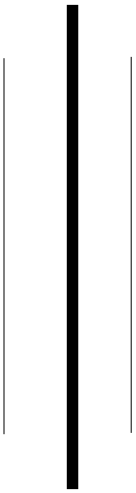
mawaridz@gmail.com

MODUL PELATIHAN NETWORK



Muhammad Fadly Mawaridz

CV. Mitra Sarana Abadi

2009

Pendahuluan

mawaridz@gmail.com

Routing memegang peranan penting dalam suatu network terutama dalam mengatur jalur data dari satu komputer ke komputer lain. Komputer yang bertugas mengatur routing di sebut **Router**.

Materi pada modul ini berisi instalasi dan penggunaan Sistem Operasi MIKROTIK. Disini sengaja di pilih Sistem Operasi MIKROTIK karena di pandang mudah dalam pengoperasiannya dan kebutuhan hardware yang relatif rendah.

Kebutuhan hardware minimal :

Pentium II
RAM 64 Mb
Harddisk IDE 400 Mb

Untuk saat ini MIKROTIK hanya bisa di install di harddisk type IDE, sedang kan harddisk dengan type SCSI dan SATA belum bisa digunakan.

MIKROTIK mempunyai banyak service atau tool sehingga bisa dijadikan DHCP server, PROXY server, RADIUS server, DNS server, VPN server selain sebagai router.

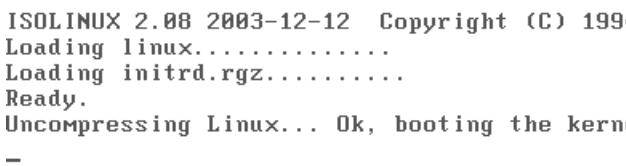
Pada modul ini, akan di bahas MIKROTIK sebagai ROUTER dan sebagai BRIDGE. Disamping itu juga di bahas setting MIKROTIK sebagai pembagi bandwidth.

mawaridz@gmail.com

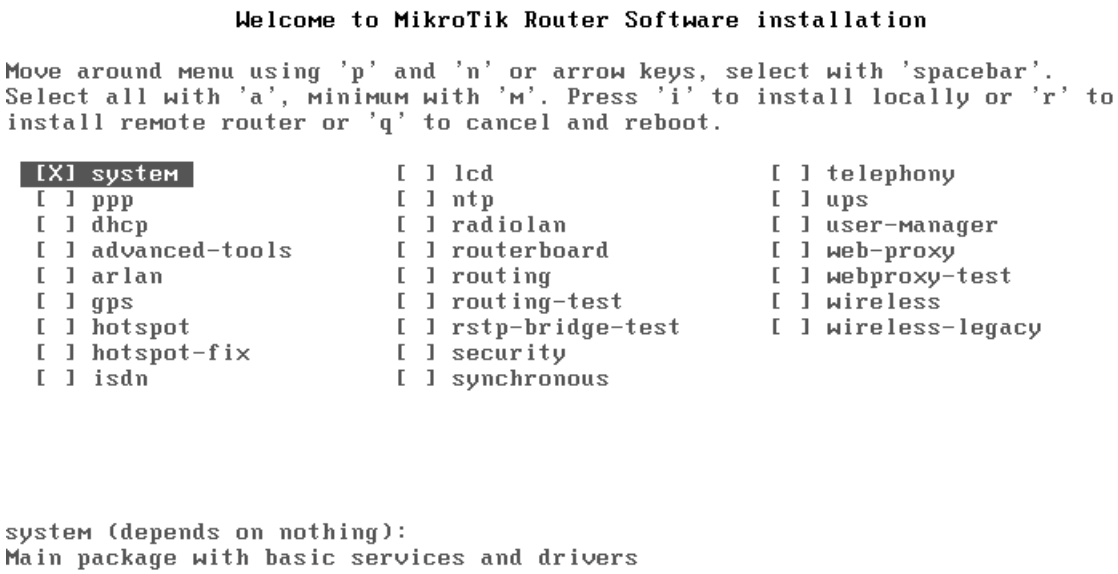
MIKROTIK SEBAGAI ROUTER

Instalasi

Cara instalasi sangat mudah tinggal setting agar komputer bisa boot dari CDROM. Kemudain masukkna CD MIKROTIK. Ketika komputer di booting CD akan mulai bekerja booting awal system MIKROTIk, bisa dilihat di gambar di bawah :



Apabila proses booting awal berjalan dengan baik kemudian akan ditampilkan menu instalasi MIKROTIK sepert berikut :



Pada menu instalasi di tampilkan service apa saja yang ingin kita install. Untuk lebih mudahnya kita pilih semua service yang di sediakan dengan menekan tombol ‘a’. maka semua service akan terpilih

mawaridz@gmail.com

```
                Welcome to MikroTik Router Software installation

Move around menu using 'p' and 'n' or arrow keys, select with 'spacebar'.
Select all with 'a', minimum with 'm'. Press 'i' to install locally or 'r' to
install remote router or 'q' to cancel and reboot.

 [X] system                [X] lcd                   [X] telephony
  [X] ppp                  [X] ntp                   [X] ups
  [X] dhcp                 [X] radiolan              [X] user-manager
  [X] advanced-tools       [X] routerboard           [X] web-proxy
  [X] arlan                [X] routing               [X] webproxy-test
  [X] gps                  [X] routing-test          [X] wireless
  [X] hotspot              [X] rstp-bridge-test      [X] wireless-legacy
  [X] hotspot-fix          [X] security
  [X] isdn                 [X] synchronous



system (depends on nothing):
Main package with basic services and drivers


Do you want to keep old configuration?  [y/n]:
```

Apabila kita menginstall baru tekan tombol 'n' atau apabila kita hanya menambahkan service baru tekan tombol 'y' agar konfigurasi yang sudah di buat tidak hilang.

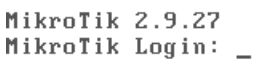
Langkah berikutnya akan disiapkan ruang harddisk yang akan di pakai oleh MIKROTIK dengan memformatnya dan mengkopikan file-file yang dibutuhkan

```
system (depends on nothing):
Main package with basic services and drivers


Do you want to keep old configuration?  [y/n]:n

Warning: all data on the disk will be erased!

Continue? [y/n]:y

Creating partition.........
Formatting disk..................

installed system-2.9.27
installed hotspot-fix-2.9.27
installed hotspot-2.9.27
installed ppp-2.9.27
installed routing-test-2.9.27
installed advanced-tools-2.9.27
installed arlan-2.9.27
installed dhcp-2.9.27
installing gps-2.9.27 [############################################################]
```

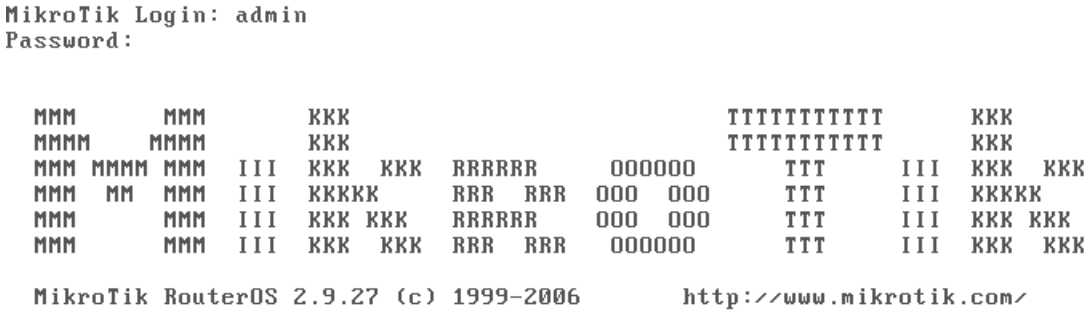
Setelah proses pengkopian file selesai kemudian proses instalasi membutuhkan reboot ulang. Apabila semua proses instalasi tidak mengalami error setelah reboot ulang di layar

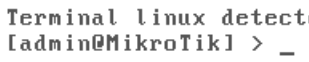
mawaridz@gmail.com

akan muncul tampilan user login dan password, seperti gambar di bawah :



Secara default user yang dipakai adalah user **admin** dengan password yang masih kosong. Setelah login tampilan awal akan seperti berikut :

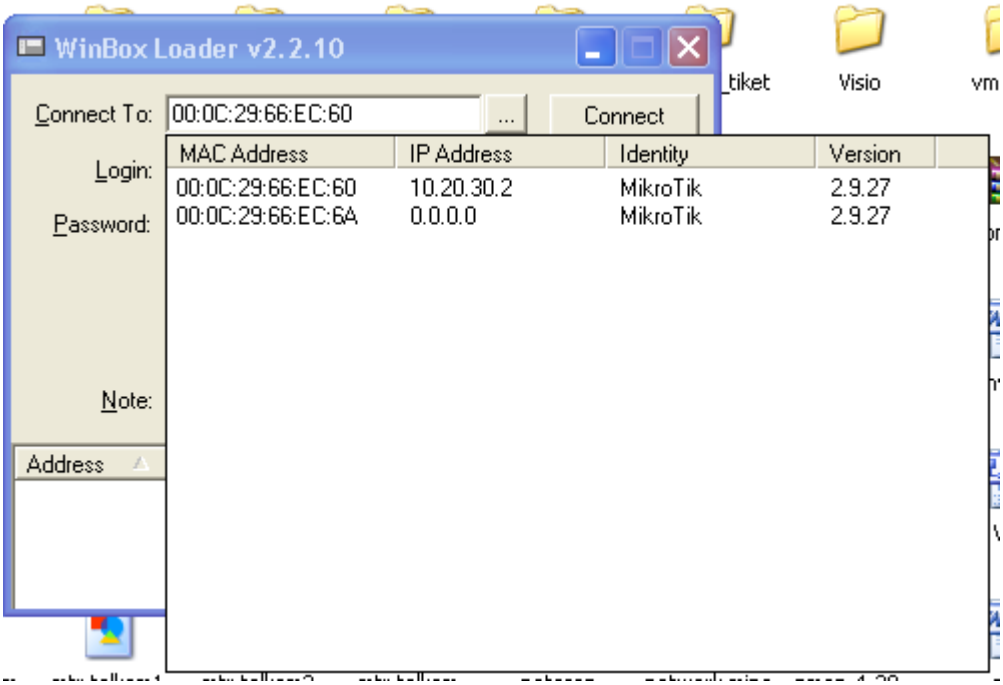




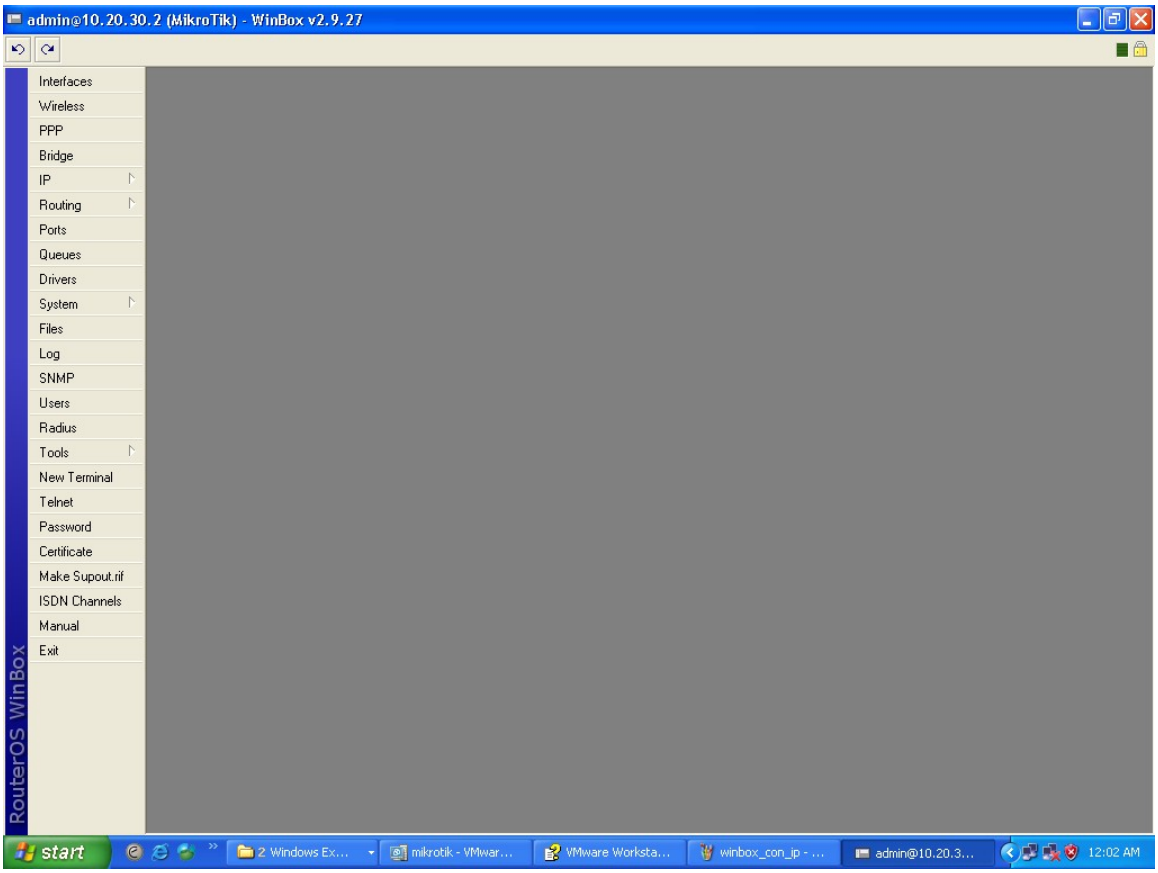
Kita tidak akan membahas perintah command line, karena akan salah rumit dan sulit untuk menghafalakannya. Untuk mensetting Mikrotik ini kita menggunakan tools lain yaitu **Winbox**. Tools winbox ini bisa diambil secara free di website http://www.mikrotik.co.id.

Dengan Winbox ini kita bisa mendeteksi System Mikrotik yang sudah di install asalkan masih dalam satu network, yaitu dengan mendeteksi MAC address dari ethernet yang terpasang di Mikrotik. Tampilan awal pertama kali mengaktifkan winbox adalah seperti berikut :

mawaridz@gmail.com

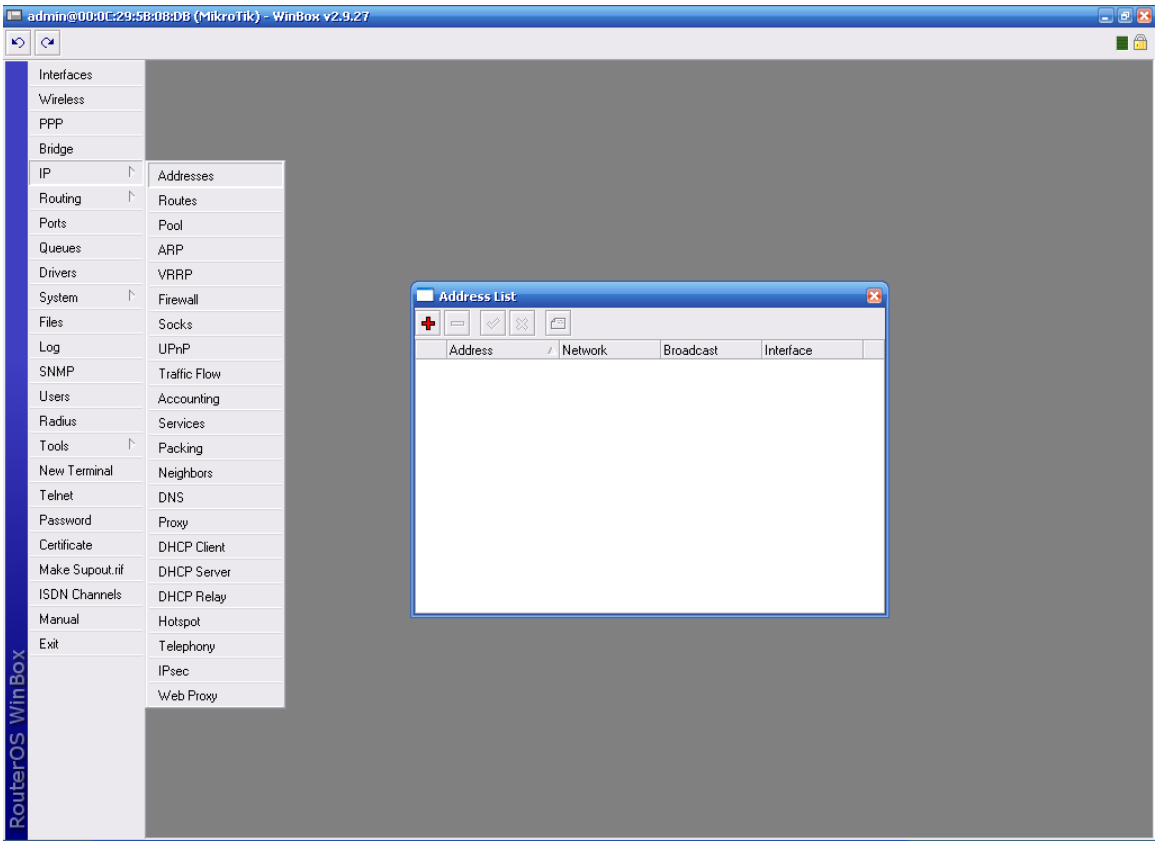


Kita tinggal pilih MAC address yang sudah terdeteksi dan klik tombol Connect. Maka akan muncul tampilan seperti di bawah :

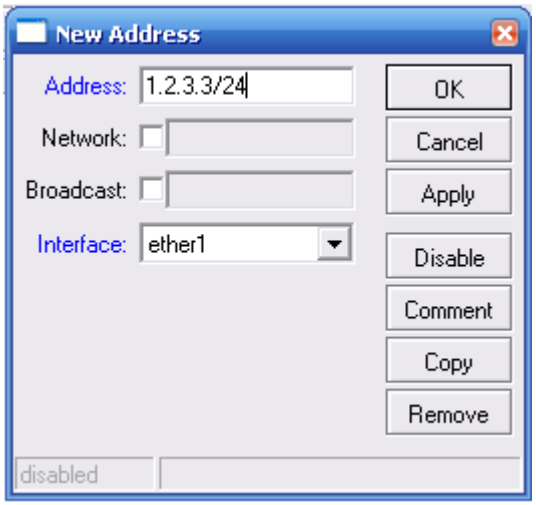


mawaridz@gmail.com

Langkah awal yang perlu dilakaukan adalah memberi IP Address, melalui menu **ip ▪ addresses**. Kemudian akan masuk ke windows yang memunculkan IP address

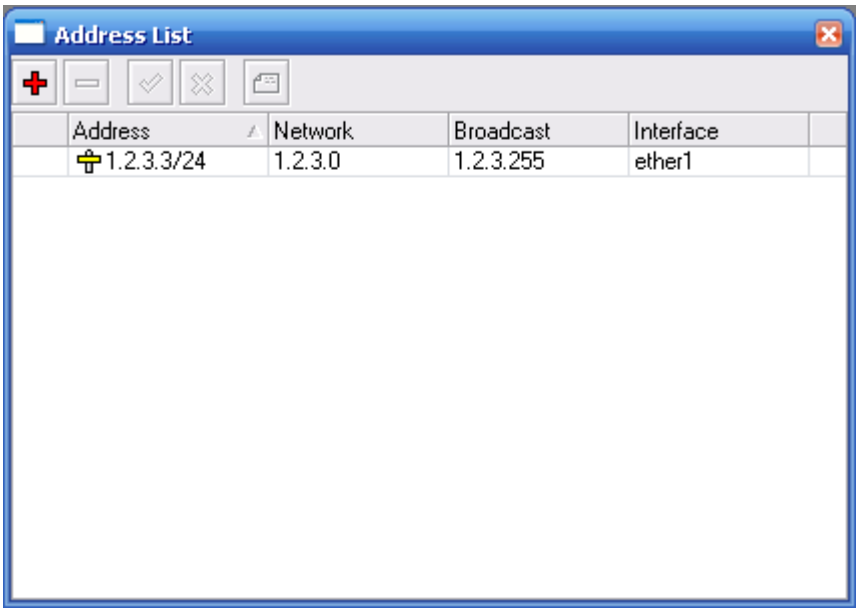


Untuk menambahkan ip address klik menu + , kemudian kita tuliskan ip address yang akan digunakan dan untuk ethernet nomor berapa. Setelah itu klik tombol **ok**



