitas yang sangat berguna untuk sebuah router. Kemampuannya jika diinstal pada komputer Pentium IV menyamai router bermerek kelas menengah, sedangkan penggunaan routerboard sebagai perangkat wireless juga cukup bisa diandalkan dan disejajarkan dengan perangkat-perangkat wireless kelas satu.

Satu hal yang bisa cukup mengganggu untuk pengguna awal adalah kebingungan saat melakukan instalasi awal dikarenakan tersedia cukup banyaknya fitur. Pengguna awal akan bingung di bagian mana harus mulai menginstalasi router-nya. Namun, jika pengguna mau sedikit sabar meneliti panduannya, Mikrotik cukup nyaman dan andal untuk digunakan dalam jaringan.

Valens Riyadi

Dimuat di Harian Kompas 23 Januari 2006

2

Dasar Jaringan Komputer

Jaringan Komputer

Jaringan komputer adalah koneksi antara dua device atau lebih, yang terhubung secara fisik maupun secara logika sehingga bisa saling bertukar informasi. Jaringan komputer dapat dikatakan terkoneksi apabila device yang ada dalam jaringan
tersebut bisa saling bertukar data/informasi dan berbagi resource yang dimiliki.

Manfaat Jaringan Komputer

Ada beberapa pertimbangan kenapa kita perlu membangun sebuah jaringan komputer. Pertimbangan ini juga merupakan manfaat dari sebuah jaringan komputer.

Resource Sharing

Dengan adanya jaringan komputer, berbagi resource bisa dilakukan tanpa terkendala jarak. Resource sharing meliputi :

- Data Sharing, dengan adanya jaringan komputer kita bisa dengan mudah berbagi data seperti dokumen, gambar, video, dll dengan kolega yang ada di lokasi yang jauh bahkan di negara yang berbeda.
- Hardware Sharing, jika dulunya satu komputer satu printer, dengan jaringan komputer, satu printer bisa digunakan oleh beberapa komputer sekaligus. Tidak hanya printer, kita bisa sharing storage dan banyak hardware lainnya.
- Internet Access Sharing, jaringan komputer kecil memungkinkan beberapa komputer berbagi satu koneksi internet. Device khusus seperti router, memiliki kemampuan mengalokasikan bandiwdth dengan mudah untuk komputer user yang membutuhkan.

Connectivity dan Communication

Individu dalam sebuah gedung atau workgroup dapat dikoneksikan dalam jaringan LAN. Beberapa LAN dengan lokasi yang berjauhan terkoneksi ke dalam jaringan WAN. Ketika jaringan sudah terbentuk dan terhubung, maka komunikasi antar user bisa terjadi, misalnya dengan menggunakan teknologi email.

Data Security and Management

Dalam Dunia bisnis, jaringan memberikan kemudahan bagi administrator untuk melakukan managemen data penting perusahaan dengan lebih baik. Daripada data penting ini ada di setiap perangkat komputer karyawan yang bisa pengelolaan data dilakukan secara serampangan, akan lebih aman dan lebih mudah ketika data tersebut disimpan secara

terpusat dengan menggunakan *Shared Server*. Dengan cara seperti ini, karyawan perusahaan lebih mudah dalam mencari data. Administrator juga dapat memastikan bahwa data dibackup secara reguler, dan memungkinkan untuk menerapkan *security* dengan cara menentukan siapa yang boleh membaca atau menulis data yang bersifat penting.

Performance Enhancement dan Balancing

Dalam kondisi tertentu sebuah jaringan dapat digunakan untuk meningkatkan kinerja dari beberapa aplikasi dengan cara mendistribusikan tugas komputasi pada beberapa komputer pada jaringan.

Entertainment

Jaringan komputer terutama Internet, biasanya menyediakan banyak jenis hiburan dan permainan. Seperti *multi-player* game yang bisa dimainkan oleh beberapa user dalam waktu yang bersamaan, atau sekedar menonton video.

Kekurangan Jaringan Komputer

Biaya Network Hardware, Software dan Setup

Jaringan komputer tidak terbentuk begitu saja, membuat jaringan komputer tentu membutuhkan investasi *hardware* dan *software*, perencanaan, *design* jaringan, dan implementasi jaringan.

Biaya Managemen Hardware/Software dan Administrasi

Jaringan komputer membutuhkan perawatan dan pemeliharaan secara berkala oleh IT profesional.

Sharing yang Tidak Diinginkan

Disamping kemudahan dalam melakukan sharing informasi, ada resiko dimana file yang disharing terinfeksi virus komputer, sehingga bisa dengan mudah tersebar.

Perilaku yang Ilegal atau Tidak Diinginkan

Hampir sama dengan point sebelumnya, jaringan komputer memudahkan untuk berkomunikasi, akan tetapi membawa resiko lain, seperti mengambil atau memproduksi konten ilegal, pembajakan, dll.

Data Security Concerns

Pada jaringan komputer yang diimplementasikan dengan baik, keamanan data bisa tetap terjaga. Sebaliknya, jika implementasi yang terkesan asal – asalan, maka data yang ada dalam jaringan tersebut juga dalam bahaya. Serangan hacker mungkin saja terjadi, sabotase, atau yang cukup riskan adalah upaya untuk mencuri dokumen penting perusahaan.

Jenis Jaringan Komputer

Berdasarkan Jenis Transmisi

Dalam mempelajari jenis jaringan komputer terdapat beberapa klasifikasi yang cukup penting yaitu teknologi transmisi dan jarak. Secara teori, jaringan komputer dibagi *berdasarkan transmisi* dan *jarak*. Terdapat dua jenis jaringan berdasarkan teknologi transmisi, yaitu jaringan *broadcast* dan *jaringan point-to-point.*

- Jaringan ***Broadcast*** memiliki saluran komunikasi tunggal yang dipakai bersama-sama oleh semua device yang terkoneksi ke jaringan. Pesan-pesan berukuran kecil, disebut paket, yang dikirimkan oleh suatu mesin akan diterima oleh mesin-mesin lainnya. *Field* alamat pada sebuah paket berisi keterangan tentang kepada siapa paket tersebut ditujukan. Saat menerima paket, mesin akan mencek *field* alamat. Bila paket tersebut ditujukan untuk dirinya, maka mesin akan memproses paket itu, bila paket ditujukan untuk mesin lainnya, mesin terserbut akan mengabaikannya.
- Jaringan ***Point-to-Point*** terdiri dari beberapa koneksi pasangan individu, dari satu device ke satu device lain. Untuk mengirim paket dari sumber ke suatu tujuan, sebuah paket pada jaringan jenis ini mungkin harus melalui satu atau lebih mesin-mesin perantara. Seringkali harus melalui banyak route yang mungkin berbeda

jaraknya. Karena itu algoritma route memegang peranan penting pada jaringan point-to-point.

Pada umumnya jaringan yang lebih kecil dan terlokalisasi secara geografis cendurung memakai *broadcasting*, sedangkan jaringan yang lebih besar menggunakan *point-to-point*.

Berdasarkan Geografis

Alternatif lain dalam melakukan klasifikasi sebuah jaringan adalah berdasarkan pada cakupan geografis sebuah jaringan. LAN, MAN, WAN, dan Internet bisa dikatakan sebagai *true network*, artinya komputer-komputer yang bekomunikasi dengan cara bertukar data/pesan melalui kabel yang lebih panjang.

- *Local Area Network (LAN)*

Local Area Network (LAN) dapat didefinisikan sebagai kumpulan komputer yang saling dihubungkan bersama didalam satu area tertentu yang tidak begitu luas, seperti di dalam satu kantor atau gedung. LAN dapat juga didefinisikan berdasarkan pada penggunaan alamat IP komputer pada jaringan. Suatu komputer atau host dapat dikatakan satu LAN bila memiliki alamat IP yang masih dalam satu alamat jaringan, sehingga tidak memerlukan router untuk berkomunikasi.

Jaringan LAN dapat juga dibagi menjadi dua tipe, yaitu jaringan *peer to peer* dan jaringan *client-server*. Pada jaringan *peer to peer*, setiap komputer yang terhubung dapat bertindak baik sebagai *workstation* maupun *server*, sedangkan pada jaringan *client-server*, hanya satu komputer yang bertindak sebagai *server* dan komputer lain sebagai *workstation*.

- *Metropolitan Area Network (MAN)*

Metropolitan Area Network (MAN) pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya memakai teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang berdekatan dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. Alasan utama memisahkan MAN sebagai kategori khusus adalah telah ditentukannya standart untuk MAN, dan standart ini sekarang sedang diimplementasikan. Standart tersebut disebut DQDB *(Distributed Queue Dual Bus)* atau

802.6 menurut standart IEEE, DQDB terdiri dari dua buah kabel *unidirectional* dimana semua komputer dihubungkan. Setiap *bus* mempunyai sebuah *head–end*, perangkat untuk memulai aktivitas transmisi.

- *Wide Area Network (WAN)*

Wide Area Network (WAN) merupakan jaringan komputer yang mencakup daerah geografis yang luas, sering kali mencakup sebuah negara atau benua.

- *Internet*

Internet (kependekan dari interconnection-networking) adalah seluruh jaringan komputer yang saling terhubung menggunakan standar sistem global Transmission Control Protocol/Internet Protocol Suite (TCP/IP) sebagai protokol pertukaran paket (*packet switching communication protocol*) untuk melayani miliaran pengguna di seluruh dunia, bahkan antar planet.

Jaringan Tanpa Kabel

Disebut juga jaringan nirkabel, hampir sama seperti halnya jaringan kabel, hanya saja koneksi antar *host* tidak lagi menggunakan media kabel. Biasanya jaringan tanpa kabel menghubungkan satu sistem komputer dengan sistem yang lain dengan menggunakan beberapa macam media transmisi tanpa kabel, seperti gelombang radio, gelombang mikro, maupun cahaya infra merah.

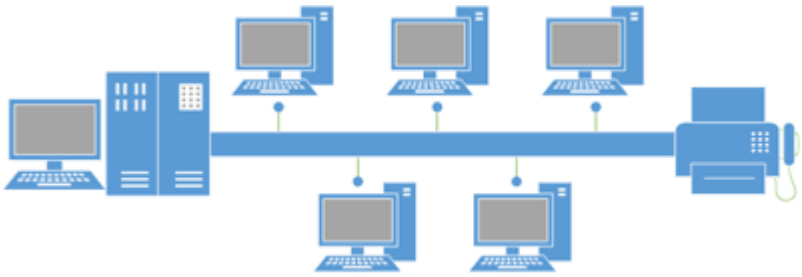
- Inframerah biasa digunakan untuk komunikasi jarak dekat, dengan kecepatan 4 Mbps. Dalam penggunaannya untuk pengendalian jarak jauh, misalnya remote control pada televisi serta alat elektronik lainnya.
- Transmisi data menggunakan gelombang radio biasa kita kenal dengan WiFi atau WLAN.

Topologi Jaringan

Topologi adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Ada beberapa macam topologi yang umum digunakan saat ini, yaitu topologi *bus*, token-ring, star, tree, dan mesh.

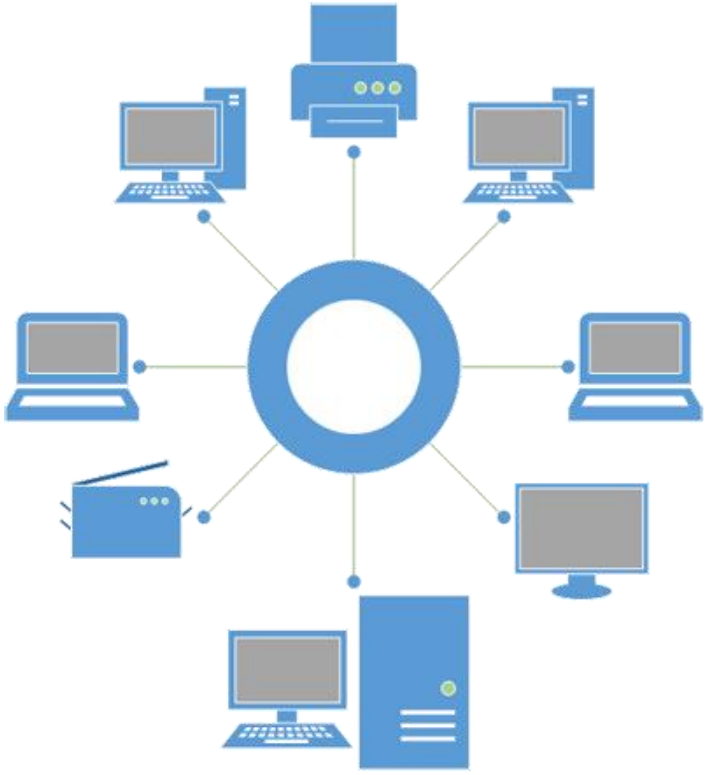
Topologi Bus

Pada topologi *bus* digunakan sebuah kabel tunggal atau kabel pusat di mana seluruh *workstation* dan server dihubungkan. Keunggulan topologi *bus* adalah pengembangan jaringan atau penambahan *workstation* baru dapat dilakukan dengan mudah tanpa mengganggu *workstation* lain. Kelemahan dari topologi ini adalah bila terdapat gangguan di sepanjang kabel pusat maka keseluruhan jaringan akan mengalami gangguan.



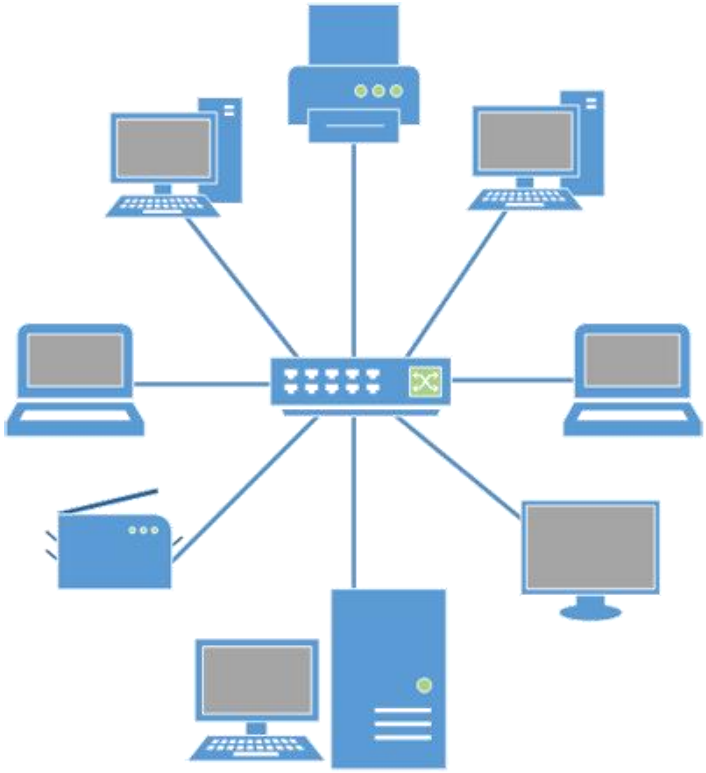
Topologi Ring

Pada topologi ring, semua *workstation* dan *server* dihubungkan sehingga terbentuk suatu pola lingkaran atau cincin. Tiap *workstation* ataupun *server* akan menerima dan melewatkan informasi dari satu komputer ke komputer lain, bila alamat-alamat yang dimaksud sesuai maka informasi diterima dan bila tidak informasi akan dilewatkan. Kelemahan dari topologi ini adalah setiap node dalam jaringan akan selalu ikut serta mengelola informasi yang dilewatkan dalam jaringan, sehingga bila terdapat gangguan di suatu node maka seluruh jaringan akan terganggu. Keunggulan topologi ring adalah tidak terjadinya *collision* atau tabrakan pengiriman data seperti pada topologi bus, karena hanya satu node dapat mengirimkan data pada suatu saat.



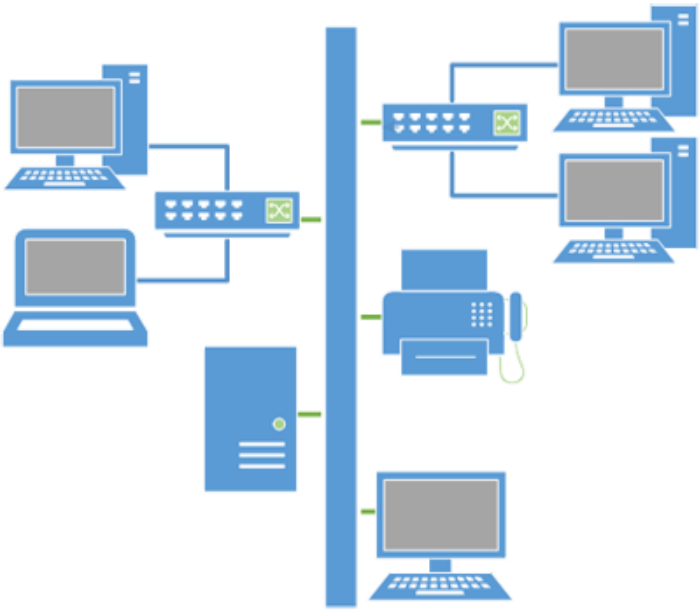
Topologi Star

Pada topologi star, masing-masing *workstation* dihubungkan secara langsung ke *server* atau *hub*. Keunggulan dari topologi star adalah dengan adanya kabel tersendiri untuk setiap *workstation* ke *server*, maka *bandwidth* atau lebar jalur komunikasi dalam kabel akan semakin lebar sehingga akan meningkatkan unjuk kerja jaringan secara keseluruhan. Bila terdapat gangguan di suatu jalur kabel maka gangguan hanya akan terjadi dalam komunikasi antara *workstation* yang bersangkutan dengan *server*, jaringan secara keseluruhan tidak mengalami gangguan. *Kelemahan* dari topologi star adalah kebutuhan kabel yang lebih besar dibandingkan dengan topologi lainnya.



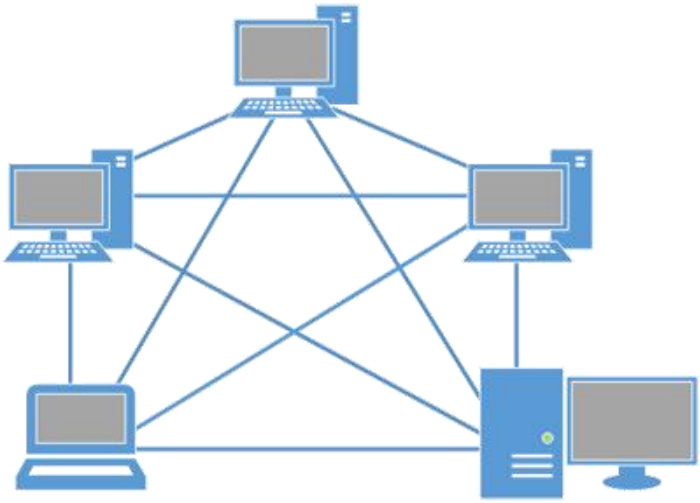
Topologi Tree

Topologi tree dapat berupa gabungan dari topologi star dengan topologi bus.



Topologi Mesh

Topologi mesh digunakan pada kondisi di mana tidak ada hubungan komunikasi terputus secara absolut antar node komputer. Topologi ini merefleksikan desain internet yang memiliki *multi path* ke berbagai lokasi.



Perangkat Jaringan

Perangkat jaringan adalah semua komputer, *peripheral*, *interface card*, dan perangkat tambahan yang terhubung ke dalam suatu sistem jaringan komputer untuk melakukan komunikasi data. Perangkat yang umun terdapat pada jaringan komputer terdiri dari :

Server

Server merupakan pusat kontrol dari jaringan komputer. *Server* berfungsi untuk menyimpan informasi dan untuk mengelola suatu jaringan komputer. Server akan melayani seluruh *client* atau *workstation* yang terhubung ke jaringan. Sistem operasi yang digunakan pada *server* adalah sistem operasi yang khusus yang dapat memberikan layanan bagi*workstation*.

Workstation

Workstation adalah komputer yang terhubung dengan sebuah LAN. Semua komputer yang terhubung dengan jaringan dapat dikatakan sebagai *workstation*. Komputer ini yang melakukan akses ke *server* guna mendapat layanan yang telah disediakan oleh *server*.

Network Interface Card

Network Interface Card (NIC) adalah *expansion board y*ang digunakan supaya komputer dapat dihubungkan dengan jaringan. Sebagian besar NIC dirancang untuk jaringan, protokol, dan media tertentu. NIC biasa disebut dengan LAN card. Contoh sebuah LAN Card seperti diperlihatkan pada Gambar

Jika dilihat dari kecepatannya, Ethernet terbagi menjadi empat jenis, yakni sebagai berikut:

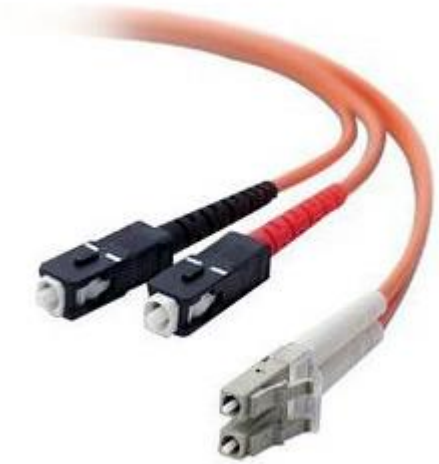
1. 10 Mbit/detik, yang sering disebut sebagai Ethernet, standar yang digunakan: 10Base2, 10Base5, 10BaseT, 10BaseF.
2. 100 Mbit/detik, yang sering disebut sebagai Fast Ethernet. Standar yang digunakan: 100BaseFX, 100BaseT, 100BaseT4, 100BaseTX.
3. 1000 Mbit/detik atau 1 Gbit/detik, yang sering disebut sebagai Gigabit Ethernet, standar yang digunakan: 1000BaseCX, 1000BaseLX, 1000BaseSX, 1000BaseT.
4. 10000 Mbit/detik atau 10 Gbit/detik, biasa disebut TenGig.

Kabel Jaringan

Kabel adalah saluran yang menghubungkan antara dua *workstation* atau lebih. Jenis-jenis kabel yang digunakan dalam jaringan antara lain Kabel *coaxial*, *Fiber Optic*, dan *Twised Pair.* *Kabel coaxial* hanya memiliki satu konduktor yang berada di pusat kabel. Kabel ini memiliki lapisan plastik yang berfungsi untuk pembatas konduktor dengan anyaman kabel yang ada pada lapisan berikutnya. Kabel coaxial memiliki kecepatan transfer sampai 10 Mbps. Kabel coaxial sering digunakan untuk kabel TV, ARCnet, thick ethernet dan thin ethernet. Thick coaxial / 10Base5 / RG-8 sering digunakan untuk *backbone*, untuk instalasi jaringan antar gedung. Kabel ini secara fisik berat dan tidak fleksibel, namun ia mampu menjangkau jarak 500m bahkan lebih. Thin coaxial / 10Base2 / RG-58 / *cheapernet* sering digunakan untuk jaringan antar *workstation*. Kabel ini secara fisik lebih mudah ditangani daripada RG-8 karena lebih fleksibel dan ringan. *Thick coax* mempunyai diameter rata-rata 12mm sedangkan thin coaxial mempunyai diameter rata-rata berkisar 5mm. Setiap perangkat dihubungkan dengan BNC Tconnector.

Kabel fiber optik memiliki inti kaca yang dilindungi oleh beberapa lapisan pelindung. Pengiriman data pada kabel ini menggunakan sinar. Kabel fiber optik memiliki jarak yang lebih jauh daripada twisted pair dan coaxial. Kabel ini juga memiliki kecepatan transfer data yang lebih baik dalam pengiriman data, yaitu mencapai 155Mbps. Kabel jenis coaxial saat ini sudah jarang digunakan.

Kabel Fiber Optic memiliki dua tipe, yaitu *single mode* dan *multi mode*. Tipe kabel *single mode* memiliki diameter core 9micron, sedangkan kabel *multi mode* memiliki diameter core sebesar 62,5micron. Kabel fiber optik mulai banyak digunakan karena kemampuan transfer data yang lebih besar, serta jangkauan kabel yang cukup jauh.



Kabel twisted pair, kabel yang biasa digunakan untuk jaringan lokal, secara umum dibagi menjadi 2 tipe, *Shielded Twisted Pair* (STP) *dan Unshielded Twisted Pair* (UTP). Sepasang kabel yang di-*twist* (pilin), yang jumlah pasangannya dapat terdiri dari dua, empat atau lebih. Fungsi *twist* bertujuan untuk mengurangi interferensi elektromagnetik terhadap kabel lain atau terhadap sumber eksternal. Kecepatan transfer data yang dapat dilayani sampai

10Mbps. Konektor yang biasa digunakan adalah RJ-11 atau RJ-45. Dari kedua tipe ini, tipe UTP adalah tipe yang sering digunakan pada jaringan LAN. UTP memiliki 4 pasang kabel terpilin (8 buah kabel) dan hanya 4 buah kabel yang digunakan dalam jaringan. Perangkat yang berkenaan dengan penggunaan jenis kabel ini adalah konektor RJ-45 dan Hub/Switch.

Hub dan Switch

Switch adalah perangkat yang juga berfungsi untuk menghubungkan *multiple* komputer. Switch secara fisik sama dengan hub tetapi logikalnya sama dengan barisan brigde. Peningkatan kecerdasan dibandingkan hub, yaitu memiliki kemampuan penyimpanan terhadap alamat MAC (*Medium Access Control*) atau pada *link layer* model OSI sehingga hanya mengirimkan data pada port yang dituju (*unicast*). Hal ini berbeda dengan hub yang mengirimkan data ke semua port (*broadcas*t). Proses kerjanya adalah apabila paket data datang, header dicek untuk menentukan di segment mana tujuan paket datanya. Kemudian data akan dikirim kembali (*forwaded*) ke segment tujuan tersebut.

- *Unmanaged Switch*, merupakan tipe pilihan termurah dan biasanya digunakan di kantor atau bisnis kecil dan rumahan. Switch Jaringan Komputer ini melakukan fungsi dasar mengelola lalu lintas data antara *printer* atau periperal dengan satu komputer atau lebih. Tipe switch ini tidak dapat kita kelola layaknya manageable switch yang memiliki fitur tambahan dalam pengaplikasiannya, seperti fungsi VLAN.
- *Managed Switch* menawarkan keunggulan yang lebih dengan memiliki User Interface atau menawarkan perangkat lunak yang memungkinkan pengguna untuk melakukan konfigurasi pada switch. Keunggulan yang ditawarkan ole jenis switch ini adalah

dapat melakukan segmentasi pada jaringan dengan konsep VLAN yang bermanfaat untuk memberikan kemanan lebih pada sebuah jaringan, Memudahkan pengguna untuk melakukan pemantauan dan pemeliharaan network traffic.

Bridge

Bridge adalah peranti yang meneruskan lalu lintas antara segmen jaringan berdasar informasi pada lapisan *data link*. Segmen ini mempunyai alamat lapisan jaringan yang sama. Bridge bekerja dengan mengenali alamat MAC asal yang mentransmisi data ke jaringan dan secara otomatis membangun sebuah tabel internal. Tabel ini berfungsi untuk menentukan ke segmen mana paket akan di route dan menyediakan kemampuan *filtering*. Bridge membagi satu buah jaringan besar kedalam beberapa jaringan kecil. Bridge juga dapat di gunakan untuk mengkoneksi*network* yang menggunakan tipe kabel yang berbeda ataupun topologi yang berbeda pula.

Router

Router adalah perangkat yang berfungsi menghubungkan suatu LAN ke suatu internetworking/WAN dan mengelola penyaluran lalu-lintas data di dalamnya. Router akan menentukan jalur terbaik untuk komunikasi data. Router bekerja pada *layer network* dari model OSI untuk memindahkan paket-paket antar jaringan menggunakan alamat logikanya. Router memliki tabel routing yang melakukan pencatatan terhadap semua alamat jaringan yang diketahui dan lintasan yang mungkin dilalui serta waktu

tempuhnya. Router bekerja hanya jika protokol jaringan yang dikonfigurasi adalah protokol yang routable seperti TCP/IP atau IPX/SPX. Ini berbeda dengan bridge yang bersifat protocol independent.

Repeater

Repeater bekerja pada level *physical layer* dalam model jaringan OSI. Repeater bertugas meregenerasi atau memperkuat sinyal-sinyal yang masuk. Pada ethernet kualitas transmisi data hanya dapat bertahan dalam range waktu dan jangkauan terbatas, yang selanjutnya mengalami degradasi. Repeater akan berusaha mempertahankan integritas sinyal dan mencegah degradasi sampai paket-paket data menuju tujuan. Kelemahan repeater yaitu tidak dapat melakukan *filter traffic* jaringan. Data (bit) yang masuk ke salah satu port dikirim ke luar melalui semua port. Dengan demikian data akan tersebar ke segmen-segmen LAN tanpa memperhitungkan apakah data tersebut dibutuhkan atau tidak.

Modem

Modem adalah sebuah *device* yang digunakan sebagai penghubung dari sebuah PC atau jaringan ke Penyedia Layanan Internet (*Internet Service Provider* / ISP). Salah satu modem

yang dipakai untuk koneksi ke internet ialah modem ADSL. Modem ini biasanya digunakan oleh ISP.

Bandwidth

Bandwidth adalah jumlah data atau volume data dalam satuan bit per second yang dapat ditransmisikan lewat sebuah media transmisi jaringan dalam satu satuan waktu.
Secara umum, *bandwidth* dapat dianalogikan seperti sebuah pipa air, dan data adalah air yang akan melewati pipa tersebut.

Semakin besar pipa air (*bandwidth*) maka semakin besar pula volume air (data) yang dapat dilewatkan. Ada beberapa alasan yang menjadikan *bandwith*merupakan salah satu faktor penting dalam sebuah jaringan komputer :

1. *Bandwidth* berperan penting dalam menentukan kualitas sebuah jaringan karena besarnya saluran data/*bandwidth* berpengaruh pada kecepatan transmisi data.
2. *Bandwidth* memiliki keterbatasan dikarenakan hukum fisika dan keterbatasan teknologi. Setiap media yang digunakan utnuk melakukan transmisi data pasti memiliki keterbatasan *bandwidth* maksimal yang bisa dicapai.