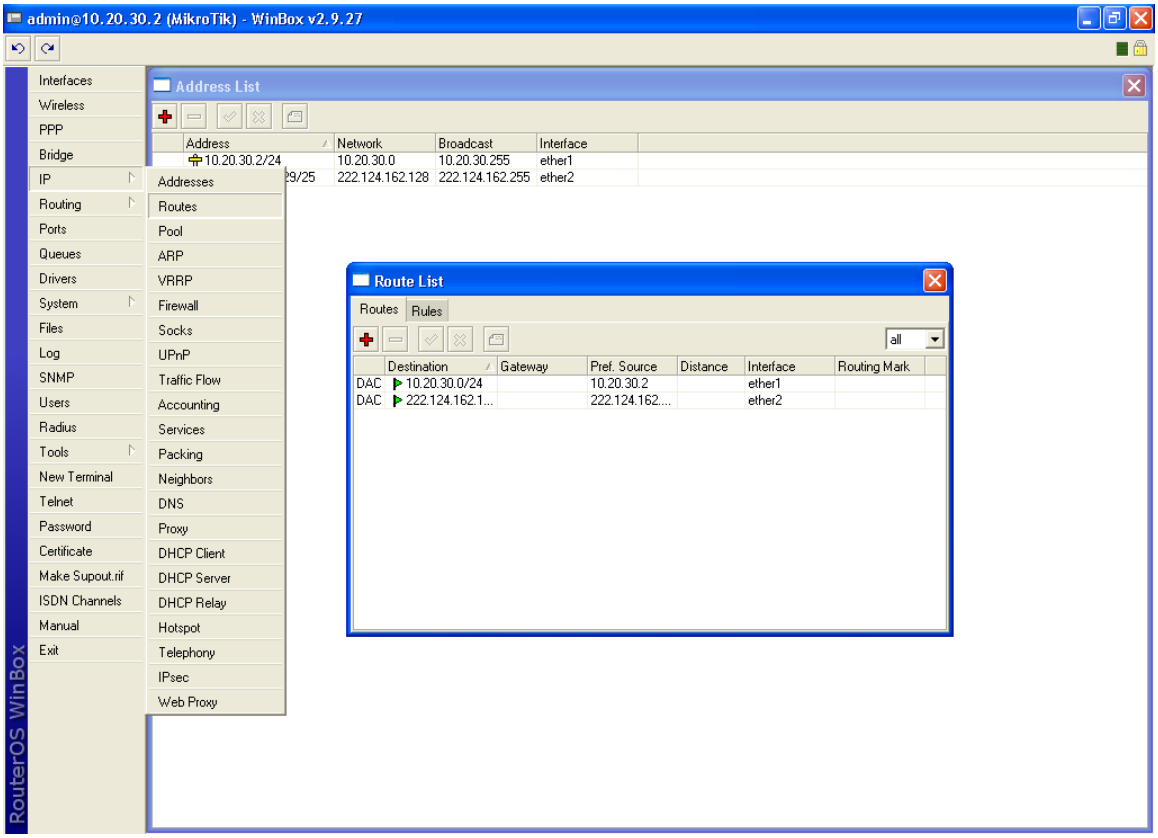
mawaridz@gmail.com

Setelah ip sudah di setting maka di daftar ip muncul nomor ip nya



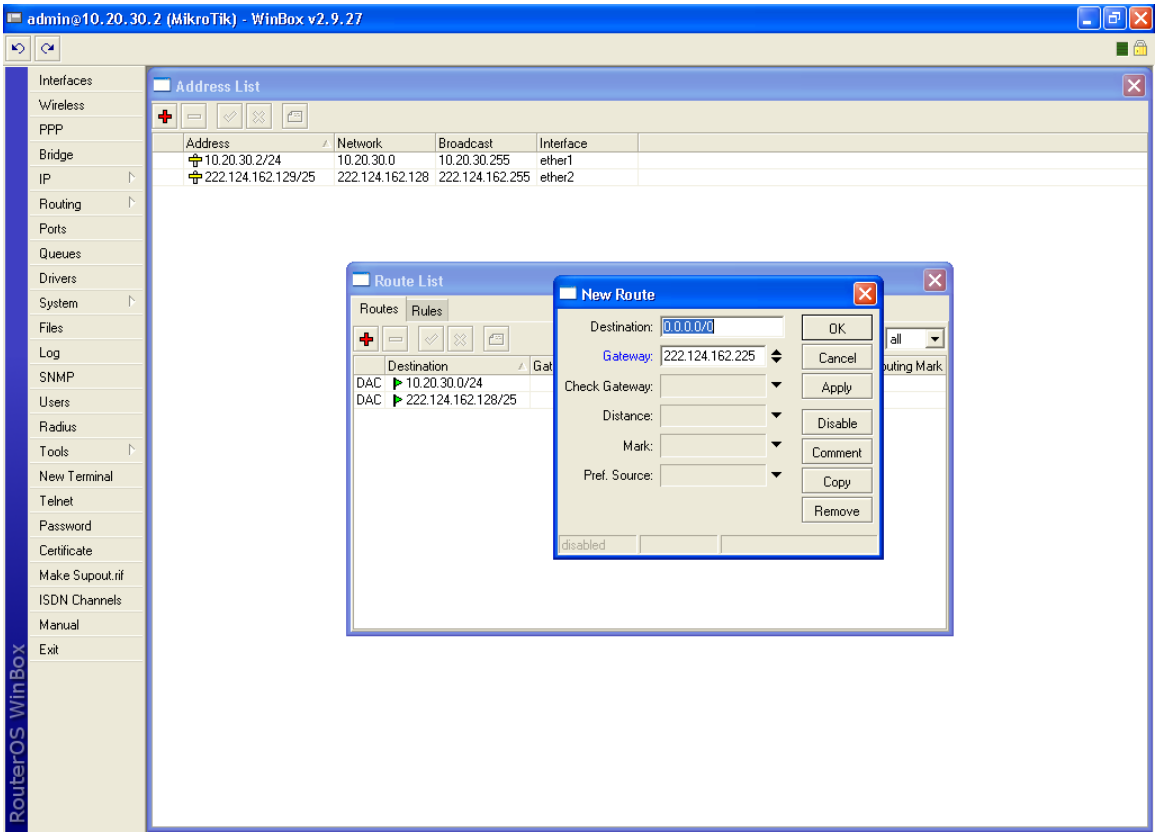
Langkah selanjutnya adalah menentukan default gatewaynya, yaitu melalui menu **ip ▪ Routes** , kemudian akan ditampilkan windows seperti di bawah untuk menambahkan default gateway dengan klik tombol +

mawaridz@gmail.com



Akan di tampilkan windows seperti dibawah

mawaridz@gmail.com



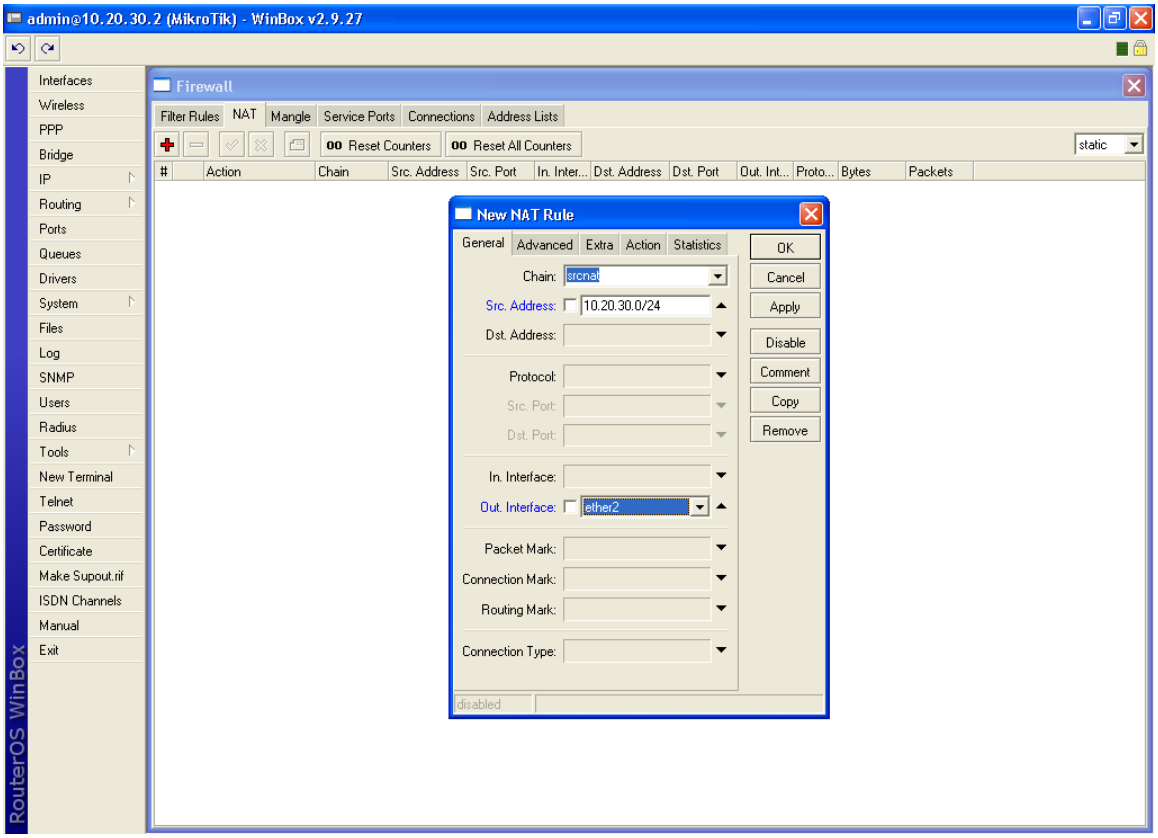
Isi di bagian **Gateway** dengan ip address default gatewaynya. Bagian **Destination** di isi 0.0.0.0/0 yang berarti semua routing di arahkan ke ip gatewaynya.

Setelah ip dan gateway terpasang tinggal pengetesan dengan ping gateway apabila sudah ping reply berarti sampai bagian ini sudah benar, tinggal membuat setting agar pc dari LAN lokal bisa terkonek.

Kita perlu membuat NAT dengan cara klik **ip** ▪ **Firewall** ▪ **NAT** , untuk menambah setting NAT tekan tombol +.

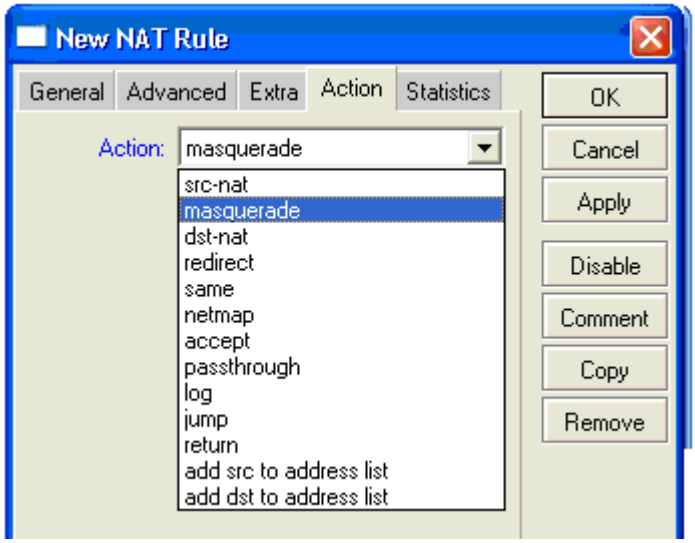
Kemudian bagian **Src. Adress** disini netwok LAN Local yang akan di NAT-kan. Bagian **Out. Interface** diisi ethernet dengan ip address yang berada di luar network LAN.

mawaridz@gmail.com



Pada Tab **Action**, di bagian **Action** diisi dengan **Masquerade**.

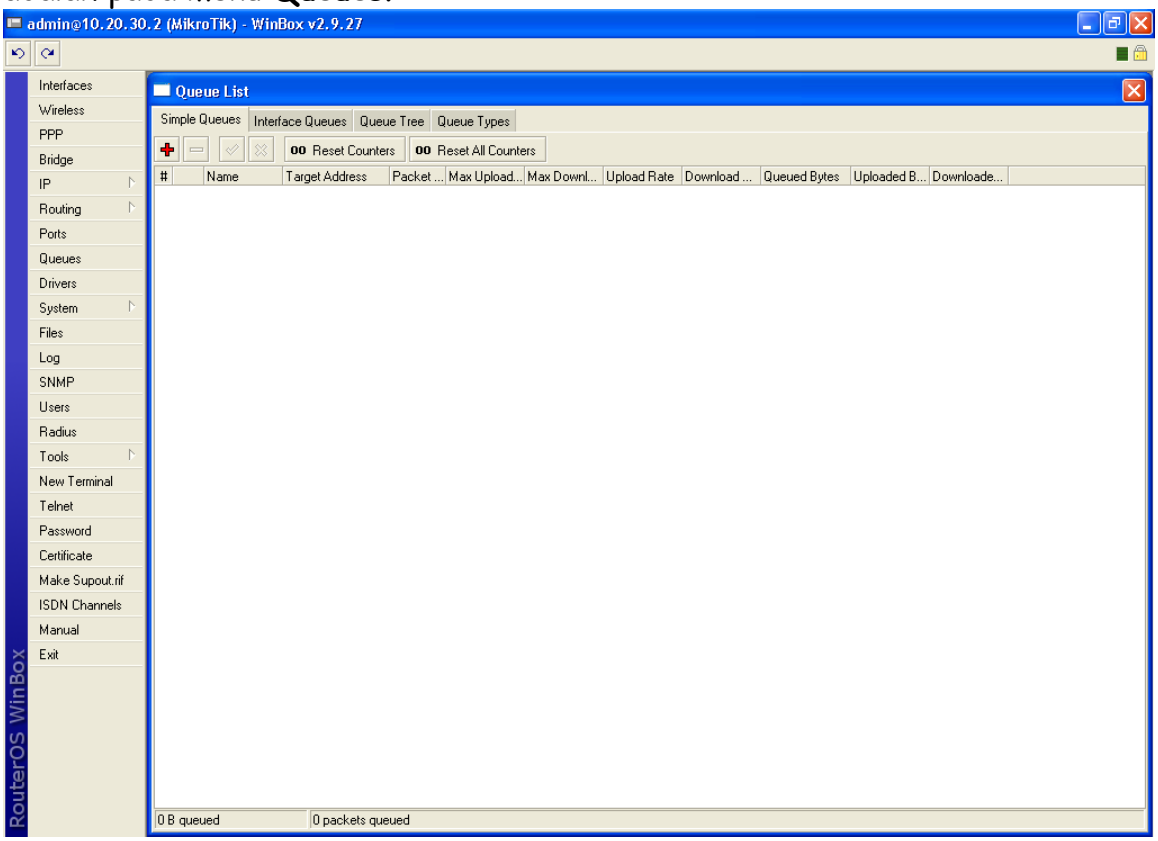
Kemudian tekan tombol OK . Maka setting NAT akan di tampilkan pada windows Firewall.



Setelah setting NAT udah OK, maka dari LAN internal sudah bisa terkoneksi dengan LAN lain melaui router ini.

mawaridz@gmail.com

Langkah selanjutnya adalah pengaturan bandwidth. Menu untuk mengatur bandwidth adalah pada menu **Queues**.



Ada beberapa Tab pada windows Queues List :

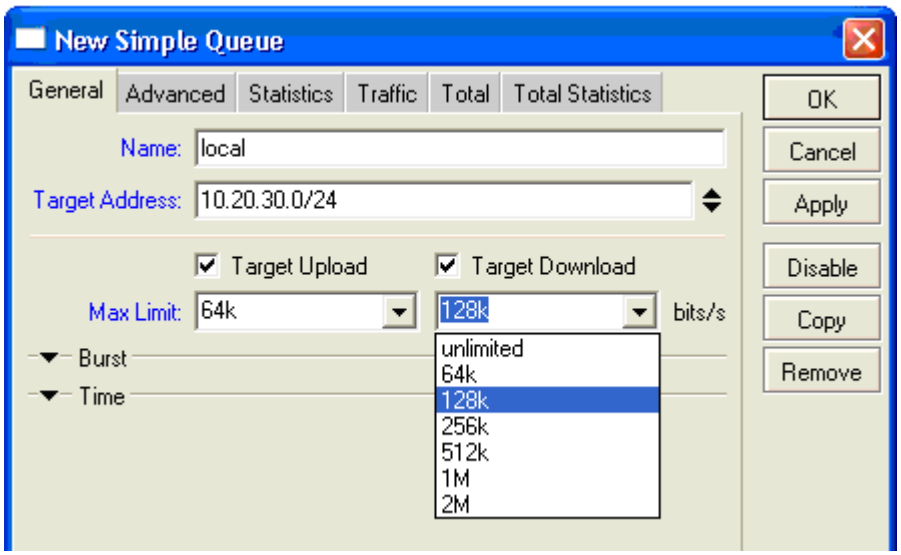
- **Simple Queues**

  Pada bagian ini pengaturan bandwidth dengan ketentuan yang sederhana dan besarnya bandwidth fix (64k, 128k, 256k, 512k, 1M dan 2M).

  Bagian Target Address di isi ip host atau network yang berada di bawah router ini yang akan di batasi penggunaan bandwidthnya.

  Di Tab Advanced, bisa di gunakan untuk membatasi bandwidth yang di gunakan oleh p2p program seperti emule, edonkey dll

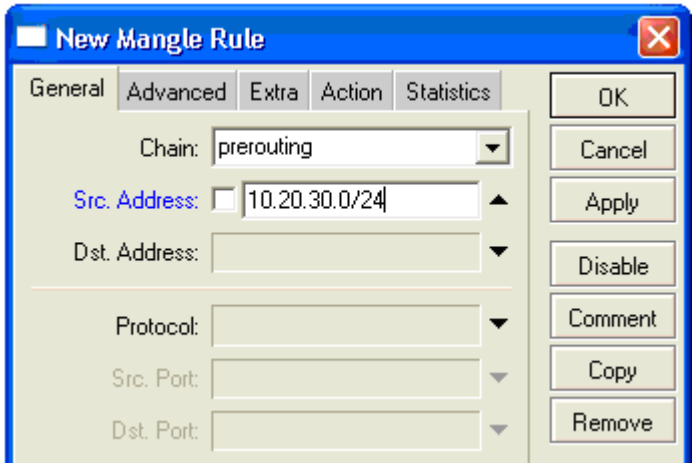
mawaridz@gmail.com

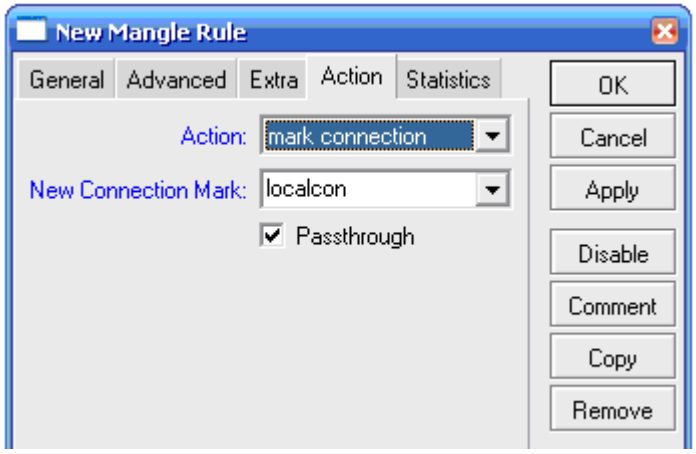


- **Queue Tree**

  Sebelum membuat Queue Tree perlu terlebih dahulu kita membuat mangle di menu Firewall. Yang perlu di buat ada dua macam : mark connection dan mark packet.

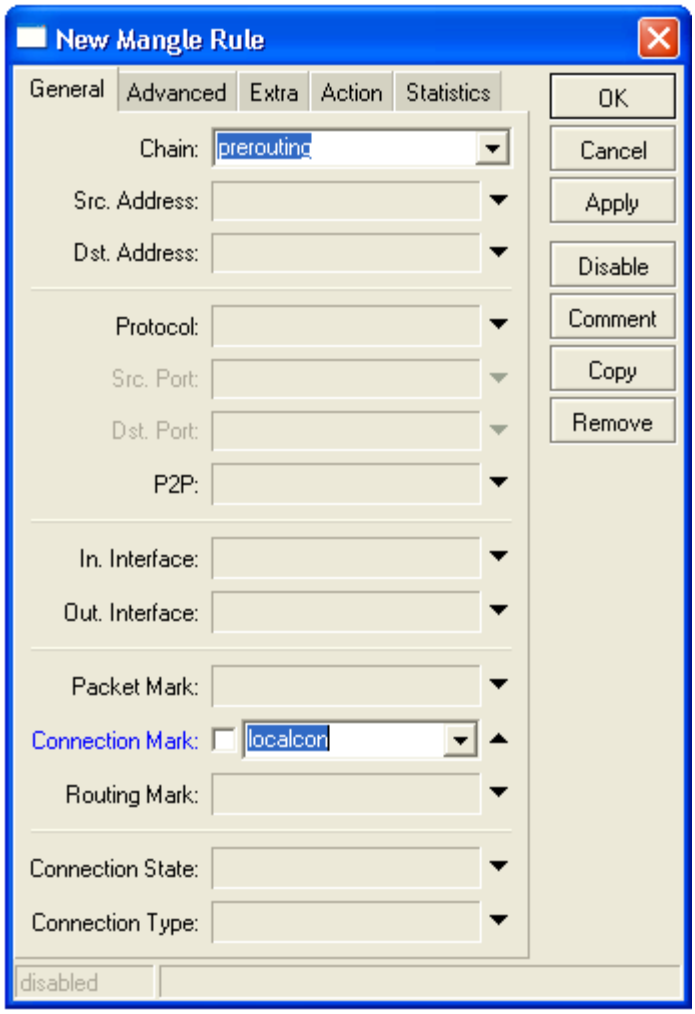
  Membuat Mark Connection : **Menu IP ▪ Firewall ▪ Mangle ▪ +**