3. *Bandwidth* tidak didapatkan dengan gratis. Tawaran *bandwidth* paling sering kita jumpai ketika kita ingin berlangganan internet.
4. Kebutuhan *bandwidth* akan selalu naik. Dengan adanya teknologi baru dan infrastruktur jaringan yang diperbaharui, aplikasi dan kebutuhan data biasanya juga akan mengalami peningkatan penggunaan *bandwidth*.

Pengkabelan

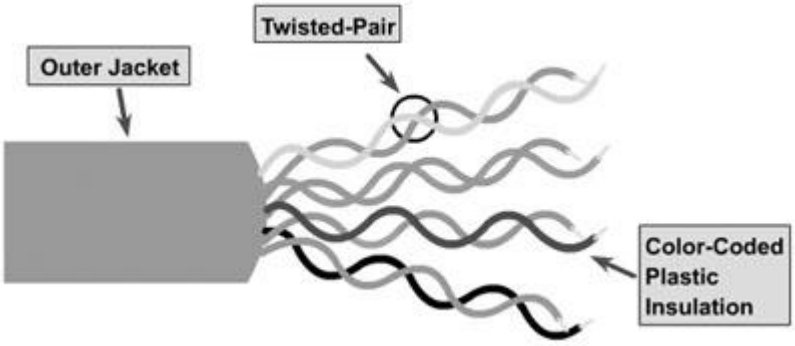
Pada saat kita berbicara, agar suara yang kita ucapkan bisa sampai ke telinga rekan yang kita ajak bicara, dibutuhkan sebuah media trasnmisi, dalam hal ini udara. Setiap jaringan komputer juga membutuhkan media transmisi. Media transmisi jaringan komputer ada banyak, bisa menggunakan media kabel, gelombang radio / wireless, infra red, bluetooth, atau saat ini yang populer menggunakan media cahaya (fiber optic). Kebanyakan media transmisi yang digunakan saat ini adalah jenis kabel. Setiap jenis kabel khususnya mempunyai kemampuan dan spesifikasinya yang berbeda, oleh karena itu dibuatlah pengenalan tipe kabel.

Kabel Twisted Pair

Kabel twisted-pair adalah jenis kabel yang digunakan untuk komunikasi telepon dan sebagian besar jaringan Ethernet modern. Sepasang kabel membentuk sebuah jalur yang dapat mengirimkan data. Pasangan kebel tersebut dibuat saling melilit untuk memberikan perlindungan terhadap “crosstalk”, atau gangguan yang dihasilkan oleh pasangan kabel yang berdekatan. Ketika arus listrik mengalir melalui kawat kabel, akan menciptakan medan magnet kecil melingkar di sekitar kawat. Ketika dua kabel dalam sebuah sirkuit listrik ditempatkan berdekatan, dan medan magnet mereka adalah kebalikan dari satu sama lain, dengan demikian dua medan magnet akan saling menghilangkan satu sama lain. Pasangan kabel tersebut juga akan menghilangkan setiap medan magnet yang berasal dari luar kabel. Dengan memutar kabel maka akan dapat meningkatkan efek saling menghilangkan medan magnet dan secara efektif dapat memberikan perlindungan pada kabel jaringan. Ada 2 jenis umum pada kabel jenis twisted-pair, **unshielded twisted pair (UTP)** dan**shielded twisted pair (STP)**

UTP

Kabel UTP adalah media transmisi yang terdiri dari 4 pasang kawat. Kabel UTP digunakan dalam berbagai jaringan. Masing-masing dari delapan kabel tembaga individu dalam kabel UTP ditutupi oleh bahan isolasi. Selain itu, kabel di setiap pasangan yang melilit satu sama lain.



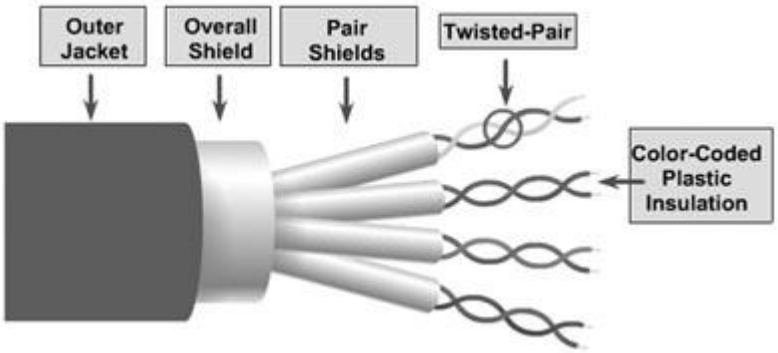
Kabel UTP sering dikombinasikan dengan menggunakan Registered Jack 45 (RJ-45) konektor. RJ-45 adalah konektor delapan kabel yang digunakan biasanya untuk menghubungkan komputer ke sebuah local-area network (LAN), khususnya Ethernet.

Kabel UTP memiliki empat pasang dengan ukuran kawat tembaga 22 atau 24 gauge (gauge merupakan standart pengurkuran kabel). Salah satu faktor yang membedakan kabel UTP dengan kabel lain salah satunya kabel UTP memiliki impedansi 100 ohm. meskipun dahulu kabel UTP dikatakan memiliki kecepatan transfer yang lambat, namun dalam

perkembangannya sekarang mampu melewatkan trafik hingga 1 Gbps. Maksimal panjang kabel UTP adalah 100 meter.

STP

Hampir sama dengan UTP hanya saja setiap pasang kawat dibungkus dengan foil logam. Keempat pasang kawan akan dibungkus lagi dengan foil logam atau serabut logam. Tujuannya adaalh untuk mengurangi gangguan seperti electric noise, medan magnet, dll. STP bisa dikombinasikan dengan STP Data Connector atau bisa juga dengan RJ45. Maksimal panjang kabel STP adalah 100 meter. Karena lebih tahan dari noise, kabel STP ini lebih banyak digunakan untuk pengaplikasian outdoor, seperti kabel yang menuju AP di tower.



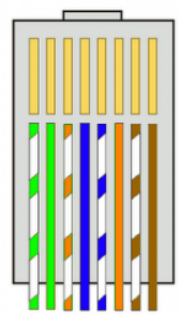
Standart Pengkabelan

Setiap kawat didalam kabel jaringan memiliki fungsi yang berbeda sehingga kita tidak bisa asal crimping. Ada dua standart pengkabelan yang paling sering digunakan yaitu : **EIA/TIA 568A** dan **EIA/TIA 568B**, dengan cara mengurutkan sususan kabel berdasarkan warna.

EIA/TIA 568A.

Susunan kabel dengan standart EIA/TIA 568A dimulai dengan kabel berwarna putih hijau. maka susunan kabel akan menjadi seperti berikut :

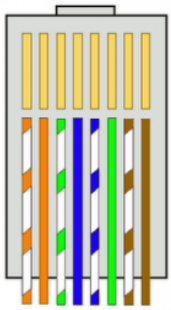
1. Putih Hijau
2. Hijau
3. Putih Orange
4. Biru



5. Putih Biru
6. Orange
7. Putih Coklat
8. Coklat

EIA/TIA 568B

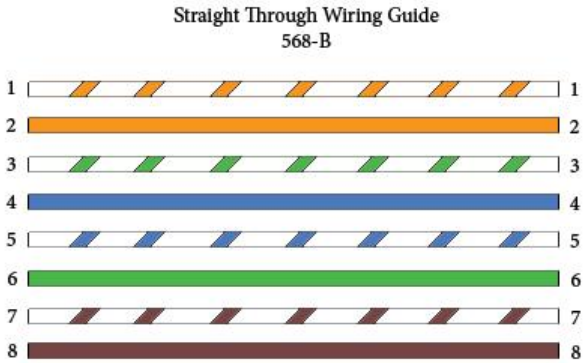
Susunan kabel dengan standart EIA/TIA 568B dimulai dengan warna putih orange. Urutan lengkap kabel dengan standart ini seperti berikut :



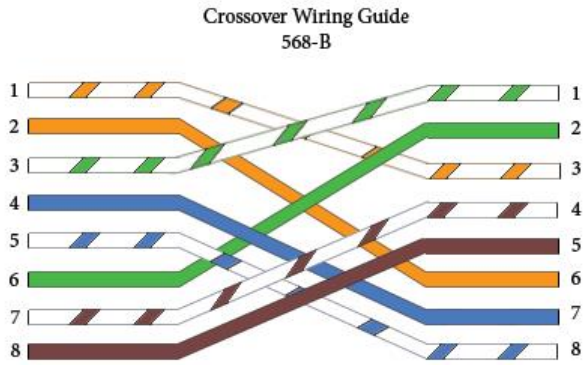
1. Putih Orange
2. Orange
3. Putih Hijau
4. Biru
5. Putih Biru
6. Hijau
7. Putih Coklat
8. Coklat

Kabel Cross & Straight

Pada saat kita bicara tentang pengurutan pin kabel jaringan, tentu sebutan*Crossover* dan *Straight* sering kita dengar. Kabel straight merupakan kabel yang ujung awal dengan ujung akhir kabel memiliki urutan pin yang sama. Contoh kabel straight dengan standart pengurutan pin EIA/TIA 568B



Maka ujung dengan dan ujung belakang sama – sama memiliki susunan pin EIA/TIA 568B. Kemudian untuk kabel cross, sesuai namanya artinya susunan pin berlawanan, atau berseberangan.



Kabel straight dan cross memang sama – sama menghubungkan device ke device lain dalam jaringan komputer, namun device yang bisa dihubungkan dengan masing – masing jenis kabel ini berbeda. Derikut tabel device yang akan dihubungkan dan kabel yang dibutuhkan :

	Hub	Switch	Router	Workstation
Hub	Crossover	Crossover	Straight	Straight
Switch	Crossover	Crossover	Straight	Straight
Router	Straight	Straight	Crossover	Crossover
Workstation	Straight	Straight	Crossover	Crossover

Auto MDI/MDI-X

Perangkat terbaru saat ini biasanya sudah mendukung Auto MDI/MDI-X. Perangkat yang sudah support Auto MDI/MDI-X bisa dihubungkan dengan kabel straight maupun kabel cross. Perangkat akan mendeteksi apakah koneksi membutuhkan crossover, dan secara otomatis akan menggunakan konfigurasi MDI atau MDIX untuk menyamakan koneksi perangkat lawan.

Pengkabelan

Sebelum melakukan pengkabelan, ada beberapa pertimbangan yang harus dilakukan terlebih dahulu, misalnya berapa jumlah komputer yang akan dihubungkan. Kemudian jarak antar node perangkat.

Alat yang Dibutuhkan

Untuk melakukan pengkabelan, siapkan beberapa alat berikut :

- Cable UTP/STP, tentukan berapa panjang kabel, dan berapa jumlah kabel yang dibutuhkan. Kualitas kabel juga berbeda pada tiap merk.
- RJ45, yang nanti akan digunakan sebagai konektor kabel.
- Crimping Tool, untuk melakukan pemasangan konekstor RJ45 ke kabel UTP/STP, biasanya disebit crimping.
- LAN Tester, ketika proses pembuatan kabel jaringan sudah selesai, hal terakhir yang perlu dilakukan adalah testing. LAN tester ini digunakan untuk melakukan tsting terhadap kabel jaringan. Indikasi apakah kabel berfungdi dengan normal bisa dari indikator buyi beep LAN tester atau bisa juga dari nyala lampu LED.

Cara Pengkabelan

1. Kupas bagian ujung kabel UTP, kira-kira 2 cm.
2. Buka pilinan kabel, luruskan dan urutankan kabel sesuai standar TIA/EIA 368B
3. Setelah urutannya sesuai standar, potong dan ratakan ujung kabel, Masukan kabel yang sudah lurus dan sejajar tersebut ke dalam konektor RJ-45, dan pastikan semua kabel posisinya sudah benar.
4. Lakukan crimping menggunakan crimping tools, tekan crimping tool dan pastikan semua pin (kuningan) pada konektor RJ-45 sudah “menggigit” tiap-tiap kabel. Setelah selesai pada ujung yang satu, lakukan lagi pada ujung yang lain.
5. Langkah terakhir adalah menge-cek kabel yang sudah kita buat tadi dengan menggunakan LAN tester, caranya masukan masing-masing ujung kabel (konektor RJ-45) ke masing2 port yang tersedia pada LAN tester, nyalakan dan pastikan semua lampu LED menyala sesuai dengan urutan kabel yang kita buat.

Pastikan ujung kabel UTP yang telah terpasang konektor RJ-45 dengan benar, selubung kabel (warna biru) juga ikut sedikit masuk kedalam konektor.

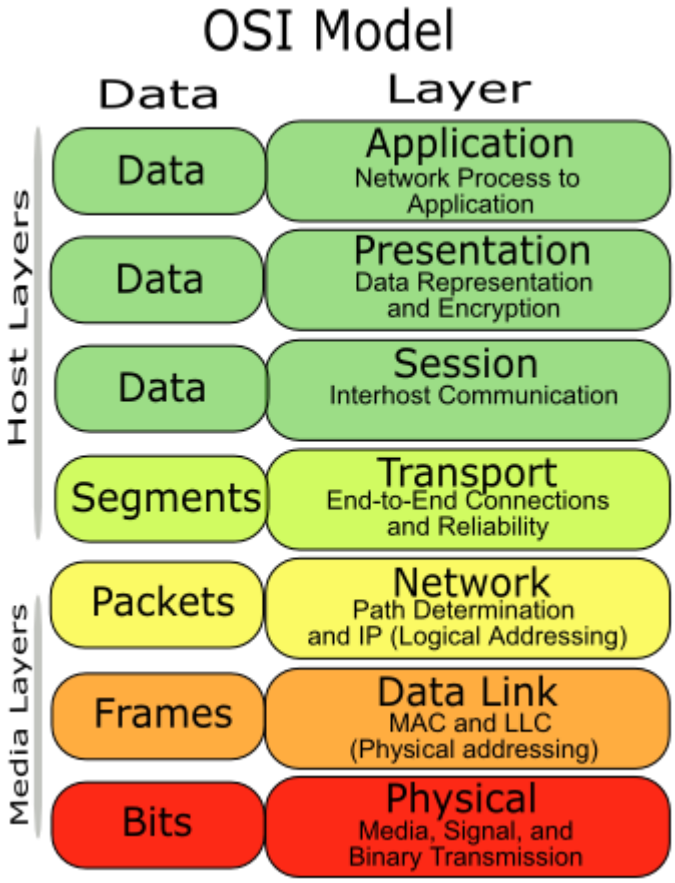
TCP/IP: Pengenalan OSI Layer

Pada saat kita memulai langkah ke dalam ilmu jaringan komputer, hal yang pertama kali kita pelajari biasanya adalah TCP/IP. TCP/IP bisa di analogikan seperti bahasa. Ketika manusia bertukar informasi, manusia akan berbicara dengan bahasa yang bisa dimengerti oleh pembicara maupun pendengar. Begitu juga halnya dengan komputer atau host dalam sebuah jaringan. Agar komunikasi dan pertukaran informasi bisa terjalin dengan baik, dibutuhkan bahasa sama.

Walaupun merek host jaringan tersebut berbeda – beda, host masih bisa berkomunikasi dengan host lain karena menggunakan standart komunikasi yang sama, yakni TCP/IP. Protokol internet pertama kali dirancang pada tahun 1980-an. Akan tetapi di tahun 1990-an dimana internet semakin populer dan host yang semakin banyak, mulai bemunculan protokol yang hanya bisa digunakan oleh kalangan tertentu, atau protokol yang dibuat oleh pabrik tertentu yang belum tentu kompatibel dengan protokol lain dari pabrik yang lain pula. Sehingga pada akhirnya badan International Standart Organization (ISO) membuat standarisasi protokol yang saat ini dikenal dengan protokol model Open System Interconnection atau disingkat OSI. Model OSI ini manjadi referensi dan konsep dasar teori tentang cara kerja sebuah protokol. Dalam perkembangannya TCP/IP digunakan sebagai standart de facto.

OSI Layer

Ketika ISO (*International Standart Organization*) membuat standarisasi protokol, maka terciptalah sebuah standar model referensi yang berisi cara kerja protokol. Model referensi yang kemudian disebut dengan *Open System Interconnection* (OSI). Berdasarkan dokumen rekomendasi X.200, standart OSI ini memiliki 7 layer. Tiap layer ini memiliki definisi fungsi yang berbeda.



Layer 7 : Application Layer

Merupakan layer dimana terjadi interaksi antarmuka end user dengan aplikasi yang bekerja menggunakan fungsionalitas jaringan, melakukan pengaturan bagaimana aplikasi bekerja menggunakan resource jaringan, untuk kemudian memberika pesan ketika terjadi kesalahan. Beberapa service dan protokol yang berada di layer ini misalnya HTTP, FTP, SMTP, dll.

Layer 6 : Presentation Layer

Layer ini bekerja dengan mentranslasikan format data yang hendak ditransmisikan oleh aplikasi melalui jaringan, ke dalam format yang bisa ditransmisikan oleh jaringan. Pada layer ini juga data akan di-enkripsi atau di-deskripsi.

Layer 5 : Session Layer

Session layer akan mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Di layer ini ada protocol *Name Recognition*, NFS & SMB.

Layer 4 : Transport Layer

Layer ini akan melakukan pemecahan data ke dalam paket-paket data serta memberikan nomor urut pada paket-paket data tersebut sehingga dapat disusun kembali ketika sudah sampai pada sisi tujuan. Selain itu, pada layer ini, akan menentukan protokol yang akan digunakan untuk mentransmisi data, misalkan protokol TCP. Protokol ini akan mengirimkan paket data, sekaligus akan memastikan bahwa paket diterima dengan sukses (acknowledgement), dan mentransmisikan ulang terhadap paket-paket yang hilang atau rusak di tengah jalan.

Layer 3 : Network Layer

Network layer akan membuat header untuk paket-paket yang berisi informasi IP, baik IP pengirim data maupun IP tujuan data. Pada kondisi tertentu, layer ini juga akan melakukan routing melalui internetworking dengan menggunakan router dan switch layer-3.

Layer 2 : Data-link Layer

Befungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai frame. Selain itu, pada level ini terjadi koreksi kesalahan, *flow control*, pengalamatan perangkat keras (seperti halnya *Media Access Control Address* (*MAC Address*)), dan menetukan bagaimana perangkat-perangkat jaringan seperti hub, bridge, repeater, dan switch layer 2 beroperasi. Spesifikasi IEEE 802, membagi level ini menjadi dua level anak, yaitu *lapisan Logical Link Control* (LLC) dan lapisan *Media Access Control* (MAC).

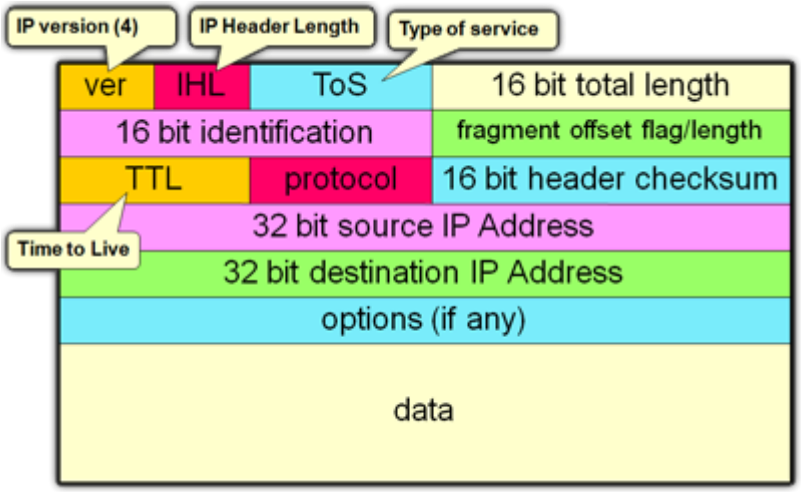
Layer 1 : Physical Layer

Layer Physcal berkerja dengan mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya Ethernet atau Token Ring), topologi jaringan dan pengabelan. Selain itu, level ini juga mendefinisikan bagaimana *Network Interface Card* (NIC) dapat berinteraksi dengan media kabel atau radio.
Proses pengiriman data melewati tiap layer ini bisa kita analogikan seperti ketika kita mengirim surat. Isi surat adalah data yang akan kita kirim (layer 7 -> 5). Kemudian sesuai standart pengiriman, isi surat tersebut kita masukkan kedalam sebuah amplop (layer – 4). Agar surat kita bisa terkirim, kita perlu menambahkan alamat kemana surat tersebut akan

dikirim, juga siapa pengirim surat tadi (layer – 3). Selanjutnya surat tersebut kita serahkan ke pihak ekspedisi, dan pihak ekspedisi yang nanti akan mengirimkan surat kita tadi (layer – 2&1).

Packet Header

Pada ulasan sebelumnya kita membahas bagaimana proses sebuah data ditransmisi, sekarang kita akan mencoba membongkar sebuah data. Apa isi sebiah data sehingga data tersebut bisa di transmisikan. ketika kita analogikan mengirim data di internet itu seperti mengirim POS, bisa dikatakan data adalah isi surat tersebut, kemudian paket header adalah amplop, perangko, alamat, dan kelengkapan lainnya. Paket header ini memberikan beberapa informasi tambahan. Jika kita bedah sebuah paket data yang ditrasnmisikan menggunakan ipv4, maka isi dari paket data tersebut bisa kita lihat seperti gambar berikut :



IPVer : Menyimpan informasi versi IP yang digunakan (IPv4 atau IPv6).

IHL (IP Header Leght) : Informasi panjang keseluruhan header paket data. Minimum panjang IP header adalah 20 bits, dan maximum panjang adalah 24 bits.

TOS **:** Adalah sebuah field dalam header IPv4 yang memiliki panjang 8 bit dan digunakan untuk menandakan jenis *Quality of Service* (QoS) yang digunakan oleh datagram yang bersangkutan untuk disampaikan ke router-router internetwork. Implementasi TOS ini biasanya saat kita melakukan limitasi HIT di web proxy mikrotik atau service VOIP.

16 Bit Total Length : Isian 16 bits ini memberikan informasi ukuran keseluruhan

paket(fragment)termasuk header dan data. Informasi ditampilkan dalam format bytes

16 Bit Identification, Fragment Offset Flag/Length : Pada saat ip packet berjalan di internet, paket ini mungkin akan melewati beberapa router yang tidak bisa menghandle ukuran packet, misalnya nilai Maximum transmission unit (MTU) yang dimilikinya lebih kecil dibandingkan ukuran datagram IP, maka paket akan di pecah atau di fragmentasi menjadi paket – paket yang lebih kecil untuk kemudian akan disusun kembali setelahnya. Parameter ini yang akan digunakan untuk fragmentasi dan penyusunan kembali.

TTL : Ada kemungkinan sebuah IP packet berjalan tanpa tujuan di jaringan Internet. Contoh kasus misalnya adanya kesalahan routing atau routing loop. Agar paket ini tidak berputar-putar di jaringan internet selamanya, nilai TTL ini akan dikurangi setiap kali paket data melewati router. Ketika nilai TTL sebuah paket data sudah habis atau memiliki nilai 0, maka paket tersebut akan di drop atau dibuang.

Protocol : Berisi informasi protokol apa yang digunakan untuk melakukan transmisi data.

16 Bit Header Checksum : informasi nilai yang dihitung berdasarkan kalkulasi content IP header. Digunakan untuk menentukan apakah ada error pada saat dilakukannya transmissi data.

32 Bit Source IP Address : 32 bits informasi sumber IP paket data.

32 Bit Destination IP Address : 32 bits informasi IP yang dituju paket data.

Options (if any) : Parameter ini termasuk jarang digunakan, memiliki panjang yang bervariasi, dari 0 sampai kelipatan 32 bits. Parameter ini bisa digunakan untuk menyimpan sebuah nilai untuk opsi security, Record Route, Time Stamp, dll.

Data : Berisi data yang ditransmisikan.

Dari informasi paket header diatas, pada akhirnya sebuah data bisa dikirim dari satu host ke host yang lain.

TCP/IP : Protokol

Artikel bagian pertama membahas tentang apa yang terjadi pada sebuah paket data ketika akan dikirim dan ketika paket data tersebut diterima. Sekarang pertanyaannya adalah apa yang berperan diantara device yang akan saling bertukar informasi sehingga paket data bisa ditrasnmisikan. Disinilah fungsi sebuah protokol. Protokol akan menentukan bagaimana cara sebuah paket data ditransmisikan. Ada beberapa jenis protokaol yang sering kita gunakan seperti TCP, UDP, ICMP, dan IP Protokol lainnya.

IP Protokol

Adalah protokol standart yang digunakan untuk mengkomunikasikan data melalui berbagai jenis perangkat dan layer berdasarkan ip address yang tersimpan di paket header. Setiap datagram memiliki dua komponen, yakni header dan payload. IP header berisi informasi source IP address, destination IP address, dan beberapa informasi data lain yang dibutuhkan router untuk mengirim datagram. Kemudian payload adalah isi dari data yang akan dikirim. Metode penggabungan data payload dan header menjadi sebuah paket data disebut encapsulation. Pengiriman data dilakukan dengan sistem “per paket” dan/atau “per connection”. Sistem ini menjamin keutuhan data, dan mencegah terjadinya kekurangan ataupun duplikasi data.

Protokol TCP

Protokol ini merupakan salah satu jenis protokol yang paling sering digunakan di internet. Contoh aplikasi yang menggunakan protokol TCP misalnya http, email, ftp, dll. TCP bekerja dengan pengalamatan port seperti berikut :

- Port 1 – 1024 : *Low Port* (*Standard Service Port*). Port ini telah digunakan oleh service standart. Disarankan jangan menggunakan low port jika Anda ingin melakukan costumize port pada sebuah aplikasi atau service.
- Port 1025 – 65536 : *High port* (untuk transmisi lanjutan). Kita bisa gunakan port ini untuk transmisi atau service yang bersifat custom/tidak standart. Misalnya kita

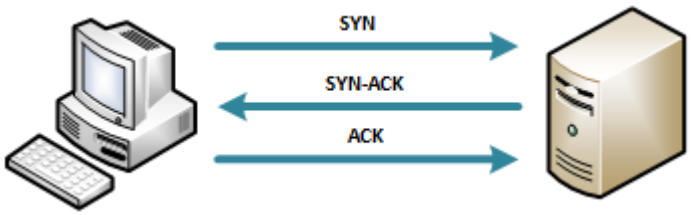
membuat proxy server. Maka port yang kita gunakan untuk proxy server adalah High Port ini. Kalau kita perhatikan, default proxy sendiri biasanya menggunakan high port, seperti port 8080 atau 3128.

Prinsip Kerja TCP

Pada saat melakukan tugasnya, protokol TCP memiliki beberapa prinsip kerja. Prinsip kerja sebuah protokol ini akan menjadi referensi bagi pembuat program atau admin jaringan untuk memilih protokol apa yang nanti akan digunakan untuk bisa melakukan trasnmisi data.

- *Connection Oriented*

Sebelum data dapat ditransmisikan antara dua host, dua proses yang berjalan pada lapisan aplikasi harus melakukan negosiasi untuk membuat sesi koneksi terlebih dahulu. Proses pembuatan koneksi TCP disebut juga dengan *"Three-way Handshake".* Tujuan metode ini adalah agar dapat melakukan sinkronisasi terhadap nomor urut dan nomor acknowledgement yang dikirimkan oleh kedua pihak dan saling bertukar ukuran TCP Window.



Client : SYN -> Server : Client akan mengirimkan SYN ke server

Server : SYN-ACK -> Client : Server merespon SYN Client dengan mengirimkan SYN-ACK ke **Client**

Client : ACK -> Server : Setelah menerima SYN-ACK dari server, client mengirim ACK ke Server.

Setelah melewati handshake tadi, baru kemudian koneksi terbentuk (established). Bisa dikatakan device yang menggunakan protokol TCP ini akan melakukan kesepakatan terlebih dahulu sebelum transmisi data terjadi. TCP menggunakan proses jabat tangan yang sama untuk mengakhiri koneksi yang dibuat. Hal ini menjamin dua host yang sedang terkoneksi

tersebut telah menyelesaikan proses transmisi data dan semua data yang ditransmisikan telah diterima dengan baik. Koneksi TCP ditutup dengan menggunakan proses terminasi koneksi FIN (*TCP connection termination*).

- *Reliable Transmission*

Data yang dikirimkan ke sebuah koneksi TCP akan diurutkan dengan sebuah nomor urut yang unik disetiap byte data dengan tujuan agar data dapat disusun kembali setelah diterima. Pada saat transmisi, bisa jadi data dipecah/difragmentasi, hilang, atau tiba di device tujuan tidak lagi urut. Pada saat data diterima, paket data yang duplikat akan diabaikan dan paket yang datang tidak sesuai dengan urutannya akan diurutkan agar dapat disusun kembali.

- *Error Detection*

Jika terjadi error, misalnya ada paket data yang hilang pada saat proses transmisi, bisa dilakukan pengiriman ulang data yang hilang. Untuk menjamin integritas setiap segmen TCP, TCP mengimplementasikan penghitungan TCP Checksum.

- *Flow Control*

Mendeteksi supaya satu host tidak mengirimkan data ke host lainnya terlalu cepat. Flow Control akan menjadi sangat penting ketika bekerja di lingkungan dimana device satu dengan device yang lain memiliki kecepatan komunikasi jaringan yang beragam. Sebagai contoh, ketika PC mengirimkan data ke smartphone. kemampuan PC dengan smartphone tentu berbeda. Smartphone lebih lambat dalam memproses data yang diterima daripada PC, maka TCP akan mengatur aliran data agar smartphone tidak kewalahan.

- *Segment Size Control*

Mendeteksi besaran MSS (maximum segment size) yang bisa dikirimkan supaya tidak terjadi *IP fragmentation.* MSS adalah infomasi ukuran data terbesar yang dapat ditransmisikan oleh TCP dalam bentuk segment tunggal. Informasi MMS ini dalam format Bytes. Untuk performa terbaik, MSS bisa ditetapkan dengan ukuran yang cukup kecil untuk menghindari

fragmentasi IP. Fragmentasi IP dapat menyebabkan hilangnya paket dan retransmisi yang berlebihan.

Congestion Control

Prisip kerja TCP terkhir yang cukup penting adalah Congestion Control. TCP menggunakan beberapa mekanisme untuk mencegah terjadinya congestion pada network. mekanisme yang dilakukan salah satunya adalah mengatur aliran data yang masuk ke dalam network.

ICMP

Salah satu jenis protokol yang biasa digunakan untuk pengecekan dan mengindikasi error pada saat transmisi dalam sebuah jaringan. ICMP disalurkan berbasis “best effort” sehingga bisa mengetahui jika terjadi error (datagram lost). Host (baik device yang mencoba transmisi ataupun device tujuan transmisi tujuan) akan mendeteksi apabila terjadi permasalahan tranmisi, dan membuat “ICMP message” yang akan dikirimkan ke host asal. Contoh penggunaan protokol ICMP yang sering kita lakukan misalnya pada saat kita menjalankan Ping atau Traceroute.

Type	Name
0	Echo Reply
1	Unassigned
2	Unassigned
3	Destination Unreachable
4	Source Quench
5	Redirect
6	Alternate Host Address
7	Unassigned
8	Echo
9	Router Advertisement
10	Router Solicitation
11	Time Exceeded

UDP

User Datagram Protocol (UDP) merupakan salah jatu jenis protokol yang biasa digunakan utnuk transmisi sederhana dengan mekanisme protokol yang minimal.

Prinsip Kerja UDP.

- Connectionless : Device yang satu bisa mengirimkan pesan/datagram ke device lainnya di jaringan, tanpa terlebih dahulu melakukan negosiasi (hand-shake).
- Unreliable : Datagram yang dikirimkan pun tidak dijamin sampai ke tujuan. Paket data UDP akan dikirimkan sebagai datagram tanpa adanya nomor urut atau pesan acknowledgment. Tidak ada flow control ataupun mekanisme lain untuk menjaga keutuhan datagram (unreliable). Akan tetapi UDP melakukan mekanisme checksums untuk data integrity.

UPD biasanya digunakan karena beberapa alasan berikut :

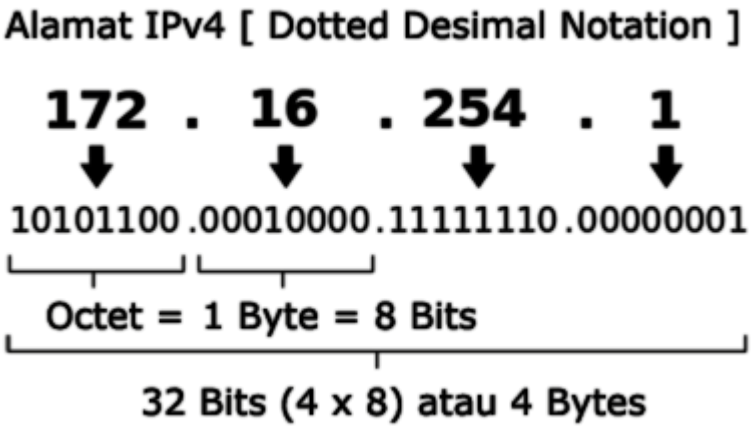
Protokol yang “ringan” (lightweight) : Lebih hemat sumber daya memori dan prosesor, beberapa protokol lapisan aplikasi membutuhkan penggunaan protokol yang ringan yang dapat melakukan fungsi-fungsi spesifik dengan saling bertukar pesan. Contoh dari protokol yang ringan adalah fungsi query nama dalam protokol lapisan aplikasi Domain Name System.

Transmisi broadcast : Untuk mengirimkan datagram, UDP tidak perlu membuat koneksi terlebih dahulu dengan sebuah host tertentu, dengan begitu UDP memungkinkan untuk membuat transmisi broadcast. Protokol TCP yang hanya dapat mengirimkan transmisi one-to-one, karena harus ada proses handshake terlebih dahulu antar device. Contoh transmisi broadcast salah satunya query nama dalam protokol NetBIOS Name Service.

Streaming dan Game Online : Streaming dan game online membutuhkan transmisi yang real time. Jika ada paket yang hilang pada saat trasmisi kemudian harus menunggu paket pengganti, maka beban network akan berlebih, dan jeda menunggu akan membuat data tidak lagi real time.

TCP/IP : IP Address

IP address adalah sebuah sistem pengalamatan unik setiap host yang terkoneksi ke jaringan berbasis TCP/IP. IP address bisa dianalogikan seperti sebuah alamat rumah. Ketika sebuah datagram dikirim, informasi alamat inilah yang menjadi acuan datagram agar bisa sampai ke device yang dituju. IP Address terbagi dalam 2 versi, IPv4 dan IPv6. Sebuah IP address versi 4 atau IPv4 terbentuk dari 32 binary bits. Dari 32 binary bits tersebut terbagi lagi menjadi 4 octet (1 octet = 8 bits). Nilai tiap oktet diatara 0 sampai 255 dalam format desimal, atau 00000000 – 11111111 dalam formal binary. Setiap octet dikonversi menjadi desimal dan dipisahkan oleh tanda titik (dot). Sehingga format akhir IP address biasanya berupa angka desimal yang dipisahkan dengan tanda titik, contohnya 172.16.254.1.



Jika pada sebuah octet semua angka biner bernilai satu, maka nilai desimal dalam octet tersebut adalah 255. Cara konversi dari biner ke desimal, adalah dengan memperhatikan nilai bits. Jika dilihat dari posisi bits, bits paling kanan memiliki nilai 2^0. Dan nilai pangkat ditambahkan untuk angka biner sebelah kirinya menjadi 2^1. Terus dilanjutkan sampai bits paling kiri.

Bits Ke -1	Bits Ke -2	Bits Ke -3	Bits Ke -4	Bits Ke -5	Bits Ke -6	Bits Ke -7	Bits Ke -8
1	1	1	1	1	1	1	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255							

Kita coba jabarkan IP address 172.16.254.1. Seperti yang telah kita pelajari sebelumnya bahwa satu IP address terbentuk dari 32 bits, maka detailnya akan menjadi seperti dibawah ini :

172	16	254	1
10101100	00010000	11111110	00000001
$2^8+0+2^6+0+2^4+2^3+0+0$	$0+0+0+2^5+0+0+0+0$	$2^8+2^7+2^6+2^5+2^4+2^3+2^2+0$	$0+0+0+0+0+0+0+2^1$
128+0+32+0+8+4+0	0+0+0+16+0+0+0+0	128+64+32+16+8+4+2+0	0+0+0+0+0+0+0+1

Jika Anda benar – benar ingin memahami konsep IP address, disarankan untuk memiliki pengetahuan dasar mengenai angka biner dan desimal, baik operasi perhitungan maupun konversi dari biner ke desimal atau sebaliknya.

Sistem komunikasi

Berdasarkan bagaimana perangkat saling berkomunikasi, terbagi menjadi beberapa jenis, yakni sebagai berikut:

- *Unicast*, merupakan komunikasi antar sebuah host atau point-to-point. Contoh : HTTP
- *Broadcast*, merupakan metode komunikasi dari sebuah host ke semua host yang masih dalam satu jaringan. Alamat broadcast digunakan dalam komunikasi one-to-everyone. Contoh : ARP Ethernet.
- *Multicast*, merupakan metode komunikasi dari sebuah host ke banyak host yang bergabung dalam group multicast yang sama. Alamat multicast digunakan dalam komunikasi one-to-many. Contoh : Video Streaming.
- *Anycast*, merupakan metode komunikasi dari sebuah host ke host atau kelompok host lain yang diset memiliki IP sama. Contoh : 6to4 relay.

Pada awal mula design network, diperkirakan konektivitas end-to-end terjadi pada seluruh host yang terkoneksi ke internet. Dan menjadi tugas IP address untuk menjadi sebuah alamat unik yang menjadi identitas sebuah host. Akan tetapi pada perkembangannya, tidak semua host butuh terkoneksi dengan dunia internet. Misalnya jaringan sebuah perusahaan yang hanya ingin masing – masing host cukup bisa berkomunikasi dengan host yang masih satu perusahaan, dan tidak perlu berkomunikasi dengan internet. Dengan adanya kasus seperti ini, maka IP address dibagi menjadi beberapa kelompok.

IP Public dan IP Private

IP Public

Public IP Address merupakan IP Address yang dapat diakses di jaringan internet.
IP Public juga dikenal sebagai globally routable unicast IP address. Ketika sebuah perangkat memiliki IP public dan terkoneksi ke jaringan internet, maka perangkat tadi bisa diakses darimanapun melalui jaringan internet juga. Akan tetapi kita tidak bisa memasang sembarang IP public di sebuah device. Ada aturan mengenai alokasi IP public. Kita bisa mendapatkan Public IP Address dari pinjaman ISP atau alokasi dari APNIC/IDNIC (www.idnic.net).

IP Private

Pada arsitektur IP address, Private IP Address adalah IP Address yang diperuntukkan untuk jaringan lokal. IP private tidak boleh ada di jaringan internet dan tidak dapat diakses di jaringan internet. Pada implementasi di jaringan real, biasanya jaringan lokal menggunakan IP Private, kemudian ditambahkan sebuah router yang menjembatani jaringan lokal yang menggunakan IP private dengan jaringan publik yang menggunakan IP Public. Untuk cakupan IP Private, Anda bisa lihat tabel IP Private di pembahasan mengenai CIDR.

IP Khusus

Selain IP Private dan IP Public, ada beberapa IP khusus lain. IP ini sudah memiliki tujuan penggunaan khusus yang sudah disepakati secara international, sehingga tidak dapat digunakan untuk pengalamatan sebuah host.

Penggunaan	IP / subnet
Self Identification	0.0.0.0/8
Localhost	127.0.0.1
Loopback	Other 127.0.0.0/8
Multicast	224.0.0.0/4
Local link/DHCP error	169.254.0.0/16
IETF Protocol Assignments	192.0.0.0/24
TEST-NET-1	192.0.2.0/24
TEST-NET-2	198.51.100.0/24
TEST-NET-3	203.0.113.0/24
6to4 Relay Anycast	192.88.99.0/24
Benchmark Test	198.18.0.0/15
Future Used	240.0.0.0/4
Limited Broadcast	255.255.255.255/32

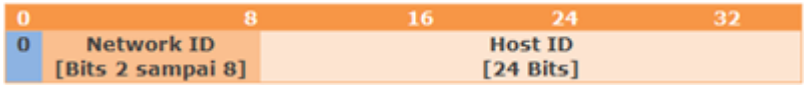
Kelas IP

Pada awal mula design IP address, IP address dibagi dalam beberapa kelas. Kelas IP dibedakan berdasarkan jumlah bits network ID. Masing masing kelas memiliki jumlah netowrk yang berbeda, dan jumlah host di tiap network yang berbeda pula. Pembagian ip address berdasarkan kelas ini sudah mulai ditinggalkan digantikan dengan sistem CIDR. Akan tetapi, ada baiknya kita coba lihat sejarah kelas IP address ini.

Kelas	Range IP Address	Jumlah Host	Jumlah Network
A	0.0.0.0 - 127.255.255.255	16,777,216	128
B	128.0.0.0 - 191.255.255.255	1,048,576	16.384
C	192.0.0.0 - 223.255.255.255	65,536	2.097.152
D	224.0.0.0 - 239.255.255.255	Tidak Didefinisikan	Tidak Didefinisikan
E	240.0.0.0 - 255.255.255.255	Tidak Didefinisikan	Tidak Didefinisikan

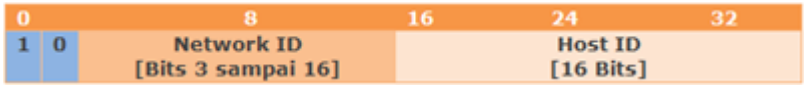
Kelas A

IP address kelas A biasa digunakan untuk jaringan dengan skala besar. Bits pertama di dalam IP address kelas A selalu diset dengan nilai 0 (nol). Bits kedua sampai bits ke delapan merupakan sebuah network identifier. 24 bit sisanya (atau tiga oktet terakhir) merepresentasikan host identifier. Dengan jumlah host identifier sampai 24 bits, artinya kelas A memiliki 16,777,214 host.



Kelas B

Kelas B biasa digunakan untuk jaringan skala menengah hingga skala besar. Dua bit pertama di dalam oktet pertama alamat IP kelas B biasanya berupa bilangan biner 10. 14 bit berikutnya merupakan network identifier. Sisa 16 bit merepresentasikan host identifier. Ip address kelas B memiliki 65,534 host.



Kelas C

Digunakan untuk jaringan berskala kecil. Tiga bit pertama bernilai biner 110. Kemudian 21 bit selanjutnya merupakan network identifier. Dan 8 bit sisanya merepresentasikan host identifier. Dengan begitu IP address kelas C memiliki 254 host untuk setiap network-nya.

Kelas D

Merupakan alokasi IP address yang disediakan hanya untuk alamat-alamat IP multicast, dan ***Kelas E*** merupakan IP alamat yang bersifat “eksperimental” atau percobaan dan dicadangkan untuk digunakan pada masa depan.

Kelas D

Kelas E

Akan tetapi pada perkembangannya, alokasi kelas IP address dengan metode ini dirasa sudah tidak cocok dan sekarang kita beralih menggunakan metode ***Classless Inter-Domain Routing (CIDR).***

Subnet Mask

Subnet Mask merupakan nilai yang dibentuk dari angka biner 32 bits. sama seperti IP address. Dari angka biner 32 bits ini, juga dipisahkan dengan tanda dot pada setiap octet. Fungsi dari subnet mask ini adalah membedakan network id dan host id. pada gambar kelas IP, kita bisa melihat alokasi nilai bits pada masing – masing identifier. Didalam subnet mask semua bit yang dialokasikan untuk network id diwakili oleh angka biner 1 sedangkan semua bit alokasi host id akan diwakili oleh angka biner 0. Selain membedakan identifier, subnet mask juga digunakan untuk menentukan letak suatu host, apakah di jaringan yang masih dalam satu segmen, atau sudah berbeda segmen.

Network Address dan Broadcast Address

Dalam sebuah alokasi IP address, ada 3 jenis IP.

- *Host address*, IP address yang dapat dipasang ke sebuah perangkat jaringan seperti komputer atau router agar dapat saling interkoneksi. Host IP ini sifatnya unik, dalam artian dalam sebuah network tidak boleh ada host IP yang sama.
- *Network address*, IP address yang mereprentasikan alamat sebuah network. Semua host dalam satu network memiliki network address yang sama. Network address merupakan IP pertama dalam sebuah subnet IP
- *Broadcast address*, jenis IP address yang digunakan untuk mengirim data ke semua host yang masih berada dalam satu network. Broadcast address adalah ip terakhir dalam sebuah subnet IP.

Network address dan broadcast address tidak dapat dipasang dalam sebuah perangkat. Contoh, kita memiliki IP address 192.168.0.1 dengan subnet mask 255.255.255.0 maka untuk

mendapatkan nilai network address dan boradcast address, kita bisa membuat perhitungan seperti berikut :

IP address 192.168.0.1 11000000.10101000.00000000 .00000001
Untuk mendapatkan nilai network address, ubah semua bit dalam alokasi host-id menjadi bernilai 0.

Susunan bit awal 11000000.10101000.00000000 .00000001
Susunan bit network address 11000000.10101000.00000000 .00000000
Dotted-decimal network address 192 168 0 0

Untuk mendapatkan nilai ubah semua bit dalam alokasi host-id menjadi bernilai 1.
Susunan bit awal 11000000.10101000.00000000.00000001
Susunan bit broadcast address 11000000.10101000.00000000.11111111
Dotted-decimal broadcast address 192 168 0 255
Jadi untuk ip address 192.168.0.1 dengan subnet mask 255.255.255.0, memiliki network address 192.168.0.0 dan broadcast address 192.168.0.255.

Subnetting (VLSM)

Subnetting adalah sebuah mekanisme perhitungan pembagian network menjadi network dengan skala yang lebih kecil, biasa disebut subnet. Subbnetting dilakukan dengan meminjam nilai bits yang dialokasikan pada host id, sehingga memungkinkan penggunaan IP address yang lebih efisien. Subnetting biasa disebut juga Variable Length Subnet Mask (VLSM). Subnetting biasa diterapkan dengan mengubah nilai subnet mask. Contoh kasus misalnya sebuah perusahaan hanya memiliki 60 komputer yang akan terhubung dalam satu jaringan menggunakan IP kelas C dengan subnet mask default 255.255.255.0. Untuk alasan keamanan dan efisisnsi jaringan, maka hanya perlu alokasi IP kurang lebih sejumlah 60 ip address. Disinilah fungsi subnetting dibutuhkan. Berikut cara sederhana untuk melakukan subnetting dengan mengubah nilai subnet mask.

Desimal 255.255.255.0

Biner 1111111.11111111.11111111.00000000

Dari nilai biner diatas, berarti alokasi porsi bits untuk network-id sebanyak 24 bits, dan porsi untuk host-id ada 8 bits. Dengan porsi sebanyak 8 bits, maka maksimal IP address adalah 254. Karena kebutuhan perusahaan tersebut hanya 60 ip address, maka porsi host id akan dikurangi dengan metode subnetting. Pertama kita ubah jumlah IP yang kita butuhkan menjadi angka biner, **60 = 111100**.

Kalau kita perhatikan, dengan jumlah kurang lebih 60 ip address, membutuhkan 6 bits nilai biner, maka kita kurangi alokasi bits pada host-id yang sebelumnya 8 bits, menjadi 6 bits. Ingat bahwa di dalam subnet mask, host-id di representasikan dengan angka biner 0.

Subnet awal 1111111.11111111.11111111.00000000 (8 bits host-id)
Subnet baru 1111111.11111111.11111111.11**000000** (6 bits host-id)
Decimal 255 255 255 192

Dengan alokasi bits host-id 6 digit, maka kita memiliki alokasi IP address dalam subnet baru tersebut adalah 111111 dalam bilangan biner atau 63 ip address dalam desimal. Dengan adanya network addres dan boardcast address , maka IP yang bisa kita pasang pada device jaringan maksimal adalah 62 ip address, contoh:

Range IP Address : 192.168.0.1 – 192.168.0.62
Netmask : 255.255.255.192
Network : 192.168.0.0
Broadcast : 192.168.0.63

Classless Inter-Domain Routing (CIDR)

Seiring dengan perkembangan dunia jaringan komputer yang cukup pesat, pembagian IP dengan menggunakan kelas A, B, dan C mulai ditinggalkan karena masih menyisakan banyak IP yang tidak digunakan. Selain mengurangi alokasi IP address, dengan cara yang sama dapat

digunakan untuk keperluan sebaliknya, yakni menambah alokasi IP address. Contohnya kelas C yang secara teoritis hanya mendukung 254 alamat tiap jaringan, akan tetapi dengan CIDR, dapat menggunakan hingga 32766 alamat IP, yang seharusnya hanya tersedia untuk alamat IP kelas B. CIDR merupakan cara alternatif baru untuk merepresentasikan alamat IP dan subnet IP. CIDR disebut juga Supernetting atau Prefix. Jika kita sebelumnya sudah membahas mengenai IP Private, berikut tabel range IP address yang dilalokasikan sebagai IP Private dengan system CIDR.

Range IP Private	Jumlah Host	CIDR Block (Subnet Mask)
10.0.0.0 - 10.255.255.255	16,777,216	10./8 (255.0.0.0)
172.16.0.0 - 172.31.255.255	1,048,576	172.16./12 (255.240.0.0)
192.168.0.0 - 192.168.255.255	65,536	192.168./16 (255.255.0.0)

Alokasi IP Private dengan system CIDR

CIDR biasanya ditulis dengan tanda "/" setelah IP address, kemudian diikuti dengan informasi jumlah bits yang dialokasikan sebagai network-id, contoh 192.168.0.0/27. Jika Anda pernah melakukan konfigurasi router Mikrotik, tentu Anda sudah familiar dengan format IP seperti ini. Dari contoh subnet 192.168.0.0/27, maka dari 32 bits IP address, 27 bits dialokasikan untuk network-id, tersisa 5 bits untuk host-id. Jumlah IP address yang ada dalam subnet tersebut bisa dihitung dengan rumus :

$$2^{(32-x)}$$

Dimana "x" adalah nilai CIDR.

Contoh, untuk subnet 192.168.0.0/27 bisa dihitung sebagai berikut :

$2^{(32-27)} = 2^{(5)} = 32$

Nilai 32 adalah total IP address yang ada dalam subnet tersebut. Dikurangi dengan network address dan broadcast address, maka IP yang bisa dipasang pada perangkat jaringan ada 30 ip address.

Range IP Address : 192.168.0.1 – 192.168.0.30

Netmask : 255.255.255.224

Network : 192.168.0.0

Broadcast : 192.168.0.31

Perhitungan IP address sebenarnya tidak harus dilakukan secara manual. Ada banyak alat bantu untuk melakukan perhitungan IP address dan subnetting, misalnya IP Subnet Calculator. Akan tetapi, ada baiknya kita tahu bagaimana konsep IP address, sehingga dalam penerapan di jaringan, kita bisa membuat sebuah jaringan yang benar – benar sehat dan ideal.

IPv6 Overview

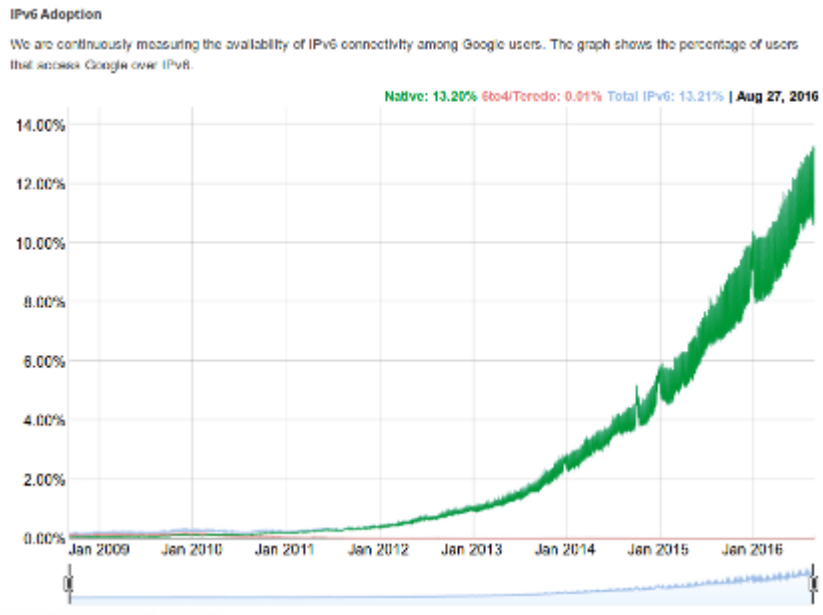
OVERVIEW

Sebuah fitur dari MikroTik yang mungkin sedikit terlupakan namun sebenarnya cukup penting untuk kebutuhan jaringan saat ini. Fitur ini bukanlah fitur yang baru namun sudah ditambahkan pada packet system di versi RouterOS yang lama sampai terbaru saat ini. Fitur tersebut adalah IPv6.

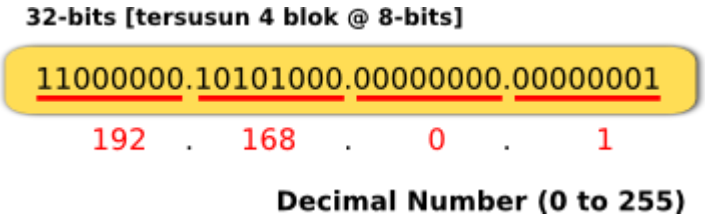
Ya, fitur ini sudah include dalam paket system dari RouterOS namun secara default fitur ini tidak aktif (disable). Dilihat dari namanya maka fungsinya tidak jauh dari pengalamatan IP sebuah perangkat di jaringan.

IPv6 (*Internet Protocol versi 6*) adalah sebuah protokol internet yang digunakan untuk melakukan pengalamatan dan routing paket data antar perangkat-perangkat di dalam jaringan berbasis TCP/IP. IPv6 merupakan generasi terbaru yang sebelumnya adalah IPv4.

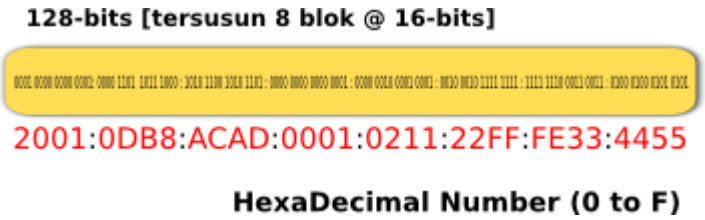
Protokol internet ini dikembangkan oleh **IETF** (Internet Engineering Task force). Mungkin belum terlalu banyak untuk penggunaan IPv6 namun seiring perembangan teknologi dan keterbatasan ruang pengalamatan dari IPv4, secara data penggunaan IPv6 semakin meningkat dari setiap tahunnya.



Secara struktur IPv6 ini berbeda dengan IPv4. Seperti yang telah kita ketahui IPv4 memiliki struktur pengalamatan sebanyak 32-bits yang tersusun dengan 4 blok yang masing-masing blok sebanyak 8-bits.



Sedangkan untuk IPv6 memiliki struktur pengalamatan sebanyak 128-bits dengan tersusun dari 8 blok yang masing-masing blok sebanyak 16-bits.

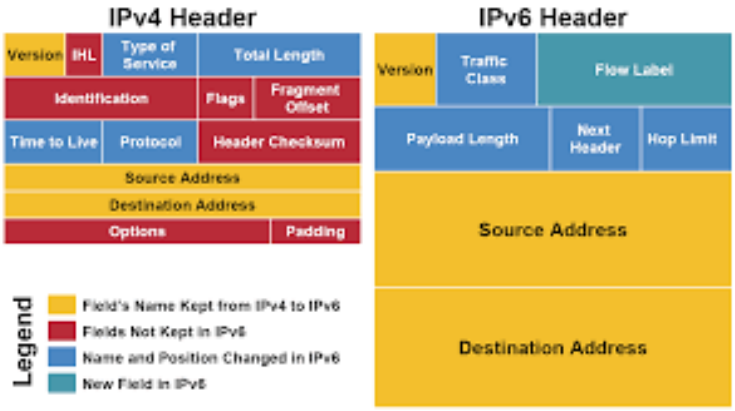


Selain struktur yang berbeda antara IPv4 dan IPv6, mekanisme pengalamatannya juga berbeda. Untuk IPv6 dikenal dengan istilah IPv6 Autoconfiguration. Dan dari sini juga dibagi menjadi 2 jenis metode, yaitu Stateless Mechanism & Stateful Mechanism.

Secara sederhananya perbedaan dengan IPv4 diantaranya adalah:

- Tidak ada subnet masks
- Tidak ada alamat Broadcast
- Tidak memerlukan DHCP Server (Stateless Mechanism - Host/Client dapat melakukan konfigurasi otomatis IPv6 Address dan gateway dengan melakukan soliciting/obtain dari router melaui RS (Router Solicitation) dan RA (Router Advertisement)
- Dapat menggunakan MAC Address dari perangkat host untuk mendefinisikan Host/Interface ID (EUI-64)
- Tidak memerlukan NAT untuk End to End Communication

Selain mekanisme pengalamatan yang berbeda, antara IPv4 dan IPv6 juga memiliki perbedaan pada 'packet header'. Perbedaannya adalah jumlah dari Basic Header pada paket data. Untuk IPv4 terdapat 10 basic header field sedangkan pada IPv6 terdapat 6 basic header field.



IPv6 Alocation

Nah, karena pada saat ini kita sudah terbiasa menggunakan IPv4 lalu bagaimana caranya kita mendapatkan alokasi IPv6 tersebut dan menggunakannya untuk komunikasi perangkat di jaringan baik secara lokal maupun public?

Secara umum untuk hal tersebut ada dua mekanisme:

- **Via native connectivity.** Misal, kita berlangganan koneksi internet dengan alokasi IPv6 secara langsung ke Internet Provider
- **Via IPv6-in-IPv4 tunnelling**. Dengan cara ini kita bisa mendapatkan alokasi IPv6 dengan menggunakan metode tunnel melalui koneksi IPv4. Dengan cara ini bisanya akan melakukan tunnel ke 6to4 relay router yang ada di Internet Provider atau juga melalui perantara tunnel broker.

Pada dasarnya distribusi dan alokasi dari IP Address diatur oleh sebuah badan organisasi dunia yang disebut IANA (Internet Assaigned Numbers Authority). Dan IANA sendiri memberikan tanggungjawab untuk pengaturan alokasi alamat IP dan juga DNS kepada lembaga lainnya yang bersifat regional (RIR) yaitu ARIN, RIPE, APNIC, LACNIC, AfriNIC. Hal ini juga tidak jauh beda untuk alokasi IPv4 yang sudah ada.

Dari semua lembaga diatas alokasi IPv6 akan dibagi menjadi berberapa network prefix seperti berikut

- **IPv6 Global Unicast Address**

Global Unicast Range dengan network prefix **2000::/3**

Dari kelima RIR (Regional Internet Registry) akan diberikan alokasi IPv6 dengan prefix /12 dari /3 yang mana masing-masing regional akan mendapatkan network prefix:

1. APNIC (2400:0000::/12)
2. ARIN (2600:0000::/12)
3. AfriNIC (2C00:0000::/12)
4. LACNIC (2800:0000::/12)
5. RipeNIC (2A00:0000::/12)

- **6to4 Addresses**

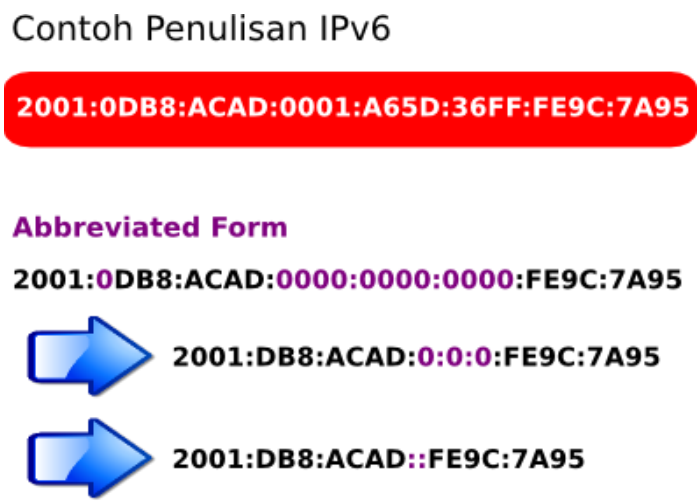
Menggunakan network prefix 2002::/16 yang mana ditujukan untuk kebutuhan khusus sebagai mekanisme tunelling [RFC 3056] koneksi IPv6 melalui IPv4.