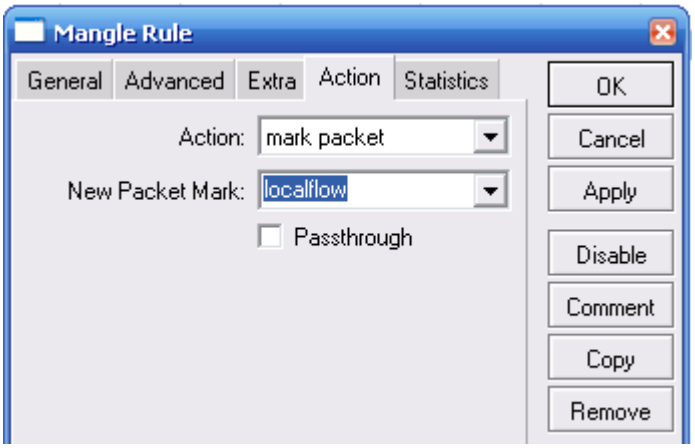




mawaridz@gmail.com

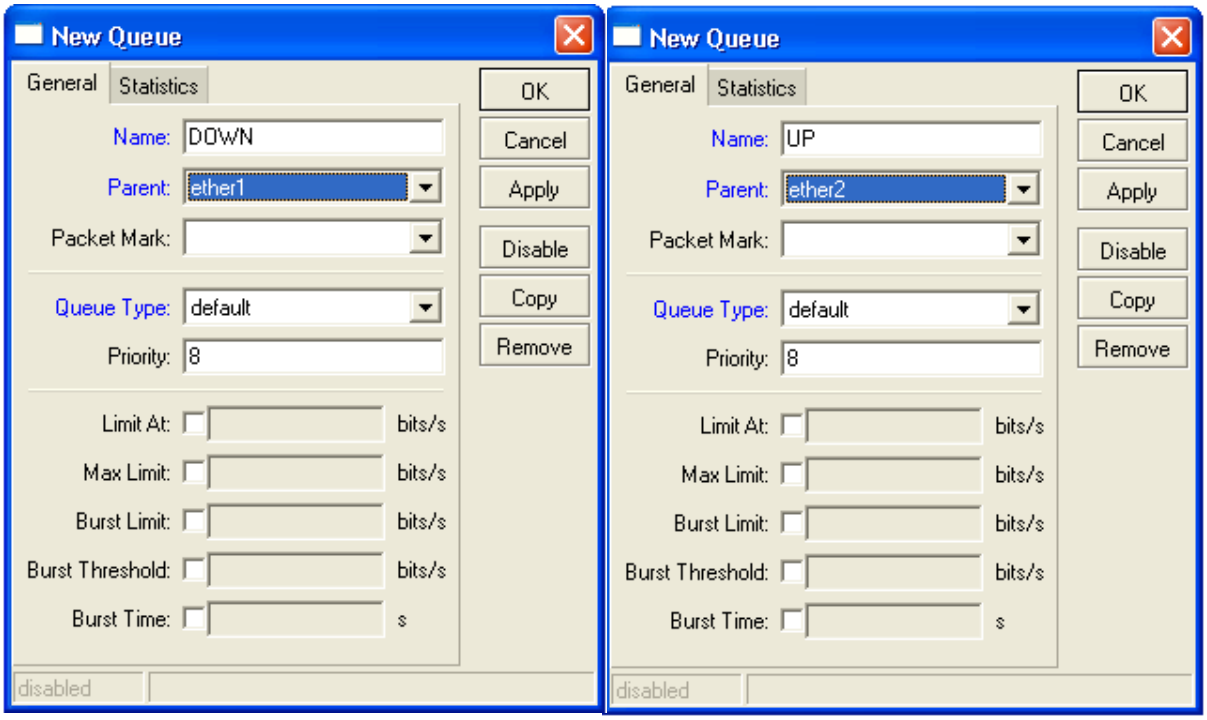
Membuat Mark Packet : **Menu IP ▪ Firewall ▪ Mangle ▪ +**



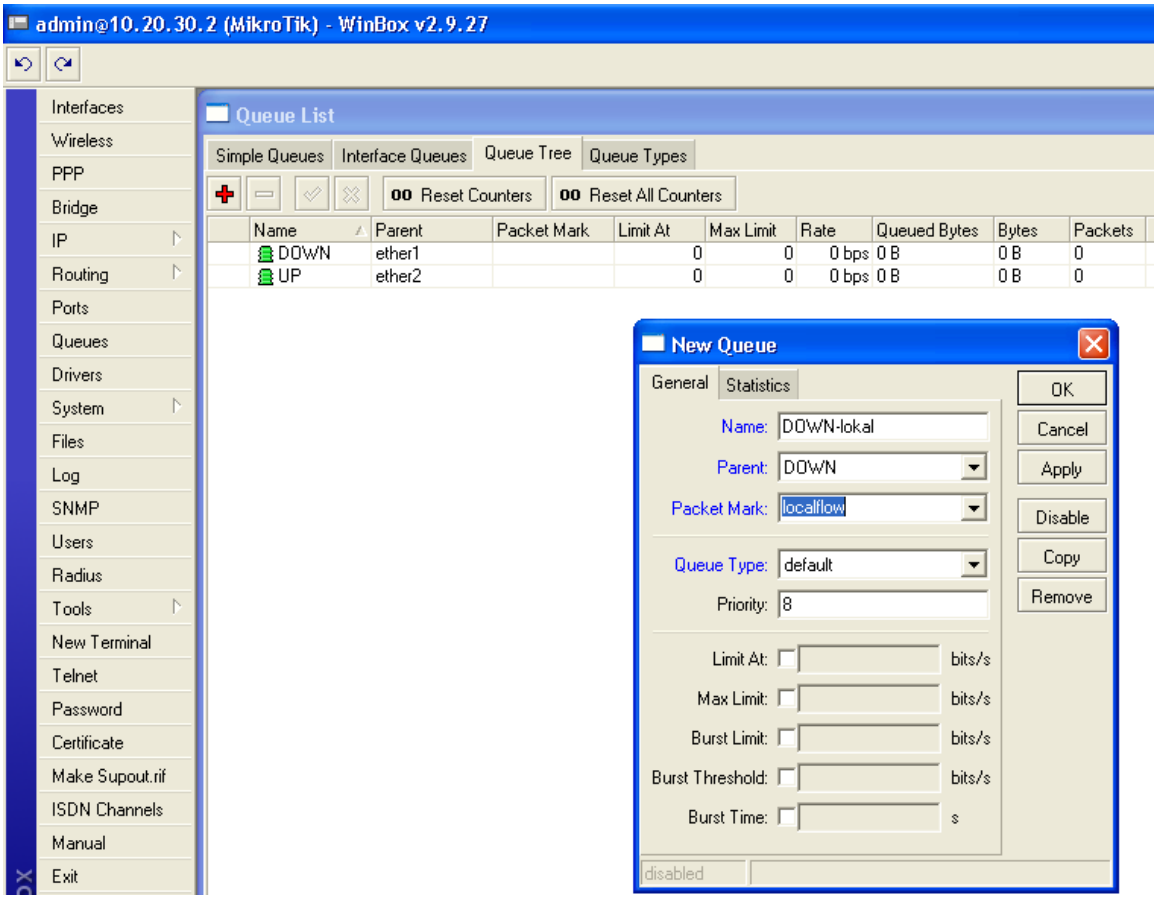


Setelah Marck Connection dan Mark Packet dibuat kemudian kita mulai membuat Queue Tree dengan terlabih dahulu menentukan Parent untuk download dan parent

untuk Upload. Pada parent ini bisa langsung di setting besarnya bandwidth yang dialokasikan pada bagian **Limit At** dan **Max Limit**

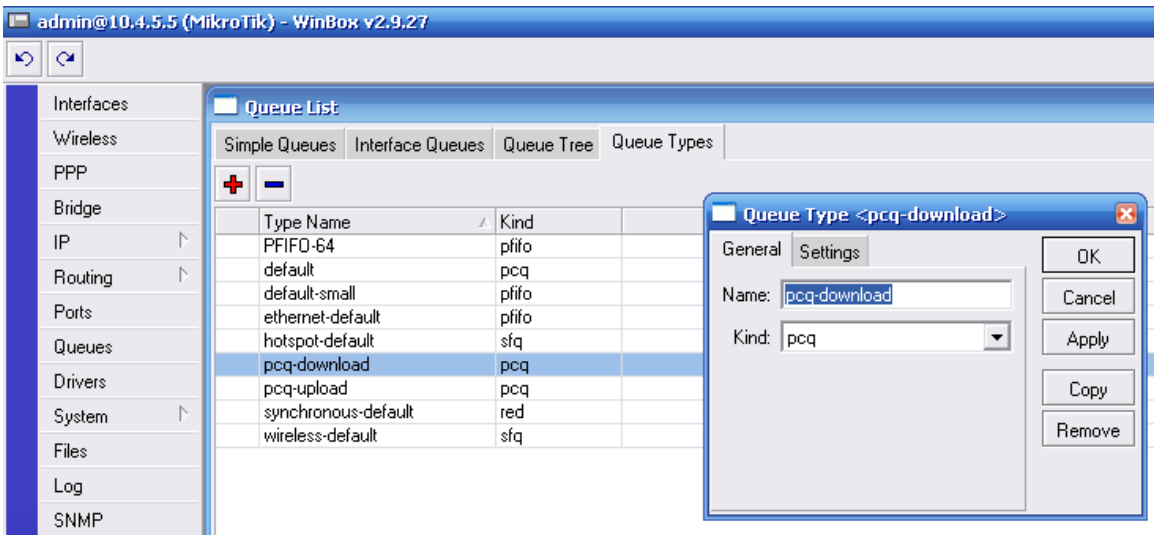


Setelah dibuat parent baru membuat child yang ada di bawah parent tersebut

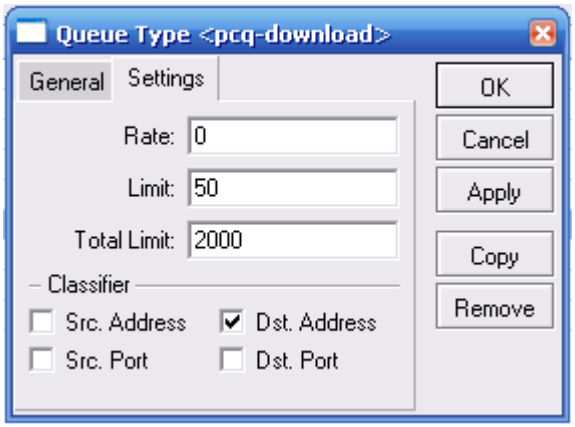


- **Queue Type**

  Queue type adalah digunakan untuk mengatur type pembatasan bandwidth yang digunakan, khusus untuk pembagian bandwidth agar pembagian bisa merata di gunakan type **pcq**. Untuk menambahkan type baru dengan cara klik tombol +



Bagian **Name** adalah untuk memberi nama type queue yang baru, sedangkan bagian **Kind** type yang mau di pakai.
Tab **Setting** digunakan untuk mengatur bentuk distribusi paket yang akan di atur oleh type queue.

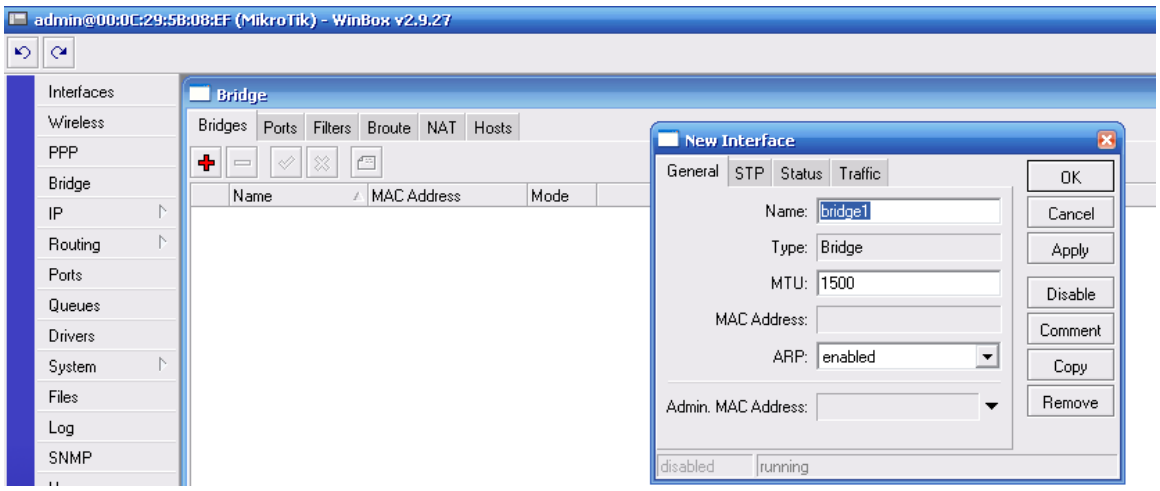


mawaridz@gmail.com

Mikrotik sebagai Bridge

Untuk instalasi awal Mikrotik sama dengan sebagai router, yang berbeda adalah kebutuhan ethernet. Khusus sebagai bridge di butuhkan 3 buah ethernet, 2 digunakan sebagai fungsi bridge dan 1 ethernet digunakan sebagai management system Mikrotiknya.

Untuk mensetting melauli menu **Bridge** , kemudian akan muncul windows awal setting bridge. Pertama kali kita perlu mendefinisikan awal nama bridgenya dengan cara klik tombol + pada Tab **Bridges**

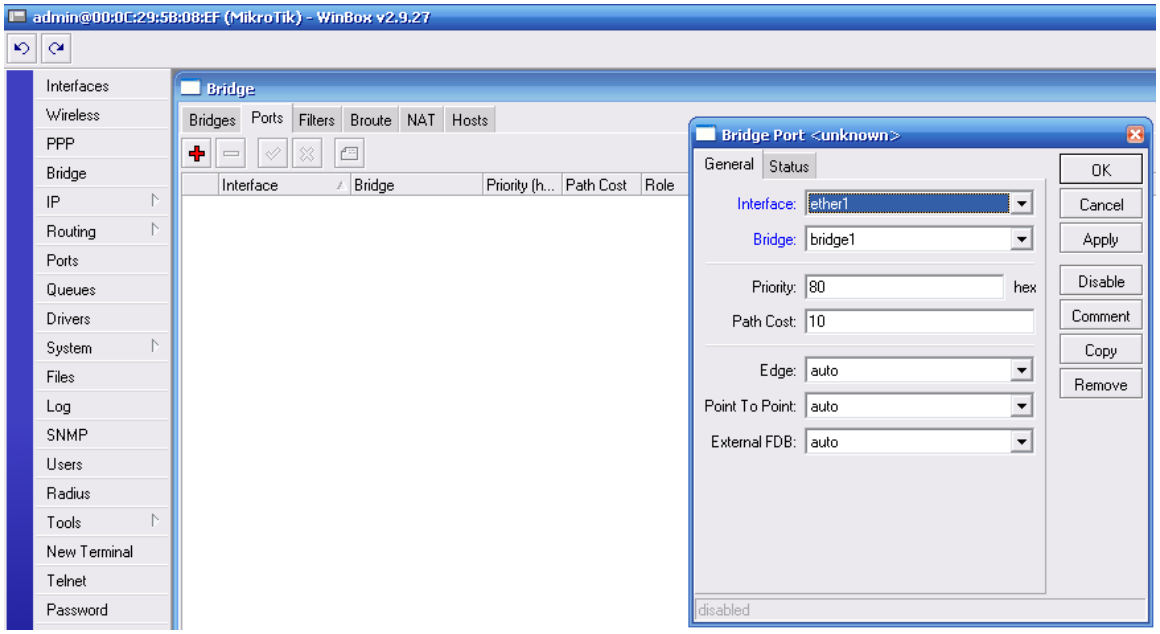


Pada bagian ini kita tidak perlu mengubah setting yang secara default di berikan oleh Mikrotik, cukup klik tombol OK.

Kemudian kita ke Tab **Ports** , di bagian ini kita mendefinisikan ethernet mana saja yang akan di jadikan sebagai interface bridge.
Seperti biasa untuk menambahkan 2 Ports dengan klik tombol + dua kali, kemudian yang perlu di ubah hanya dibagian **Interface** saja.

Proses membuat Mikrotik sebagai Bridge sudah selesai. Untuk setting pembagi bandwidth sama dengan sewaktu sebagai router.

mawaridz@gmail.com



mawaridz@gmail.com

Kumpulan Artikel Jaringan dan Mikrotik

Kumpulan Istilah dan Pengertian Dalam Jaringan Komputer

==========

Istilah Internet Indonesia adalah istilh-istilah yang disierap dari bahsa asing karena kemajuan

teknologi internet. Mayoritas istilah-istilah tersebut adalah berasal dari bahasa Inggris Amerika,

karena dipandang memiliki kekayaan kosakta internet yang paling luas.

Berikut ini adalah istilah-istilah internet yang diserap dari bahasa asing:

ADN - Advanced Digital Network. Biasanya merujuk kepada saluran leased line

A berkecepatan 56Kbps.

ADSL - Asymetric Digital Subscriber Line. Sebuah tipe DSL dimana upstream dan downstream

berjalan pada kecepatan yang berbeda. Dalam hal ini, downstream biasanya lebih tinggi.. Secara

teori, ASDL dapat melayani kecepatan hingga 9 mbps untuk downstream dan 540 kbps untuk

upstream.

Anonymous FTP - Situs FTP yang dapat diakses tanpa harus memiliki login tertentu. Aturan

standar dalam mengakses Anonymous FTP adalah dengan mengisikan "Anonymous" pada isian

Username dan alamat email sebagai password.

ARPANet - Advanced Research Projects Agency Network. Jaringan yang menjadi cikal-bakal

terbentuknya Internet. Dibangun pada akhir dasawarsa 60-an hingga awal dasawarsa 70-an oleh

Departemen Pertahanan Amerika Serikat sebagai percobaan untuk membentuk sebuah jaringan

berskala besar (WAN).

Arsitektur - jaringan dapat diklasifikasikan ke dalam arsitektur peer-to-peer atau client/server..

ASCII - American Standard Code for Information Interchange. Standar yang berlaku di seluruh

dunia untuk kode berupa angka yang merepresentasikan karakter-karakter, baik huruf, angka,

maupun simbol yang digunakan oleh komputer. Terdapat 128 karakter standar ASCII yang masing-

masing direpresentasikan oleh tujuh digit bilangan biner mulai dari 0000000 hingga 1111111.

Backbone - Jalur berkecepatan tinggi atau satu seri koneksi yang menjadi jalur utama dalam

B sebuah network.

Backup - Salingan dari sebuh file yang dibuat untuk memstikan bahwa jika file orisinil rusah atau

dihncurka, maka yang hilang akn diminimalkan dan kebanyakan tidak semua data bisa diperbaiki.

Secara khusus, backup dibuat dalm interval reguler, yang disimpan di media yang dapat

dipindahkan, misalnya disk Zip dan diletakkan di lokasi yang terpisah dari komputer.

Bandwidth - Besaran yang menunjukkan seberapa banyak data yang dapat dilewatkan dalam

koneksi melalui sebuah network.

Binary - Biner. Yaitu informasi yang seluruhnya tersusun atas 0 dan 1. Istilah ini biasanya merujuk

pada file yang bukan berformat teks, seperti halnya file grafis.

Bit - BInary digiT. Satuan terkecil dalam komputasi, terdiri dari sebuah besaran yang memiliki nilai

antara 0 atau 1.

Bps - Bit Per Seconds. Ukuran yang menyatakan seberapa cepat data dipindahkan dari satu tempat

ke tempat lain.

mawaridz@gmail.com

Browser - Sebutan untuk perangkat lunak (software) yang digunakan untuk mengakses World Wide

Web.

Bridge - adalah peranti yang meneruskan lalu lintas antara segmen jaringan berdasar informasi

pada lapisan data link. Segmen ini mempunyai alamat lapisan jaringan yang sama. Setiap jaringan

seharusnya hanya mempunyai sebuah bridge utama.

Broadband connection - jenis kabel internet yang relatig cepat, selalu aktif dan cocok untuk

mempertukarkan file-file besar, misalnya grafis, video, atau musik melalui internet.

Byte - Sekumpulan bit yang merepresentasikan sebuah karakter tunggal. Biasanya 1 byte akan

terdiri dari 8 bit, namun bisa juga lebih, tergantung besaran yang digunakan.

Cable – Jenis Koneksi broadband yang populer yang memakai saluran televisi kabel yang

C sudah ada untuk berhubungan ke internet. Ini membutuhkan modem khusus dan tidak

mengganggu siaran TV.

CGI - Common Gateway Interface. Sekumpulan aturan yang mengarahkan bagaimana sebuah

server web berkomunikasi dengan sebagian software dalam mesin yang sama dan bagaimana

sebagian dari software (CGI Program) berkomunikasi dengan server web.

cgi-bin - Nama yang umum digunakan untuk direktori di server web dimana program CGI

disimpan.

Chat - Secara harfiah, chat dapat diartikan sebagai obrolan, namun dalam dunia internet, istilah ini

merujuk pada kegiatan komunikasi melalui sarana baris-baris tulisan singkat yang diketikkan

melalui keyboard

Coaxial – Jenis kabel yang terdiri dari sebuah kabel tembaha yang dikelilingi oleh siolasi dan

pelindung lubang kabel yang dihubungkan dengan tanah

Cookie – Kepingan data kecil yang disimpan pada komputer oleh situs Web. Cookie mengaktifkan

situs Web untuk mengenali kembali para pengunjung dalam menyimpan setting masing-masing

seperti nam logon, pasword.

DHCP - Dynamic Host Control Protocol memungkinkan satu komputer atau peralatan

D jaringan lainnya(seperti router) memberikan serangkaian alamat IP pribadi kita ke PC

yang lain

Dial-up Connection - Suatu jenis koneksi Internet yang memakai saluran telepon untuk

menentukan koneksi. Koneksi ini populer tapi sangat lambat. Komputer menentukan koneksi

internet dengan telepon sebagai modemnya.

DNS - Domain Name Service. Merupakan layanan di Internet untuk jaringan yang menggunakan

TCP/IP. Layanan ini digunakan untuk mengidentifikasi sebuah komputer dengan nama bukan

dengan menggunakan alamat IP (IP address). Singkatnya DNS melakukan konversi dari nama ke

angka. DNS dilakukan secara desentralisasi, dimana setiap daerah atau tingkat organisasi memiliki

domain sendiri. Masing-masing memberikan servis DNS untuk domain yang dikelola.

DSS – Digital Satelleite System. Jenis dial-up connection yang memakai piting satelit untuk men-

download informsi dari internet. Koneksi ini cepat tapi hanya satu arah, maka harus menentukan

dial up connection lewat saluran telepon untuk memulai internet.

DSL - Digital Subscriber Line. Sebuah metode transfer data melalui saluran telepon reguler. Sirkuit

DSL dikonfigurasikan untuk menghubungkan dua lokasi yang spesifik, seperti halnya pada sambungan Leased Line (DSL berbeda dengan Leased Line). Koneksi melalui DSL jauh lebih cepat dibandingkan dengan koneksi melalui saluran telepon reguler walaupun keduanya sama-sama menggunakan kabel tembaga. DSL menawarkan alternatif yang lebih murah dibandingkan dengan ISDN..

Download - Istilah untuk kegiatan menyalin data (biasanya berupa file) dari sebuah komputer yang terhubung dalam sebuah network ke komputer lokal. Proses download merupakan kebalikan dari upload.

Downstream - Istilah yang merujuk kepada kecepatan aliran data dari komputer lain ke komputer lokal melalui sebuah network. Istilah ini merupakan kebalikan dari upstream.

Email - Electronic Mail. Pesan, biasanya berupa teks, yang dikirimkan dari satu alamat ke E alamat lain di jaringan internet. Sebuah alamat email yang mewakili banyak alamat email sekaligus disebut sebagai mailing list. Sebuah alamat email biasanya memiliki format semacam username@host.domain, misalnya: myname@mydomain.com.