- **Example & Documentation Prefix**

Untuk tujuan pembelajaran dan juga dokumentasi, IETF telah memberikan pengaturan prefix yang bisa digunakan [RFC 3849] yaitu **2001:0db8::/32 & 3fff:ffff::/32**

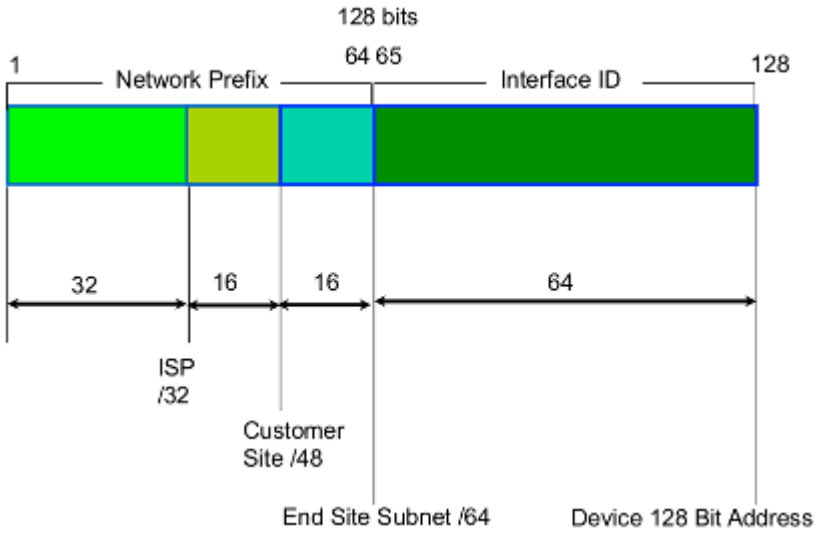
IPv6 ADDRESSING & SUBNETTING

Diatas telah kita singgung sedikit bagaimana model pengalamatan dari IPv6. Memang dari segi pengalamatan berbeda seperti kita melakukannya pada IPv4. Pada IPv6 memiliki panjang alamat sebanyak 128 bits. Dari 128-bits ini IPv6 ditulis dalam format Hexadecimal dimana memiliki **'8 fields'** yang dipisahkan dengan tanda 'Colon (:)'. Dan setiap 'field' memiliki panjang 16 bit yang di-convert menjadi 4 digit hexadecimal. Misal, dengan format X:X:X:X:X:X:X:X (dimana X=16 bit, ex:ACAD).

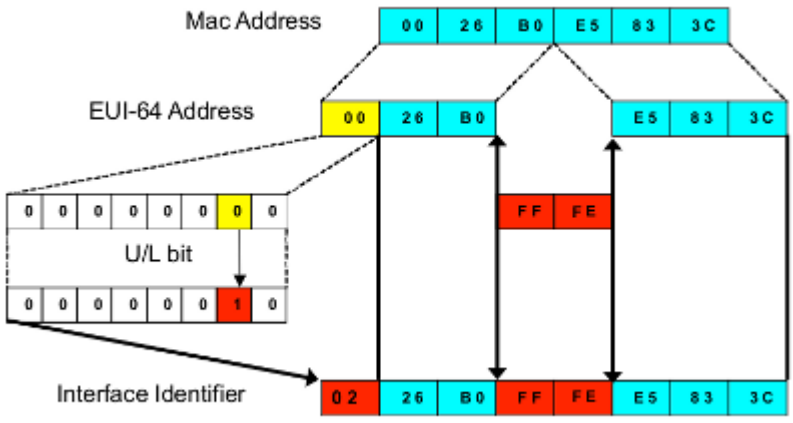


Dalam penulisan IPv6 kita bisa meringkas jika terdapat angka nol didepan atau biasa disebut sebagai **'Leading Zeroes'**. Dan jika terdapat group angka nol kita bisa meringkas penulisan dengan menggunakan **'Double Colons'.**

Kemudian secara struktur penulisan alamat IPv6 dibagi menjadi 2 **yaitu Network Prefix** dan Interface ID. Untuk **Network Prefix** adalah alokasi alamat yang diberikan dari RIR (Regional Internet Registry) dan juga alokasi dari ISP untuk customer. Untuk Interface ID merupakan pengalamatan pada sisi host/perangkat di jaringan.



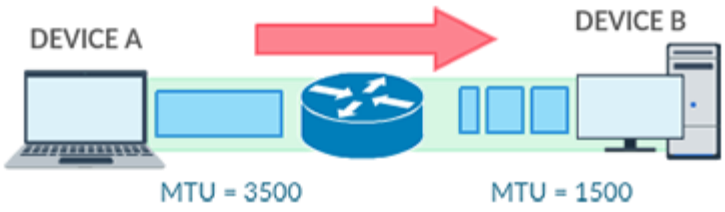
Khusus pengalamatan pada **Interface ID** selain kita bisa menuliskan dengan hexadecimal secara manual menggunakan subnetting, secara otomatis bisa dapat didefiniskan secara otomatis berdasarkan MAC Address dari perangkat yang ada. Metode ini disebut sebagai **EUI-64** yang mana bisa digunakan untuk menjaga keunikan di setiap alamat IPv6.



Perhitungan MTU pada MikroTik

Maximum Transmission Unit adalah istilah dalam teknologi informasi yang merujuk kepada ukuran paket data terbesar yang dapat ditransmisikan melalui sebuah media jaringan. Ukuran MTU adalah bervariasi, tergantung teknologi jaringan yang digunakan. Contohnya adalah dalam jaringan berbasis teknologi Ethernet, ukuran MTU maksimum adalah 1500 bytes. Adalah tugas lapisan data-link yang harus menentukan ukuran MTU.

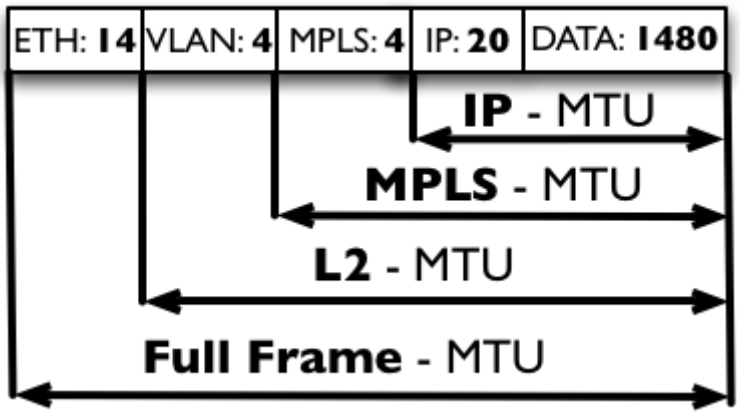
Setting MTU biasanya dilakukan pada perangkat networking semacam switch, router dan sebagainya. Sangat jarang melakukan setting MTU secara manual pada workstation atau host. Jika ip layer menerima paket yang akan diteruskan ke dalam jaringan, maka perangkat akan mengkalkulasi ukuran paket jika ditambahkan dengan 20 bytes ip header. Jika ternyata paket yang akan dikirimkan memiliki ukran MTU yang lebih besar dari MTU perangkat yang menerima paket tersebut, maka paket akan difragmentasi, atau dipotong menjadi ukuran yang lebih kecil.



Nilai MTU yang besar memungkinkan untuk mengirimkan data lebih cepat, bayangkan jika Anda punya banyak data kemudian dikumpulkan jadi satu box besar. Maka kita cukup mengirimkan semua data satu kali menggunakan satu box besar. Namun jika untukran box kecil, maka kita perlu mengirim beberapa kali. Nilai MTU besar tidak kemudian selalu berefek baik. Semakin panjang MTU, semakin tidak reliable proses pengiriman data. Jika ada kerusakan paket dalam pengiriman maka seluruh paket yang rusak akan dikirim ulang oleh protokol TCP (Transmission Control Protocol).

Begitu juga pada sistem di MikroTik yaitu RouterOS yang mana memiliki ukuran standart dari besar MTU masing-masing interface. Pada RouterOS untuk MTU ini dibagi ke beberapa tipe yaitu **L3 MTU** (*IP/Layer-3*), **L2.5 MTU** (*MPLS/Layer2.5*), **L2 MTU** (*MAC/Layer-2*), **Full Frame MTU**. Dari tipe-tipe MTU tersebut memiliki nilai standart yang berbeda-beda.

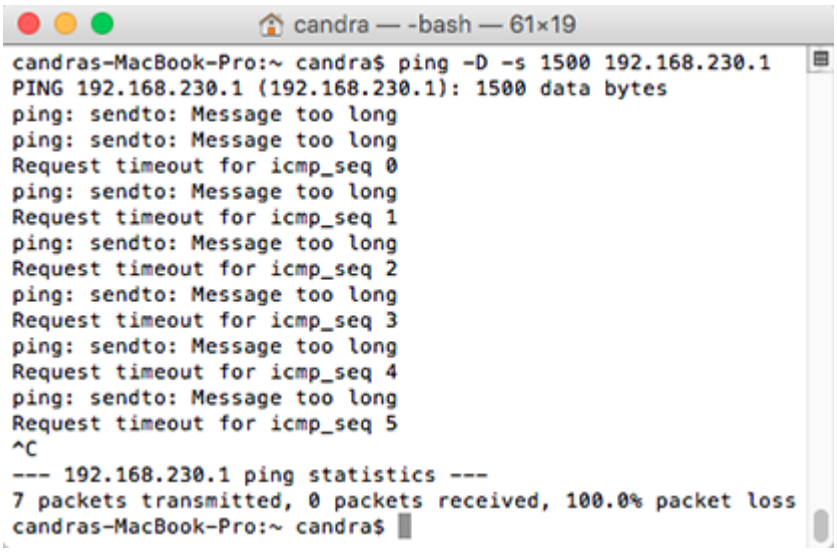
- L3 MTU = 1500 (Data: 1480 + IP:20),
- L2.5 MTU = 1504 (Data: 1480 + IP: 20 + MPLS: 4)
- L2 MTU = 1508 (Data: 1480 + IP: 20 + MPLS: 4 + VLAN:4)
- FULL Frame MTU = 1522 (Data: 1480 + IP: 20 + MPLS: 4 + VLAN: 4 + ETH:14).



Perbedaan besar nilai setiap tipe MTU tergantung pada jenis trafik yang akan di handle. Jika ukuran MTU hanya dipatok di nilai 1500 (L3 MTU) tanpa menambahkan tipe MTU Yang lain maka untuk trafik dengan service VLAN, MPLS, tidak akan bisa lewat. Pada kondisi normal paket data yang memiliki ukuran terlalu besar akan di fragment oleh perangkat secara otomatis. Terlalu banyak paket yang difragment akan mengakibatkan antrian paket yang juga panjang, kemudian perangkat yang menerima paket juga harus menyusun kembali paket yang diterima. Ukuran MTU yang disupport produk Mikrotik bisa dilihat **disini**.

Terlebih jika ada aplikasi yang membutuhkan nilai paket data yang statis, maka admin jaringan harus mampu menentukan ukuran paket data yang akan dilewatkan agar paket dapat diterima dengan baik. Beberapa service yang mengirimkan data lewat jaringan biasanya akan menambahkan header pada paket data, misalnya ping.

Pada saat data keluar dari perangkat, paket data akan ditambah dengan beberapa header, antara lain IP Header 20bytes, dan ICMP header 8bytes. Untuk melakukan test, Anda bisa gunakan perintah *ping -f -s* pada OS windows, *ping -M -s* pada Linux, atau *ping -D -s* pada Mac OSX. Misal kita coba ping dengan ukuran paket 1500, tanpa melakukan fragmentasi.



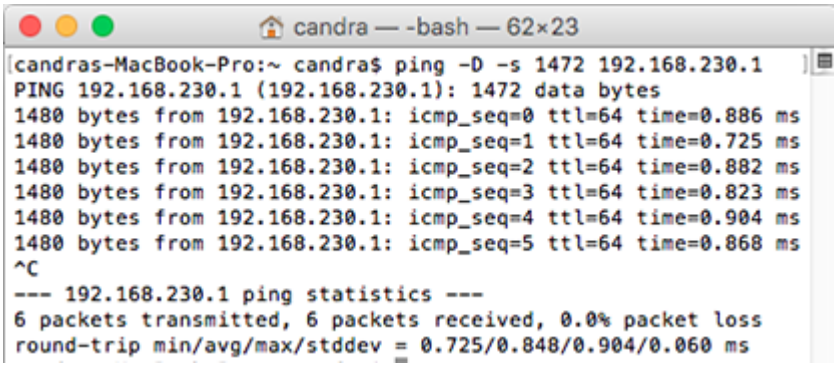
Yang terjadi perangkat yang dituju tidak dapat menerima karena ukuran paket terlalu besar. Kenapa bisa demikian, padahal perangkat lawan memiliki setting MTU 1500 ?. Ukuran 1500 adalah ukuran paket data sebelum ditambahkan header. Maka kita bisa hitung berapa ukuran data tepat agar paket ping bisa diterima.

1500 = 20 (IP header) + 8 (ICMP header) + Data

Data = 1500 - 20 (IP header) - 8 (ICMP header)

Data = 1472

Jika kita coba ping dengan size 1472, maka paket bisa diterima dengan baik



Service lain biasanya juga menambahkan header dengan nilai tertentu, misalnya VPN PPTP dan PPPOE. Service ini akan menambahkan pptp header dan checksum, sedangkan PPPoE menambahkan PPPoE header, PPP ID, DST & SRC Address.

PPTP :

Data = 1500 – 20 (IP Header) – 28 (PPTP Header) – 2 (Checksum) = 1450

PPPOE

1500 – 6 (PPPoE Header) – 2 (PPP ID) – 12 (DST & SRC Adress) = 1480

Perhitungan seperti diatas juga berlaku ketika menggunakan service lainBisa disimpulkan bahwa dengan bertambahnya ukuran ip header, maka ukuran data pada yang ditrasmisikan juga semakin kecil. Ukuran miminum MTU adalah 576 bytes.

MTU Path Discovery

Untuk mengetahui nilai MTU perangkat lawan, perangkat yang terkoneksi ke jaringan memiliki mekanisme yang disebut dengan MTU path discovery. Mekanisme ini sama sekali tidak membuthkan fitur atau service khusus, namun menggunakan cara yang cukup sederhana yakni dengan memanfaatkan mekanisme error reporting pada ICMP.

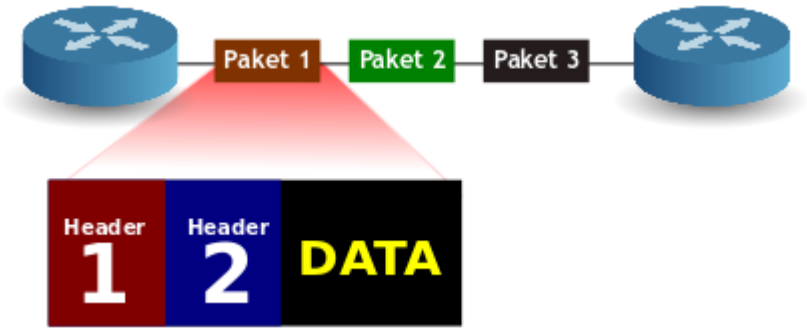
Fitur IP Packing di Mikrotik

Ada sebuah fitur yang terdapat di RouterOS Mikrotik yang disebut dengan “Packing”. Apabila kita pernah melihat fitur ini pada list menu RouterOS, mungkin diantara kita ada yang bertanya-tanya untuk apakah fungsi dari fitur ini? Secara singkat fungsi dari fitur ini adalah untuk melakukan ‘***re-packs***‘ (mengemas ulang) dari paket data yang dikirimkan.

Fitur ini tidak dapat digunakan pada setiap topologi jaringan, jadi kita perlu cermat untuk menerapkannya. Ini berguna apabila dalam kondisi jaringan yang sangat sibuk di mana terdapat **pps** (*packet per second*) yang memerlukan banyak proses dari kinerja di sisi *hardware*/*software*. Hal tersebut banyak ditemukan pada koneksi wireless dengan terlalu banyak paket-paket kecil yang meningkatkan pps. Jadi, kita mungkin bertanya-tanya mengapa kinerja jaringan menurun sementara tidak ada banyak trafik.

Berikut adalah gambar sebuah trafik dari “**paket normal**” di jaringan:

Setiap paket yang dikirimkan akan ditambahkan "**Header**". Header ini memberikan berbagai informasi dari paket tersebut.



Nah, dengan fitur **/ip packing** kita bisa "*mengemas*" paket-paket kecil tersebut menjadi satu paket besar, sehingga penggunaan bandwith menjadi lebih efektif.

Untuk membuat sebuah paket yang besar, Router harus menunggu paket-paket kecil datang dan selanjutnya dikemas. Dengan proses tersebut, maka akan ditemukan beberapa "**Timeout**" untuk paket yang datang. Hal ini berarti latensi akan meningkat apabila pada kondisi "**Low Traffic**" dan latensi akan turun pada saat kondisi "**High Traffic**". Ini kebalikan dari trafik normal (***unpacked***), apabila pada kondisi trafik yang tinggi (*High traffic*) latensi akan meningkat.

Semua paket-paket kecil tersebut akan dikemas (**Packing**) di sumber/asal (***Source***) dan akan dibongkar (*unpacked*) setelah sampai ditujuan (**Destination**). '*Source*' dan '*Destination*' harus mengetahui akan "***Packing Capability***" satu sama lain. Kenapa? Karena apabila tidak demikian router akan mengirim paket-paket yang sudah dikemas (*Packing*) dan juga paket-paket yang '*Unpacked*' ke network yang lain, misal jika kita memiliki router yang lain di dalam jaringan namun tidak

menggunakan fitur '**Packing**', maka router tersebut tidak tahu bagaimana cara untuk membongkar (*unpacked*) paket tersebut dan akan menganggap sebagai *invalid packet*, kemudian di '*drop*'.

Mikrotik menggunakan '***Network Neighborhood***' untuk mengetahui router mana yang menggunakan fitur '**Packing**' dan mana yang tidak. Dan berikut adalah bagaimana langkah-langkah untuk melakukan konfigurasi '**/ip packing**'. Pada contoh kali ini kita akan menghubungkan dua router via wlan dan mengirimkan paket dari **router A** ke**router B**.

Pertama, kita aktifkan 'Neighbour' pada interface **router A** dan **router B**. Untuk format scriptnya adalah sebagai berikut:

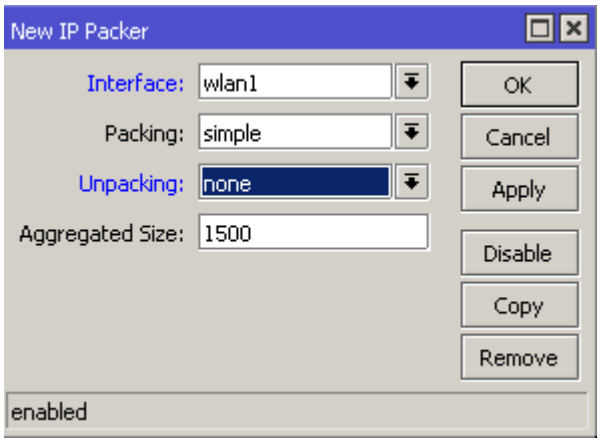
/ip neighbor discovery set wlan1 discover=yes

Selanjutnya, kita akan melakukan konfigurasi untuk **/ip packing** di masing-masing router. Seperti topologi diatas kita akan menghubungkan antra Router A dan router B, dimana pada router A kita set IP Address di interface wlan yaitu 172.16.2.1/24 (**AP Bridge**) dan pada router B yaitu 172.16.2.5/24 (**Station**).

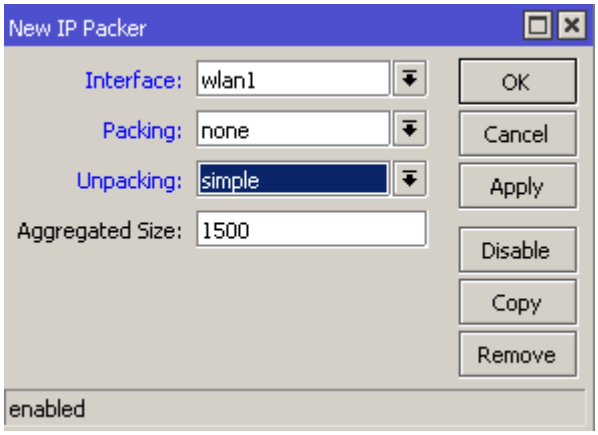
Untuk mengaktifkannya kita pilih pada menu **IP -> Packing**, dan klik **Add (+)**. Apabila memakai script kita bisa menuliskan pada terminal seperti berikut:

– Pada **Router A**

/ip packing add interface=wlan1 aggregated-size=1500 packing=simple unpacking=none



– Pada **Router B**



/ip packing add interface=wlan1 aggregated-size=1500 packing=none unpacking=simple

3

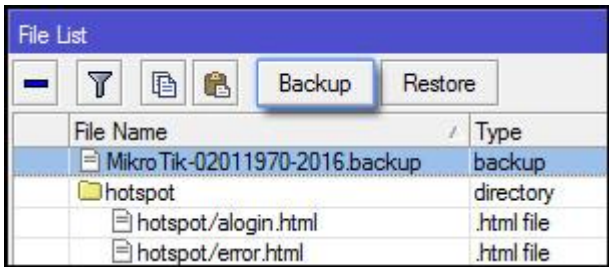
Cara Backup Mikrotik RouterOS

Backup Konfigurasi Mikrotik

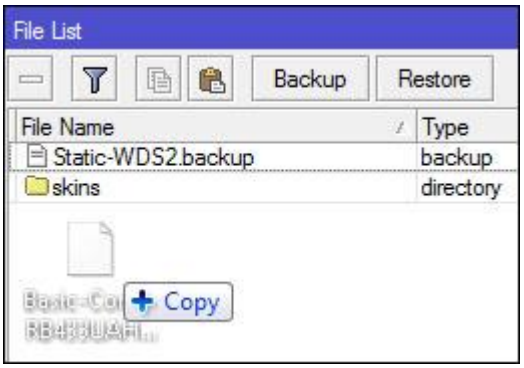
Backup/Restore

Untuk mencegah hal – hal yang tidak diinginkan, disarankan untuk selalu melakukan backup konfigurasi router secara berkala. Cara paling mudah untuk melakukan backup adalah dengan masuk ke Menu Files pada winbox, kemudian tekan tombol "**Backup**". Nama file

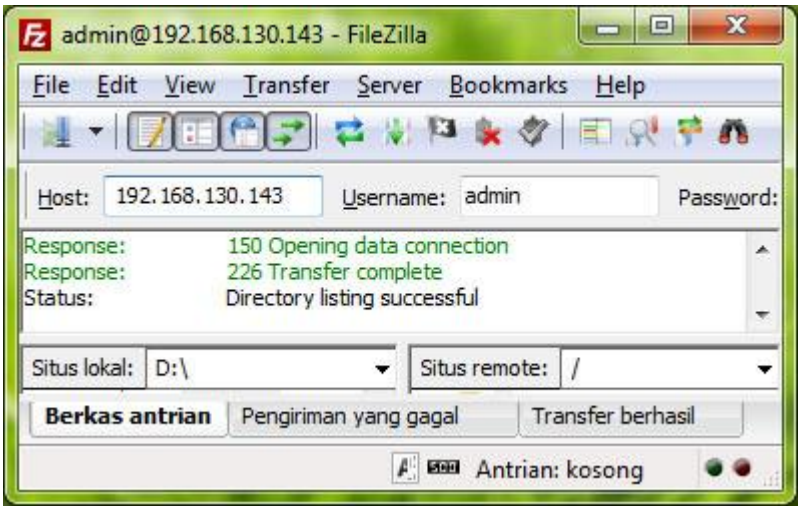
backup akan digenerate secara otomatis oleh router berdasarkan tanggal dan jam backup dilakukan. Jika ingin memberikan nama yang spesifik, diperlukan perintah backup melalui comand console : / system backup save name=”Basic-Config”



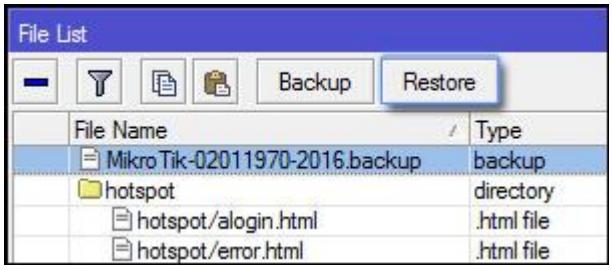
Akan tetapi Backup konfigurasi tidak cukup hanya dengan itu saja. Dengan hanya menekan Tombol backup atau perintah console, konfigurasi memang sudah terbackup, namun file backup masih tersimpan di storage router. Jika router diinstall ulang dengan netinstall file backup akan hilang karena proses netinstall melakukan format storage router. Agar file backup aman, jangan lupa untuk download file tersebut dari router. Jika menggunakan windows, caranya bisa dengan drag & drop file backup dari menu “Files” ke Local komputer.



Alternatif lain, atau ketika OS yang kita gunakan bukan Windows, kita bisa download via FTP. Ada banyak program FTP Client gratis yang beredar di internet, contohnya FileZilla. Login terlebih dahulu ke router, Kemudian Download file backup dari router.



Setelah berhasil login via FTP, tinggal download file backup router ke dalam lokal komputer. Nah, jika suatu saat router ada masalah, atau kita ingin kembali ke konfig sebelumnya, tinggal upload file backup ke router, kemudian klik **Restore**.



Export/Import

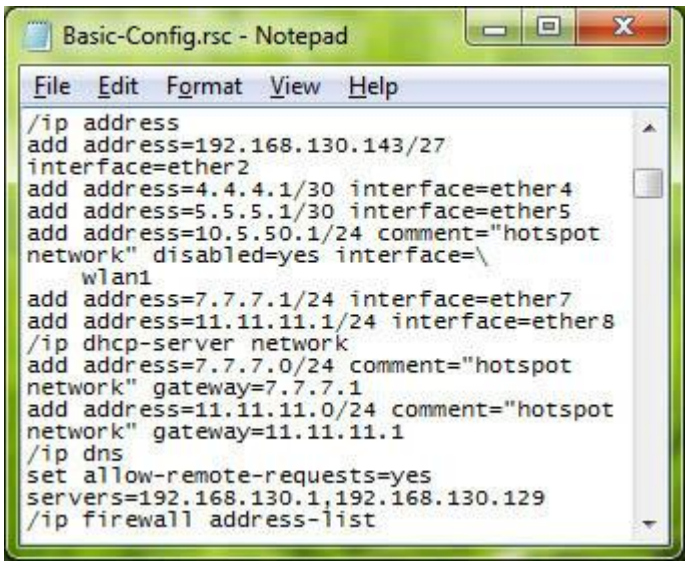
Ada kalanya kita menambah router, namun kira tidak ingin melakukan konfigurasi ulang. Kemudian terpikir untuk mengambil konfigurasi router yang sudah ada dengan fitur *backup*, kemudian di *restore* di router baru. Tapi tunggu dulu, penggunakan fitur backup dan restore hanya disarankan untuk router yang sama atau router dengan seri dan tipe yang identik. Maksud dari router indentik, adalah antara router lama dan router baru masih dengan seri yang sama dan spesifikasi hardware yang juga sama. Misal sama – sama RB1100AHX2. Jika sudah berbeda router, kami sarankan jangan menggunakan backup-restore, karena ada kemungkinan malah akan terjadi error. Solusinya adalah dengan menggunakan fitur Export dan Import.

By default perintah Export hanya akan menampilkan kumpulan perintah konfigurasi pada terminal. Akan tetapi, kumpulan perintah yang ditampilkan oleh fitur export bisa juga

disimpan dalam bentuk file dengan menambah parameter “file”. Pada versi routerOS 5.12 keatas, ada tambahan fungsi menarik di fitur Export/Import ini. yakni fungsi “compact”. Dengan fungsi “compact”, maka hanya konfigurasi yang ditambahkan secara manual yang akan ditampilkan atau disimpan. Maka perintah Export dan Import bisa kita tulis seperti gambar berikut :

```
[admin@MikroTik] > export compact file="Basic-Config"
[admin@MikroTik] > import file-name="Basic-Config"
```

Hasil perintah Export berupa file dengan extensi *.RSC. Kita bisa download, kemudian membuka dan mengedit file tersebut dengan text editor. Berbeda dengan file backup. File backup merupakan file yang berbentuk binary sehingga jika dibuka dengan text editor, konfigurasi tidak dapat dibaca. Jika kita buka file hasil export dengan notepad misalnya hasilnya akan seperti ini :



Jika router baru memiliki spesifikasi dan tipe yang berbeda, kita bisa edit dulu hasil export router lama, disesuaikan dengan spesifikasi hardware router baru, baru kemudian kita import ke router baru. Salah satu nilai lebih, export bisa digunakan untuk menampilkan konfigurasi salah satu fitur tertentu, tanpa harus menampilkan semua konfigurasi router. Misalnya kita hanya perlu export konfig ip address, maka tinggal jalankan perintah : */ip address export compact*

```
[admin@MikroTik] > ip address export compact
# jan/01/2002 01:13:27 by RouterOS 5.24
# software id = [redacted]
#
/ip address
add address=192.168.130.143/27 interface=ether2
add address=4.4.4.1/30 interface=ether4
add address=5.5.5.1/30 interface=ether5
```

Perlu diketahui, perintah export tidak akan menyimpan/menampilkan konfigurasi account dan password internal user MikrotikOS. Jadi, mulai saat ini Anda harus bisa mempertimbangkan kapan menggunakan backup/restore dan kapan menggunakan export/import.

Backup System dengan Partition

Partition merupakan sebuah fitur baru yang ditawarkan oleh mikrotik untuk menunjang kebutuhan networking. Fitur ini hadir pada RouterOS mulai versi **6rc5** dan hanya di support untuk routerboard dengan paltform Mipsbe, Mipsle, PowerPC/PPC, CCR (*kecuali x86 dan juga platform baru Smips*). Jika kita menggunakan RouterOS versi 5 atau dengan platform x86/Smips, maka kita tidak mendapatkan fitur ini pada menu di RouterOS.

Lalu, apakah fungsi dari fitur partition ini? Contoh kasus apabila kita melakukan penambahan konfigurasi dan mengalami masalah dengan konfigurasi yang baru, bisa juga karena gagal *upgrade* maka partisi yang lain akan mengambil alih system dari routerboard. Dengan kata lain fitur ini bisa digunakan sebagai Backup OS, jika pada OS utama mengalami 'error'. Fitur ini juga cocok bagi kita yang akan melakukan uji coba untuk sebuah konfigurasi baru pada router tanpa mengganggu konfigurasi utama.

Nah, untuk kebutuhan tersebut kita diharuskan untuk membagi (partisi) dari *storage* router. Namun sebelumnya ada ketentuan yang harus diperhatikan yaitu ukuran minimal partisi :

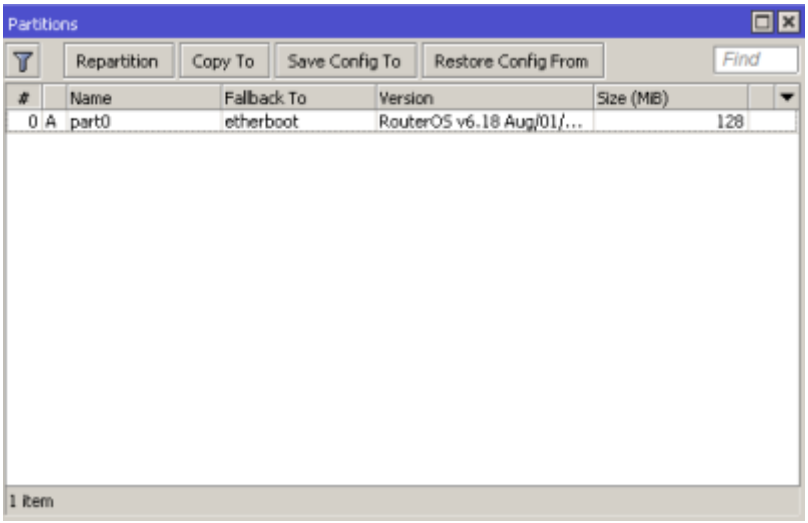
- 32 MB untuk MIPS series
- 40MB untuk PowerPC

- 48MB untuk CCR

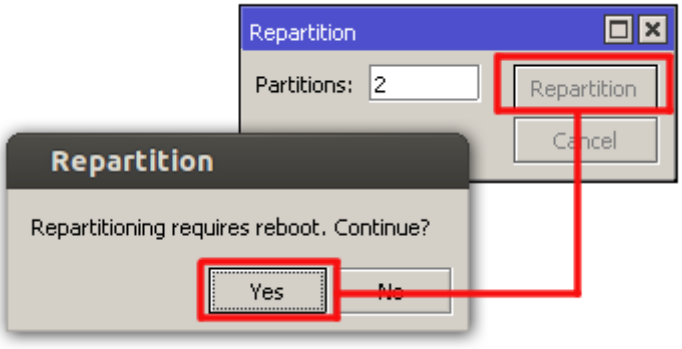
Dan jumlah maksimal untuk partisi adalah **8 partisi**.

Untuk langkah-langkah konfigurasi dari fitur partition adalah sebagai berikut:
Pertama, Pilih pada menu '**Partition**', maka akan muncul tampilan seperti pada gambar dibawah ini. Pada contoh kali ini kita menggunakan Router **RB 751Ui-2HnD** (*Mipsbe v6.18, storage 128MB*).

Kita bisa melihat pada list '**Partitions**' telah terdapat sebuah partisi utama yang menyimpan semua konfigurasi dari router dan termasuk didalamnya *system* operasi router itu sendiri.

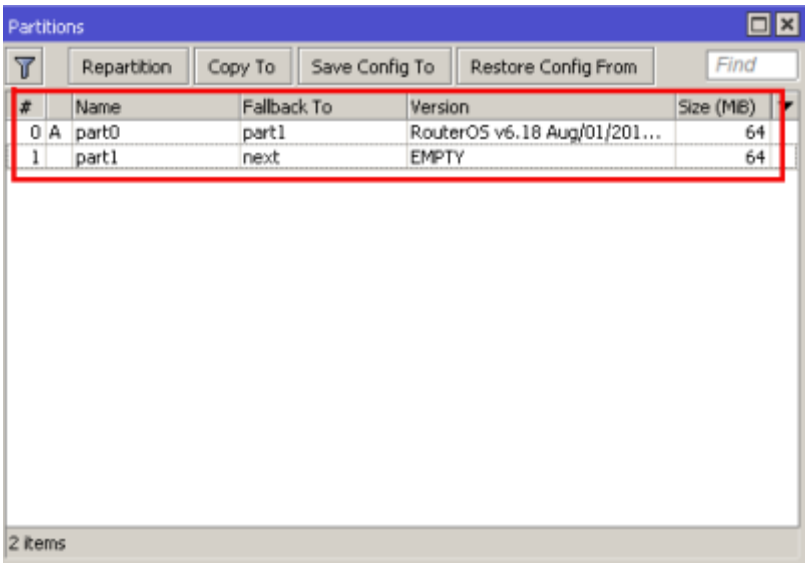


Untuk membuat partisi baru klik pada tombol command '**Repartition**'. Tentukan jumlah partisi yang akan dibuat pada parameter ***Partitions***, misal disini kita akan membuat 2 partisi. Selanjutnya klik tombol '*Repartition*' dan akan muncul dialog box untuk me-reboot router. Pilih '*Yes*'. Tunggu router hingga proses *reboot* selesai.



Setelah proses *reboot* selesai kita *remote* kembali router tersebut dan kita lihat pada menu '***Partitions***'. Kita akan mendapatkan satu lagi list partisi dengan nama **Part1**. Apabila kita perhatikan pada kolom size, ukuran *storage* router terbagi menjadi dua yang sebelumnya *128*MB terbagi menjadi *64*MB untuk **Part0** dan **Part1**.

Kemudian pada kolom version untuk **Part1** masih tertulis '**EMPTY**'. Ini berarti partisi tersebut masih belum ada system dan konfigurasi. Nah, kita bisa memanfaatkan untuk **Part1** sebagai backup dari system dan konfigurasi **Part0**. Kita bisa mengubah parameter '**Fallback To**' pada **Part0** menjadi **Part1**. Sehingga apabila terdapat kesalahan konfigurasi pada **Part0** dan mengalami gagal booting maka secara otomatis router akan mengarahkan proses booting ke **Part1**.

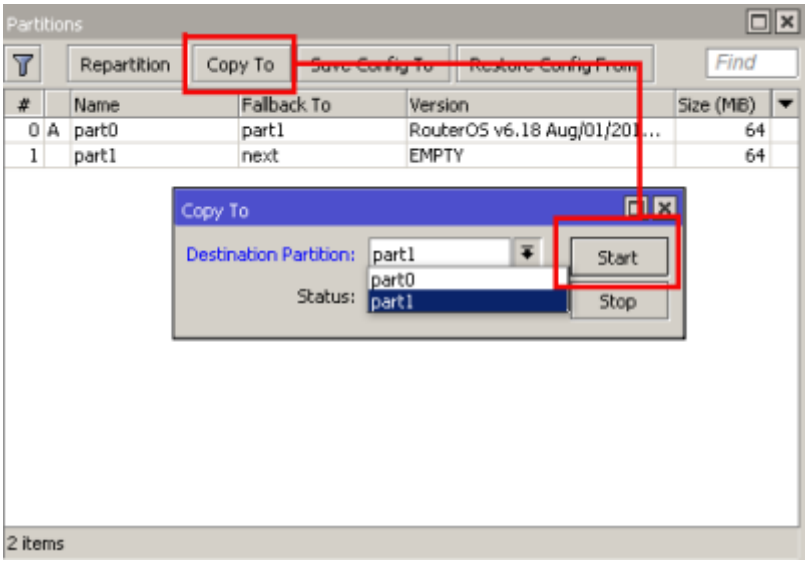


Nah, lalu bagaimana cara membuat backup dari **Part0**? Jika kita lihat pada bagian atas disamping tombol perintah '***Repartition***' terdapat beberapa tombol lagi diantaranya. '***Copy To***', '***Save Config To***', '***Restore Config From***'. Dan penjelasan masing-masing command tersebut adalah sebagai berikut:

- **Copy To** - Memiliki fungsi untuk membuat *back up* atau *cloning* OS yang sedang berjalan danjuga konfigurasi didalamnya ke partisi tertentu. Perlu diketahui bahwa data yang telah tersimpan pada partisi yang dituju akan dihapus dan di-*replace* dengan data backup yang baru.
- **Save Config To** - Memiliki fungsi untuk membuat *backup* atau *cloning*konfigurasi yang sedang berjalan saja ke partisi tertentu. Selain itu tidak dibuat *backup* atau *cloning*.

- **Restore Config From** - Memiliki fungsi untuk menyalin atau *restore*konfigurasi dari partisi tertentu ke partisi yang aktif.

Kita bisa menggunakan tombol command '***Copy To***' untuk melakukan backup System dan juga konfigurasi partisi yang aktif. Caranya pun juga cukup mudah, kita tinggal klik pada command '***Copy To***' kemudian tentukan '***Destination Partition***' ke **Part1**. Kemudian tekan '*Start*' dan tunggu sampai proses *copy* selesai.



Jika sudah selesai maka pada kolom version untuk **part1** berubah menjadi seperti yang terdapat pada **part0**. System dan konfigurasi pada **part0** berhasil di *backup*.

Mengirim File Backup Router Melalui Email Otomatis

Melakukan backup konfigurasi pada Router adalah salah satu langkah terbaik agar admin tidak perlu melakukan config ulang pada saat router ter-reset. Akan lebih baik jika file backup tidak disimpan pada storage/disk internal agar tidak ikut hilang saat Router rusak.Misalnya disimpan pada komputer atau PC.

Pada artikel ini akan diberikan contoh melakukan backup config router serta mengirimkannya melalui email secara berkala dan otomatis. Secara teknis kebutuhan tersebut dapat di penuhi dengan menggunakan kombinasi beberapa perintah.

Backup Config

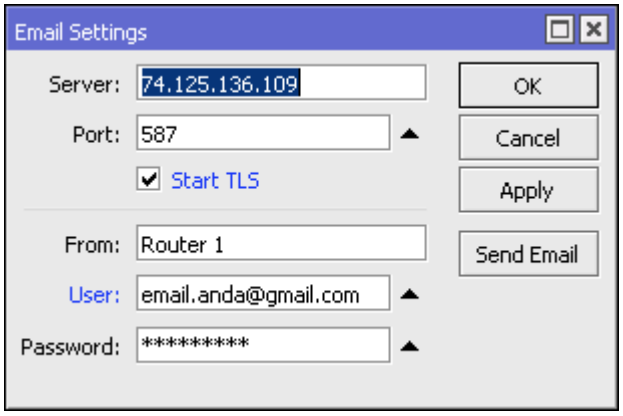
Perintah untuk melakukan backup config dapat dilakukan melalui CLI (command line interface), berikut contoh perintah nya

```
[admin@Router1] > /system backup save name=Router1
```

Perintah tersebut digunakan untuk menyimpan konfigurasi router dengan nama **Router1.backup**

Tool Email

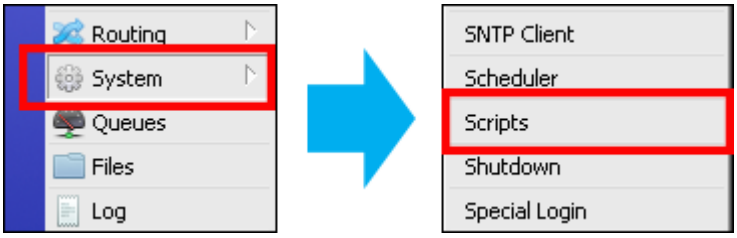
Untuk bisa melakukan pengiriman email dari Router, lakukan setting SMTP Server serta username dan password email pada menu **/tool email**



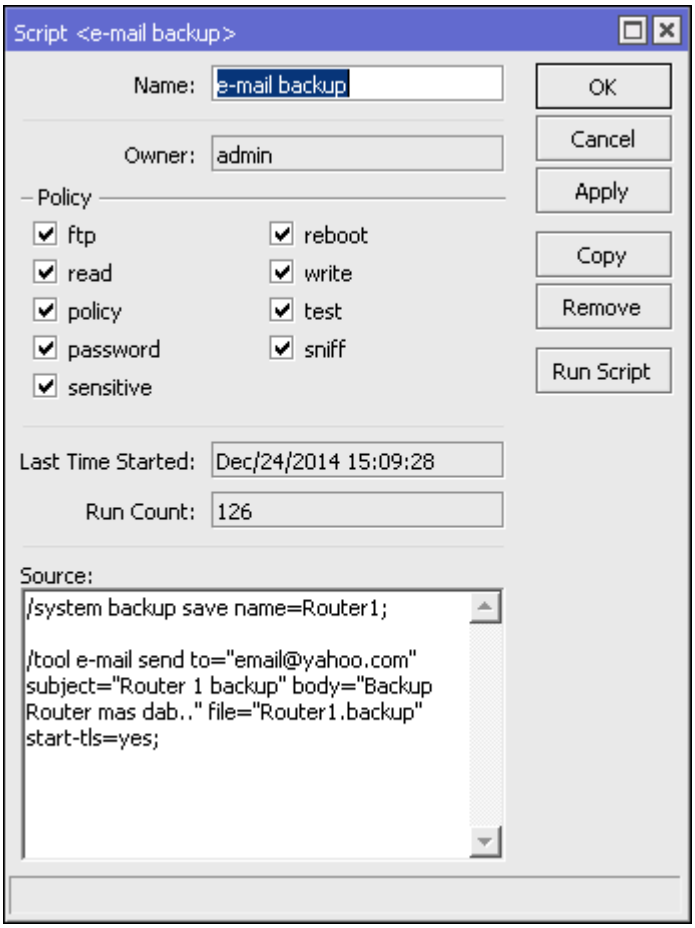
Contoh tersebut menggunakan smtp dari google dan harus melakukan pengaturan pada sisi security akun google agar bisa digunakan. Akan lebih baik jika menggunakan smtp server milik sendiri.

Script

Tool Script digunakan untuk menentukan perintah/command yang akan dieksekusi.



Tambahkan script baru dengan perintah untuk melakukan backup router, sekaligus mengirim file backup ke sebuah alaman email.

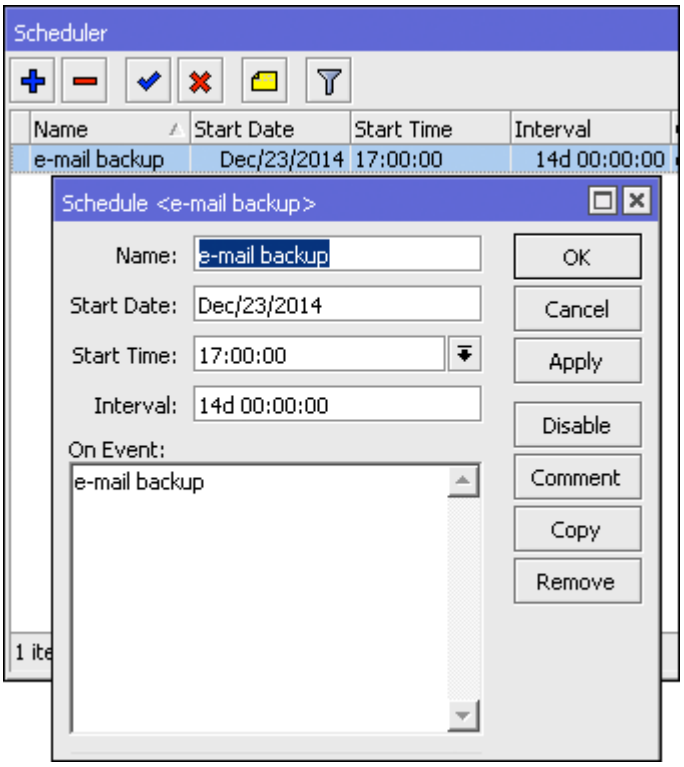


Sesuaikan parameter **"send-to"** dengan email tujuan anda. Untuk melakukan pengecekan apakah script sudah benar, jalankan script secara manual dengan menekan tombol **"Run Script"**.

Scheduler

Scheduler digunakan untuk mengeksekusi perintah tersebut berdasarkan waktu dan interval tertentu.

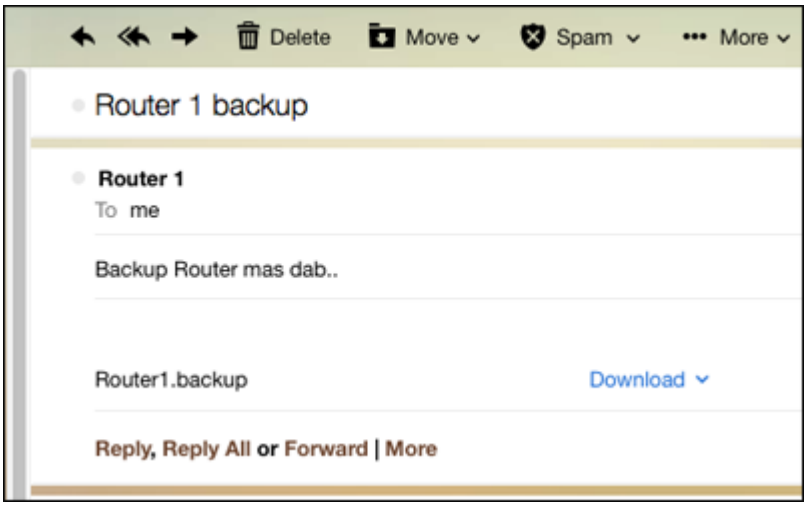
Kita bisa menentukan script yang sebelumnya dibuat kapan akan dieksekusi.



Pada contoh tersebut, script akan dieksekusi setiap 14 hari sekali pada jam 17.00.

Hasil

Terakhir cek pada email tujuan yang telah ditentukan pada script sebelumnya



Jika anda memutuskan untuk menggunakan scheduler, pastikan NTP Client anda aktif dan setting waktu Router sudah tepat.

Fitur SMS di Mikrotik

Seperti yang kita ketahui bahwa router MikroTik dengan didukung oleh RouterOS memiliki berbagai macam fitur. Karena banyaknya fitur yang ada di MikroTik, mungkin ada beberapa fitur yang jarang digunakan. Sehingga bisa diibaratkan seperti fitur yang terlupakan. Nah, salah satu contohnya adalah fitur **SMS** (*Short Massage Service*). Kita bisa menemukan fitur tersebut pada menu "**Tools**".

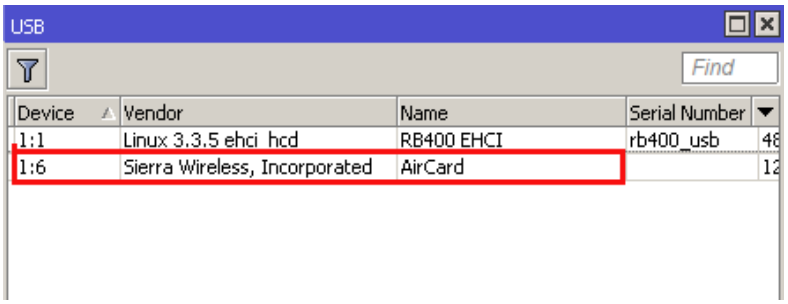
Walaupun tidak dijelaskan secara panjang lebar, secara umum kita telah mengetahui fungsi dari fitur tersebut. Seperti halnya sebuah layanan SMS pada perangkat handphone, fitur SMS di MikroTik juga memiliki fungsi yang sama, yaitu ***Mengirim/Menerima pesan SMS***.
Untuk menggunakan fitur ini kita juga memerlukan sebuah koneksi ke provider telekomunikasi. Kita bisa memanfaatkan sebuah modem untuk terhubung ke provider dan juga RouterBoard yang memiliki **port USB** atau**slot SIM 3G/4G miniPCIe**.

Dengan fitur SMS ini kita bisa memanfaatkan untuk menunjang keperluan*networking*, diantaranya yaitu,
1. Membuat/men-disable User
2. Merubah rule Queue
3. Reset/Shutdown Router
4. Monitoring koneksi internet
5. Memberikan informasi bila ada sebuah link yang down.

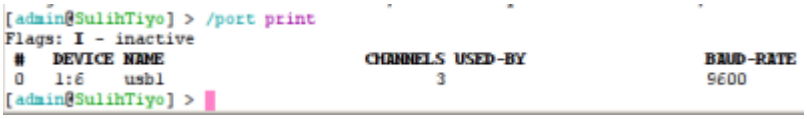
Dan masih banyak lagi yang bisa kita manfaatkan dari fitur SMS ini. Kita bisa lebih fleksibel dan lebih mudah dalam memanajemen jaringan kita. Seperti contoh lain kita bisa mereboot router hanya dengan mengirim SMS ke Mikrotik. Namun, untuk dapat melakukan semua hal diatas, kita harus memadukan fitur ini dengan fitur script yang ada di MikroTik.
Untuk contoh kali ini kita akan menggunakan USB 3G Modem (Sierra AirCad) dan RB 751U (v6.26 mipsbe). Sebelumnya perlu diketahui bahwa tidak semua perangkat modem yang disupport oleh RouterOS. Kita bisa melihat perangkat modem apa saja yang telah disupport oleh RouterOS disini.

Setting 3G Modem dan SMS

Pertama, kita hubungkan modem ke port USB router. Kemudian kita cek apakah modem terhubung ke router dengan baik dan disupport oleh RouterOS. Kita bisa melihatnya melaui menu **System** > **Resources** > pilih**USB**. Maka akan muncul tampilan seperti berikut.



Dan kita juga bisa melihatnya menggunakan **New Terminal** > ketik **/Port Print**. Maka akan muncul tampilan seperti berikut.

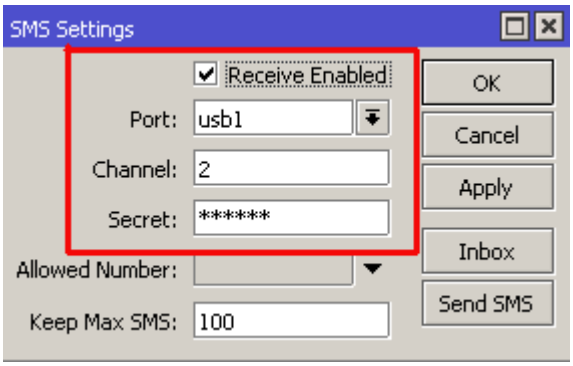


Apabila kita bisa melihat informasi seperti tampilan diatas, maka USB Modem telah terhubung dan disupport oleh RouterOS.

Selanjutnya kita akan melakukan konfigurasi untuk fitur SMS. Pilih pada menu**Tools** > **SMS**. Centang untuk opsi '**Recieve Enabled**' (*Ini memiliki fungsi supaya router bisa menerima SMS untuk menjalankan script atau command*). Kemudian tentukan parameter untuk '**Port**' pilih **usb1** (*Parameter ini disesuaikan dengan port usb yang aktif untuk perangkat Modem. Masing-masing router biasanya berbeda*). Untuk '**Channel**' bisa disesuaikan dengan perangkat modem masing-masing, karena setiap modem memiliki channel yang berbeda-beda.

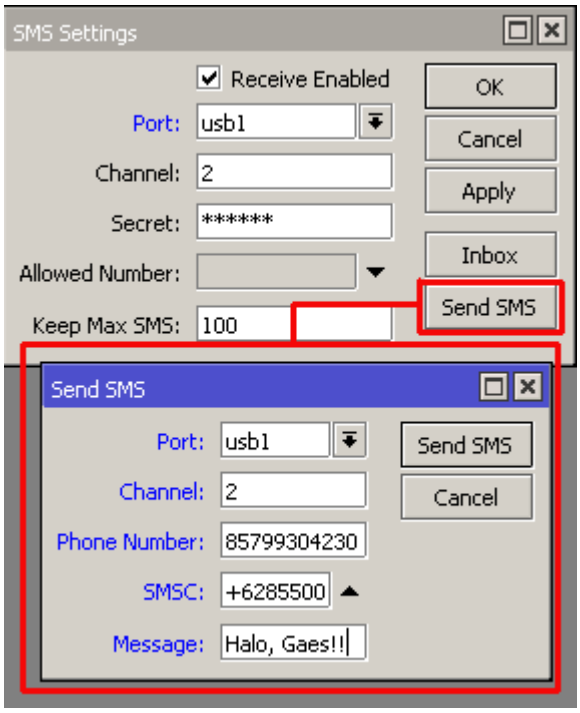
Tentukan juga untuk parameter '**Secret**', misal disini kita isi **696969** (*Ini berfungsi sebagai password yang akan digunakan untuk menjalankan script/command ketika router menerima sebuah SMS*).

Terakhir klik **Apply**.



Mengirim SMS melalui MikroTik

Kali ini kita akan mencoba mengirim SMS melalui Mikrotik. Caranya pun juga mudah, tinggal klik pada tombol '**Send SMS**'. Kemudian kita tentukan parameter-parameter yang ada.
Pada **Port** dan **Channel** kita sesuaikan dengan konfigurasi sebelumnya.
Pada **Phone Number**, isikan dengan nomor yang akan dituju.
Pada **SMSC**, kita isikan dengan nomor SMS Center dari provider yang kita gunakan.
Pada **Message**, kita isikan dengan pesan yang kita kirimkan.



Selanjutnya untuk mengirim pesan tinggal klik '**Send SMS**'.

Menjalankan Script/Command ketika menerima SMS

Apabila kita memilih opsi '**Receive Enabled**' maka router bisa menerima SMS dan dapat kita lihat di '**Inbox**' pada SMS Settings. Disamping itu, kita juga bisa menjalankan script/command pada saat router menerima SMS.

Sebagai contoh kali ini kita akan ***me-reboot router via SMS***. Untuk konfigurasi nya adalah seperti berikut.

Pertama, kita buat sebuah script yang digunakan untuk melakukan reboot router.

```
/system script
add name=reboot
policy=ftp,reboot,read,write,policy,test,winbox,password,sniff,sensitive,api source="/system reboot"
```

Setelah itu kita coba mengirim SMS dari telepon selular ke nomor SIM yang terdapat pada USB Modem dengan pola seperti berikut.

```
:cmd 696969 script reboot
```

Penjelasan dari maksud pola SMS tersebut adalah :

:cmd – Memberikan informasi kepada router untuk melakukan eksekusi terhadap SMS tersebut.

696969 – Merupakan password yang telah kita setting sebelumnya pada 'Secret'.

script – Memberikan informasi kepada router untuk eksekusi fungsi script.

reboot – Nama dari fungsi script untuk mereboot router yang telah kita buat sebelumnya.

_____

TIPS:

Ketika router reboot maka untuk opsi '**Receive Enabled**' akan secara otomatis ter-disable. Untuk mengatasi hal ini, kita bisa memanfaatkan script & scheduler untuk mengaktifkan opsi tersebut secara otomatis.

4

Dasar Keamanan Mikrotik RouterOS

Protected Bootloader

Di Mikrotik terdapat sebuah fitur yang berfungsi untuk melakukan proteksi terhadap akses ke system router terutama berkaitan dengan penggunaan tombol reset. Fitur tersebut adalah "***Protected RouterBOOT***". Ketika fitur ini diaktifkan maka beberapa fungsi tidak dapat dilakukan sebagaimana defaultnya yaitu tombol reset dan juga reset pin-hole. Dan akses router dari console juga akan ter-disabled.

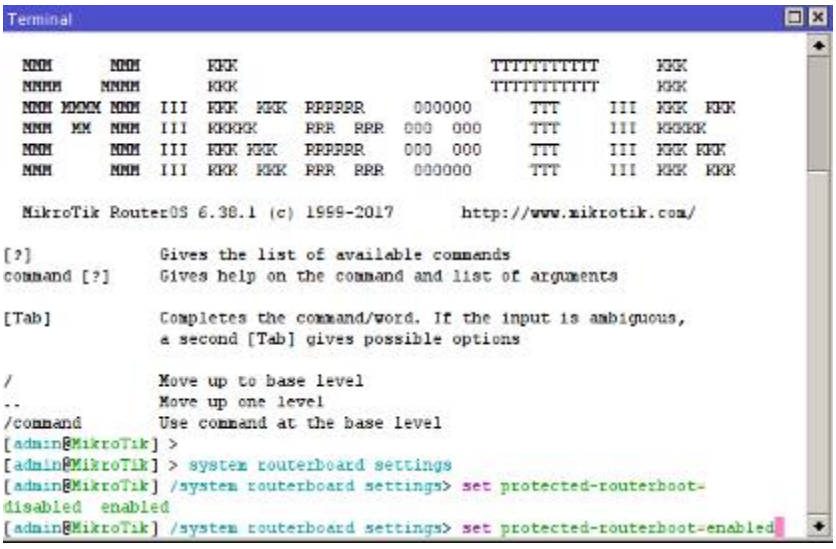
Jika ingin melakukan perubahan konfigurasi untuk melakukan perubahan boot mode atau RouterBOOT maka hanya bisa dilakukan melalui RouterOS (remote via winbox). Fitur ini secara default tidak ditambahakan langsung ke system sehingga kita harus melakukan instalasi paketnya secara manual. Untuk mengaktifkannya firmware dari router harus diatas v3.24 dan tidak bisa digunakan dibawah versi tersebut. Untuk saat ini hanya terdapat di beberapa jenis arsitektur routerboard yaitu SMIPS, MIPSBE, TILE.