Ethernet - Ethernet adalah protokol LAN yang dikembangkan oleh Xerox Corporation yang bekerjasama dengan DEC dan Intel pada tahun 1976. Ethernet menggunakan topologi bus atau star dan medukung transfer data sampai dengan 10 Mbps. Versi terbarunya, Gigabit Ethernet, mendukung tranfer data sampai dengan 1 Gigabit per detik atau 1000 Mbps.

Ethernet Crossover Cable – Jenis kabel ethernet khusus yang membolehkan dua koputer berhubungan satu sama lain secara langsung melalui adapter jaringan Ethernetnya.

Fast Ethernet - Fast Ethernet seperti Ethernet biasa, namun dengan kecepatan

transfer data

F yang lebih cepat, sampai dengan 100 mbps. Ethernet ini juga disebut 100BaseT.

Firewall - Kombinasi dari hardware maupun software yang memisahkan sebuah network menjadi

dua atau lebih bagian untuk alasan keamanan.

First-party cookie - Cookie yang diletakkan pada komputer oleh situs Web yang sedang

dikunjungi.

File server - Sebuh komputer pada suatu jaringan yang menyediakan lokasi senteral untkk

menyimpan file sehingga semua komputer lain pada jaringan bisa mengaksesnya.

FTP - File Transfer Protocol. Protokol standar untuk kegiatan lalu-lintas file (upload maupun

download) antara dua komputer yang terhubung dengan jaringan internet. Sebagian sistem FTP

mensyaratkan untuk diakses hanya oleh mereka yang memiliki hak untuk itu dengan mengguinakan

login tertentu. Sebagian lagi dapat diakses oleh publik secara anonim. Situs FTP semacam ini

disebut Anonymous FTP.

Gateway - Dalam pengertian teknis, istilah ini mengacu pada pengaturan hardware maupun

G software yang menterjemahkan antara dua protokol yang berbeda. Pengertian yang lebih

umum untuk istilah ini adalah sebuah mekanisme yang menyediakan akses ke sebuah sistem

lain yang terhubung dalam sebuah network

GPRS - General Packet Radio Service. Salah satu standar komunikasi wireless (nirkabel).

Dibandingkan dengan protokol WAP, GPRS memiliki kelebihan dalam kecepatannya yang dapat

mencapai 115 kbps dan adanya dukungan aplikasi yang lebih luas, termasuk aplikasi grafis dan

multimedia.

mawaridz@gmail.com

GPS - Global Positioning System adalah sistem navigasi menggunakan 24 satelit MEO (medium

earth orbit atau middle earth orbit) yang mengelilingi bumi dan penerima-penerima di bumi.

Guest computer - Sebuah komputer yang menerima koneksi dari komputer lain, yang ditunjuk

sebagai host computer.

Home Page/Homepage - Halaman muka dari sebuah situs web. Pengertian lainnya adalah

H halaman default yang diset untuk sebuah browser.

Host - Sebuah komputer dalam sebuah network yang menyediakan layanan untuk komputer lainnya

yang tersambung dalam network yang sama.

HTML - Hypertext Markup Language, merupakan salah satu varian dari SGML yang dipergunakan

dalam pertukaran dokumen melalui protokol HTTP.

HTTP - Hyper Text Transfer Protocol. Protokol yang didisain untuk mentransfer dokumen HTML

yang digunakan dalam World Wide Web.

HTTPD - Lihat World Wide Web

IEEE - Institute of Electrical and Electronics Engineers, Inc. Suatu organisasi profesional

I teknik yang mengembangkan standar-standar di bidang teknologi elektronika

IMAP - Internet Message Access Protocol. Protokol yang didisain untuk mengakses e-mail.

protokol lainnya yang sering digunakan adalah POP

Internet - Sejumlah besar network yang membentuk jaringan inter-koneksi (Inter-connected

network) yang terhubung melalui protokol TCP/IP. Internet merupakan kelanjutan dari ARPANet

dan kemungkinan merupakan jaringan WAN yang terbesar yang ada saat ini.

mawaridz@gmail.com

Internet surfing - Pemakaian browser Web Anda untuk melihat informasi yang disimpan pada

banyak komputer berbeda di Internet. Informasi diakses melalui pages yang dikelola sebagai Web

sites

Intranet - Sebuah jaringan privat dengan sistem dan hirarki yang sama dengan internet namun tidak

terhubung dengan jaringan internet dan hanya digunakan secar internal.

Industry Standard Architecture (ISA) slot - Ruang di dalam sebuah komputer untuk menginstal

perluasan card, misalnya adapter jaringan. ISA slot biasanya berwarna hitam dan umumnya

ditemukan hanya di dalam komputer-komputer yang sudah kuno.

Instant communication - Perluasan penyampaian pesan instan dari teks ke modus komunikasi lain,

seperti suara dan video. PC berkemampuan multimedia yang menyertakan speaker, mikrofon, atau

headset, bisa menghasilkan suara; kamera Web bisa menghasilkan video

IP Address - Alamat IP (Internet Protocol), yaitu sistem pengalamatan di network yang

direpresentasikan dengan sederetan angka berupa kombinasi 4 deret bilangan antara 0 s/d 255 yang

masing-masing dipisahkan oleh tanda titik (.), mulai dari 0.0.0.1 hingga 255.255.255.255.

IPX/SPX - Jenis protocol komunikasi yang dipakai oleh komputer-komputer untuk berkomunikasi

satu sama lain pada suatu jaringan. Kebanyakan jaringan lebih menyukai TCP/IP ketimbang

SPX/IPX, karena TCP/IP adalah protocol yang dipakai di Internet

ISDN - Integrated Services Digital Network. Pada dasarnya, ISDN merupakan merupakan jalan

untuk melayani transfer data dengan kecepatan lebih tinggi melalui saluran telepon reguler. ISDN

memungkinkan kecepatan transfer data hingga 128.000 bps (bit per detik). Tidak seperti

DSL,

ISDN dapat dikoneksikan dengan lokasi lain seperti halnya saluran telepon, sepanjang lokasi

tersebut juga terhubung dengan jaringan ISDN.

ISP - Internet Service Provider. Sebutan untuk penyedia layanan internet.

LAN - local-area network. Komputer yang terhubung berada pada tempat yang berdekatan

L secara gografis (misalkan satu gedung).

Leased Line - Saluran telepon atau kabel fiber optik yang disewa untuk penggunaan selama 24

jam sehari untuk menghubungkan satu lokasi ke lokasi lainnya. Internet berkecepatan tinggi

biasanya menggunakan saluran ini.

Login - Pengenal untuk mengakses sebuah sistem yang tertutup, terdiri dari username (juga disebut

login name) dan password (kata kunci).

Mailing List - Juga sering diistilahkan sebagai milis, yaitu sebuah alamat email yang

M digunakan oleh sekelompok pengguna internet untuk melakukan kegiatan tukar menukar

informasi.

Mapping - Pemberian sebuah huruf drive ke suatu folder di jaringan sehingga huruf drive itu

muncul di jendela My Computer

Mbps - megabyte per second. Ukuran bandwidth, atau aliran komunikasi, melalui suatu

jaringan atau media komunikasi lain

MIME - Multi Purpose Internet Mail Extensions. Ekstensi email yang diciptakan untuk

mempermudah pengiriman berkas melalui attachment pada email

MTA - Mail Transport Agent. Perangkat lunak yang bekerja mengantarkan e-mail kepada user.

Adapun program untuk membaca e-mail dikenal dengan istilah MUA (Mail User Agent).

MUA - Lihat MTA.

Network - adalah sekumpulan dua atau lebih sistem komputer yang digandeng dan

N membentuk sebuah jaringan. Internet sebenarnya adalah sebuah network dengan skala

yang sangat besar.

Network bridge - Bagian dari device hardware atau software yang membuat koneksi di antara

jenis-jenis media jaringan yang berbeda. Windows XP menyediakan software network bridge yang

mudah di-setup.

Network card - Papan sirkuit komputer yang diinstal di sebuah komputer untuk mengizinkan

komputer berhubungan ke jaringan.

Network hub - Jenis hardware tempat kabel masuk dari banyak komputer dan data dipertukarkan

serta dikirimkan ke komputer-komputer lain di jaringan.

NNTP - Network News Transfer Protocol. protokol yang digunakan untuk mengakses atau transfer

artikel yang diposkan di Usenet news. Program pembaca news (news reader) menggunakan

protokol ini untuk mengakses news.

Node - Suatu komputer tunggal yang tersambung dalam sebuah network.

Packet Switching - Sebuah metode yang digunakan untuk memindahkan data dalam

P jaringan internet. Dalam packet switching, seluruh paket data yang dikirim dari sebuah node

akan dipecah menjadi beberapa bagian. Setiap bagian memiliki keterangan mengenai asal

dan tujuan dari paket data tersebut.

Parallel - Jenis komunikasi yang mentransmisikan data secara serentak melalui kawat yang

dihubungkan secara paralel.

PERL - Sebuah bahasa pemrograman yang dikembangkan oleh Larry Wall yang sering

dipakai

untuk mengimplementasikan script CGI di World Wide Web. Bahasa Perl diimplementasikan dalam

sebuah interpreter yang tersedia untuk berbagai macam sistem operasi, diantaranya Windows, Unix

hingga Macintosh.

Platform for Privacy Preferences (P3P) - Standar Internet yang terbukti didesain untuk

memudahkan bagi situs Web mengiklankan kebijaksanaan privasinya dan bagi para pemakai

menentukan preferensi privasinya.

POP - Post Office Protocol. Protokol standar yang digunakan untuk mengambil atau membaca

email dari sebuah server. protokol POP yang terakhir dan paling populer digunakan adalah POP3.

protokol lain yang juga sering digunakan adalah IMAP. Adapun untuk mengirim email ke sebuah

server digunakan protokol SMTP.

Port - Titik koneksi pada sebuah komputer yang datanya bisa diberikan dan diambil. Beberapa port

berbentuk fisik, misalnya port TCP/IP yang dipakai sebuah komputer untuk berkomunikasi dengan

komputer-komputer lain di Internet.

PPP - Point to Point Protocol. Sebuah protokol TCP/IP yang umum digunakan untuk

mengkoneksikan sebuah komputer ke internet melalui saluran telepon dan modem.

Protokol - Protocol. Seperangkat aturan yang mengatur secara tepat format komunikasi antar

sistem. Sebagai contoh, protokol HTTP mengatur format komunikasi antara browser web dan

browser server. Protokol IMAP mengatur format komunikasi antara server email IMAP dengan

klien.

PSTN - Public Switched Telephone Network. Sebutan untuk saluran telepon konvensional yang

menggunakan kabel.

Repeater - Suatu perangkat yang dipasang di titik-titik tertentu dalam jaringan untuk

R memperbarui sinyal-sinyal yang di transmisikan agar mencapai kembali kekuatan dan

bentuknya yang semula, guna memperpanjang jarak yang dapat di tempuh. Ini di perlukan

karena sinyal-sinyal mengalami perlemahan dan perubahan bentuk selama transmisi.

RFC - Request For Comments. Sebutan untuk hasil dan proses untuk menciptakan sebuah standar

dalam internet. Sebuah standar baru diusulkan dan dipublikasikan di internet sebagai sebuah

Request For Comments. Apabila standar tersebut kemudian diaplikasikan, maka ia akan tetap

disebut sebagai RFC dengan referensi berupa nomor atau nama tertentu, misalnya standar format

untuk email adalah RFC 822.

RJ-11 - Stopkontak modul standar yang dipakai untuk koneksi telepon. RJ-11 bisa mencapai enam

pin tetapi biasanya hanya memakai empat pin.

RJ-45 connector - Stopkontak modul standar yang dipakai untuk jaringan Ethernet. RJ-45

connector mempunyai delapan pin, yang kadang-kadang dinamakan position

Router - Sebuah komputer atau paket software yang dikhususkan untuk menangani koneksi antara

dua atau lebih network yang terhubung melalui packet switching. Router bekerja dengan melihat

alamat tujuan dan alamat asal dari paket data yang melewatinya dan memutuskan rute yang harus

digunakan oleh paket data tersebut untuk sampai ke tujuan.

Routing - Proses dari penentuan sebuah path yang di pakai untuk mengirim data ke tujuan

tertentu.

SDSL - Symmetric Digital Subscriber Line. Salah satu tipe DSL yang memungkinkan S transfer data untuk upstream maupun downstream berjalan pada kecepatan yang sama.

SDSL umumnya berkerja pada kecepatan 384 kbps (kilobit per detik).

Serial - Jenis komunikasi yang mentransmisikan data secara berurutan, satu bit pada suatu waktu,

melalui kabel tunggal. Pada umumnya komunikasi serial agak lambat dibanding komunikasi

paralel.

Server - Suatu unit yang berfungsi untuk menyimpan informasi dan untuk mengelola suatu jaringan

komputer.komputer server akan melayani seluruh client atau workstation yang terhubung ke

jaringannya.

SGML - Standard Generalized Markup Language. Nama populer dari ISO Standard 8879 (tahun

1986) yang merupakan standar ISO (International Organization for Standarization) untuk

pertukaran dokumen secara elektronik dalam bentuk hypertext

SMTP - Simple Mail Transfer Protocol. Protokol standar yang digunakan untuk mengirimkan email

ke sebuah server di jaringan internet. Untuk keperluan pengambilan email, digunakan protokol POP.

SSH - Secure Shell. Protokol pengganti Telnet yang memungkinkan akses yang lebih secure ke

remote-host.

Streaming - Suatu metode mengirimkan isi yang di dalamnya isi diletakkan di sebuah server yang

ditransmisikan melalui suatu jaringan dalam aliran yang terus-menerus, lalu dimainkan oleh

software client.

TCP/IP - Transmission Control Protocol/Internet Protocol. Satu set protokol standar yang

T digunakan untuk menghubungkan jaringan komputer dan mengalamati lalu lintas dalam

jaringan. protokol ini mengatur format data yang diijinkan, penanganan kesalahan (error

handling), lalu lintas pesan, dan standar komunikasi lainnya. TCP/IP harus dapat bekerja diatas

segala jenis komputer, tanpa terpengaruh oleh perbedaan perangkat keras maupun sistem operasi

yang digunakan.

Telnet - Perangkat lunak yang didesain untuk mengakses remote-host dengan terminal yang

berbasis teks, misalnya dengan emulasi VT100. Penggunaan Telnet sangat rawan dari segi sekuriti.

Saat ini penggunaan Telnet telah digantikan oleh protokol SSH dengan tingkat keamanan yang lebih

baik.

Third-party cookie - Cookie yang diletakkan di komputer Anda oleh situs Web selain situs Web

yang sedang Anda kunjungi. Third-party cookie mampu melewati banyak pelindung privasi yang

dipasang ke cookie, yang mengakibatkannya terjadi resiko privasi yang lebih tinggi.

Topologi - pengaturan keterhubungan antar sistem komputer. Terdapat bermacam-macam topologi

seperti bus, star, dan ring.

Twisted Pair – Media yang digunakn pada topologi star. Media ini saat ini paling umum dipakai

karena topologi star paling banyak digunakan.

UDP - User Datagram Protocol. Salah satu protokol untuk keperluan transfer data yang

U merupakan bagian dari TCP/IP. UDP merujuk kepada paket data yang tidak

menyediakan

keterangan mengenai alamat asalnya saat paket data tersebut diterima.

Upload - Kegiatan pengiriman data (berupa file) dari komputer lokal ke komputer lainnya yang

terhubung dalam sebuah network. Kebalikan dari kegiatan ini disebut download.

Upstream - Istilah yang merujuk kepada kecepatan aliran data dari komputer lokal ke komputer

lain yang terhubung melalui sebuah network. Istilah ini merupakan kebalikan dari downstream.

URI - Uniform Resource Identifier. Sebuah alamat yang menunjuk ke sebuah resource di internet.

URI biasanya terdiri dari bagian yang disebut skema (scheme) yang diikuti sebuah alamat. URI

diakses dengan format skema://alamat.resource atau skema:alamat.resource. Misalnya, URI

http://yahoo.com.

URL - Uniform Resource Locator. Istilah ini pada dasarnya sama dengan URI, tetapi istilah URI

lebih banyak digunakan untuk menggantikan URL dalam spesifikasi teknis.

USB port - Interface Plug and Play yang standar di antara sebuah komputer dan device tambahan.

USB port memudahkan untuk menambahkan device ke komputer Anda tanpa harus menambahkan

adapter card atau bahkan menonaktifkan komputer. Anda bisa menambahkan device, misalnya

printer, joystick, mouse, keyboard, dan adapter jaringan.

Usenet - Usenet news, atau dikenal juga dengan nama "Net news", atau "news" saja, merupakan

sebuah buletin board yang sangat besar dan tersebar di seluruh dunia yang dapat digunakan untuk

bertukar artikel. Siapa saja dapat mengakses Usenet news ini dengan program-program tertentu,

yang biasanya disebut newsreader. Akses ke server news dapat dilakukan dengan menggunakan

protokol NNTP atau dengan membaca langsung ke direktori spool untuk news yaitu direktori

dimana artikel berada (cara terakhir ini sudah jarang dilakukan).

UUENCODE - Unix to Unix Encoding. Sebuah metode untuk mengkonfersikan file dalam format

Biner ke ASCII agar dapat dikirimkan melalui email.

VLAN - virtual local-area network adalah jaringan komputer yang seakan terhubung

V menggunakan kabel yang sama meskipun mungkin secara fisik berada pada bagian LAN

yang lain. VLAN dikonfigurasi melalui software dan tidak hardware, yang membuatnya

sangat fleksible.

VOIP - Voice over IP. VoIP adalah suatu mekanisme untuk melakukan pembicaraan telepon (voice)

dengan menumpangkan data dari pembicaraan melalui Internet atau Intranet (yang menggunakan

teknologi IP).

VPN - Virtual Private Network. Istilah ini merujuk pada sebuah network yang sebagian diantaranya

terhubung dengan jaringan internet, namun lalu lintas data yang melalui internet dari network ini

telah mengalami proses enkripsi (pengacakan). Hal ini membuat network ini secara virtual

"tertutup" (private).

VSAT - Very Small Aperture Terminal stasiun bumi yang digunakan pada satelit komunikasi sinyal

data, suara, dan video, kecuali pemancaran televisi. VSAT terdiri dari dua bagian: sebuah

transceiver yang diletakkan ditempat terbuka sehingga dapat secara langsung menerima sinyal dari

satelit dan sebuah piranti yang diletakkan dalam ruangan untuk menghubungkan transceiver dan

piranti komunikasi pengguna akhir(end user), seperti PC. VSAT dapat mengirimkan data sampai

dengan kecepatan 56 Kbps.

WAN - wide-area network. Komputer yang terhubung berada pada tempat yang berjauhan

W dan dihubungkan dengan line telepon atau gelombang radio.

WAP - Wireless Application Protocol. Standar protokol untuk aplikasi wireless (seperti yang

digunakan pada ponsel). WAP bekerja dalam modus teks dengan kecepatan sekitar 9,6 kbps.

Belakangan juga dikembangkan protokol GPRS yang memiliki beberapa kelebihan dibandingkan

WAP.

Webmail - Fasilitas pengiriman, penerimaan, maupun pembacaan email melalui sarana web.

Wi-Fi - Wi-Fi Wireless Fidelity adalah nama dagang resmi untuk IEEE 802.11b yang dibuat oleh

Wireless Ethernet Compatibility Aliance (WECA).

Wireless – Media tanpa kabel untuk mengirimkan data meliankan menggunakan sinyal elektrik

yang dihantrakan udara yang bisa diatangkap melalui ebuah alat.

WML - Wireless Markup Language. Salah satu turunan dari format HTML yang khusus

dikembangkan untuk dipakai pada protokol WAP.

World Wide Web - Sering disingkat sebagai WWW atau "web" saja, yakni sebuah sistem dimana

informasi dalam bentuk teks, gambar, suara, dan lain-lain dipresentasikan dalam bentuk hypertext

dan dapat diakses oleh perangkat lunak yang disebut browser. Informasi di web pada umumnya

ditulis dalam format HTML. Informasi lainnya disajikan dalam bentuk grafis (dalam format GIF,

JPG, PNG), suara (dalam format AU, WAV), dan objek multimedia lainnya (seperti MIDI,

Shockwave, Quicktime Movie, 3D World). WWW dijalankan dalam server yang disebut HTTPD.

Workstation – adalah komputer yang terhubung dengan sebuah Local Area Network (LAN)

X.25 - adalah International Telecommunication Union-Telecomunication Standardization

X Sector(ITU-T),protocol standard untuk komunikasi WAN. Bagaimana cara mengkoneksi

antara perlengkapan pengguna dan perlengkapan jaringan. X.25 didesain untuk

mengoperasikan keefektivan tanpa memperhatikan tipe system koneksi ke jaringan. Ini khususnya

digunakan untuk mengoperasikan dalam Packet Switched Networks (PSNs), contohnya perusahaan

telepon.

XML - Extensible Markup Language. Pengembangan lebih lanjut dari format yang digunakan

dalam World Wide Web jumlah kelebihan dibandingkan HTML, diantaranya dokumen lebih

terstruktur, memungkinkan manipulasi tampilan data tanpa harus berhubungan dengan webserver,

serta pertukaran data antar dokumen.

XNS - Xerox Network System (XNS) yang dibuat Perusahaan Xerox di akhir 1970an dan awal

tahun 1980an. Mereka didesain agar dapat digunakan sebagai jarak lintas dari variasi media

komunikasi, seperti processor dan aplikasi perkantoran. Beberapa protocol XNS menyerupai

Internet Protocol (IP) dan Transmission Control Protocol (TCP).