Paket "*Protected RouterBOOT*" bisa di-download di link berikut:

- SMIPS, download disini.
- MIPSBE, download disini.
- TILE (Tilera), download disini.

Dan untuk fitur ini hanya dapat berjalan di RouterOS versi 6.33 keatas.

Setelah paket terinstall, untuk mengaktifkan kita bisa mengakses fiturnya melalui New Terminal karena fitur tersebut tidak terdapat di menu GUI. Kita ketikkan dengan perintah CLI yaitu ***/system routerboard settings set protected-routerboot=enabled***



Dengan konfigurasi diatas secara otomatis fungsi dari Protected-RouterBOOT sudah aktif.

Lupa Password?

Lalu bagaimana jika terdapat masalah ketika kita lupa password dari routernya. Secara umum langkah yang bisa diambil ketika kita lupa password adalah dengan melakukan reset router atau juga netinstall. Namun disini dengan mengaktifkan fitur Protected-RouterBOOT

maka fungsi dari tombol reset yang ada tidak dapat digunakan sebagaimana mestinya sehingga reset dan juga netinstall tidak dapat dilakukan.

Untuk mengatasi masalah tersebut didalam fitur Protected RouterBOOT juga ada konfigurasi "***Reformat-Hold-Button***".

```
[SulihTiyo@MikroTik] >
[SulihTiyo@MikroTik] >
[SulihTiyo@MikroTik] > system routerboard settings print
            boot-device: nand-if-fail-then-ethernet
          cpu-frequency: 400MHz
          boot-protocol: bootp
   force-backup-booter: no
            silent-boot: no
  protected-routerboot: enabled
  reformat-hold-button: 20s
[SulihTiyo@MikroTik] >
[SulihTiyo@MikroTik] >
```

Supaya dapat mengakses kembali router ketika kita lupa password maka kita akan melakukan re-format NAND dengan cara menekan tombol reset selama nilai yang tersetting di '*reformat-hold-button*' atau lebih. Secara default nilainya adalah **20s (detik)**, namun kita juga bisa mengubah nilainya sesuai dengan keinginan kita.

Dengan cara tersebut maka akan diproses beberapa hal berikut:

1. Semua setting mode routerBOOT akan di-reset ke default
2. Router akan melakukan reboot
3. Secara otomatis first BOOT akan tersetting ke etherboot.
4. Dengan mode etherboot maka dibutuhkan aplikasi Netinstall untuk melakukan re-format NAND
5. RouterOS, file dan konfigurasi akan dihapus dengan proses reformat NAND tersebut

****) Catatan:***

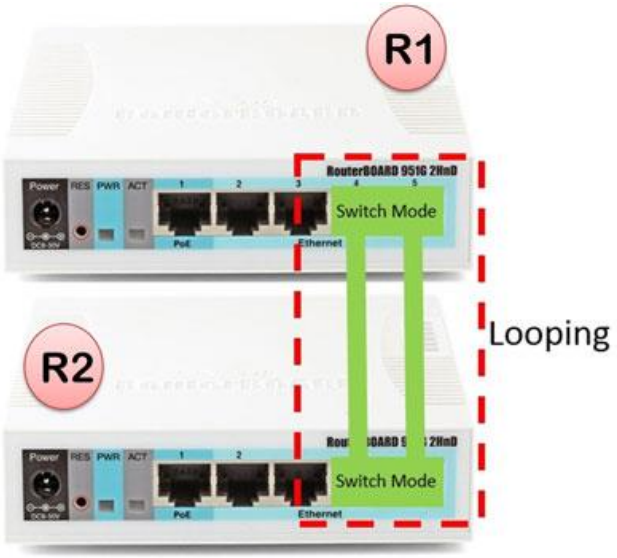
Karena proses re-format NAND akan menghapus seluruh konfigurasi dari router, maka sebaiknya ketika akan mengaktifkan fitur 'Protected RouterBOOT' kita juga melakukan backup konfigurasi yang ada.

Fitur Baru - Loop Protect

Pada artikel sebelumnya kita sudah membahas mengenai pencegahan loop dengan menggunakan STP / RSTP pada jaringan bridge. Lalu bagaimana mengatasi loop apabila kita menerapkan fungsi switch layer 2 ?. Nah, kali ini kita akan mencoba konfigurasi untuk mencegah loop di layer 2.

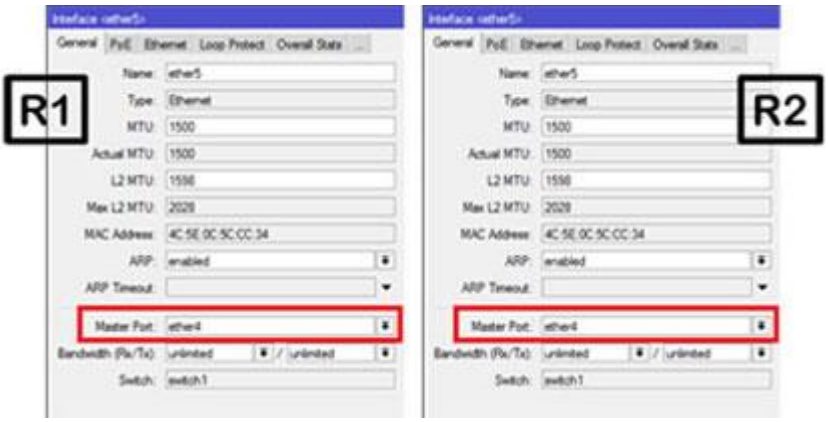
Ketika kita dengan "sengaja" maupun tidak sengaja menancapkan kabel LAN dari satu port ke port yang lain pada switch yang sama maka yang akan terjadi adalah lopping pada jaringan tersebut. Loop pada jaringan terjadi karena switch yang menghubungkan kabel dengan dirinya sendiri atau menghubungkan dua switch atau lebih. Ketika perangkat tersebut saling terhubung dengan kondisi tersebut maka akan terjadi lonjakan paket data pada kedua switch tersebut.

Jika sebuah routerboard mengaktifkan fitur switching maka perangkat tersebut bekerja dengan mengirim dan meneruskan paket data keluar menuju tujuannya, jika perangkat tersebut tidak mengetahui tujuan datanya maka switch akan mengirimkan paket data ke semua port. Apabila paket data tersebut "kembali" diterima oleh switch yang sama pada port yang berbeda, maka akan terjadi yang namanya looping. Untuk mengatasi hal tersebut, kita bisa menggunakan fitur baru yakni fitur Loop Protect. Fitur ini baru ditambahkan pada RouterOS versi 6.37. Interface yang bisa menggunakan fitur ini yaitu ethernet, vlan, eoip, dan eoipv6.

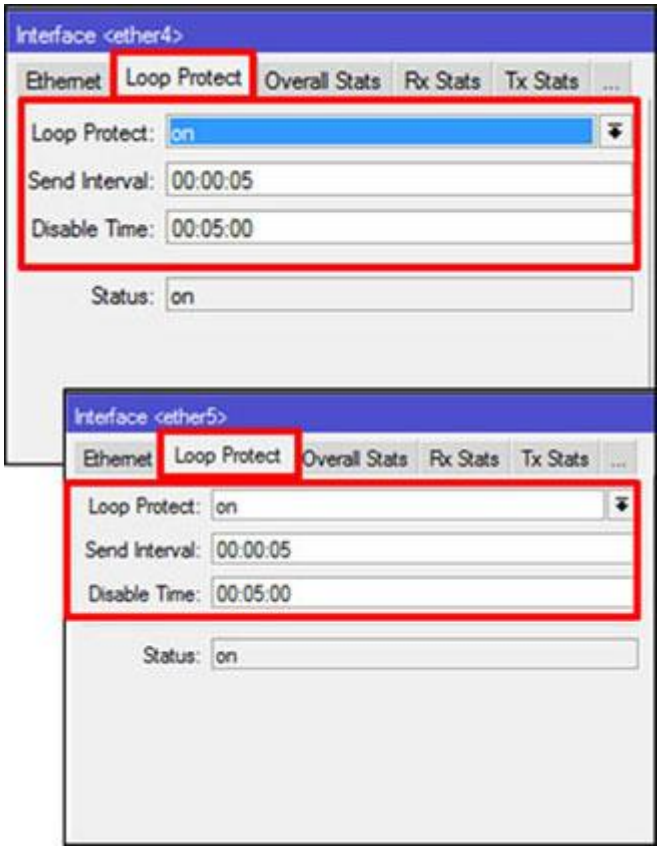


Gambar topologi diatas merupakan contoh topologi yang dibangun untuk menguji fitur Loop protect. Topologi seperti ini sengaja dibuat untuk menciptakan looping antara router R1 dan R2 yang sama-sama mengunakan mode switch.

Langkah pertama yang dilakukan adalah kita aktifkan terlebih dahulu mode switch pada router R1 dan R2 seperti berikut ini



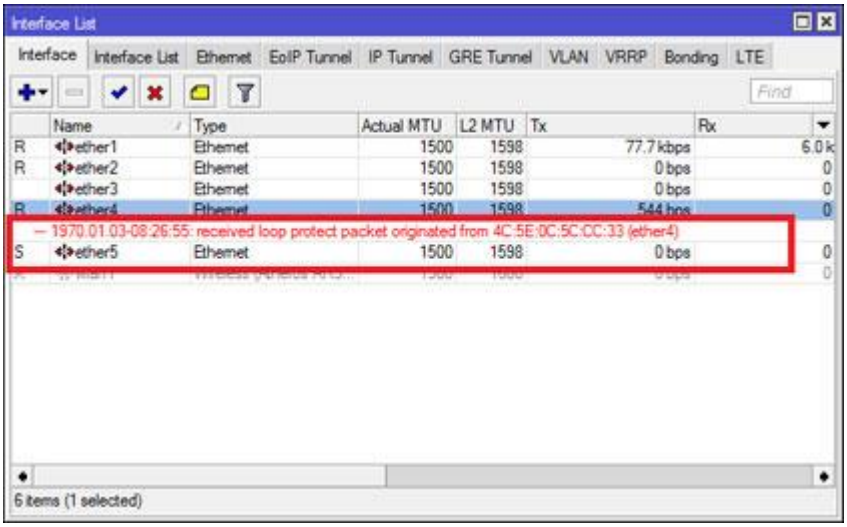
Selanjutnya kita aktifkan fitur Loop Protect. Untuk mengaktifkan fitur ini hanya dilakukan pada salah satu router saja. Secara default, fitur Loop Protect ini dinonaktifkan. Nah, untuk mengkatifkannya cukup mudah, yakni pilih menu interface -> pilih salah satu ethernet -> tab Loop Protect. Dalam satu jaringan kita hanya perlu mengaktifkan Loop Protect di salah satu router saja. Pada kasus ini, ether4 dan ether5 pada router R1 yang akan diaktifkan fungsi Loop Protect.



Setelah mengaktifkan loop protect (ON), kita juga bisa menyesuaikan Send Interval dan Disable Time-nya. Send Interval digunakan sebagai interval waktu untuk melakukan

pengiriman loop protect protcol packets. Sedangkan Disable Time digunakan sebagai lama waktu interface tersebut dibuat tidak berfungsi oleh router setelah terdeteksi adanya loop. Dan interface tersebut akan kembali berfungsi setelah timer kadaluarsa atau disable time-nya habis. Setelah waktunya habis maka interface Loop Protect tadi akan mengirimkan loop protect packet kembali.

Apabila semua langkah-langkah diatas sudah dilakukan maka terlihat bahwa ketika terjadi loop atau terdeteksi adanya looping pada jaringan tersebut, segera muncul log pesan merah seperti gambar berikut ini. Status ether4 berubah menjadi "disable" sampai loop berakhir dan disable timernya berakhir.



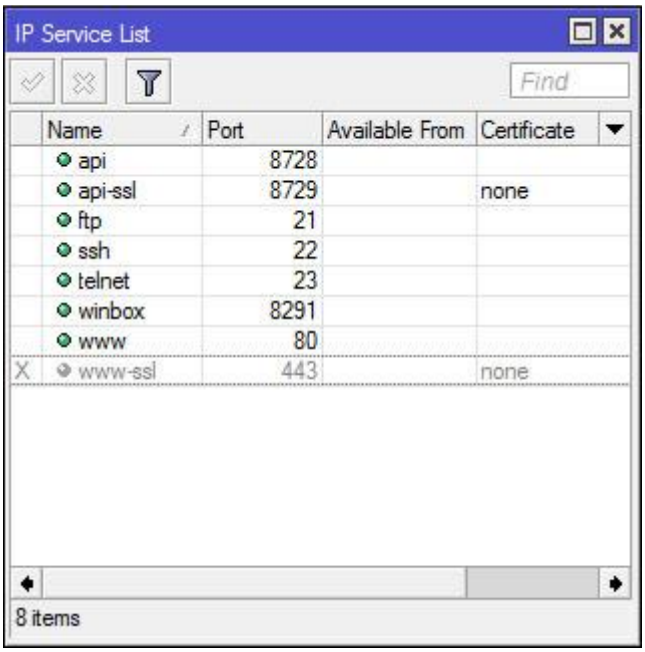
Dengan menggunakan fitur Loop Protect ini, maka permasalahan jaringan di Layer 2 seperti lonjakan paket data akibat looping akan dapat dicegah, sehingga pengguna bisa merasakan performa jaringan yang lebih stabil.

Langkah Pertama Menjaga Keamanan Router

Setelah selesai dengan setting fitur yang dibutuhkan, terkadang admin jaringan mengabaikan sisi keamanan router. Hal ini akan sangat riskan akan terjadinya serangan terhadap router, terlebih ketika router langsung terkoneksi ke internet dan memiliki ip public. Namun jangan salah, serangan terhadap router tidak selalu berasal dari jaringan internet, bisa juga berasal dari jaringan lokal. Kita akan coba bahas langkah pertama yang perlu dilakukan untuk menjaga router dari orang yang tidak bertanggung jawab.

Services

Router Mikrotik menjalankan beberapa service untuk memudahkan cara user dalam mengakses router, atau menggunakan fitur lainnya. Service ini by-default akan dijalankan oleh router terus menerus. Kita bisa cek service yang dijalankan oleh mikrotik di menu IP –> Services



Ada beberapa service yang secara default dijalankan oleh router mikrotik. Berikut detail informasi service router MikroTik dan kegunaannya.

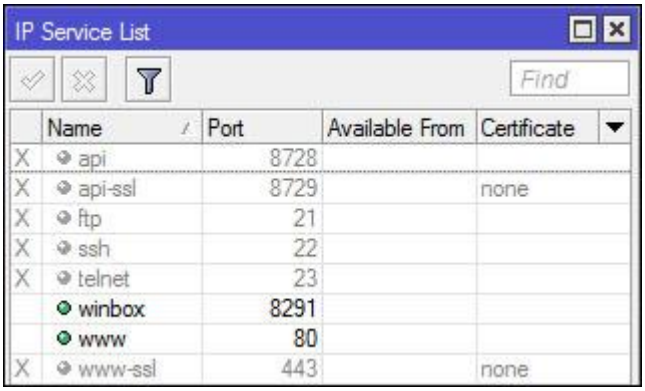
- ***API*** : Application Programmable Interface, sebuah service yang mengijinkan user membuat custom software atau aplikasi yang berkomunikasi dengan router, misal untuk mengambil informasi didalam router, atau bahkan melakukan konfigurasi terhadap router. Menggunakan port 8728.

- ***API-SSL*** : Memiliki fungsi yang sama sama seperti API, hanya saja untuk API SSL lebih secure karena dilengkapi dengan ssl certificate. API SSL ini berjalan dengan menggunakan port 8729.
- ***FTP*** : Mikrotik menyediakan standart service FTP yang menggunakan port 20 dan 21. FTP biasa digunakan untuk upload atau download data router, misal file backup. Authorisasi FTP menggunakan user & password account router.
- ***SSH*** : Merupakan salah satu cara remote router secara console dengan secure. Hampir sama seperti telnet, hanya saja bersifat lebih secure karena data yang ditrasmisikan oleh SSH dienskripsi. SSH MikroTik by default menggunakan port 22.
- ***Telnet*** : Memiliki fungsi yang hampir sama dengan ssh hanya saja memiliki beberapa keterbatasan dan tingkat keamanan yang rendah. Biasa digunakan untuk remote router secara console. Service telnet MikroTik menggunakan port 23.
- ***Winbox*** : Service yang mengijinkan koneksi aplikasi winbox ke router. Tentu kita sudah tidak asing dengan aplikasi winbox yang biasa digunakan untuk meremote router secara grafik. Koneksi winbox menggunakan port 8291.
- ***WWW*** : Selain remote console dan winbox, mikrotik juga menyediakan cara akses router via web-base dengan menggunakan browser. Port yang digunakan adalah standart port HTTP, yaitu port 80.
- ***WWW-SSL*** : Sama seperti service WWW yang mengijinkan akses router menggunakan web-base, akan tetapi www-ssl ini lebih secure karena menggunakan certificae ssl untuk membangun koneksi antara router dengan client yang akan melakukan remote. By default menggunakan port 443.

Selanjutnya adalah pertanyaan bagi administrator jaringan, apakah kemudian semua service tersebut akan digunakan ?. Terkadang admin jaringan tidak terlalu peduli, service tetap berjalan padahal tidak dibutuhkan, sehingga service ini bisa dimanfaatkan oleh orang yang tidak bertanggung jawab setiap saat. Pernahkah Anda membuka terminal router MikroTik kemudian muncul pemberitahuan *"failure for user root from xx.xx.x.xxx via ssh"* ? Error tersebut menginformasikan bahwa ada user yang mencoba mengakses router dengan menebak username dan password router.

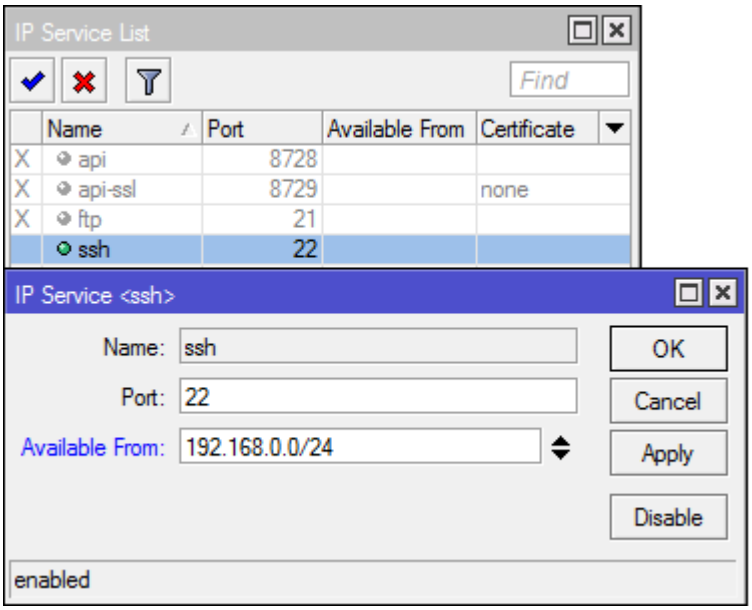
Disable Service

Untuk meminimalisasi user mencoba mengakses router menggunakan service tertentu, administrator jaringan bisa mematikan service yang dirasa tidak digunakan. Misal kita hanya butuh memngakses router via winbox dan web-base, maka kita bisa matikan service selain dua service tadi.



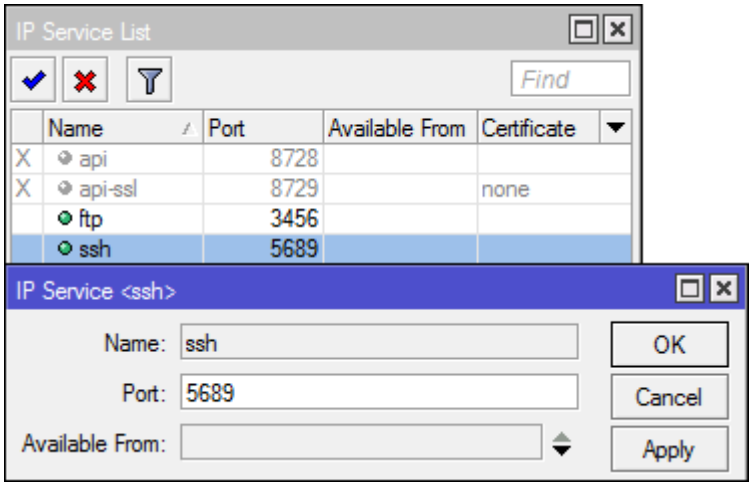
Available From

Administrator jaringan bisa membatasi dari jaringan mana router bisa diakses pada service tertentu dengan menentukan parameter “Available From” pada setting service. dengan menentukan “Available From”, maka service hanya bisa diakses dari jaringan yang sudah ditentukan. Ketika ada yang mencoba mengakses router dari jaringan diluar allowed-address, secara otomatis akan ditolak oleh router. Parameter “Available From” bisa diisi dengan IP address ataupun network address.



Ubah Port

Selain menentukan allowed address, administrator jaringan juga bisa mengubah port yang digunakan oleh service tertentu. Seseorang yang berkecimpung di dunia jaringan bisa menebak dengan mudah port default yang biasa digunakan oleh service – service tertentu.

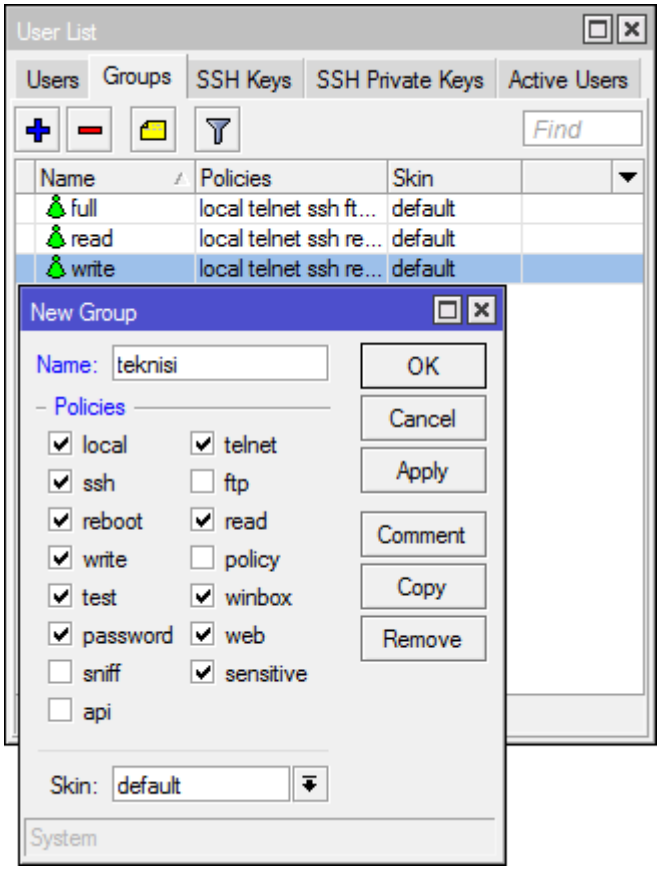


Management User

Beberapa administrator kadang berpikir bahwa dengan memberi password saja sudah cukup. Kemudian men-share username dan password ke beberapa rekan teknisi, bahkan untuk teknisi yang hanya memiliki akses monitoring router juga diberikan hak akses admin. Hal ini tentu akan sangat riskan ketika router yang dihandle merupakan router penting. Berikut beberapa tips management user yang bijak.

Group Policies

Teknisi yang hanya memiliki tanggung jawab monitoring jaringan tidak membutuhkan hak akses full terhadap router. Biasanya hak akses full hanya dimiliki oleh orang yang paling tahu terhadap kondisi dan konfigurasi router. Admin jaringan bisa membuat user sesuai dengan tanggung jawab kerja masing – masing dengan menentukan group dan policies pada setting user. Jika menggunakan Winbox, masuk ke menu **System –> User –> Tab Group.**



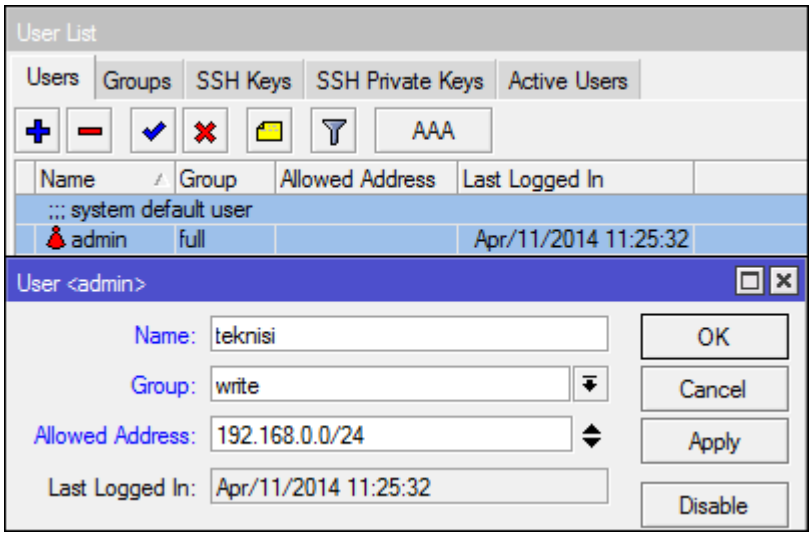
Ada beberapa opsi kebijakan yang akan diberikan untuk menentukan priviledge user. berikut detail opsi policy dan hak yang dimiliki :

- *local* : kebijakan yang mengijinkan user login via local console (keyboard, monitor)
- *telnet* : kebijakan yang mengijinkan use login secara remote via telnet
- ssh : kebijakan yang mengijinkan user login secara remote via secure shell protocol
- *ftp* : Kebijakan yang mengijinkan hak penuh login via FTP, termasuk transfer file dar/menuju router. User dengan kebijakan ini memiliki hak read, write, dan menghapus files.
- *reboot* : Kebijakan yang mengijinkan user me-restart router.

- read : Kebijakan yang mengijinkan untuk melihat Konfigurasi router. Semua command console yang tidak bersifat konfigurasi bisa diakses.
- *write* : Kebijakan yang mengijinkan untuk melakukan konfigurasi router, kecuali user management. Policy ini tidak mengijinkan user untuk membaca konfigurasi router, user yang diberikan policy wirte ini juga disarankan juga diberikan policy read.
- *policy* : Kebijakan yang meemberikan hak untuk management user. Should be used together with write policy. Allows also to see global variables created by other users (requires also 'test' policy).
- *test* : Kebijakan yang memberikan hak untuk menjalankan ping, traceroute, bandwidth-test, wireless scan, sniffer, snooper dan test commands lainnya.
- *web* : Kebijakan yang memberikan hak untuk remote router via WebBox
- *winbox* : Kebijakan yang memberikan hak untuk remote router via WinBox
- *password* : Kebijakan yang memberikan hak untuk mengubah password
- *sensitive* : Kebijakan yang memberikan hak untuk melihat informasi sensitif router, misal secret radius, authentication-key, dll.
- *api* : Kebijakan yang memberikan hak untuk remote router via API.
- *sniff* : Kebijakan yang memberikan hak untuk menggunakan tool packet sniffer.

Allowed Address

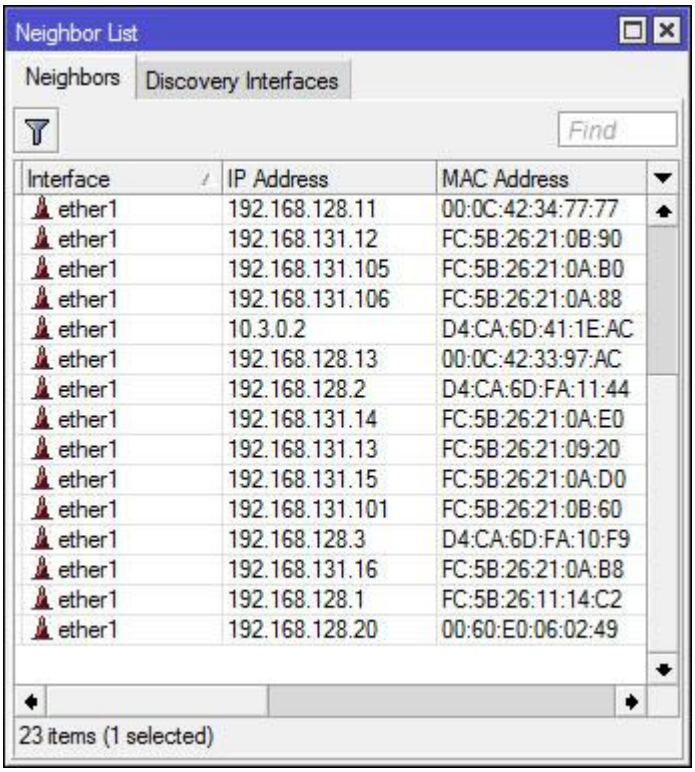
"Allowed Address" digunakan untuk menentukan dari jaringan mana user tersebut boleh akses ke router. Misalkan admin jaringan memiliki kebijakan bahwa teknisi hanya boleh mengankses router melalui jaringan lokal, tidak boleh melalui jaringan public. pada kasus seperti ini, kita bisa menggunakan opsi "Allowed Address".



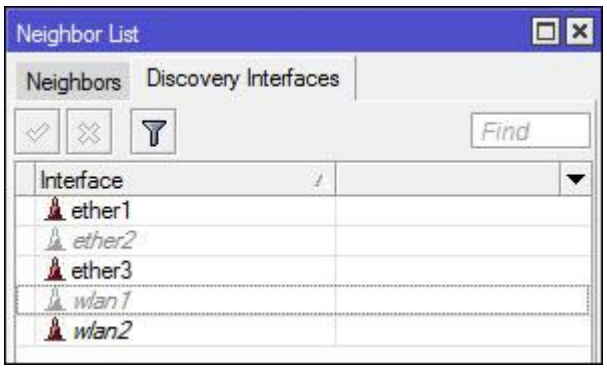
Allowed address bisa dengan ip address atau network addresss. Jika kita isi dengan ip address, maka user hanya bisa login ketika menggunakan ip address tertentu, jika kita isi network address, user bisa digunakan pada segmen Ip address tertentu.

MikroTik Neighbor Discovery Protocol (MNDP)

Merupakan layer 2 broadcast domain yang mengijinkan perangkat yang support MNDP atau CDP untuk saling "menemukan". Contoh paling sederhana ketika kita scan winbox untuk meremote router. Dengan melakukan scan, akan muncul informasi mac address, identity, dan ip address router. Sehingga pada saat MNDP ini berjalan, user yang berada dalam jaringan router bisa dengan mudah menemukan router, dan mengetahui beberapa informasi router. Pada router Mikrotik, router yang menjalankan MNDP bisa dilihat di menu **IP –> Neighbors**. Akan terlihat router yang sedang terkoneksi dan menjalankan MNDP.



Agar router tidak menampilkan informasi ketika ada user yang melakukan scan discovery protokol, administrator jaringan disarankan untuk men-disable discovery interface. Jika menggunakan Winbox, masuk ke menu IP –> Neighboor –> Tab Discovery Interfaces.



Misalnya kita disable ether2 pada setting discovery interfaces, maka router tidak dapat di scan atau “ditemukan” dari jaringan yang terkoneksi ke ether2.

Meminimalkan Kesalahan Konfigurasi Dengan Safe Mode

Kesalahan setting secara sengaja atau tidak sengaja mungkin pernah kita alami, dan efek terburuk bisa jadi router malah tidak bisa diremote. Akan menjadi sangat merepotkan ketika router yang sedang kita setting secara remote router berada di lokasi yang jauh, sehingga kita tidak bisa reset router untuk mengembalikan kondisi router. Untuk meminimalkan kejadian yang cukup menganggu seperti diatas, kita bisa memanfaatkan fitur Safe Mode pada Mikrotik.

Safe Mode

Salah satu fitur mikrotik yang berkerja pada sebuah mode “safe” dimana router akan menyimpan konfigurasi secara sementara. Jika pada saat melakukan setting router pada kondisi safe mode ini koneksi router terputus, baik karena kesalahan setting atau kesalahan teknis lain, maka konfigurasi yang sudah dilakukan pada kondisi safe-mode akan hilang, dan konfigurasi router akan kembali ke konfigurasi sebelum safe-mode. Jika konfigurasi sudah sesuai dengan apa yang kita harapkan, kita cukup menonaktifkan safe-mode untuk menyimpan konfigurasi yang sudah dibuat di safe-mode. Pada saat melakukan konfigurasi di safe-mode, bukan berarti kemudian rule yang dibuat tidak dijalankan router. Rule tetap dijalankan oleh router, hanya saja disimpan secara sementara. System history router menyimpan maksimal 100 perintah, sehingga jika rule yang dibuat di safe-mode terlalu banyak (lebih dari 100), maka router otomatis kan keluar dari safe-mode dan konfigurasi yang sudah dilakukan akan disimpan.

Fitur safe-mode bisa kita jalankan dengan menggunakan console, misalkan remote SSH atau telnet, safe-mode bisa diaktifkan dengan menekan tombol**[CTRL]+[X]**. Kemudian untuk menyimpan konfigurasi dan keluar dari safe-mode, tekan kembali tombol **[CTRL]+[X]**. Untuk keluar dari safe-mode tanpa menyimpan konfigurasi, tekan**[CTRL]+[D]**.

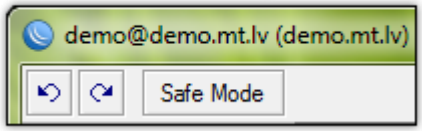
Command Console

```
[admin@Router MikroTik] >
[Safe Mode taken]
[admin@Router MikroTik] <SAFE>
```

Jika pada saat safe-mode terjadi kesalahan setting yang mengakibatkan router tidak dapat diremote, maka router akan mengabaikan konfigurasi yang dilakukan dalam safe-mode, dan kembali ke konfigurasi sebelum safe-mode kurang lebih dalam waktu 9 menit (TCP Connection Time Out). Memang agak lama, namun akan lebih baik daripada harus ke lokasi router jika ternyata router berada di kota lain. Pada winbox, juga menyediakan tombol safe-mode, akan tetapi fitur safe-mode pada winbox masih dalam tahap pengembangan, kami sendiri pun menjumpai sendiri safe mode tidak bekerja dengan optimal seperti pada saat digunakan pada console.**Undo & Redo.**

MikroTik juga memiliki fitur Undo & Redo, memiliki fungsi hampir sama dengan Undo & Redo yang sering kita gunakan pada aplikasi Word misalnya. Fungsi Undo digunakan untuk membatalkan/menghapus konfigurasi yang baru saja dilakukan, jika ternyata tidak bekerja sebagaimana yang kita inginkan, atau ada kesalahan rule. Sedangkan Redo berfungsi untuk mengembalikan konfigurasi yang terhapus/hilang karena proses Undo. Untuk menggunakan fitur Undo & Redo tidak harus berada dalam konsidi safe-mode, kondisi biasa pun fitur ini bisa dijalankan. Posisi tombol Undo & Redo pada winbox terletak dibawah tittle bar dengan icon tanda panah berbelok.

Tombol Undo & Redo pada Winbox



Jika kita ingin melakukan Undo atau Redo padahal kita sedang remote via console, ssh misalnya, Undo & Redo tetap bisa dijalankan dengan perintah console. Cukup ketikkan perintah :

```
[admin@MikroTik] > undo
[admin@MikroTik] > redo
```

Kemudian untuk mengetahui konfigurasi apa saja yang bisa di Undo atau Redo. Bisa dilihat melalui console dengan perintah : ***/system history print***

```
[admin@MikroTik] > system history print
Flags: U - undoable, R - redoable, F - floating-undo
  ACTION                                   BY
R changed snmp settings                    admin
R item changed                             admin
U changed snmp settings                    admin
U changed snmp settings                    admin
U dns changed                              admin
U dns changed                              admin
U route added                              admin
U address added                            admin
```

Akan muncul informasi konfigurasi dan flag dibagian kanan. Flag **U**(*Undoable*) artinya konfigurasi tersebut bisa dibatalkan. Flag **R** (*Redoable*) artinya konfigurasi tersebut bisa dikembalikan setelah terhapus oleh proses Undo.

Mengamankan Jaringan dengan ARP

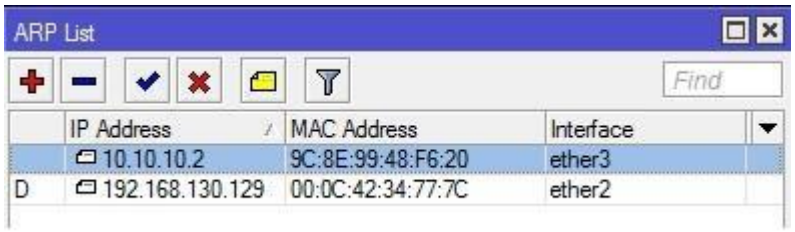
Pernahkah anda menerapkan konsep pengelompokan kebijakan Client pada jaringan lokal berdasarkan IP Address.? Misalnya, anda buat limitasi bandwidth yang berbeda antara Group IP Manajemen dengan Group IP Karyawan pada sebuah kantor. Anda berikan bandwidth yang besar untuk Group Manajemen, sedangkan untuk Karyawan anda berikan kecil.

Penerapan konsep tersebut akan efektif ketika pemakaian IP Address sesuai. Akan tetapi bagaimana jika Karyawan mengganti IP PC mereka menjadi IP yang seharusnya digunakan oleh Manajemen.? Maka Karyawan akan mendapatkan bandwidth yang besar sesuai limitasi untuk group Manajemen.

Kita bisa menerapkan sebuah konsep, ketika client mengubah IP Address pada PC, Router tidak akan memberikan response terhadap request client tersebut sehingga client malah tidak bisa melakukan akses ke jaringan lain (internet) .

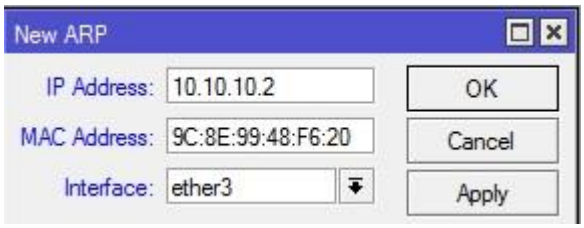
Kita bisa memanfaatkan ARP untuk menerapkan konsep tersebut.

Sebuah router memiliki tabel ARP yang berisi entri ARP. Entri ARP terdiri darialamat IP dan alamat hardware (MAC Address) yang sesuai . Pada Router Mikrotik tabel ARP bisa dilihat pada menu **/ip arp**

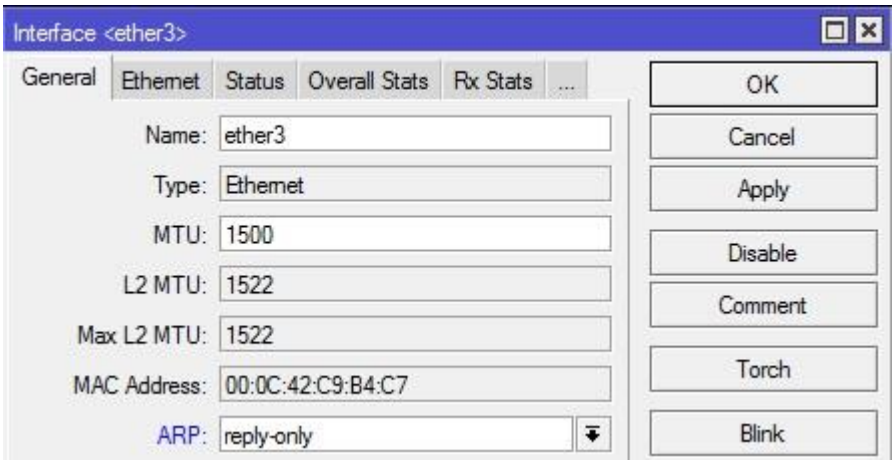


By default, entri ARP ini akan ditambahkan secara otomatis oleh interface Router ketika ada perangkat yang terkoneksi pada interface tersebut (dynamic ARP).

Akan tetapi, untuk meningkatkan keamanan jaringan, kita bisa menambahkan entri ARP ini secara manual (Static ARP).



Selanjutnya ubah setting pada interface lokal menjadi **arp=reply only**.



Pada kondisi ini, interface Router hanya akan meresponse request client dengan kombinasi IP Address dan MAC Address yang sesuai dengan tabel ARP, tanpa menambahkan entri ARP secara otomatis.

Karyawan tidak lagi bisa menggunakan IP Address Manajer. Saat karyawan mengubah IP Adress kombinasi yang terbentuk tidak sesuai dengan ARP Tabel.

Konsep ini bisa juga digunakan untuk mencegah IP Address lain yang tidak dikehendaki menggunakan akses jaringan kita.

DHCP Security : Add ARP Leases, Address Pool Static-Only, DHCP Alert

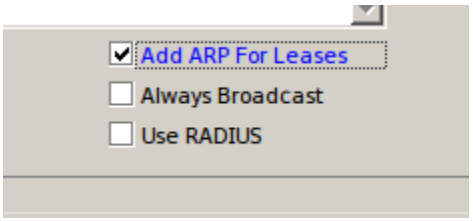
Distribusi IP Address secara dinamis memang memudahkan kita untuk pengelolaan perangkat-perangkat yang terkoneksi ke dalam network. Terlebih lagi perangkat-perangkat tersebut adalah jenis mobile device yang tidak secara statis tersambung ke network tersebut.

Nah, untuk kebutuhan tersebut kita perlu mengaktifkan DHCP Server pada network kita. Selain sebagai distribusi IP Address secara dinamis kita bisa melakukan beberapa konfigurasi pada DHCP Server sebagai langkah preventif/pencegahan dan keamanan.

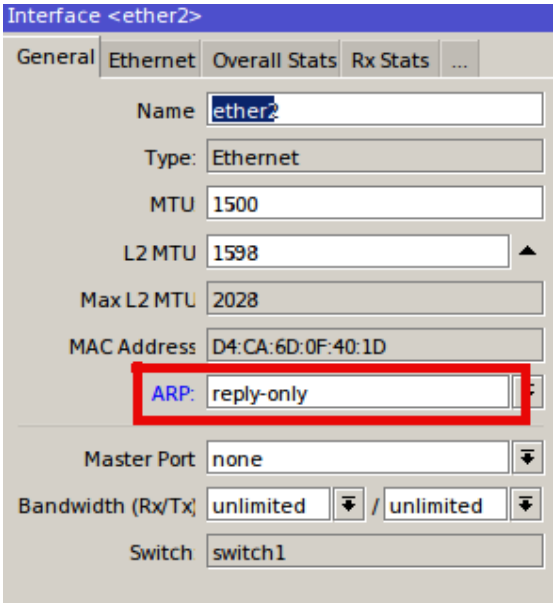
Dan langkah preventif yang akan kita coba bahas disini adalah semisal setiap perangkat yang terkoneksi diharuskan melakukan obtain dan tidak diperkenankan untuk melakukan setting IP Addres secara statis pada perangkatnya. Hal ini untuk mencegah kemungkinan terjadinya IP Conflict pada network tersebut. Selanjutnya kita bisa mengaktifkan 'DHCP Alert' yang berfungsi untuk mendeteksi adanya multiple DHCP Server/DHCP Rogue pada network tersebut.

1. DHCP Security: *Add ARP fo Leases*

Supaya setiap perangkat hanya bisa terkoneksi hanya dengan alokasi IP Address dari DHCP Server kita perlu mengaktifkan opsi '*Add ARP for Leases*'. Caranya klik dua kali pada DHCP Server dan centang opsi tersebut yang terletak di bagian bawah.



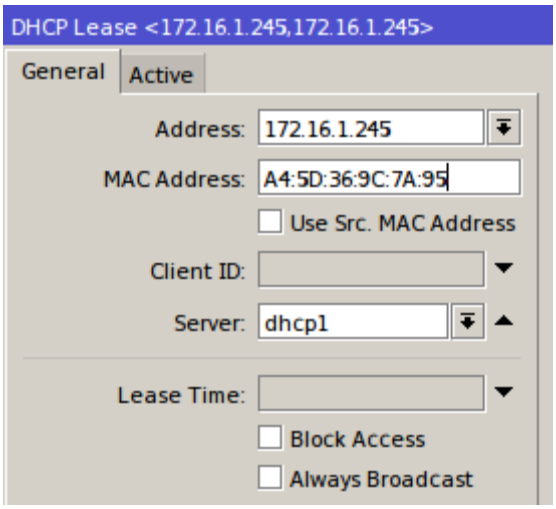
Selain itu pada interface router dimana DHCP Server berada kita ubah parameter 'ARP' dengan opsi '***reply-only***'. Hal ini ditujukan supaya router tidak akan melakukan update secara otomatis pada tabel ARP List ketika ada client yang terkoneksi menggunakan IP Address Static.



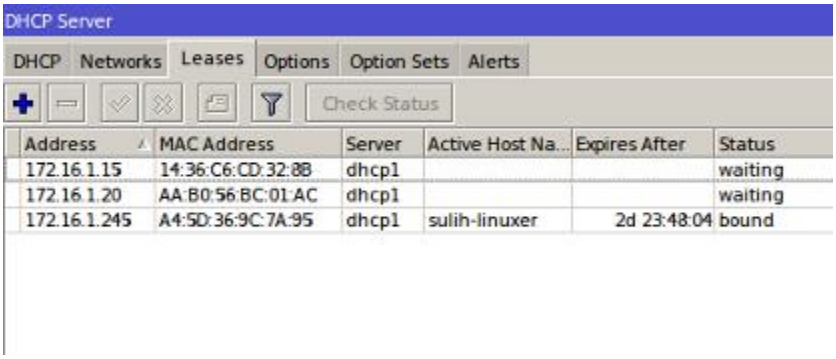
Setting diatas akan membuat router hanya mengijinkan interkoneksi client yang mendapatkan ip address dari proses DHCP. User yang melakukan setting ip address manual justru tidak bisa interkoneksi ke router.

2. DHCP Security : *Adress Pool Static Only*

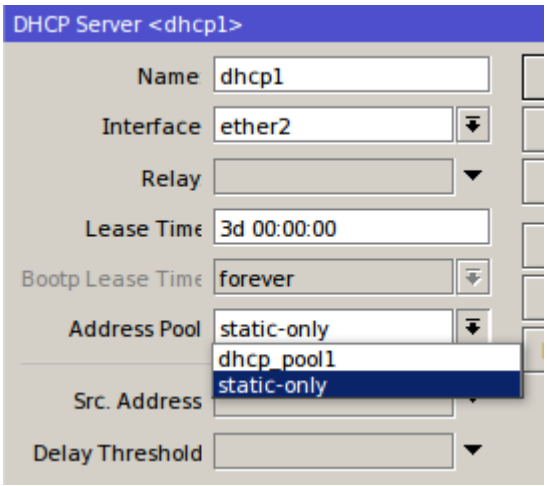
Selanjutnya dengan menggunakan parameter '***Add ARP for Leases***' seperti konfigurasi diatas, kita juga bisa membatasi lagi perangkat yang terkoneksi via DHCP Server hanya perangkat yang sudah kita tentukan saja. Untuk kebutuhan tersebut bisa mengatur parameter pada DHCP Server yaitu Address Pool dengan di-set ke opsi '***Static-Only***'. Namun, sebelumnya kita harus mendaftarkan dulu perangkat yang diijinkan untuk terkoneksi ke daftar *Static Leases*. Untuk penambahannya sendiri bisa pilih pada menu **IP** --> **DHCP Server** --> **Tab Leases** --> Klik **Add [+]**.



Setelah ditambahkan, kita bisa lihat daftar dari perangkat tersebut di Tab Leases.

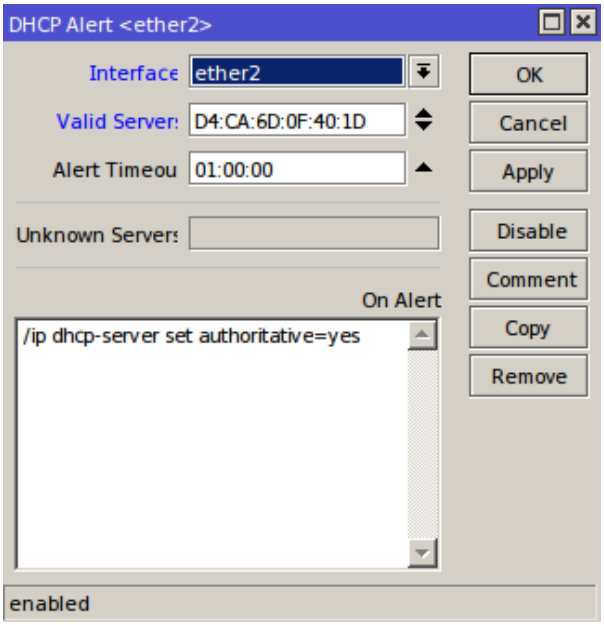


Selanjutnya kita akan setting parameter Address Pool menjadi 'Static-Only'. Untuk pengaturannya bisa di klik 2kali pada DHCP Server yang ada dan pilih pada parameter Address Pool.



3. DHCP Security : *DHCP ALert*

Fitur ini bisa digunakan untuk mendeteksi adanya multiple dhcp server pada satu jaringan yang sama. Hal ini bisa mengacaukan distribusi IP Address dan koneksi dari client. Untuk konfigurasi ada pada menu DHCP Server -> Pilih Tab Alert. Selanjutnya tambahkan rule dengan parameter seperti berikut.



- **Interface** : Untuk menentukan interface router yang menjalankan DHCP Server.
- **Valid Server** : Berisi MAC Address dari DHCP Server yang asli.
- **On Alert** : Script yang akan di eksekusi ketika terdeteksi ada DHCP Rogue.

Pada contoh konfigurasi diatas ketika terdeteksi adanya DHCP Rogue maka script akan dieksekusi dengan aksi membuat parameter Authoritative=YES pada DHCP Server yang asli.

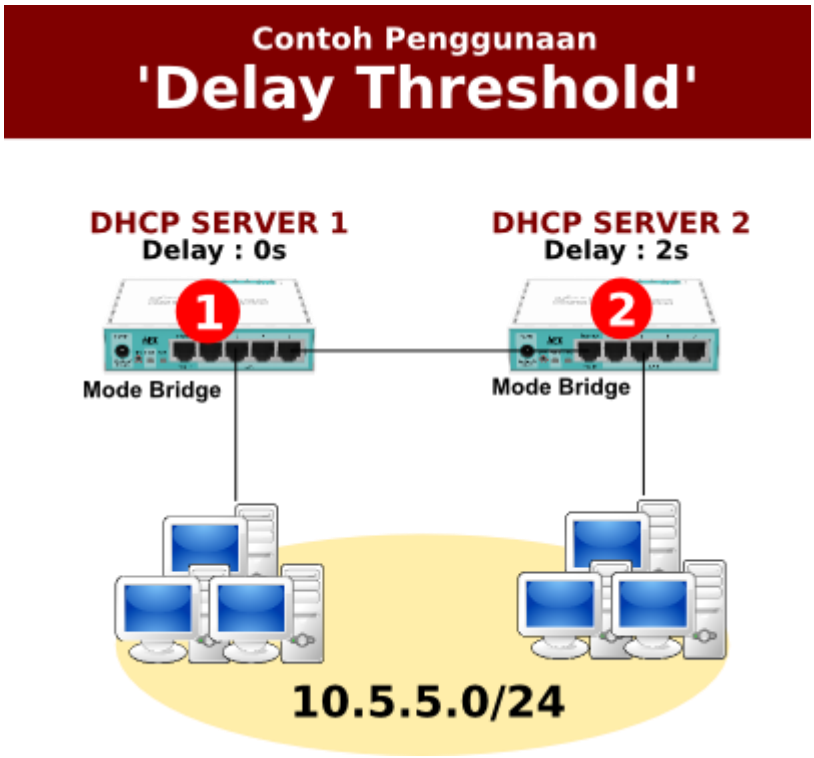
DHCP Security : Delay Threshold & Authoritative

Masih mengenai konfigurasi DHCP pada Mikrotik, pada artikel sebelumnya telah dibahas tentang fungsi dari fitur DHCP Relay. Nah, untuk pembahasan kali ini kita akan mencoba mengulas salah satu fitur dari DHCP di Mikrotik yang bisa dimanfaatkan sebagai *DHCP Security*. Fitur tersebut terletak pada DHCP Server, yaitu**Delay Threshold** dan **Authoritative**.

Delay Threshold

Dengan menggunakan parameter ini, maka kita dapat menentukan DHCP Server manakah yang akan diprioritaskan untuk distribusi alamat IP ke client. Jadi, semakin besar nilai dari *threshold* maka semakin rendah pula prioritasnya.

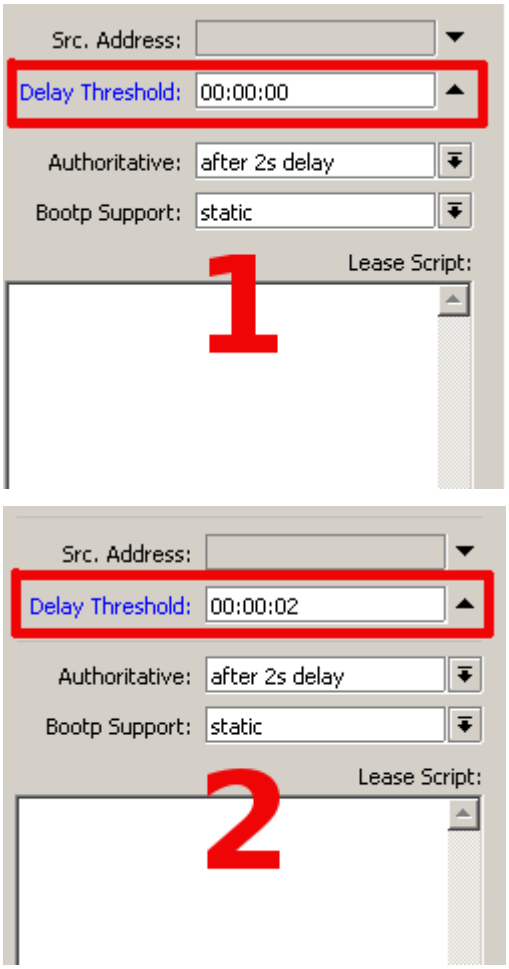
Hal ini sangat bermanfaat jika kita memiliki lebih dari satu DHCP Server. Kita bisa menggunakan DHCP server yang lain sebagai '***backup***'. Jika sewaktu-waktu DHCP Server yang satu mengalami *error* maka distribusi alamat IP bisa di-*cover* oleh DHCP Server yang lain. Untuk penggunaan di RouterBoard Mikrotik, bisanya diimplemantasikan pada topologi jaringan satu segment dengan menggunakan mode bridge. Sebagai contoh kasus dapat dilihat dari gambaran topologi berikut.



Apabila dilihat dari gambar diatas, diketahui bahwa kedua router saling terhubung dan disetting dengan mode bridge. Masing-masing client yang terhubung di router 1 dan router 2 adalah satu segment. Nah, untuk alokasi alamat IP secara dinamic maka ditambahkan DHCP

Server pada router 1 dan juga router 2 pada interface bridge di setiap router. Sehingga kita bisa menggunakan salah satu DHCP Server sebagai '***Backup***'.

Pada contoh topologi diatas DHCP Server yang menjadi 'backup' adalah router 2. Untuk itu kita harus melakukan konfigurasi pada parameter '***Delay Threshold***' di masing-masing router. Router yang menjadi 'backup' disetting dengan nilai threshold lebih tinggi.



Authoritative

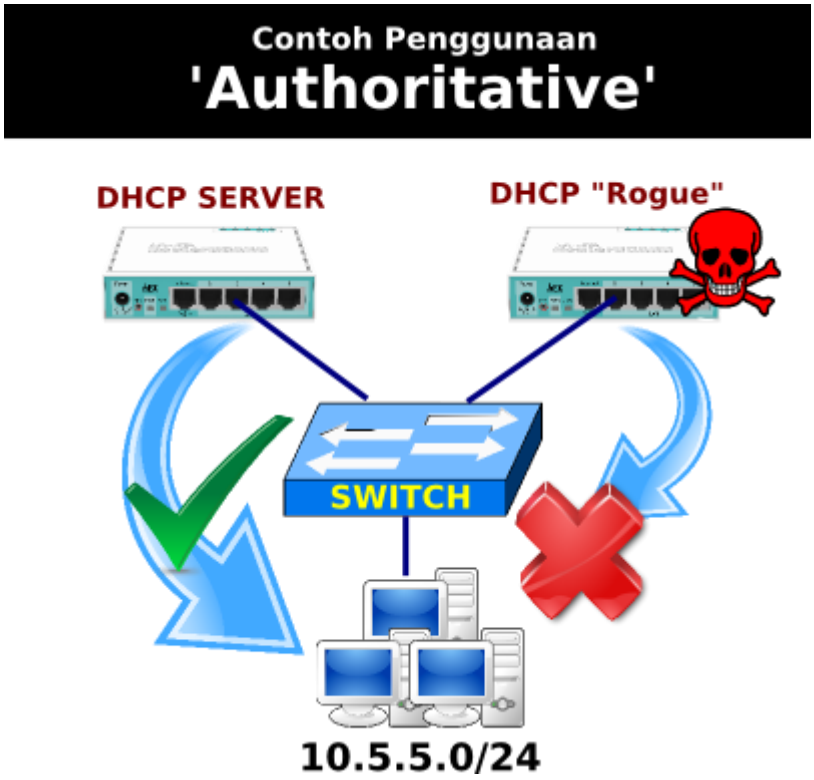
Dengan menggunakan parameter ini kita bisa menentukan bagaimana respon dari DHCP Server terhadap *DHCP request*. Apabila ada request alamat IP dari client yang mana tidak dikenali dalam konfigurasi DHCP server dan parameter '**Authoritative=YES**', maka DHCP Server akan merespon dengan mengirimkan pesan ***NACK*** (*Negative Acknowledgment*). Sehingga hal ini mengharuskan client untuk melakukan '*DHCP Discover*'.

Jika disetting dengan '**Authoritative=NO**', maka DHCP Server akan menolak request alamat IP dari client tersebut (dianggap barangkali ada DHCP Server lain yang meng-handle request tersebut).

Selain itu ada juga pilihan lain untuk parameter 'Authoritative' yaitu *after-10sec-delay* dan *after-2sec-delay*.

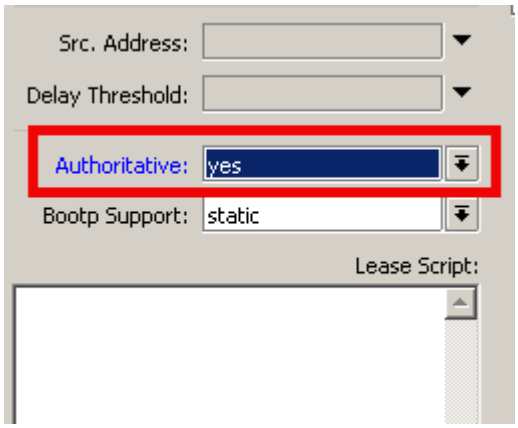
– ***After-10sec-delay*** : Proses DHCP request dari client dengan nilai "secs<10" akan diproses seperti menggunakan parameter "NO" namun jika nilai "secs>=10" akan diproses seperti menggunakan parameter "YES".
– ***After-2sec-delay*** : Proses DHCP request dari client dengan nilai "secs<2" akan diproses seperti menggunakan parameter "NO" namun jika nilai "secs>=2" akan diproses seperti menggunakan parameter "YES".

Nah, dengan mekanisme tersebut, parameter ini bisa digunakan untuk menanggulangi apabila ada DHCP server "tandingan" atau DHCP Rogue dalam sebuah jaringan. Misalnya seperti contoh berikut.