==========

Dalam jaringan komputer banyak sekali kita menemukan istilah-istilah yang digunakan didalamnya. Hambatan yang sering terjadi dalam belajar jaringan komputer adalah banyaknya istilah atau kata yang digunakan terkadang istilah tersebut tidak didalam buku atau kamus bahasa inggris karena memang istilah yang digunakan bukan merupakan kata-

kata namun singkatan seperti TCP/IP atau IP banyak orang yang terframe dipikirannya ketika mendengar kata IP langsung mengartikan bahwa IP adalah nomor komputer atau komputer ini nomornya berapa. Hal-hal yang demikian jika tidak dilurusankan nantinya dikhawatirkan akan merubah makna dari singkatan tersebut.
Kebanyakan singkatan yang digunakan dalam jaringan komputer menjadikan singkatan itu sebagai nama dari kata yang dimaksud seperti RJ 45, mendengar kata tersebut pikiran kita langsung tertuju pada bendanya, langsung membayangkan RJ 45 padahal RJ 45 sendiri adalah sebuah singkatan yaitu Registered Jack nomor 45.
Kumpulan istilah ini sengaja di buat guna memberikan inputan bagi siapa saja yang sedang atau akan belajar jaringan komputer atau sekedar menghangatkan kembali ingatan-ingatan kita pada jaringan komputer.
Dengan senang hati jika ada yang ingin menambahkannya …

10BaseT

Bagian dari standar asli IEEE 802.3, 10BaseT adalah spesifikasi Ethernet 10 Mbps baseband yang menggunakan dua pasang kabel yang saling terbelit (twisted pair), kabel kategori 3, 4, 5 menggunakan satu pasang kabel untuk mengirim data datu satu pasang lainnya untuk menerima. 10BaseT mempunyai batas jarak sekita 100 meter per segmen.

100BaseT

Berdasarkan standar IEEE 802.3u, 100BaseT adalah spesifikasi Fast Ethernet untuk baseband 100Mbps yang menggunakan kabel UTP. 100BaseT mengirimkan link pulse (yang berisi lebih banyak informasi dibandingkan dengan yang digunakan 10BaseT) melalui network ketika tidak ada lalu lintas data.

100BaseTX

Berdasarkan standar IEEE 802.3u, 100BaseTX adalah spesifikasi Fast Ethernet baseband 100Mbps yang menggunakan dua pasang kabel UTP atau STP. Kabel pasang pertama menerima data, pasang kedua mengirimkan data. Untuk memastikan waktu sinyal yang tepat, sebuah segmen 100BaseTX panjangnya tidak bias melebihi 100 meter.

A&B Bit Signaling

Pensinyalan bit A & B. digunalan dalam fasilitas transmisi T1 dan terkadang dinamakan "24th" channel signaling (pensinyalan kanal ke 24). Setiap 24 T1 subchanel pada procedur ini menggunakan satu bit untuk setiap frame keenam untuk mengirimkan informasi sinyal pengawasan (supervisory).

AAA

Authentication, Authorization, Accounting. Sebuah system yang dibuat oleh cisco untuk menyediakan keamanan jaringan.

AAL

ATM Adaption Layer. Sebuah sublayer yang service-dependent (bergantung pada layanan) dari layer data link, yang menerima data dari aplikasi lain dan membawanya ke

layer ATM dengan segmen-segmen payload (data yang dikirim) berukuran 48 byte. CS dan SAR adalah dua sublayer yang membentuk AAL-AAL. Saat ini empat tipe AAL yang direkomendasikan oleh ITU-T adalah AAL1, AAL2, AAL3/4, dan AAL5. semua AAL dibedakan oleh source-destination timming (waktu dari sumber ke tujuan) yang digunakan, apakah CBR atau VBR, serta apakah mereka digunakan untuk transmisi data yang connection-oriented atau connectionless.

AAL1

ATM Adaption Layer 1. satu dari empat AAL yang direkomendasikan oleh ITU-T AAL1 digunakan untuk layanan yang connection-oriented dan time-sensitive yang memerlukan bit rate yang stabil, seperti lalu lintas isochronous dan video yang tidak di kompresi.

AAL2

ATM Adaption Layer 2. Satu dari empat AAL (sebuah produk dari dua layer yang direkomendasikan oleh ITU-T. AAL2 digunakan untuk layanan connection-oriented yang mendukung bit rate yang bervariasi, seperti lalu lintas suara (voice) yang dikompresi.

AAL3/4

ATM Adaption Layer $\frac{3}{4}$. Satu dari empat AAL (sebuah produk dari dua layer yang pada awalnya berbeda) yang direkmendasikan oleh ITU-T, mendukung baik link connectionless maupun link connection-oriented. Terutama digunakan untuk mengirimkan paket-paket SMDS melalui network ATM.

AAL5

Adaption Layer 5. Satu dari empat AAL yang direkomendasikan oleh ITU-T, digunakan untuk mendukung layanan VBR connection-oriented terutama untuk mentransfer network IP yang klasik, melalui lalu lintas ATM dan LANE. Rekomendasi AAL yang lebih sederhana ini menggunakan SEAL, menawarkan biaya bandwidth yang lebih rendah dan kebutuhab pemrosesan yang lebih sederhana, tetapi juga menyediakan bandwidth yang dikurangi dan kemampuan error-recovery.

AARP

AppleTalk Address Resolution Protocol. Protokol di dalam stack atau kumpulan protocol AppleTalk yang memetakan alamat data-link alamat network.

AARP Probe Packets

Paket-paket yang dikirim oleh AARP untuk menentukan apakah sebuah node ID (identifikasi dari sebuah titik atau node) yang diberikan sedang digunakan oleh node lain pada sebuah network AppleTalk yang nonextended. Jika node ID tidak sedang digunkan oleh node lain, node pengirim akan memilih node ID tersebut. Jika node ID sedang digunakan oleh node lain, node pengirim akan memilih sebuah ID lain dan kemudian mengirimkan keluar AARP probe packets yang lebih banyak.

ABM

Asynchronous Balanced Mode. Ketika dua station bias mlakukan inisialisasi pengirim, ABM

adalah sebuah teknologi komunikasi HDLC yang mendukung komunikasi yang peer-oriented dan point-to-point di antara kedua station tersebut.

ABR

Area Border Router. Sebuah router OSPF yang terletak pada perbatasan dari satu atau lebih area OSPF. ABR digunakan untuk menghubungkan area OSPF dengan area backbone OSPF.

Acces Layer

Salah satu layer dari model hierarkis tiga layer Cisco. Layer menyediakan akses internetworking untuk pengguna.

Access Link

Sebuah link yang digunakan dengan switch yang merupakan bagian dari hanya satu Virtual LAN (VLAN). Trunk link membawa informasi dari beberapa VLAN.

Access List

Sebuah kumpulan dari kondisi-kondisi pengujian yang disimpan oleh router yang emnentukan lalulintas yang menarik ke dan dari router untuk berbagi layanan pada network.

Access Methode

Metode Akses. Cara peralatan network untuk mendapatkan akses ke networknya sendiri.

Accsess Rate

Kecepatan akses. Menentukan kecepatan bandwidth dari rangkaian (circuit). Sebagai contoh kecepatan akses T1 adalah 1.544 Mbs. Pada frame relay dan teknologi lain, terdapat kemungkinan sebuah pecahan dari koneksi T1, contohnya 256 Kbps walaupun demikian kecepatan akses dan clock rate tetap 1.544 Mbps.

Access Server

Server akses. Juga dikenal sebagai network access server merupakan sebuah proses komunikasi yang menghubungkan peralatan asynchronous ke LAN atau WAN melalui network dan software terminal emulation, menyediakan routing synchronous atau asynchronous dari protokol-protokol yang didukung.

Accounting

Satu dari tiga komponen AAA. Accounting menyediakan fungsi audit dan log untuk model keamanan.

Acknowledgment

Verifikasi yang dikirim oleh satu peralatan network ke peralatan lainnya untuk menandakan bahwa sebuah kejadian telah terjadi. Bias disingkat menjadi ACK. Berlawanan dengan NAK.

ACR

Allowed cell rate. Sebuah nama yang didefinisikan oleh forum ATM untuk mengelola lalu lintas ATM. ACR secara dinamik dikendalikan dengan menggunakan pengukuran congestion

control dan bervariasi antara minimum cell rate (MCR) dan peak cell rate (PCR).

Active Monitor

Mekanisme yang digunakan untuk mengelola sebuah network token ring. Titik (node) network dengan alamat MAC yang paling tingi pada token ring menjadi active monitor dan bertanggung jawab untuk tugas-tugas manajemen seperti mencegah loop-loop dan memastikan token tidak hilang.

Active State

Status aktif. Berkenaan dengan sebuah table routing EIGRP, sebuah rute berada dalam status aktif ketika router mengalami router convergence (selesai melengkapi table routingnya).

Address Learning

Mempelajari alamat. Digunakan dengan transparent brigde untuk mempelajari alamat-alamat hardware dari semua peralatan di sebuah network. Switch kemudian melakukan penyaringan (filter) terhadap network dengan alamat hardware (MAC) yang telah diketahui.

Address Mapping

Pemetaan alamat. Dengan menerjemahkan alamat network dari satu format ke format lainnya, metodelogi ini memungkinkan protocol-protokol yang berbeda beroprasi dan bisa saling dipertukarkan.

Address Mask

Sebuah descriptor (keterangan) kombinasi bit yang mengidentifikasikan bagaimana dari sebuah alamat yang menunjukkan network atau subnet dan bagian mana yang menunjukkan host. Kadang-kadang hanya disebut mask.

Address Resolution

Penerjemah alamat. Proses yang digunakan untuk menyelesaikan perbedaan di natara skema-skema pengalamatan komputer. Penerjemah alamat biasanya mendefinisikan sebuah metode untuk pelacakan (tracing) alamat layer network (layer 3) ke alamat layer data link (layer 2).

Adjacency

Kedekatan. Hubungan yang dibuat antara router-router tetangga yang ditentukan dan node-node akhir, menggunakan sebuah segmen media yang umum, untuk saling mempertukarkan informasi routing.

Administrative distance (AD)

Sebuah angka di antara 0 dan 255 yang menunjukkan tingkat kepercayaan terhadap sebuah sumber informasi routing. Semakin rendah angkanya semakin tinggi tingkat kepercayaannya.

Administrative Weight

Sebuah nilai yang dipilih oleh seorang administration network untuk menentukan

tingkatan preferensi yang diberikan kepada sebuah jaringan network. Merupakan satu dari empat metric link yang dipertukakrkan oleh PTSP-PTSP untuk menguji ketersediaan resource network ATM.

ADSU

ATM Data Service Unit. Terminal adapter yang digunakan untuk berhubungan dengan sebuah network ATM melalui sebuah mekanisme yang HSSI-compatible.

Advertising

Pengumuman. Proses di mana update-update routing atau layanan ditransmisikan pada interval waktu tertentu, yang memungkinkan router-router lain pada network memelihara sebuah catatan dari rute-rute yang bias digunakan.

AEP

AppleTalk Echo Protocol. Sebuah tes untuk koneksivitas antara dua node atau terminal AppleTalk di mana satu terminal mengirimkan paket ke terminal lain dan menerima sebuag echo atau copy sebagai tanggapan.

AFI

Authory and Format Identifier. Bagian dari sebuah alamat NSAP ATM yang menggambarkan tipe dan format bagian IDI dari sebuah alamat ATM.

AFP

AppleTalk Filling Protocol. Sebuah protocol layer presentation, mendukung file sharing AplleShare dan Mac OS, yang mengizinkan user melakukan sharing file dan aplikasi pada sebuah server.

AIP

ATM Interface Processor. Mendukung AAL $\frac{3}{4}$ dan AAL5, interfaceini untuk router Cisco seri 7000 meminimalkan performace bottlenecks pada UNI.

Algorithm

Algoritma. Sekumpulan peraturan atau proses yang digunakan untuk menyelesaikan sebuah masalah. Pada networking, algoritma biasanya digunakan untuk menemukan rute terbaik untuk lalu lintas dari sumber ke tujuan.

Alignment Error

Sebuah error yang terjadi di dalam network Ethernet, dimaa frame yang diterima mempunyai bit-bit tambahan yaitu sebuah angka yang tidak habis dibagi dengan delapan. Alignment error umumnya disebabkan oleh frame yang rusak akibat collisions.

All-Routes Explorer Packet

Sebuah packet penjelajah (explorer) yang bias bergerak melalui selruh network SRB, melacak semua jalur yang memungkinkan ke sebuah tujuan yang diberikan. Juga dikenal sebgai all-ring explorers packet.

AM

Amplitudo Modulation. Sebuah metode modulasi yang menyatakan informasi dengan

memvariasikan amplitude dengan sinyal pembawa.

AMI

Alternate Mark Inverson. Sebuah tipe line-code pada sirkuit T1 dan E1 yang menampilkannol sebagi "01" dalam setiap bit cell dan satu sebagai "11" atau "00", sevara bergantian, dalam setiap bit cell. Alat pengirim harus memelihara apa yang disebut ones density dalam AMI, tetapi tidak terlepas dari stream data. Juga dikenal sebagai binary-coded, alternate mark inversion. Berlawanan dengan B8ZS.

Amplitude

Sebuah nilai tertinggi dari gelombang analog atau digital

Analog Transmission

Pengirim sinyal dimana informasi ditampilkan dengan berbagai kombinasi amplitude, frekuensi, dan fase dari sinyal.

ANSI

American Nasional Standards Institute. Organisasi yang terdiri dari perusahaan pemerintah, dan anggota-anggota sukarela yang mengkoordinasikan kegiatan-kegiatan yang berhubungan dengan standar, menyetuji standar nasional Amerika Serikat, dan membantu dalam pembuatan standar internasional dan Amerika Serikat untuk bidang seperti komunikasi, networking, dan berbagai bidang teknik. ANSI telah mempublikasikan lebih dari 13.000 standar, untuk produk-produk rekaya dan teknologi, mulai dari the international electrotechnical commission (IEC) dan international organization for standardization (ISO).

Anycast

Sebuah alamat ATM yang dapat dibagi oleh lebih dari satu system client, memungkinkan permintaan layanan di route ke sebuah node yang meyediakan layanan tersebut.

AppleTalk

Pada saat ini terdapat dua versi, emrupakan kumpulan protocol-protokol komunikasi yang dirancang oleh Apple Computer untuk digunakan dilingkungan Macinthos. Protocol-protokol Fase 1 yang lebih awal mendukung satu network fisikal dengan hanya stu nomor network yang berada di satu zone. Protocol Fase 2 yang lebih baru mendukung lebih dari satu network logika pada sebuah network fisikal, memungkinkan network-network berada di lebih dari satu zone.

Application Layer

Layer Application. Layer ke 7 dari model OSI, meyediakan layanan-layanan untuk prosedur-prosedur aplikasi (seperti electronic mail atau transfer file) yang berada di luar model OSI. Layer ini memilih dan menentukan ketersediaan dari partner komunikasi dan juga sumber daya yang diperlukan untuk membentuk sebuah kesepakatan terhadap prosedur-prosedur untuk mengendalikan integritas data dan error recovery.

ARA

AppleTalk Remote Access. Sebuah protocol untuk pengguna Macinthos untuk menetapkan akses mereka ke sumber daya dan data dari sebuah local AppleTalk yang remote.

Area

Sebuah kumpulan lagikal, bukan fiscal, dari segmen-segmen (berdasarkan CLNS, DECnet, atau OSPF) berikut peralatan-peralatan yang terhubung dengan segmen-segmen tersebut. Area biasanya dihubungkan dengan area lain menggunakan router-router untuk menciptakan sebuah autonomus system tunggal.

ARM

Asynchonous Respone Mode. Sebuah mode komunikasi HDLC yang menggunakan satu station utama dan paling sedikit satu station tambahan, dimana transmisi dapat dimulai dari station utama atau salah satu unit sekunder.

ARP

Address Resolution Protocol. Didefinisikan di RFC 826, merupaka protocol yang melacak alamat IP ke alamat MAC.

AS

Autonomous system. Sebuah kumpulan network di bawah administrasi bersama yang berbagi metodelogi routing yang sama. Autonomous system dibagi lagi menjadi area-area dan harus diberikan sebuah nomor 16 bit tunggal oleh IANA.

AS Path Prepending

Penggunaan peta-peta rute dalam BGP untuk memperpanjang jalur autonomous system dengan menambahkan ASN-ASN palsu.

ASBR

Autonomous System Boundary Router. Sebuah router area border yang ditempatkan di antara sebuah autonomous system OSPF dan sebuah network non OSPF yang bekerja dengan OSPF dan protocol routing tambahan, seperti RIP. ASBR harus ditempatkan disebuah area OSPF yang non stub.

ASCII

American Standard Code For International Interchange. Sebuah kode 8 bit untuk mempresentasikan karakter-karakter, terdiri dari 7 bit data ditambah 1 bit binary.

ASICs

Application Specific Integrated Circuits. Digunakan di switch layer 2 untuk membuat keputusan filtering. ASIC melihat kedalam table filter dari alamat-alamat MAC dan menetukan port mana yang dituju oleh alamat hardware tujuan dari sebuah alamat hardware yang diterima. Frame akan diizinkan untuk melalui satu segmen itu saja. Jika alamat hardware tidak diketahui, frame akan di forward ke semua port.

SNA.1

Abstract Syntac Notation One. Sebuah bahasa OSI yang digunakan untuk menggambarkan jenis-jenis data yang tidak bergantung pada struktur computer dan

metode penggambarannya. Dideskripsikan oleh standart internasional 8824 ISO.

ASP

AppleTalk Session Protocol. Sebuah protocol yang menggunakan ATP untuk menetapkan, memelihara, dan memutuskan session-session, dan juga permintaan-permintaan yang berurut.

AST

Automatics Spanning Tree. Sebuah fungsi yang menyediakan satu jalur untuk frame explore berjalan dari satu node di network ke node lain, mendukung resolusi otomatis dari spanning tree dalam networks SRB. AST berdasarkan pada standard IEEE 802.1d.

Asynchronous Transmission

Asynchronous Transmission. Sinyal digital yang dikirim tanpa timming yang tepat, biasanya dengan frekuensi-frekuensi dan hubungan fase yang berbeda. Transmissi asynchronous biasanya memasukkan karakter-karakter individual dalam bit-bit pengendali (yang disebut bit start dan stop) yang memperlihatkan permulaan dan akhir dari setipa karakter. Berlawanan dengan isochronous transmission dan synchronous transmission.

ATCP

AppleTalk Control Program. Protokol untuk menetapkan dan mengkonfigurasi AppleTalk di atas PPP, didefinisikan dalam RFC 1378.

ATDM

Asynchronous Time Division Multiplexing. Sebuah teknik untuk mengirimkan informasi, ia berbeda dengan TDM normal dalam hal slot waktu yang dipilih ketika diperlukan, disbanding slot yang sudah ditentukan sebelumnya pada transmitter tertentu. Berlawanan dengan FDM, statistical multiplexing, dan TDM

ATG

Address Translation Gateway. Mekanisme di dalam software routing cisco DECnet yang memungkinkan router untuk melakukan routing ke beberapa tempat sekaligus, dengan tidak bergantung pada network DECnet dan menetapkan sebuah terjemahan alamat yang dipilih oleh user untuk node tertentu diantara network-network.

ATM

Asynchronous Transfer Mode. Standar internasional, didefinisikan oleh sel-sel (cells) 53 byte yang panjangnya sudah ditetapkan, untuk menstransmisikan sel-sel dalam banyak system-sistem layanan, seperti voice, video atau data. Delay dari transit dikurangi karena sel-sel dengan panjang yang sudah ditetapkan tersebut memungkinkan pemrosesan untuk terjadi di hardware. ATM dirancang untuk memaksimalkan keuntungan dari media transmisi kecepatan tinggi, seperti SONET, E3 dan T3.

ATM ARP server

Sebuah alat yang menyediakan subnet-subnet logical yang menjalankan network klasik IP di atas ATM dengan layanan penerjemah alamat.

mawaridz@gmail.com

ATM Endpoint
Koneksi pemulai atau pemutus dalam sebuah network ATM, ATM endpoint termasuk server, workstation, switch ATM ke LAN dan router ATM.
ATM Forum
Organisasi internasional yang didirikan bersama oleh Northern Telecom, Sprint, Cisco System, dan NET/ADAPTIVE pada tahub 1991 untuk mengembangkan dan mempromosikan kesepakatan-kesepakatan implementasi yang berdasarkan standar untuk teknologi ATM. ATM forum memperluas standar resmi yang dikembangkan oleh ANSI dan ITU-T dan menciptakan kesepakatan-kesepakatan implementasi sebelum standar resmi dipublikasikan.
ATM Layer
Sebuah sublayer dari layer data link dalam sebuah network ATM yang bergantung pada layanan. Untuk menciptakan sel-sel ATM 53 byte yang standar, layer ATM menerima segmen-segmen 48 byte dari AAL dan menempelkan sebuah header 5 byte ke setiap segmen. Sel-sel ini kemudian dikirim ke layer physical untuk ditransmisikan melalui media fisikal.
ATMM
ATM management. Sebuah prosedur yang bekerja pada switch-switch ATM, mengelola rate enforcement dan VCI translation.
ATM user-user connection
Sebuah koneksi yang dibuat oleh layer ATM untuk menyediakan komunikasi antara paling sedikit dua pengguna layanan ATM, seperti proses-proses ATMM. Komunikasi ini dapat berupa komunikai searah atau dua arah, masing-masing menggunakan satu atau dua VC.
Attenuation
Dalam komunikasi berate perlemahan atau kehilangan energi sinyal, biasanya disebabkan oleh jarak.
AURP
AppleTAlk Update-based Routing Protokol. Sebuah teknik untuk mengenkapsulasi lalu lintas ApplTalk dalam header dari sebuah protocol asing yang memungkinkan koneksi dari paling sedikit dua internetwork ApplteTalk yang tidak bersambungan melalui sebuah network asing (seperti TCP/IP) untuk menciptakan sebuah WAN AppleTalk yang lengkap.
AURP Tunnel
Sebuah koneksi yang dibuat di sebuah WAN AURP yang bertindak sebagai sebuah link virtual tunggal antara internetwork-internetwork AplleTalk yang terpisah secara fisik oleh sebuah network asing seperti network TCP/IP.
Authentication
Komponen pertama dalam model AAA. User biasanya diotentikasikan melalui sebuah username dan password, yang digunakan secara unik untuk mengidentifikasikan mereka.

mawaridz@gmail.com

Authority Zone
Sebuah bagian dari pohon domain-name yang terkait dengan DNS dimana sebuah name server menjadi otoritasnya.
Authorization
Tindakan memperbolehkan akses ke sebuah sumber daya berdasarkan informsi otentikasi dalam model AAA.
Auoto-detect Mechanism
Digunakan di switch, hub, dan kartu interface Ethernet, untuk menentukan duplex dan kecepatan yang akan didapat.
Auto Duplex
Sebuah setting pada peralatan layer 1 dan layer 2 yang menset duplex dari sebuah port pada switch atau hub secara otomatis.
Automatics Call Reconnect
Sebuah fungsi yang memungkinkan proses roting kembali (rerouting) dengan panggil otomatis untuk berpindahdari sebuah sambungan trunk yang gagal.
Autonomous confederation
Sebuah koleksi dari system-sistem yang diadministrasikan sendiri (self-governed) yang lebih bergantung pada akses dan infromasi routing di network mereka sendiri daripada informasi yang diterima dari system-sistem atau group lain.
Autonomous swithing
Kemampuan router-router cisco untuk memproses paket-paket secara lebih cepat dengan menggunakan ciscoBus untuk melakukan switch paket secara terpisah dari prosesor system.
Autoreconfiguration
Sebuah prosedur yang dieksekusi oleh node-node di dalam domain yang gagal dari sebuah token ring, dimana node-node tersebut secara otomatis melakukan diagnosis, mencoba mengkonfigurasi kembali network di sekeliling area yang gagal.
Auxiliary port
Konsol port di belakang router-router cisco yang memungkinkan untuk menghubungkan sebuah modem dan melakukan panggilan ke router dan melakukan setting konfigurasi konsol.
B8ZS
Binary 8 Zero Subtitution
Sebuah tipe line-code, yang diinterpretasikan pada remote dari koneksi, yang menggunakan sebuah subtitusi kode khusus ketika 8 nol secara berurutan ditransmisikan melalui link pada rangkaian T1 da E1. teknik ini menjamin ones density terlepas dari stream data. Juga dikenal sebagai subtitusi 8 nol bipolar. Berlawanan dengan AMI.
Backbone

mawaridz@gmail.com

Bagian dasar dari network yang menyediakan jalur utama untuk lalu lintas yang dikirimkan ked an dimulai dari network lain.

Back End

Sebuah node atau program software yang menyediakan layanan ke sebuah server front end.

Bandwidth

Selisih antara frekuensi tertinggi dan terendah yang digunakan oleh sinyal network. Lebih umum, ia mengacu pada kapasitas throughput yang diukur dari sebuah protocol atau media network.

Bandwidth on Demand (BoD)

Fungsi ini memungkinkan sebuah kanal B tambahan digunakan untuk menambah bandwidth yang tersedia untuk sebuah koneksi tertentu.

Baseband

Sebuah fitur dari teknologi network yang menggunakan hanya satu pembawa (carrier) frekuensi. Contohnya adalah Ethernet. Juga disebut "narrowband (pita sempit).

Baseline

Informasi baseline termasuk data historis tentang network dan informasi utilitisasi atau penggunaan network yang rutin. Informasi ini dapat digunakan untuk menentukan apakah ada perubahan terbaru pada network yang mungkin menyebabkan sebuah masalah yang sedang dihadapi.

Basic Management Setup

Digunakan dengan router cisco ketika dalam mode setup. Hanya menyediakan manajemen dan konfigurasi yang cukup untuk membuat router bakerja agar seseorang dapat melakukan telnet ke router tersebut dan mengkonfigurasinya.

Baud

Sinonim dari bit per second (bps), jika setiap elemen sinyal menyatakan 1 bit. Baud adalah sebuah satuan dari kecepatan pensinyalan yang ekivalen dengan jumlah elemen sinyal yang terpisah yang ditransmisikan perdetik.

B Channel

Kanal bearer (pembawa), sebuah kanal full duplex dan 64 Kbps di ISDN yang mentransmisikan data user. Bandingkan dengan D Channel, E Channel, dan H Channel.

BDR

Backup designation router, digunakan di sebuah network OSPF untuk melakukan backup untuk router yang dipilih jika terjadi kegagalan.

Beacon

Sebuah frame FDDI atau token atau token ring yang menunjukkan sebuah masalah yang serius dengan ring, missalnya kabel yang putus. Frame beacon membawa alamat dari station yang dianggap down.

mawaridz@gmail.com

BECN
Backward explicit congestion notification. Adalah bit yang di set oleh network frame relay yang bergerak menjauh dari frame yang menuju ke sebuah jalur yang congested (jenuh). Sebuah DTW yang menerima frame dengan BECN dapat menanyakan protocol di level yang lebih untuk mengambil tindakan yang diperlukan untuk mengendalikan aliran data.
BGP4
BGP version 4. versi 4 dari protocol routing interdomain yang paling sering digunakan di internet. BGP4 mendukung CIDR dan menggunakan mekanisme penghitungan rute untuk mengurangi ukuran table routing.
BGP indentifier
Field ini mendukung sebuah nilai yang mengidentifikasi pembicara BGP. Ini adalah sebuah nilai acak yang dipilih oleh router BGP ketika mengirimkan sebuah pesan OPEN.
BGP Neighbors
Dua router menjalankan BGP yang memulai sebuah proses komunikasi TCP pada layer 4 dari model referensi OSI. Secra khusus, yang digunakan adalah port TCP 179.
BGP Speaker
Sebuah router yang mengumumkan prefix-prefix atau rute-rutenya.
Bidirectional Shared Tree
Sebuah metode forwarding multicast dengan pohon (tree) yang dibagi. Metode ini memungkinkan anggota-anggota group menerima data dari sumber atau RP, bergantung pada yang mana yang lebih dekat.
Binary
Sebuah metode penomoran dengan dua karakter yang menggunakan satu dan nol. System penomoran binary mendasari semua pernyataan digital dari informasi.
Binding
Mengkonfigurasi sebuah protocol layer network untuk menggunakan sebuah jenis frame tertentu pada sebuah LAN.
BIP
Bit Interleaved parity. Sebuah metode yang digunakan di ATM untuk memonitor error-error pada sebuah link, mengirim sebuah check bit atau check word pada overhead dari link untuk blok atau frame sebelumnya. Ini memungkinkan error pada bit yang sedang ditransmisikan dapat ditemukan dan dikirimkan sebagai informsi untuk pemeliharaan network.

mawaridz@gmail.com

==========

Setting mikrotik

==========

MikroTik RouterOS™ adalah sistem operasi linux yang dapat digunakan untuk menjadikan komputer menjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan wireless, cocok digunakan oleh ISP dan provider hostspot.

Ada pun fitur2 nya sbb:

* Firewall and NAT - stateful packet filtering; Peer-to-Peer protocol filtering; source and destination NAT; classification by source MAC, IP addresses (networks or a list of networks) and address types, port range, IP protocols, protocol options (ICMP type, TCP flags and MSS), interfaces, internal packet and connection marks, ToS (DSCP) byte, content, matching sequence/frequency, packet size, time and more…

* Routing - Static routing; Equal cost multi-path routing; Policy based routing (classification done in firewall); RIP v1 / v2, OSPF v2, BGP v4

* Data Rate Management - Hierarchical HTB QoS system with bursts; per IP / protocol / subnet / port / firewall mark; PCQ, RED, SFQ, FIFO queue; CIR, MIR, contention ratios, dynamic client rate equalizing (PCQ), bursts, Peer-to-Peer protocol limitation

* HotSpot - HotSpot Gateway with RADIUS authentication and accounting; true Plug-and-Play access for network users; data rate limitation; differentiated firewall; traffic quota; real-time status information; walled-garden; customized HTML login pages; iPass support; SSL secure authentication; advertisement support

* Point-to-Point tunneling protocols - PPTP, PPPoE and L2TP Access Concentrators and clients; PAP, CHAP, MSCHAPv1 and MSCHAPv2 authentication protocols; RADIUS authentication and accounting; MPPE encryption; compression for PPPoE; data rate limitation; differentiated firewall; PPPoE dial on demand

* Simple tunnels - IPIP tunnels, EoIP (Ethernet over IP)

* IPsec - IP security AH and ESP protocols; MODP Diffie-Hellman groups 1,2,5; MD5 and

SHA1 hashing algorithms; DES, 3DES, AES-128, AES-192, AES-256 encryption algorithms; Perfect Forwarding Secrecy (PFS) MODP groups 1,2,5

* Proxy - FTP and HTTP caching proxy server; HTTPS proxy; transparent DNS and HTTP proxying; SOCKS protocol support; DNS static entries; support for caching on a separate drive; access control lists; caching lists; parent proxy support

* DHCP - DHCP server per interface; DHCP relay; DHCP client; multiple DHCP networks; static and dynamic DHCP leases; RADIUS support

* VRRP - VRRP protocol for high availability

* UPnP - Universal Plug-and-Play support

* NTP - Network Time Protocol server and client; synchronization with GPS system

* Monitoring/Accounting - IP traffic accounting, firewall actions logging, statistics graphs accessible via HTTP

* SNMP - read-only access

* M3P - MikroTik Packet Packer Protocol for Wireless links and Ethernet

* MNDP - MikroTik Neighbor Discovery Protocol; also supports Cisco Discovery Protocol (CDP)

* Tools - ping; traceroute; bandwidth test; ping flood; telnet; SSH; packet sniffer; Dynamic DNS update tool

Layer 2 connectivity:

* Wireless - IEEE802.11a/b/g wireless client and access point (AP) modes; Nstreme and Nstreme2 proprietary protocols; Wireless Distribution System (WDS) support; virtual AP; 40 and 104 bit WEP; WPA pre-shared key authentication; access control list; authentication with RADIUS server; roaming (for wireless client); AP bridging

* Bridge - spanning tree protocol; multiple bridge interfaces; bridge firewalling, MAC

mawaridz@gmail.com

* VLAN - IEEE802.1q Virtual LAN support on Ethernet and wireless links; multiple VLANs; VLAN bridging

* Synchronous - V.35, V.24, E1/T1, X.21, DS3 (T3) media types; sync-PPP, Cisco HDLC, Frame Relay line protocols; ANSI-617d (ANDI or annex D) and Q933a (CCITT or annex A) Frame Relay LMI types

* Asynchronous - s*r*al PPP dial-in / dial-out; PAP, CHAP, MSCHAPv1 and MSCHAPv2 authentication protocols; RADIUS authentication and accounting; onboard s*r*al ports; modem pool with up to 128 ports; dial on demand

* ISDN - ISDN dial-in / dial-out; PAP, CHAP, MSCHAPv1 and MSCHAPv2 authentication protocols; RADIUS authentication and accounting; 128K bundle support; Cisco HDLC, x75i, x75ui, x75bui line protocols; dial on demand

* SDSL - Single-line DSL support; line termination and network termination modes

Instalasi dapat dilakukan pada Standard computer PC yang akan dijadikan router dan tidak memerlukan resource yang cukup besar untuk penggunaan standard, misalnya hanya sebagai gateway.

Berikut spec_minimal nya :

* CPU dan motherboard - bisa dgn P1 ~ P4, AMD, cyrix asal yang bukan multi-prosesor

* RAM - minimum 32 MiB, maximum 1 GiB; 64 MiB atau lebih sangat dianjurkan, kalau mau sekalian dibuat proxy , dianjurkan 1GB… perbandingannya, 15MB di memori ada 1GB di proxy..

* HDD minimal 128MB parallel ATA atau Compact Flash, tidak dianjurkan menggunakan UFD, SCSI, apa lagi S-ATA (mungkin nanti Ver. 3.0)

* NIC 10/100 atau 100/1000

Untuk keperluan beban yang besar (network yang kompleks, routing yang rumit dll) disarankan untuk mempertimbangkan pemilihan resource PC yang memadai.

mawaridz@gmail.com

Lebih lengkap bisa dilihat di www.mikrotik.com. Meskipun demikian Mikrotik bukanlah free software, artinya kita harus membeli licensi terhadap segala fasiltas yang disediakan. Free trial hanya untuk 24 jam saja.

Kita bisa membeli software MikroTik dalam bentuk "licence" di CITRAWEB, UFOAKSES, PC24 (atau download cracknya, he he he …) yang diinstall pada HardDisk yang sebelumnya download/dibuat MikroTik RouterOS ISO kekeping CD atau disk on module (DOM). Jika kita membeli DOM tidak perlu install tetapi tinggal pasang DOM pada slot IDE PC kita.

Langkah-langkah berikut adalah dasar-dasar setup mikrotik yang dikonfigurasikan untuk jaringan
sederhana sebagai gateway server.

1. Langkah pertama adalah install Mikrotik RouterOS pada PC atau pasang DOM.

2. Login Pada Mikrotik Routers melalui console :

MikroTik v2.9.39

Login: admin

Password: (kosongkan)

Sampai langkah ini kita sudah bisa masuk pada mesin Mikrotik. User default adalah admin dan tanpa password, tinggal ketik admin kemudian tekan tombol enter.

3. Untuk keamanan ganti password default

[admin@Mikrotik] > password

old password: *****

new password: *****

retype new password: *****

[admin@ Mikrotik] >

4. Mengganti nama Mikrotik Router, pada langkah ini nama server akan kita ganti menjadi "r-WLI" (bebas, disesuaikan dengan nama jaringan kita…)

[admin@Mikrotik] > system identity set name=r-WLI

[admin@r-WLI] >

5. Melihat interface pada Mikrotik Router

[admin@r-WLI] > interface print

Flags: X - disabled, D - dynamic, R - running

NAME TYPE RX-RATE TX-RATE MTU

0 R ether1 ether 0 0 1500

1 R ether2 ether 0 0 1500

[admin@r-WLI] >

6. Memberikan IP address pada interface Mikrotik. Misalkan ether1 akan kita gunakan untuk koneksi ke Internet dengan IP 192.168.0.1 dan ether2 akan kita gunakan untuk network local kita dengan IP 172.16.0.1

[admin@r-WLI] > ip address add address=192.168.0.1 /

netmask=255.255.255.0 interface=ether1

[admin@r-WLI] > ip address add address=172.16.0.1 /

netmask=255.255.255.0 interface=ether2

7. Melihat konfigurasi IP address yang sudah kita berikan

[admin@r-WLI] >ip address print

Flags: X - disabled, I - invalid, D - dynamic

mawaridz@gmail.com

ADDRESS NETWORK BROADCAST INTERFACE

0 192.168.0.1/24 192.168.0.0 192.168.0.63 ether1

1 172.16.0.1/24 172.16.0.0 172.16.0.255 ether2

[admin@r-WLI] >

8. Memberikan default Gateway, diasumsikan gateway untuk koneksi internet adalah 192.168.0.254

[admin@r-WLI] > /ip route add gateway=192.168.0.254

9. Melihat Tabel routing pada Mikrotik Routers

[admin@r-WLI] > ip route print

Flags: X - disabled, A - active, D - dynamic,

C - connect, S - static, r - rip, b - bgp, o - ospf

DST-ADDRESS PREF-SRC G GATEWAY DISTANCE INTERFACE

0 ADC 172.16.0.0/24 172.16.0.1 ether2

1 ADC 192.168.0.0/26 192.168.0.1 ether1

2 A S 0.0.0.0/0 r 192.168.0.254 ether1

[admin@r-WLI] >

10. Tes Ping ke Gateway untuk memastikan konfigurasi sudah benar

[admin@r-WLI] > ping 192.168.0.254

192.168.0.254 64 byte ping: ttl=64 time

mawaridz@gmail.com

11. Setup DNS pada Mikrotik Routers

```
[admin@r-WLI] > ip dns set primary-dns=192.168.0.10 /

allow-remoterequests=no

[admin@r-WLI] > ip dns set secondary-dns=192.168.0.11 /

allow-remoterequests=no
```

12. Melihat konfigurasi DNS

```
[admin@r-WLI] ip dns> pr

primary-dns: 192.168.0.10

secondary-dns: 192.168.0.11

allow-remote-requests: no

cache-size: 2048KiB

cache-max-ttl: 1w

cache-used: 21KiB

[admin@r-WLI] ip dns>
```

13. Tes untuk akses domain, misalnya dengan ping nama domain

```
[admin@r-WLI] > ping yahoo.com

216.109.112.135 64 byte ping: ttl=48 time=250 ms
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 571/571.0/571 ms
[admin@r-WLI] >
```

Jika sudah berhasil reply berarti seting DNS sudah benar.

mawaridz@gmail.com

14. Setup Masquerading, Jika Mikrotik akan kita pergunakan sebagai gateway server maka agar client computer pada network dapat terkoneksi ke internet perlu kita masquerading.

[admin@r-WLI]> ip firewall nat add action=masquerade /

outinterface=ether1 chain:srcnat

[admin@r-WLI] >

15. Melihat konfigurasi Masquerading

[admin@r-WLI]ip firewall nat print

Flags: X - disabled, I - invalid, D - dynamic

0 chain=srcnat out-interface=ether1 action=masquerade

[admin@r-WLI] >

Setelah langkah ini bisa dilakukan pemeriksaan untuk koneksi dari jaringan local. Dan jika berhasil berarti kita sudah berhasil melakukan instalasi MikroTik Router sebagai Gateway server. Setelah terkoneksi dengan jaringan Mikrotik dapat dimanage menggunakan WinBox yang bisa didownload dari MikroTik.com atau dari server mikrotik kita.

Misal Ip address server mikrotik kita 192.168.0.1, via browser buka http://192.168.0.1 dan download WinBox dari situ.
Jika kita menginginkan client mendapatkan IP address secara otomatis maka perlu kita setup dhcp server pada Mikrotik. Berikut langkah-langkahnya :

1. Buat IP address pool
/ip pool add name=dhcp-pool ranges=172.16.0.10-172.16.0.20

2. Tambahkan DHCP Network dan gatewaynya yang akan didistribusikan ke client Pada contoh ini networknya adalah 172.16.0.0/24 dan gatewaynya 172.16.0.1
/ip dhcp-server network add address=172.16.0.0/24 gateway=172.16.0.1

3. Tambahkan DHCP Server (pada contoh ini dhcp diterapkan pada interface ether2)
/ip dhcp-server add interface=ether2 address-pool=dhcp-pool

4. Lihat status DHCP server

[admin@r-WLI] > ip dhcp-server pr

Flags: X - disabled, I - invalid

NAME INTERFACE RELAY ADDRESS-POOL LEASE-TIME ADD-ARP

x dhcp1 ether2 dhcp_pool1 4w2d yes

[admin@r-WLI] >

Tanda X menyatakan bahwa DHCP server belum enable maka perlu dienablekan terlebih dahulu pada langkah 5.

5. Jangan Lupa dibuat enable dulu dhcp servernya
/ip dhcp-server enable 0

Kemudian cek kembali dhcp-server seperti langkah 4, jika tanda X sudah tidak ada berarti sudah aktif.

6. Tes Dari client

Run dari Comman Prompt

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\EsDat>ping www.yahoo.com

Pinging www.yahoo-ht3.akadns.net [69.147.114.210] with 32 bytes of data:

Reply from 124.158.129.5: bytes=32 time=34ms TTL=59
Reply from 124.158.129.5: bytes=32 time=24ms TTL=59

mawaridz@gmail.com

Reply from 124.158.129.5: bytes=32 time=41ms TTL=59
Reply from 124.158.129.5: bytes=32 time=29ms TTL=59

Ping statistics for 69.147.114.210:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 24ms, Maximum = 41ms, Average = 32ms

7. Untuk bandwith controller, bisa dengan sistem simple queue ataupun bisa dengan mangle

[admin@r-WLI] queue simple> add name=Komputer01 /

interface=ether2 target-address=172.16.0.1/24 max-limit=65536/131072

[admin@r-WLI] queue simple> add name=Komputer02 /

interface=ether2 target-address=172.16.0.2/24 max-limit=65536/131072

dan seterusnya…

==========

Setting dial-up Speedy

==========

Tip ini saya tulis dari pengalaman saya memakai Speedy dengan modem ADSL Articonet ACN-100R dan TP-Link TD 8817 yang kualitasnya tidak jauh berbeda. Dari pengalaman, jika dial-up speedy dilakukan oleh kedua modem tersebut, secara periodik koneksi akan terputus tanpa sebab yang jelas. *It sucks!* Menurut analisa beberapa rekan dan tenaga *outsource* Telkom Speedy sendiri, hal ini disebabkan karena buffer memori modem sudah

kelebihan beban. Hal ini menyebabkan proses *dialing* terganggu.

Karena sampai beberapa tahap gangguan ini membuat jengah, saya kepikiran untuk mengalihkan fungsi dial-up koneksi speedy ke komputer yang difungsikan sebagai router.

Saat itu saya langsung teringat pada beberapa perangkat komputer yang sudah tidak digunakan lagi teronggok di gudang. Daripada beli komputer atau router baru, mending saya 'hidupkan kembali' perangkat-perangkat veteran tersebut agar bisa merasakan masa kejayaannya lagi. he he he …

Akhirnya setelah semalaman berkutat dengan perangkat lawas dan debu, akhirnya saya bisa satukan kembali sebuah PC dengan processor P III 750MHz , 256MB SDRAM, dan sebuah harddisk 40GB. Ya, lumayan lah…

Selanjutnya komputer Veteran saya akan mengambil alih tugas modem melakukan dial-up speedy. Kurang dari 5 menit, seting mikrotik sudah selesai. Selanjutnya saya tempatkan posisinya dalam jaringan sebagai berikut

[INTERNET]——[MODEM ADSL]——[ROUTER MIKROTIK]——[SWITCH]———[CLIENT]
xxx.xxx—192.168.1.1/192.168.1.100—192.168.1.103/192.168.30.1—192.168.30.2-192.168.30.254

PERSIAPAN

Untuk mengantisipasi hal yang tidak diinginkan, saya sarankan Anda melakukan backup setting modem Speedy Anda terlebih dahulu. Hampir tiap modem dilengkapi dengan fasilitas ini. Konfigurasi yang diberikan oleh petugas dapat Anda backup dalam bentuk satu file yang kelak dapat Anda panggil lagi untuk mengembalikan setting modem ADSL ke kondisi semula dengan mudah.

Silakan masuk ke jendela setting Modem dengan memuka browser dan masukkan alamat modem (defaultnya: http://192.168.1.1).

Masuk pada bagian informasi service seperti berikut dan catat semua keterangan tentang LAN dan WAN yang ada.