Seperti gambar topologi diatas, terlihat ada 2 router yang berfungsi sebagai DHCP Server untuk distribusi alamat IP ke jaringan lokal 10.5.5.0/24. Kita bisa melakukan setting pada

DHCP Server dengan '*Authoritive=YES*', sehingga secara otomatis DHCP Request akan langsung menuju ke DHCP Server tersebut dan mengabaikan DHCP Server 'tandingan'.



*) **Catatan**: Jika pada parameter '**Delay Threshold**' disetting, maka untuk '**Authoritive**' akan diabaikan.

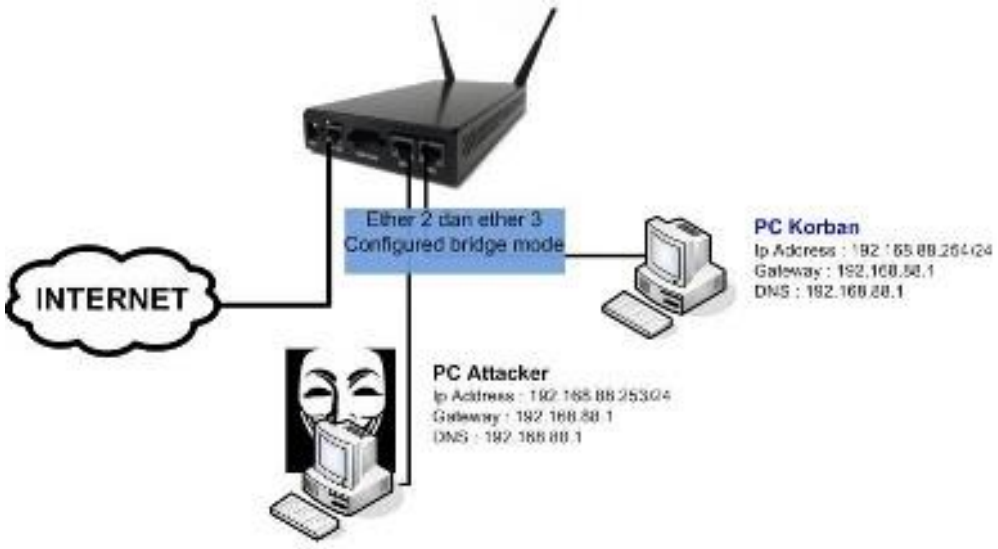
PPPoE Sebagai Penangkal NetCut

Aplikasi NetCut menyerang pada Layer2. Pada saat diaktifkan Netcut akan melakukan broadcast ARP pada jaringan dengan segment yang sama dengan PC Penyerang, sehingga didapatkan informasi MAC Address dan IP Address yang terpasang pada perangkat client lain di jaringan tersebut.

Setelah informasi tersebut didapatkan, penyerang akan dengan mudah melakukan pemutusan trafik jaringan atas sebuah client. Pemutusan ini dilakukan dengan mengirimkan informasi ARP palsu kepada Router (gateway) serta kepada Client, sehingga posisi Penyerang berada di antara Router Gateway dengan Client.

Contoh:

Misalnya ada topologi seperti gambar. Terdapat PC Penyerang dan PC Korban berada dalam jaringan satu segment.

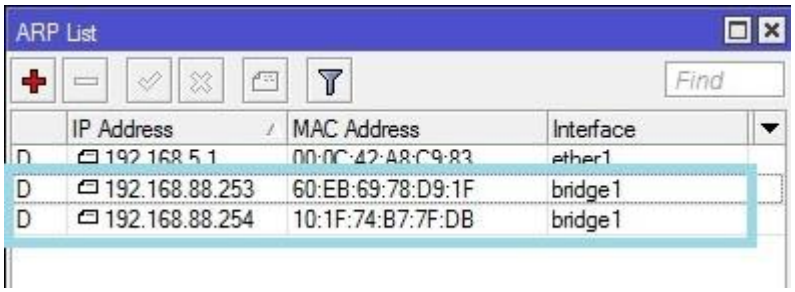


Informasi masing-masing PC

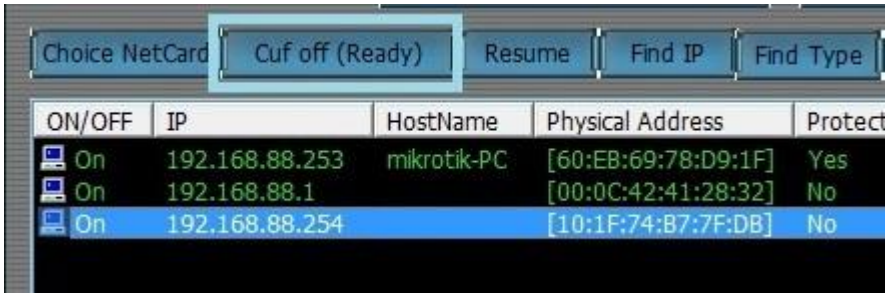
- PC Penyerang : Mac Address=60:eb:69:78:d9:1f ; IP Address=192.168.88.253/24
- PC Korban : MAC Address=10:1f:74:b7:7f:db ; IP Address=192.168.88.254/24

Fungsi ARP sebenarnya adalah sebagai jembatan komunikasi OSI Layer 2 dan Layer3, untuk memetakan IP Address terhadap MAC-Address. List ARP pada Mikrotik bisa anda lihat pada

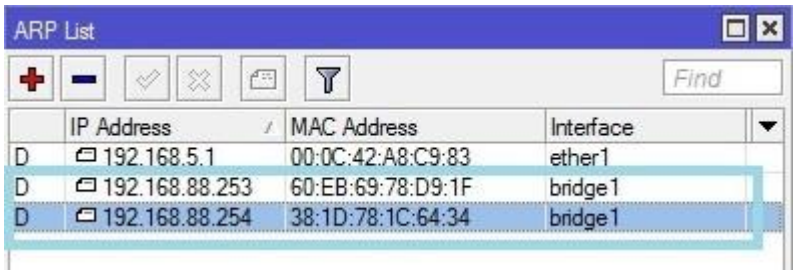
menu **/ip arp**. Terlihat daftar perangkat yang terhubung ke router dengan informasi kombinasi IP Address dan Mac-Address.



Sekarang kita lihat bagaimana saat PC Penyerang sudah mengaktifkan NetCut untuk memutus koneksi korban. NetCut akan melakukan scanning perangkat yang berada dalam segment yang sama.



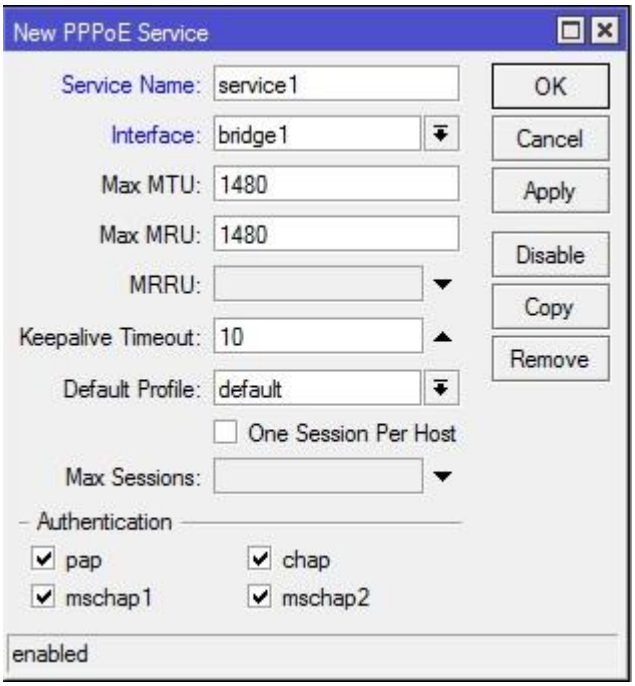
Saat sudah menekan tombol cut off, coba cermati List ARP menu **/ip arp** pada Mikrotik. Coba perhatikan MAC Address dari PC korban. Informasi MAC-Address PC Korban sudah berubah, bandingkan dengan kondisi awal.



Inilah penyebab trafik jaringan korban terputus. Packet data dari internet yang ingin kembali ke PC Korban tidak sampai karena informasi MAC Address telah berubah, bukan lagi MAC Address asli dari PC Korban.

Langkah yang paling efektif untuk melakukan pencegahan adalah dengan melakukan semacam isolasi sehingga setiap PC (atau yang diduga mengaktifkan Netcut) tidak bisa berkomunikasi dengan Client yang lain dan melakukan scanning.
Pada Router Mikrotik, pencegahan ini bisa dilakukan dengan memanfaatkan service **PPPoE (point to point over ethernet)**, khususnya untuk jaringan kabel seperti topologi. Kita buat agar komunikasi Client hanya point to point dengan Router Gateway tanpa bisa berkomunikasi dengan Client lain di bawah Router yang sama.

Langkah awal, aktifkan pppoe server Mikrotik pada interface yang mengarah ke client. Pada Lab ini kita menggunakan interface bridge. Bisa dikonfigurasi via Winbox pada menu **PPP->PPPoE Server -> Add**



Langkah selanjutnya, tentukan user dan password untuk client yang ingin terhubung ke Mikrotik menggunakan pppoe. Masuk tab **Secrets** pada menu**PPP** kemudian anda tentukan user name, password, profile, local address dan remote address.

Langkah pembuatan secret sama dengan pembuatan secret untuk PPTP dan service PPP yang lain. Untuk parameter profile, jika client anda menggunakan windows 7 pilih “default encryption”.

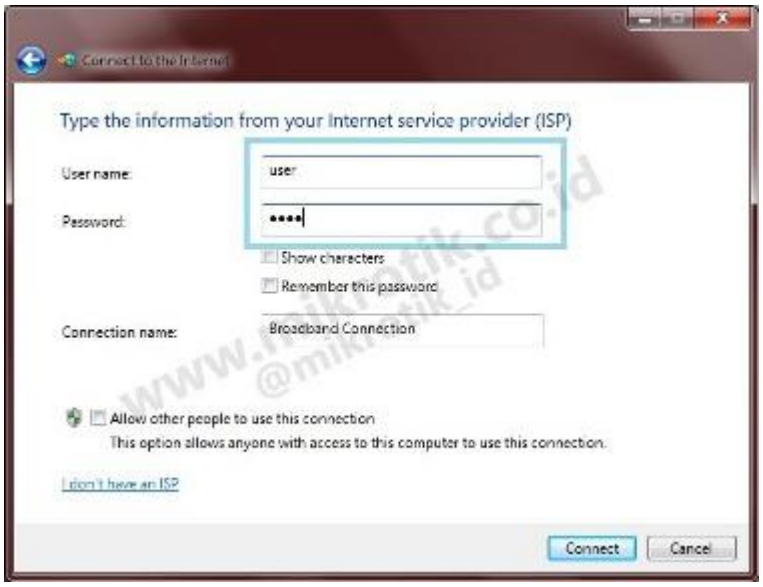
Langkah selanjutnya buat **pppoe client** di sisi perangkat PC. Kita coba pada sisi PC Korban terlebih dahulu.

Berikut langkah pembuatan PPPoE Client pada Windows 7, kita buat sebuah koneksi baru pada pengaturan **Network and Sharing center**, lalu pilih**Setup a New Connection or Network**.

Langkah kedua pilih **Connect to the internet**

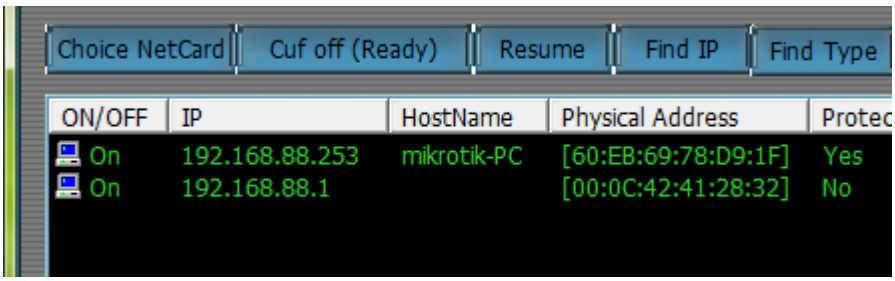
Pada langkah selanjutnya pilih **Broadband (PPPoE)**

Selanjutnya, masukkan **user** dan **password** sesuai pengaturan secret pada PPPoE server. Lalu Klik **Connect**.



Tunggu hingga proses selesai.

Sampai di sini , coba aktifkan NetCut di sisi PC Penyerang, dia tidak bisa melihat PC Korban yang saat ini sudah menggunakan PPPoE untuk terkoneksi ke Router.



Saat ini PC Korban telah menggunakan PPPoE sebagai jalur koneksi ke Router Gateway, sehingga tidak bisa dilihat dari client yang lain di bawah Router yang sama.

Deteksi dan Filter Trafik Ultrasurf VPN dengan MikroTik

Banyak kasus yang dialami dilapangan ketika kita melakukan filtering trafik client untuk akses internet. Seiring berkembangnya teknologi banyak aplikasi-aplikasi yang dibuat untuk melakukan 'bypass' koneksi sehingga filtering yang dibuat tidak akan berguna lagi. Client yang menggunakan aplikasi tersebut tetap bebas 'berselancar' di internet tanpa terkena filtering.

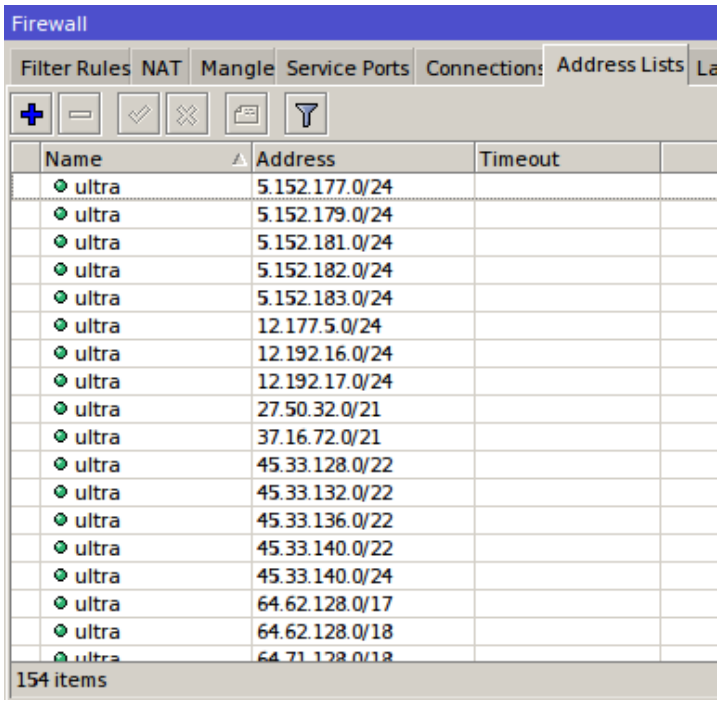
Salah satu aplikasi yang banyak digunakan adalah ***Ultrasurf VPN***. Aplikasi ini menggunakan protokol TCP dan port 443. Hal ini yang menjadi alasan cukup sulit untuk mencegah atau memblokir koneksi dari ultrasurf VPN. Terlebih lagi aplikasi ini menggunakan IP Public yang dinamis untuk konektivitasnya. Sudah banyak cara yang kita coba untuk menaklukkan aplikasi Ultrasurf VPN dengan menggunakan router MikroTik. Namun, tidak sedikit dari cara-cara tersebut yang akhirnya bisa kembali ditembus.

Pada artikel ini kita akan melakukan percobaan dengan sebuah metode yang nantinya bisa diimplementasikan dalam jaringan untuk melakukan filtering trafik ultrasurf. Cara yang digunakan adalah kombinasi antara fitur Firewall Mangle, Address List dan juga Filter.

Deteksi Trafik Ultrasurf

Kita akan mendeteksi terlebih dahulu trafik Ultrasurf VPN yang dijalankan dari perangkat-perangkat client. Langkah pendeteksian akan menggunakan fitur Firewall Mangle. Jika ada client yang terdeteksi mengaktifkan UltraSurf maka akses client ke internet akan diblock.

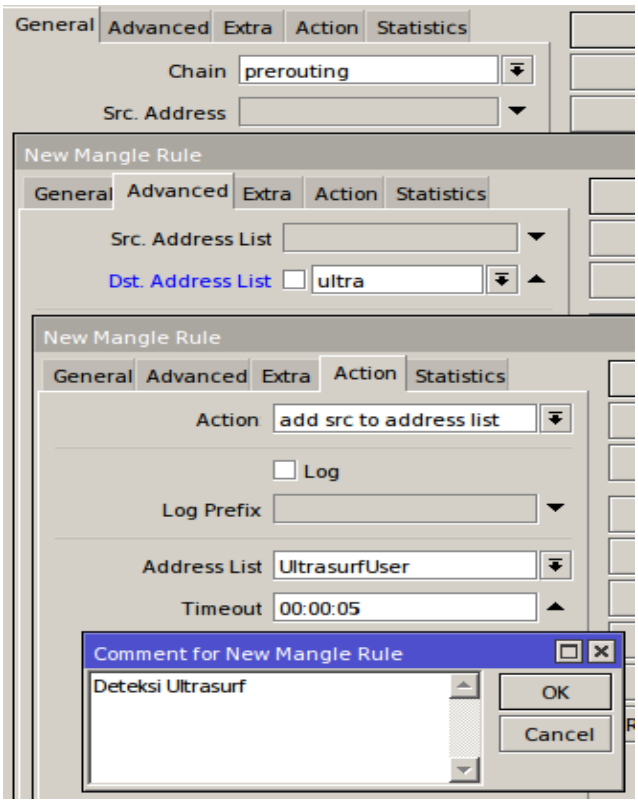
Pertama lakukan import IP Public dari Ultrasurf Server ke 'Address-List' di Firewall. Untuk daftar IP Public bisa di-download disini. Setelah download tinggal dilakukan 'import' ke router.



Selanjutnya tambahkan sebuah rule mangle yang akan digunakan untuk men-deteksi trafik ultrasurf VPN dari client. Contoh konfigurasi mangle-nya seperti berikut:

/ip firewall mangle

*add action=**add-src-to-address-list** address-list=**UltrasurfUser** address-list-timeout=**5s** chain=**prerouting** comment="Deteksi Ultrasurf" dst-address-list=**ultra** dst-port=443 protocol=tcp*

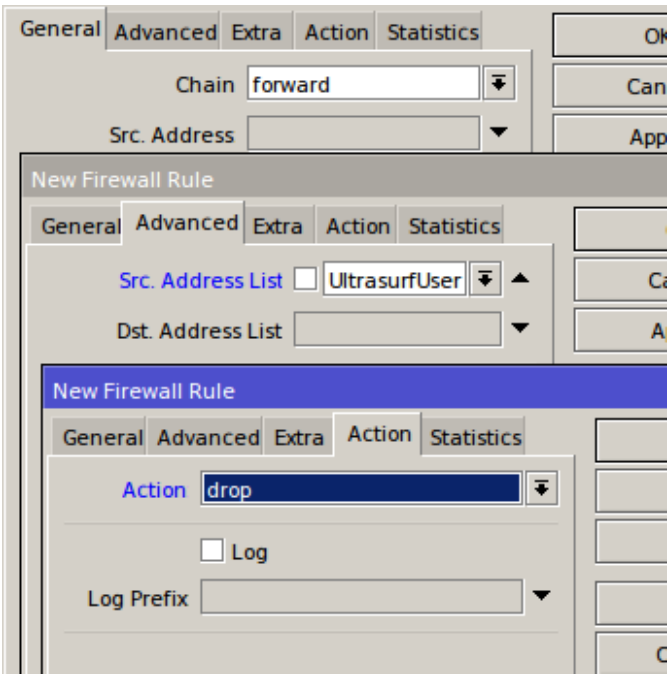


Mekanisme dari rule diatas ketika ada client yang mencoba menjalankan Ultrasurf VPN dengan tujuan IP Public Ultrasurf Server maka IP Address dari client tersebut akan di masukkan ke dalam Address List ***UltrasurfUser***' secara otomatis.

Block/Filter Trafik Client

Langkah selanjutnya setelah kita membuat rule 'Mangle' untuk mendeteksi trafik Ultrasurf VPN dari client, maka kita akan buat rule untuk block/filter trafik client tersebut.

Masuk dimenu **IP** --> **Firewall** --> **Filter** --> Klik **Add [+]**. Kemudian kita tambahkan konfigurasi seperti berikut:



Sampai langkah ini, konfigurasi sudah selesai. Untuk pengetesan tinggal kita coba untuk mengkoneksikan aplikasi Ultrasurf VPN dari masing-masng perangkat client.

Cara Kerja Rule?

Secara garis besar mekanisme dari rule yang telah kita buat diatas adalah ketika ada user yang melakukan koneksi Ultrasurf VPN maka IP Address dari perangkatnya akan dimasukkan kedalam Address-List UltrasurfUser secara dinamis. Dengan hal itu maka kita bisa melakukan drop aktivitas koneksi internet client dari IP Address-nya secara langsung.

Seberapa lama IP Address client pada Address-List UltrasurfUser sesuai dengan rule mangle yang kita setting diatas yaitu selama 5 detik. Selama Client tidak menutup aplikasi Ultrasurf, maka IP Client akan tetap dicatat dengan penambahan waktu 5 detik secara berkala. Namun ketika client menutup aplikasi Ultrasurf VPN maka setelah 5 detik dan dideteksi oleh Router tidak ada aktivitas dari aplikasi tersebut maka IP Address client akan dihapus dari Address-List dan koneksi akan berjalan normal kembali.

Troubleshooting Router Mikrotik

Setiap router miktrotik di design untuk hidup selama 24 jam 7 hari berturut – turut. Jika router mikrotik Anda yang sudah berbulan – bulan atau bahkan bertahun – tahun berjalan normal tiba tiba tidak bekerja sebagaimana mestinya, jangan panik dulu. Pertama kita harus pikirkan terlebih dahulu apakah perangkat tersebut masih bisa kita cek dan perbaiki sendiri atau perlu klaim garansi. Seperti halnya bidang kedokteran, kita perlu tahu penyakit yang diderita pasien dan apa sebabnya. Hal tersebut diterapkan juga di dunia IT yang biasa disebut dengan troubleshooting, yakni mencari sumber masalah secara sistematis sehingga masalah tersebut bisa diatasi. Berikut tips untuk troubleshooting router Mikrotik.
Sebelum cek hal yang lebih detail, cek terlebih dahulu kondisi fisik router. Apakah kabel tercabut atau indikasi ketidakberesan secara fisik lainya. Anda bisa juga coba perhatikan bunyi beep dan nyala lampu indikator LED ethernet atau indikator LED Power saat kabel power dihubungkan. Jika router masih bisa bunyi beep, Anda bisa ikuti step selanjutnya dengan cek proses booting. Ada beberapa router yang tidak memiliki beeper, untuk routerboard jenis seperti ini, selama indikator LED power menyala, anda bisa ikuti langkah perbaikan selanjutnya.

Jika Anda memiliki kabel serial dan router Anda adalah jenis router yang memiliki port serial, Anda bisa melihat proses booting router mikrotik. Anda bisa cek apakah proses booting normal atau ada masalah, seperti misalnya kernel panic. Kernel panic menyebabkan router gagal booting, sehingga router tidak dapat di remote dan membuat router tidak berjalan sebagaimana mestinya. Biasanya kernel panic dikarenakan lonjakan listrik yang tidak stabil atau terlalu sering mematikan router tanpa proses shutdown via software. Nah, dari tahapan cek awal tadi nantinya kita bisa menentukan langkah perbaikan awal.

Tombol Reset

Ketika router Anda mengalami kerusakan ringan, misal karena kesalahan setting sehingga router tidak dapat diremote. Pertolongan pertama yang bisa Anda lakukan ada dengan melakukan reset konfigurasi. Reset konfigurasi bisa dilakukan dengan menggunakan tombol

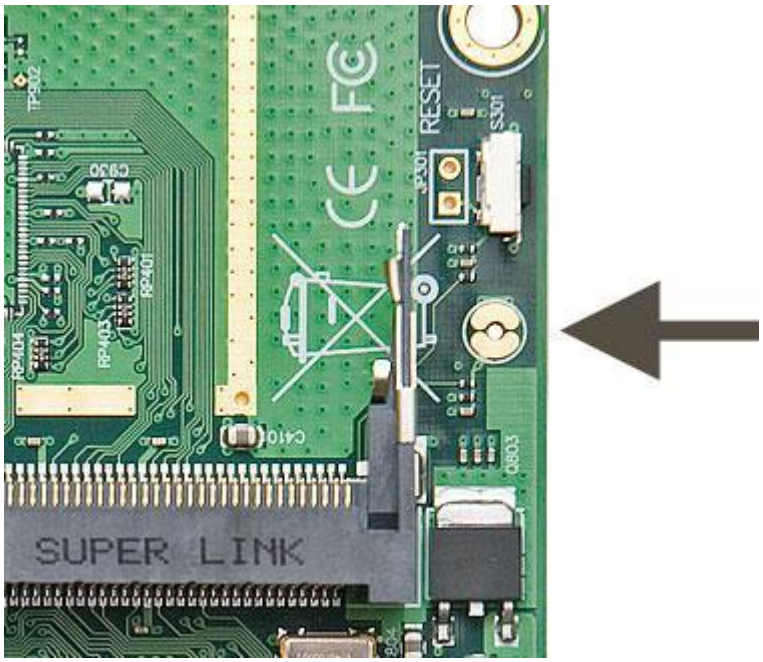
reset yang terdapat di setiap board mikrotik, letaknya mungkin berbeda – beda tergantung jenis router. Pada router indoor, dibagian casing biasanya terdapat lubang kecil dengan keterangan “Reset” didekatnya. Sedangkan untuk router outdoor, Anda perlu membuka casing terlebih dahulu. Contoh gambar
tombol reset :

Untuk melakukan reset konfigurasi pada routerboard bisa dilakukan dengan langkah-langkah sebagai berikut :

- Lepas power adaptor.
- Tekan tombol reset yang disediakan.
- Sambil tetap ditahan tombol resetnya, tancapkan power adaptornya.
- Tunggu kurang lebih 30 detik, dan lepaskan tombol resetnya.
- Restart ulang router anda, dan router anda sudah kembali ke default konfigurasi.

Hard Reset

Jika sudah mencoba melakukan reset menggunakan tombol reset namun proses reset belum berhasil, Anda bisa lakukan hard reset. Pada beberapa produk tertentu, Anda harus membuka casing untuk bisa melakukan hard reset . Jangan khawatir, kami tidak memasang segel pada casing router sehingga memungkinkan untuk buka casing. Pada bagian board, akan ada tembaga berbentuk lingkaran namun satu sisi dengan sisi lainnya tidak saling terhubung, jadi seperti huruf C yang saling berhadapan. Lebih jelasnya, silahkan lihat gambar dibawah ini :



Untuk produk yang sudah embedded sepeti RB750, RB751U-2HnD, dll biasanya ada lubang dibagian bawah. Di dalam lubang tersebut akan terlihat tembaga seperti yang kami sebutkan tadi. Untuk melakukan hard reset pada router anda, silahkan ikuti langkah berikut:

- Matikan power adaptor router anda
- Sambungkan/short sisi-sisi yang terpotong jumper hole dengan pinset/obeng.
- Contoh reset hole seperti pada gambar dibawah
- Sambil tetap ditahan reset holenya, anda nyalakan power adaptor anda.
- Tunggu -+30 detik, kemudian lepaskan jumper reset hole anda
- Selesai, router anda sudah tereset.

Saat anda melakukan reset konfigurasi, semua konfigurasi yang ada didalam router akan dihapus, termasuk username dan password anda. Untuk login setelah reset, anda bisa menggunakan username=admin, password=(kosong tidak usah diisi)

Netinstall

Ketika router mengalami gagal booting karena system corrupt, perbaikan tidak dapat dilakukan dengan cara reset. Namun Anda harus melakukan Netinstall. Langkah ini mungkin menjadi langkah terakhir untuk pertolongan pertama pada router yang bermasalah. Netinstall adalah salah satu cara untuk melakukan install ulang router.
Untuk langkah yang harus dilakukan saat netinstall, Anda bisa pelajari video berikut

: http://www.mikrotik.co.id/artikel_lihat.php?id=25

Beberapa router tidak memiliki port serial, sehingga kit tidak dapat mensetting BIOS router via serial console supaya booting via ethernet. Solusinya adalah dengan menggunakan tombol reset. Persiapannya hampir sama dengan video netinstall diatas, akan tetapi tanpa kabel serial. Untuk cara melakukan netinstall router tanpa menggunakan kabel serial, Anda bisa ikuti langkah berikut :

- Cabut power adaptor router anda
- Tekan tombol reset kecil yang ada di router anda, dan anda tahan.
- Sambil tetap ditahan, anda nyalakan power adaptornya
- Tunggu beberapa saat, nanti di program Netinstall anda akan muncul mac-address dari router anda. Selanjutnya, lakukan installasi seperti di video link sebelumnya.

Troubleshooting diatas merupakan langkah awal sebelum Anda melakukan klaim garansi pada saat router mengalami kerusakan yang masih dalam taraf kerusakan ringan. Dalam artian router masih menyala ketika dikoneksikan kabel power. Jika tidak ada bunyi beep dan indikator LED ether mati atau Anda sudah mencoba semua langkah daiatas namun belum juga berhasil, silahkan isi formulis RMA untuk melakukan klaim garansi.

5

Penutup

Sampailah kita pada bagian akhir dari Ebook ini. Semoga dengan uraian singkat di atas memberikan inspirasi dan membantu kawan-kawan untuk meningkatkan pemahaman dan kewaspadaan dalam mengamankan Router Mikrotiknya.

Semoga bermanfaat untuk kemajuan penggunaan Mikrotik RouterOS dan Mikrotik RouterBoard di Indonesia

Terimakasih atas perhatiannya. Mohon ma'af atas segala kekurangannya.

Maret 2017

Teddy Yuliswar & Primadonal

Kontak: admin@sahoobi.com

www.sahoobi.com

Mikrotik Security For Beginner’s