SETTING MODEM ADSL

Buka browser Anda, masukkan alamat modem (defaultnya adalah http://192.168.1.1)

- Masukkan *username* dan *password* : admin/admin
- Masuk ke menu "*Advanced Setup*" kemudian pilih "*WAN*" dan klik tombol "*Edit*" Masukkan nilai PVC
- *Configuration* : (masukkan nilainya sesuai wilayah TELKOM masing-masing daerah)

VPI = X (setting saya=8)
VCI = XX (setting saya=8)
informasi ini bisa didapatkan dari petugas Telkom atau teknisi yang melakukan instalasi. Jika Anda masih belum yakin dengan setting yang tepat di lokasi Anda, silakan cek konfigurasi dalam tulisan berikut:
Setting Modem Speedy dari Berbagai Daerah

- *Service Category* = UBR Without PCR, kemudian klik Next
- *Connection type* = Bridging
- *Encapsulation* = LLC, kemudian klik tombol Next
- Tandai *check box* pilihan "*Enable Bridge Service*", Next dan akhiri dengan Save
- Selanjutnya klik tombol Save/Reboot, tunggu beberapa saat +- 2 menit hingga proses reboot modem selesai.

Jika Anda menggunakan paket Modem TP-Link TD8117 caranya lebih mudah. Ikuti saja langkah step-by-step nya dari Menu **Start Up** > **Wizard** > Pilih koneksi **Bridge** > Akhiri dengan **Finish**. *That's it!*

Jika Anda memerlukan panduan yang dilengkapi dengan gambar, silakan lihat panduannya di sini:
Setting Speedy pada Modem ADSL TP-Link TD-8817

SETTING ROUTER MIKROTIK

Sudah banyak dimaklumi bahwa Mikrotik agak susah memberikan identifikasi pada Lan Card. Agar lebih mudah mengingat, **Pertama** kita beri nama masing-masing *LAN Card* yang ada pada Mikrotik. sebagai berikut.

```
/interface ethernet set ether1 name=speedy
/interface ethernet set ether2 name=lokal
```

Setelah masing-masing *LAN card* diberi nama, tentukan IP-nya

```
ip address add address=192.168.1.103/24 interface=speedy
ip address add address=192.168.30.1/24 interface=lokal
```

periksa apakah nama card lan dan ip yang diberikan sudah benar.

```
ip address print
```

Kemudian lakukan test ping ke masing masing IP tersebut untuk memastikan konfigurasi sudah tepat.

Selanjutnya, aktifkan fitur PPOE Mikrotik untuk melakukan dial ke modem ADSL Speedy. Berikut ini akan kita bahas cara dial-up dengan menggunakan baris perintah di terminal.

mawaridz@gmail.com

Anda bisa juga lakukan hal ini lewat Winbox. Baca juga Panduan **Setting PPOE-Client Speedy dari Winbox** di bagian lain blog ini.

```
/interface pppoe-client add name=pppoe-client-speedy
user=142xxxxxxxxx@telkom.net
password=XXXXXXXXXX interface=speedy service-name=internet
disabled=no
/ip route add gateway= 125.124.123.1
```

Keterangan: IP Gateway ini bisa ditemukan dari dengan mengetik perintah *ipconfig* dari command pada saat speedy sudah di dial dari Windows. Anda juga bisa dapatkan informasi ini dari informasi konfigurasi modem (lewat browser seperti yang disampaikan pada setting modem di atas) atau yang sudah Anda catat sebelumnya.

Periksa sekali lagi apakah settingan yang kita lakukan sudah benar dengan:

```
/ip route print
```

SETTING DNS

Masukkan kode berikut untuk melakukan setting DNS Speedy:

```
/ip dns set primary-dns=202.134.1.10 allow-remote-request=yes
/ip dns set secondary-dns=202.134.0.155 allow-remote-request=yes
```

Selanjutnya setting **masquerade,** untuk meneruskan perintah dari routing dari semua client ke NAT firewall mikrotik.

```
/ip firewall nat add chain=srcnat action=masquerade
```

Langkah terakhir, buka winbox, pada menu pppoe yang barusan Anda buat, masuk ke menu PPP > *Interfaces* > dobel klik koneksi Anda > pilih Tab *Dial Out*, pastikan untuk menandai check box "*add default route*".

Setelah Proses diatas selesai, lakukan ping ke 202.134.0.10. jika koneksi terhubung berarti Gateway speedy sudah dimasukkan dalam daftar mikrotik dan Anda dapat mulai berselancar.

TROUBLESHOOT

Jika BELUM UP, periksa kembali:

1. Cek koneksi kabel dari modem ke perangkat mikrotik
2. Cek username dan password speedy

mawaridz@gmail.com

Jika Ping belum jalan atau muncul pesan error "*Invalid value for argument addresses*" berarti ada satu hal yang terlewat.

- Buka Winbox, masuk menu PPP. Dobel klik pada ppoe yang aktif. Tandai Check Box "*Add default route*" dan "*Use peer DNS*"

Jika masih ada yang bingung, baca panduan di forum dan lihat step-by-step toturial di bawah,,

Setting Mikrotik Wireless Bridge

kali, kita ingin menggunakan Mikrotik Wireless untuk solusi point to point dengan mode jaringan bridge (bukan routing). Namun, Mikrotik RouterOS sendiri didesain bekerja dengan sangat baik pada mode routing. Kita perlu melakukan beberapa hal supaya link wireless kita bisa bekerja untuk mode bridge.

Mode bridge memungkinkan network yang satu tergabung dengan network di sisi satunya secara transparan, tanpa perlu melalui routing, sehingga mesin yang ada di network yang satu bisa memiliki IP Address yang berada dalam 1 subnet yang sama dengan sisi lainnya.

Namun, jika jaringan wireless kita sudah cukup besar, mode bridge ini akan membuat traffic wireless meningkat, mengingat akan ada banyak traffic broadcast dari network yang satu ke network lainnya. Untuk jaringan yang sudah cukup besar, saya menyarankan penggunaan mode routing.

Berikut ini adalah diagram network yang akan kita set.

Konfigurasi Pada Access Point

1. Buatlah sebuah interface bridge yang baru, berilah nama bridge1

2. Masukkan ethernet ke dalam interface bridge

3. Masukkan IP Address pada interface bridge1

4. Selanjutnya adalah setting wireless interface. Kliklah pada menu Wireless (1), pilihlah tab interface (2) lalu double click pada nama interface wireless yang akan digunakan (3). Pilihlah mode AP-bridge (4), tentukanlah ssid (5), band 2.4GHz-B/G (6), dan frekuensi yang akan digunakan (7). Jangan lupa mengaktifkan default authenticated (8) dan default forward (9). Lalu aktifkankanlah interface wireless (10) dan klik OK (11).

5. Berikutnya adalah konfigurasi WDS pada wireless interface yang digunakan. Bukalah kembali konfigurasi wireless seperti langkah di atas, pilihlah tab WDS (1). Tentukanlah WDS Mode dynamic (2) dan pilihlah bridge interface untuk WDS ini (3). Lalu tekan tombol OK.

6. Langkah selanjutnya adalah menambahkan virtual interface WDS. Tambahkan interface WDS baru seperti pada gambar, lalu pilihlah interface wireless yang kita gunakan untuk WDS ini. Lalu tekan OK.

7. Jika WDS telah ditambahkan, maka akan tampak interface WDS baru seperti pada gambar di bawah.

Konfigurasi pada Wireless Station

Konfigurasi pada wireless station hampir sama dengan langkah-langkah di atas, kecuali pada langkah memasukkan IP Address dan konfigurasi wirelessnya. Pada konfigurasi station, mode yang digunakan adalah *station-wds*, frekuensi tidak perlu ditentukan, namun harus menentukan scan-list di mana frekuensi pada access point masuk dalam scan list ini. Misalnya pada access point kita menentukan frekuensi 2412, maka tuliskanlah scan-list 2400-2500.

Pengecekan link

Jika link wireless yang kita buat sudah bekerja dengan baik, maka pada menu wireless, akan muncul status R (lihat gambar di bawah).

mawaridz@gmail.com

Selain itu, mac-address dari wireless yang terkoneksi juga bisa dilihat pada jendela registration (lihat gambar di bawah).

Konfigurasi keamanan jaringan wireless

Pada Mikrotik, cara paling mudah untuk menjaga keamanan jaringan adalah dengan mendaftarkan mac-address wireless pasangan pada access list. Hal ini harus dilakukan pada sisi access point maupun pada sisi client. Jika penginputan access-list telah dilakukan, maka matikanlah fitur *default authenticated* pada wireless, maka wireless lain yang mac addressnya tidak terdaftar tidak akan bisa terkoneksi ke jaringan kita.

Jika kita menginginkan fitur keamanan yang lebih baik, kita juga bisa menggunakan enkripsi baik WEP maupun WPA.

Settingan pppoe speedy saya sudah saya tanam di dalam modem jadi saya gak pakai pppoe di mikrotik.

berikut contohnya buat mikrotik versi 3.xx (saya pakai di mikrotik 3.16) :

Ip Modem 01 : 192.168.1.1 interface=speedy1
IP Modem 02 : 192.168.2.1 interface=speedy2
IP Local : 10.18.92.1 interface=Local

Setting Buat Mangle

```
/ip firewall mangle
add chain=prerouting action=mark-connection new-connection-mark=Santaria1 \
passthrough=yes connection-state=new in-interface=Local nth=2,1 \
comment="" disabled=no
add chain=prerouting action=mark-routing new-routing-mark=Santaria1 passthrough=no \
in-interface=HotSpot connection-mark=Santaria1 comment="" disabled=no
add chain=prerouting action=mark-connection new-connection-mark=Santaria2 \
passthrough=yes connection-state=new in-interface=Local nth=1,1 \
comment="" disabled=no
add chain=prerouting action=mark-routing new-routing-mark=Santaria2 passthrough=no \
```

mawaridz@gmail.com

in-interface=HotSpot connection-mark=Santaria2 comment="" disabled=no

Setting NAT

/ip firewall nat
add chain=srcnat action=masquerade out-interface=speedy1
add chain=srcnat action=masquerade out-interface=speedy2
add chain=srcnat action=masquerade src-address="10.18.92.0/24"

Setting Routenya

/ ip route
add dst-address=0.0.0.0/0 gateway=192.168.1.1 scope=255 target-scope=10 \
routing-mark=Santaria1 comment="" disabled=no
add dst-address=0.0.0.0/0 gateway=192.168.2.1 scope=255 target-scope=10 \
routing-mark=Santaria2 comment="" disabled=no
add dst-address=0.0.0.0/0 gateway=192.168.1.1 scope=255 target-scope=10 \
comment="primary connection" disabled=no

Silahkan di coba untuk yg versi 2.9xx nyusul

Terima Kasih

Berikut scripting Load Balancing dengan konfigurasi 2 Line untuk Mikrotik versi 2.9.27
Sesuaikan IP masing-masing interface menurut network kita.

Note : 10.11.90.1 = IP Local
192.168.1.1 = IP Modem Speedy 1
192.168.2.1 = IP Modem Speedy 2

By JoySolutions.

/ ip address
add address=10.11.90.1/24 network=10.11.90.0 broadcast=10.11.90.255 \
interface=local comment="" disabled=no
add address=192.168.1.254/24 network=192.168.1.0 broadcast=192.168.1.255 \
interface="Internet" comment="" disabled=no

mawaridz@gmail.com

```
add address=192.168.2.254/24 network=192.168.2.0 broadcast=192.168.2.255 \
interface="Speedy" comment="" disabled=no

/ ip firewall mangle
add chain=prerouting in-interface=local connection-state=new nth=1,1,0 \
action=mark-connection new-connection-mark=santaria1 passthrough=yes \
comment="Load Balancing Client" disabled=no
add chain=prerouting in-interface=local connection-mark=santaria1 \
action=mark-routing new-routing-mark=santaria1 passthrough=no comment="" \
disabled=no
add chain=prerouting in-interface=local connection-state=new nth=1,1,1 \
action=mark-connection new-connection-mark=santaria2 passthrough=yes \
comment="" disabled=no
add chain=prerouting in-interface=local connection-mark=santaria2 \
action=mark-routing new-routing-mark=santaria2 passthrough=no comment="" \
disabled=no

/ ip firewall nat
add chain=srcnat out-interface="Internet" action=masquerade comment="" \
disabled=no
add chain=srcnat out-interface="Speedy" action=masquerade comment="" \
disabled=no

/ ip route
add dst-address=0.0.0.0/0 gateway=192.168.2.1 scope=255 target-scope=10 \
routing-mark=santaria1 comment="" disabled=no
add dst-address=0.0.0.0/0 gateway=192.168.1.1 scope=255 target-scope=10 \
routing-mark=santaria2 comment="" disabled=no
add dst-address=0.0.0.0/0 gateway=192.168.1.1 scope=255 target-scope=10 \
comment="primary connection" disabled=no
```

Thanks to Joysolution @ www.forummikrotik.com
Load Balancing nth buat Mikrotik Ver 3.xx dan 2.9xxkomentar (15)Load Balancing nth buat Mikrotik Ver 3.xx dan 2.9xx |

Redirect Mikrotik ke Komputer Proxy Squid (tanpa parent proxy MT)
Author: Ricky Mahardhika
•04:43

mawaridz@gmail.com

Redirect Mikrotik ke Komputer Proxy Squid (tanpa parent proxy MT)
Redirect Mikrotik ke Komputer Proxy Squid (tanpa parent proxy MT)

Siang rekan-rekan semua, saya mau berbagi pengalaman tapi sebelumnya mohon dima`afkan kalau ada kesalahan ya, maklum masih newbie banget. Begini Saya meredirect Mikrotik (MT) ke squid Proxy tanpa menghidupkan web-proxy yang ada di MT nya, saya sempat kesulitan mencari solusi supaya dapat me redirect port 80, 8080, ke port 3128 (transparent proxy), karena kalau saya pakai web-proxy MT internet saya jadi lemot koneksinya, pernah saya pakai parent proxy MT redirect ke squid tapi hasilnya gak

maksimal internet kadang masih lemot karena web-proxy di hidupkan (enable), makanya saya mencoba meng kotak-kotak eh meng kotak-katik akhirnya dapet referensi dari http://tldp.org/HOWTO/TransparentProxy-6.html, yang intinya bisa redirect port 80 ke 3128 tanpa menghidupkan web-proxy mikrotik. Topology yang saya gunakan adalah sebagai berikut :

ISP -? Mikrotik --? Switch -? Client
..... |
..... |
.....Squid-Box

Spesifikasi Mikrotik saya DOM 256Mb + Licensi level 5 Versi 3.3 up-grade (intel P3 1Ghz, Mem 512Mb)

Spesifikasi squid (Intel P4 3.0Ghz DDR 1Gb, HDD 80Gb SATA) OS Linux Ubuntu server 7.10 Gitsu Gibbon

Di mikrotik ada 3 LAN card terus saya namai lan, wan, proxy
Lan = 192.168.1.1
Wan = 202.114.12.112
Proxy = 192.168.0.1

Squid (Ubuntu 7.10 server)
Eth0 = 192.168.0.2

Untuk settingan awal MT gak perlu saya tulis disini ya, termasuk pembagian bandwidth nya, serta konfigurasi squidnya. saya langsung saja cara translasinya

mawaridz@gmail.com

Buat NAT nya dulu di IP firewall NAT (sharing internet)

/ip firewall nat add chain=srcnat out-interface=wan action=masquerade

Terus buat nat untuk redirect ke squid

/ip firewall nat add chain=dst-nat src-address=!192.168.0.2 protocol=tcp dst-port=80 in-interface=lan action=dst-nat to-address=192.168.0.2 to-port=3128

/ip firewall nat add chain=dst-nat src-address=!192.168.0.2 protocol=tcp dst-port=8080 in-interface=lan action=dst-nat to-address=192.168.0.2 to-port=3128

/ip firewall nat add chain=src-nat src-address=192.168.1.0 out-interface=lan action=srcnat src-address=192.168.1.1 to-port=3128

Terus buat filter rules nya

/ip firewall filter add chain=forward src-address=192.168.1.0 dst-address=192.168.0.2 dst-port=3128 in-interface=lan out-interface=wan action=accept

Nah sekarang coba deh, jadi bisa simpan cache di squid-proxy external tanpa harus lewat parent proxy nya mikrotik…

Kalau ada kendala coba di ubuntu servernya di tambahin ini (sebaiknya jgn diisi dulu di Ubuntunya kalau belum bisa konek baru isi iptables dibawah ini) :
iptables –t nat –A PREROUTNG –I eth0 –s ! SQUID – tcp –dport 80 –j DNAT –to SQUID:3128
iptables –t nat –A PREROUTNG –I eth0 –s ! SQUID – tcp –dport 8080 –j DNAT –to SQUID:3128
iptables –t nat –A POSTROUTING –o eth0 –s LAN –d SQUID –j SNAT –to iptables-box
iptables –A FORWARD –s LAN –d SQUID -i eth0 -p tcp -dport 3128 –j ACCEPT

sekali lagi mohon ma`af rekan-rekan semua, karena masih tahap belajar, mungkin kalau ada kesalahan mohon dikoreksi, atau ada tambahan mohon di benahi..

mawaridz@gmail.com

thx
Thanks to emruxc @ www.forummikrotik.com
Redirect Mikrotik ke Komputer Proxy Squid (tanpa parent proxy MT)komentar (0)Redirect Mikrotik ke Komputer Proxy Squid (tanpa parent proxy MT) |

Tutz Load Balancing Plus plus [Chaozz version]
Author: Ricky Mahardhika
•04:41
Tutz Load Balancing Plus plus [Chaozz version]
This is my first tutz i post in this forum. i hope this tutz is useful for all of you. i think this tutz is almost same with other but this is my version. bukan forum english ne. pk bhs indo aja ar..

ISP 1 IIX : 10.0.68.1
ISP 2 Vsat : 10.0.32.1 <- internasional
ISP 3 Speedy : 10.0.22.1 <- internasional Contoh aje

IP router ether1 (IIX) : 10.0.68.2/29
IP router ether2 (Vsat) : 10.0.32.2/29
IP router ether3 (Speedy) : 10.0.22.2/29
IP router ether4 (ke lan) : 192.168.1.1//24

Mangle

/ip fi ma add chain=prerouting src-address list=Vsat action=mark-routing new-routing-mark=Game comment=Vsat

/ip fi ma add chain=prerouting src-address list=Vsat dst-address list=nice action=mark-routing new-routing-mark=Vsat-iix comment=Vsat-iix

/ip fi ma add chain=prerouting src-address list=Speedy action=mark-routing new-routing-mark=Game comment=Speedy

/ip fi ma add chain=prerouting src-address list=Speedy dst-address list=nice

mawaridz@gmail.com

action=mark-routing new-routing-mark=Speedy-iix comment=Speedy-iix

/ip fi address-list add address=x.x.x.x list=nice (masukin ip iix)

http://ixp.mikrotik.co.id/download/nice.rsc

NAT

/ip fi nat

add chain=srcnat action=src-nat to-addresses=10.0.32.2 to-ports=0-65535
out-interface=ether2 routing-mark=Vsat

add chain=srcnat action=src-nat to-addresses=10.0.68.2 to-ports=0-65535
out-interface=ether2 routing-mark=Vsat-iix

add chain=srcnat action=src-nat to-addresses=10.0.22.2 to-ports=0-65535
out-interface=ether3 routing-mark=Speedy

chain=srcnat action=src-nat to-addresses=10.0.68.3 to-ports=0-65535
out-interface=ether3 routing-mark=Speedy-iix

/ip ro add dst-address=0.0.0.0/0 gateway=10.0.68.1
/ip ro add dst-address=0.0.0.0/0 gateway=10.0.32.1 mark=Vsat
/ip ro add dst-address=0.0.0.0/0 gateway=10.0.68.1 mark=Vsat-iix
/ip ro add dst-address=0.0.0.0/0 gateway=10.0.22.1 mark=Speedy
/ip ro add dst-address=0.0.0.0/0 gateway=10.0.68.1 mark=Speedy-iix

Sekarang da siap ne..
tinggal masukin ip mana yg anda mo di kasi akses internet (klo ga ga di address-list ya gak jln hehe) di masukin ke Vsat,Speedy di Address-list

Contoh:
/ip fi address-list add address=192.168.1.2 list=Vsat
/ip fi address-list add address=192.168.1.3 list=Speedy
/ip fi address-list add address=192.168.1.4 list=Speedy
/ip fi address-list add address=192.168.1.5 list=Speedy

mawaridz@gmail.com

/ip fi address-list add address=192.168.1.6 list=Vsat
/ip fi address-list add address=192.168.1.7 list=Speedy
/ip fi address-list add address=192.168.1.8 list=Vsat
/ip fi address-list add address=192.168.1.9 list=Speedy

Akhirnya Siap juga
mohon maaf klo ada yg salah.

Let's click "thank" if this posting is usefull.. Thank you
Thanks to Chaozz @ www.forummikrotik.com
Tutz Load Balancing Plus plus [Chaozz version]komentar (0)Tutz Load Balancing Plus plus [Chaozz version] |

LoadBalance + WebProxy Internal MikroTik
Author: Ricky Mahardhika
•04:37
LoadBalance + WebProxy Internal MikroTik + HOTSPOT --UPDATE--
--!!! WARNING Tested on MIKROTIK v3.10 !!!--

Yak... Udah Akang edit lagi karena ada beberapa yang perlu di "patch" tutorialnya, dan lagi-lagi seperti biasa, DILARANG COPY PASTE tanpa memberikan LINK ke Forum MikroTik, BIASAKAN HARGAI HASIL KARYA. Credit People Please.....

Well, pertama mari kita selaraskan dahulu dengan tutorial Akang sebelumnya yang berada di sini Setting PPPoE 5 Speedy lalu refer per-ILMU-an dari bro Deva dan rekan forum MT disini ip firewall mangel NTH untuk load balance kemudian membaca panduan dari beliau Mr. Valens di http://wiki.mikrotik.com/wiki/MUM_2008_ID

Catatan :
1. URUTAN MENENTUKAN PRESTASI Jangan ketuker
2. Akang menggunakan 1 NIC untuk Lokal dan HotSpot (dengan sistem bypass)
3. Oleh karena dan sebab no.2, jika menemukan "HotSpot" di interface itu sama saja interface lokal.

mawaridz@gmail.com

Code:

```
/ip firewall nat
add chain=srcnat src-address=IP Lokal action=masquerade
```

Yang Akang bold, penting agar HotSpot juga bisa menikmati akses, kemudian jangan lupakan tutz dari bro [a], yaitu Redirect Proxy

Konfigurasi NAT + HOTSPOT

Code:

```
/ip firewall nat add chain=dstnat src-address-list="IP Lokal" protocol=tcp dst-port=80
in-interface=Interface Lokal action=redirect to-ports=8888

--> NAT u/ HotSpot <--
/ip firewall nat add action=redirect chain=dstnat comment="NAT Proxy HotSpot"
disabled=no \
dst-port=80 hotspot=from-client,auth in-interface=HotSpot protocol=tcp \
src-address-list="IP HotSpot" to-ports=8888
```

Update!!!
Waspada dan patut diperhatikan, pada saat setting konfigurasi di IP HotSpot user profile, jangan di centang "transparent proxy", klient tetep bisa jalan dan terkena proxy tapi di NAT, rule tidak terkena paket.

Load Balance Versi-1
Code:

```
/ip firewall mangle
add action=mark-connection chain=prerouting comment="Load Balance" connection-
state=new disabled=no in-interface=HotSpot new-connection-mark=Line-1 nth=3,1 \
passthrough=yes
add action=mark-routing chain=prerouting comment="" connection-mark=Line-1
disabled=no in-interface=HotSpot new-routing-mark=Line-1 passthrough=no
add action=mark-connection chain=prerouting comment="" connection-state=new
```

```
disabled=no in-interface=HotSpot new-connection-mark=Line-2 nth=2,1 passthrough=\
yes
add action=mark-routing chain=prerouting comment="" connection-mark=Line-2
disabled=no in-interface=HotSpot new-routing-mark=Line-2 passthrough=no
add action=mark-connection chain=prerouting comment="" connection-state=new
disabled=no in-interface=HotSpot new-connection-mark=Line-3 passthrough=yes
add action=mark-routing chain=prerouting comment="" connection-mark=Line-3
disabled=no in-interface=HotSpot new-routing-mark=Line-3 passthrough=no
```

Load Balance Versi-2
Code:

```
/ip firewall mangle
add action=mark-connection chain=prerouting comment="Load Balance" connection-
state=new disabled=no in-interface=HotSpot new-connection-mark=Line-1 nth=3,1 \
passthrough=yes
add action=mark-routing chain=prerouting comment="" connection-mark=Line-1
disabled=no in-interface=HotSpot new-routing-mark=Line-1 passthrough=yes
add action=mark-connection chain=prerouting comment="" connection-state=new
disabled=no in-interface=HotSpot new-connection-mark=Line-2 nth=3,2 passthrough=\
yes
add action=mark-routing chain=prerouting comment="" connection-mark=Line-2
disabled=no in-interface=HotSpot new-routing-mark=Line-2 passthrough=yes
add action=mark-connection chain=prerouting comment="" connection-state=new
disabled=no in-interface=HotSpot new-connection-mark=Line-3 nth=3,3 passthrough=yes
add action=mark-routing chain=prerouting comment="" connection-mark=Line-3
disabled=no in-interface=HotSpot new-routing-mark=Line-3 passthrough=yes
```

Load Balance Untuk Proxy Versi-1
Code:

```
/ip firewall mangle
add action=mark-connection chain=output comment="Proxy Load Balance " connection-
state=new disabled=no new-connection-mark=koneksi-proxy-1 nth=3,1 \
passthrough=yes
add action=mark-routing chain=output comment="" connection-mark=koneksi-proxy-1
disabled=no new-routing-mark=Line-1 passthrough=no
add action=mark-connection chain=output comment="" connection-state=new disabled=no
```

new-connection-mark=koneksi-proxy-2 nth=2,1 passthrough=yes
add action=mark-routing chain=output comment="" connection-mark=koneksi-proxy-2 disabled=no new-routing-mark=Line-2 passthrough=no
add action=mark-connection chain=output comment="" connection-state=new disabled=no new-connection-mark=koneksi-proxy-3 passthrough=yes
add action=mark-routing chain=output comment="" connection-mark=koneksi-proxy-3 disabled=no new-routing-mark=Line-3 passthrough=no

Load Balance Untuk Proxy Versi-1
Code:

/ip firewall mangle
add action=mark-connection chain=output comment="Proxy Load Balance " connection-state=new disabled=no new-connection-mark=koneksi-proxy-1 nth=3,1 \
passthrough=yes
add action=mark-routing chain=output comment="" connection-mark=koneksi-proxy-1 disabled=no new-routing-mark=Line-1 passthrough=yes
add action=mark-connection chain=output comment="" connection-state=new disabled=no new-connection-mark=koneksi-proxy-2 nth=3,2 passthrough=yes
add action=mark-routing chain=output comment="" connection-mark=koneksi-proxy-2 disabled=no new-routing-mark=Line-2 passthrough=yes
add action=mark-connection chain=output comment="" connection-state=new disabled=no new-connection-mark=koneksi-proxy-3 nth=3,3 passthrough=yes
add action=mark-routing chain=output comment="" connection-mark=koneksi-proxy-3 disabled=no new-routing-mark=Line-3 passthrough=yes

Mangle untuk Queue
Code:

/ip firewall mangle
add action=mark-connection chain=prerouting comment="Mangle for Queue" disabled=no new-connection-mark=koneksi-klien passthrough=yes src-address=\
[b]IP Lokal[/ip]
add action=mark-packet chain=prerouting comment="" connection-mark=koneksi-klien disabled=no in-interface=HotSpot new-packet-mark=paket-upload passthrough=no
add action=mark-packet chain=prerouting comment="" connection-mark=koneksi-klien disabled=no new-packet-mark=paket-download passthrough=no
add action=mark-packet chain=output comment="" connection-mark=koneksi-klien

disabled=no dscp=4 new-packet-mark=paket-hit-download out-interface=HotSpot \
passthrough=no
add action=mark-packet chain=output comment="" connection-mark=koneksi-klien
disabled=no new-packet-mark=paket-download out-interface=HotSpot passthrough=no

Code:

/ip route
add comment="" disabled=no distance=1 dst-address=0.0.0.0/0 gateway=ADSL-1 \
routing-mark=Line-1
add comment="" disabled=no distance=1 dst-address=0.0.0.0/0 gateway=ADSL-2 \
routing-mark=Line-2
add comment="" disabled=no distance=1 dst-address=0.0.0.0/0 gateway=ADSL-3 \
routing-mark=Line-3
add comment="" disabled=no distance=1 dst-address=0.0.0.0/0 gateway=ADSL-1

Setelah sukses route jangan sampai kelupaan, ntar ga bisa jalan internetnya yaitu disini...

Code:

/ip proxy
set always-from-cache=yes cache-administrator=Akangage@ei-ji.net cache-
drive=system cache-hit-dscp=4 cache-on-disk=yes enabled=yes max-cache-
size=unlimited \
max-client-connections=600 max-fresh-time=3d max-server-connections=600 parent-
proxy=0.0.0.0 parent-proxy-port=0 port=8888 serialize-connections=no \
src-address=0.0.0.0

NOTES : Baca TELITI Jangan TERBURU NAPSU

Nah.... setelah semua itu beres, silahkan di tes dan di-uji-coba kan, sory no pics untuk Tutz... sengaja biar akal sehat temen2 MT disini jalan semua dan tidak sembarang Copy Paste tanpa refer back ke ForumMikrotik. Akang lampirkan hasil-nya saja yah...

Mari kita budayakan "Thanks" atas setiap jernih payah usaha seseorang agar lebih semangat
lagi dalam mencari ilmu yang baru..... jangan lupa klik "Thanks"

mawaridz@gmail.com

Thanks to Akangage @ www.forummikrotik.com
LoadBalance + WebProxy Internal MikroTikkomentar (3)LoadBalance + WebProxy Internal MikroTik |

contoh queue simple mikrotik
Author: Ricky Mahardhika
•01:24

```
/ queue simple
add name="Net_1" target-addresses=192.168.1.11/32 dst-address=0.0.0.0/0 \
interface=all parent=none direction=both priority=8 \
queue=default-small/default-small limit-at=0/0 max-limit=50000/512000 \
burst-limit=512000/512000 burst-threshold=256000/256000 burst-time=30s/30s \
total-queue=default-small time=0s-1d,sun,mon,tue,wed,thu,fri,sat \
disabled=no


add name="Net_2" target-addresses=192.168.1.12/32 dst-address=0.0.0.0/0 \
interface=all parent=none direction=both priority=8 \
queue=default-small/default-small limit-at=0/0 max-limit=50000/512000 \
burst-limit=512000/512000 burst-threshold=256000/256000 burst-time=30s/30s \
total-queue=default-small time=0s-1d,sun,mon,tue,wed,thu,fri,sat \
disabled=no
add name="Net_3" target-addresses=192.168.1.13/32 dst-address=0.0.0.0/0 \
interface=all parent=none direction=both priority=8 \
queue=default-small/default-small limit-at=0/0 max-limit=50000/512000 \
burst-limit=512000/512000 burst-threshold=256000/256000 burst-time=30s/30s \
total-queue=default-small time=0s-1d,sun,mon,tue,wed,thu,fri,sat \
disabled=no
add name="Net_4" target-addresses=192.168.1.14/32 dst-address=0.0.0.0/0 \
interface=all parent=none direction=both priority=8 \
queue=default-small/default-small limit-at=0/0 max-limit=50000/512000 \
burst-limit=512000/512000 burst-threshold=256000/256000 burst-time=30s/30s \
total-queue=default-small time=0s-1d,sun,mon,tue,wed,thu,fri,sat \
disabled=no
add name="Net_5" target-addresses=192.168.1.15/32 dst-address=0.0.0.0/0 \
interface=all parent=none direction=both priority=8 \
```

```
queue=default-small/default-small limit-at=0/0 max-limit=50000/512000 \
burst-limit=512000/512000 burst-threshold=256000/256000 burst-time=30s/30s \
total-queue=default-small time=0s-1d,sun,mon,tue,wed,thu,fri,sat \
disabled=no
add name="Net_6" target-addresses=192.168.1.16/32 dst-address=0.0.0.0/0 \
interface=all parent=none direction=both priority=8 \
queue=default-small/default-small limit-at=0/0 max-limit=50000/512000 \
burst-limit=512000/512000 burst-threshold=256000/256000 burst-time=30s/30s \
total-queue=default-small time=0s-1d,sun,mon,tue,wed,thu,fri,sat \
disabled=no
add name="Net_7" target-addresses=192.168.1.17/32 dst-address=0.0.0.0/0 \
interface=all parent=none direction=both priority=8 \
queue=default-small/default-small limit-at=0/0 max-limit=50000/512000 \
burst-limit=512000/512000 burst-threshold=256000/256000 burst-time=30s/30s \
total-queue=default-small time=0s-1d,sun,mon,tue,wed,thu,fri,sat \
disabled=no
add name="Net_8" target-addresses=192.168.1.18/32 dst-address=0.0.0.0/0 \
interface=all parent=none direction=both priority=8 \
queue=default-small/default-small limit-at=0/0 max-limit=50000/512000 \
burst-limit=512000/512000 burst-threshold=256000/256000 burst-time=30s/30s \
total-queue=default-small time=0s-1d,sun,mon,tue,wed,thu,fri,sat \
disabled=no
add name="Net_9" target-addresses=192.168.1.19/32 dst-address=0.0.0.0/0 \
interface=all parent=none direction=both priority=8 \
queue=default-small/default-small limit-at=0/0 max-limit=50000/512000 \
burst-limit=512000/512000 burst-threshold=256000/256000 burst-time=30s/30s \
total-queue=default-small time=0s-1d,sun,mon,tue,wed,thu,fri,sat \
disabled=no
add name="Operator" target-addresses=192.168.1.20/32 dst-address=0.0.0.0/0 \
interface=all parent=none direction=both priority=8 \
queue=default-small/default-small limit-at=0/0 max-limit=50000/512000 \
burst-limit=512000/512000 burst-threshold=256000/256000 burst-time=30s/30s \
total-queue=default-small time=0s-1d,sun,mon,tue,wed,thu,fri,sat \
disabled=no
add name="papap" target-addresses=192.168.1.30/32 dst-address=0.0.0.0/0 \
interface=all parent=none direction=both priority=8 \
queue=default-small/default-small limit-at=0/0 max-limit=50000/512000 \
burst-limit=512000/512000 burst-threshold=256000/256000 burst-time=30s/30s \
```

mawaridz@gmail.com

```
total-queue=default-small time=0s-1d,sun,mon,tue,wed,thu,fri,sat \
disabled=no
add name="anton" target-addresses=192.168.1.240/32 dst-address=0.0.0.0/0 \
interface=all parent=none direction=both priority=8 \
queue=default-small/default-small limit-at=0/0 max-limit=50000/512000 \
burst-limit=512000/512000 burst-threshold=256000/256000 burst-time=30s/30s \
total-queue=default-small time=0s-1d,sun,mon,tue,wed,thu,fri,sat \
disabled=no
add name="laptop" target-addresses=192.168.1.239/32 dst-address=0.0.0.0/0 \
interface=all parent=none direction=both priority=8 \
queue=default-small/default-small limit-at=0/0 max-limit=50000/512000 \
burst-limit=512000/512000 burst-threshold=256000/256000 burst-time=30s/30s \
total-queue=default-small time=0s-1d,sun,mon,tue,wed,thu,fri,sat \
disabled=no
```

contoh queue simple mikrotikkomentar (0)contoh queue simple mikrotik |

Redirect Mikrotik ke Komputer Proxy Squid (tanpa parent proxy MT)

Author: Ricky Mahardhika

•06:37

Redirect Mikrotik ke Komputer Proxy Squid (tanpa parent proxy MT)

by kusnan hadinata di 1:31 AM

Siang rekan-rekan semua, saya mau berbagi pengalaman tapi sebelumnya mohon dima`afkan kalau ada kesalahan ya, maklum masih newbie banget. Begini Saya meredirect Mikrotik (MT) ke squid Proxy tanpa menghidupkan web-proxy yang ada di MT nya, saya sempat kesulitan mencari solusi supaya dapat me redirect port 80, 8080, ke port 3128 (transparent proxy), karena kalau saya pakai web-proxy MT internet saya jadi lemot koneksinya, pernah saya pakai parent proxy MT redirect ke squid tapi hasilnya gak maksimal internet kadang masih lemot karena web-proxy di hidupkan (enable), makanya saya mencoba meng kotak-kotak eh meng kotak-katik akhirnya dapet referensi dari http://tldp.org/HOWTO/TransparentProxy-6.html, yang intinya bisa redirect port 80 ke 3128 tanpa menghidupkan web-proxy mikrotik. Topology yang saya gunakan adalah sebagai berikut

```
ISP - ▪ Mikrotik -- ▪ Switch - ▪ Client
..... |
..... |
```

mawaridz@gmail.com

.....Squid-Box

Spesifikasi Mikrotik saya DOM 256Mb + Licensi level 5 Versi 3.3 up-grade (intel P3 1Ghz, Mem 512Mb)

Spesifikasi squid (Intel P4 3.0Ghz DDR 1Gb, HDD 80Gb SATA) OS Linux Ubuntu server 7.10 Gitsu Gibbon

Di mikrotik ada 3 LAN card terus saya namai lan, wan, proxy
Lan = 192.168.1.1
Wan = 202.114.12.112
Proxy = 192.168.0.1

Squid (Ubuntu 7.10 server)
Eth0 = 192.168.0.2

Untuk settingan awal MT gak perlu saya tulis disini ya, termasuk pembagian bandwidth nya, serta konfigurasi squidnya. saya langsung saja cara translasinya

Buat NAT nya dulu di IP firewall NAT (sharing internet)

/ip firewall nat add chain=srcnat out-interface=wan action=masquerade

Terus buat nat untuk redirect ke squid

/ip firewall nat add chain=dst-nat src-address=!192.168.0.2 protocol=tcp dst-port=80 in-interface=lan action=dst-nat to-address=192.168.0.2 to-port=3128

/ip firewall nat add chain=dst-nat src-address=!192.168.0.2 protocol=tcp dst-port=8080 in-interface=lan action=dst-nat to-address=192.168.0.2 to-port=3128

/ip firewall nat add chain=src-nat src-address=192.168.1.0 out-interface=lan action=srcnat src-address=192.168.1.1 to-port=3128

Terus buat filter rules nya

/ip firewall filter add chain=forward src-address=192.168.1.0 dst-address=192.168.0.2

mawaridz@gmail.com

dst-port=3128 in-interface=lan out-interface=wan action=accept

Nah sekarang coba deh, jadi bisa simpan cache di squid-proxy external tanpa harus lewat parent proxy nya mikrotik…

Kalau ada kendala coba di ubuntu servernya di tambahin ini (sebaiknya jgn diisi dulu di Ubuntunya kalau belum bisa konek baru isi iptables dibawah ini) :
iptables –t nat –A PREROUTNG –I eth0 –s ! SQUID – tcp –dport 80 –j DNAT –to SQUID:3128
iptables –t nat –A PREROUTNG –I eth0 –s ! SQUID – tcp –dport 8080 –j DNAT –to SQUID:3128
iptables –t nat –A POSTROUTING –o eth0 –s LAN –d SQUID –j SNAT –to iptables-box
iptables –A FORWARD –s LAN –d SQUID -i eth0 -p tcp -dport 3128 –j ACCEPT

sekali lagi mohon ma`af rekan-rekan semua, karena masih tahap belajar, mungkin kalau ada kesalahan mohon dikoreksi, atau ada tambahan mohon di benahi
Redirect Mikrotik ke Komputer Proxy Squid (tanpa parent proxy MT)komentar (2)Redirect Mikrotik ke Komputer Proxy Squid (tanpa parent proxy MT) |

[How To] Blok Konten not WebSite
Author: Ricky Mahardhika
•22:31
[How To] Blok Konten not WebSite
Akhirnya nemu juga cara blokir konten dan bukan website-nya, silahkan di baca dan pahami serta ini adalah modifikasi punya Akang. All Credits goes to Bapak Harijanto DataUtama.Net, thanks pak atas Email-nya untuk saya!

ONLY FOR MikroTik Versi 3

Ok langsung aja menuju caranya...
1. Kumpulkan link yang ingin di blok, kalo Akang kebetulan nyobanya link ini
Code:

http://youtube.com/watch?v=QAg12t6UvcQ

mawaridz@gmail.com

2. Langsung menuju TKP di
Code:

/Ip firewall layer7-protocol add name="Blok-Konten"
regexp="http://youtube.com/watch?v=QAg12t6UvcQ"

3. Pindah ke Mangle
Notes : gunakan "Prerouting" jika pakai Masquerade dan "forward" jika tnapa Masquerade.
Code:

/ip fi ma add chain=prerouting action=mark-connection new-connection-mark=ilegal-url-connection passthrough=yes layer7-protocol="Blok-Konten"
/ip fi ma add chain=prerouting action=mark-packet new-packet-mark=ilegal-url-packet passthrough=yes connection-mark=ilegal-url-connection

4. Lalu menuju ke Filter
Notes : jika MikroTik untuk HotSpot gunakan "chain=hs-input" jika bukan untuk hotspot gunakan "chain=forward"
Code:

/ip fi fi add chain=forward action=jump jump-target=ilegal-url packet-mark=ilegal-url-packet
/ip fi fi add chain=ilegal-url action=log log-prefix="Ilegal"
/ip fi fi add chain=ilegal-url action=drop
atau boleh
/ip fi fi add chain=ilegal-url action=reject reject-with=icmp-network-unreachable

Yak sudah!! Silahkan dicoba, tapi itu hanya untuk 1 situs web dan 1 konten, jika ada 20 ya masukin satu-satu alamatnya beserta rule-nya

Once again, please don't copy paste without credit people, Thiz Tutz created by Mr. Harijanto DataUtama.Net and Modified by Akangage! so All the Credits goes to Mr. Harijanto
[How To] Blok Konten not WebSitekomentar (0)[How To] Blok Konten not WebSite |

Load Balance 2 ISP -Policy Routing based

mawaridz@gmail.com

Author: Ricky Mahardhika
•22:29
Load Balance 2 ISP -Policy Routing based on Client IP Address-
Waktu itu kalo g salah pernah ada di salah satu thread tapi g ada tuts-nya makanya sekarang mau nyumbang dulu....

ISP 1 : 10.0.128.13
ISP 2 : 202.6.238.253

mawaridz@gmail.com

Mari kita berandaikan jika jaringan kamu memiliki IP Address seperti ini :
Game : 192.178.40.0/26
Internet : 192.178.40.32/26
Router : 192.178.40.125/25

lalu, kita perlu menyeting mangle...
/ip fi ma add chain=prerouting src-address=192.178.40.0/26 action=mark-routing new-routing-mark=Game comment=Game
/ip fi ma add chain=prerouting src-address=192.178.40.32/26 action=mark-routing new-routing-mark=Internet comment=Internet

kemudian, menuju ke Route...
/ip ro add gateway=10.0.128.13 mark=Game
/ip ro add gateway=202.6.238.153 mark=Internet

Jangan melupakan NAT Masquerade yah
/ip na add chain=srcnat src-address=192.178.40.0/25 action=masquerade

Silahkan di coba di komputer client "Game" apakah sudah masuk ke jalur ISP 1 dan client "Internet" apakah sudah masuk ke jalur ISP 2

Thanks to Akangage @ www.forummikrotik.com
Load Balance 2 ISP -Policy Routing basedkomentar (0)Load Balance 2 ISP -Policy Routing based |

VPN di Speedy
Author: Ricky Mahardhika
•20:29
VPN di Speedy

Barangkali ada dari anda yang ingin menggabungkan 2 jaringan LAN speedy yang terpisah, yang tidak bisa di jangkau dengan jaringan wifi, tanpa biaya apapun disini saya pernah me-implementasikan pada warnet yang beda tempat, bisa juga di digunakan untuk kantor yang mempunyai cabang di beberapa tempat. saya sengaja mengunakan VPN ini dengan alasan untuk mempermudah saya dalam memaintence beberapa warnet yang saya kelola. cukup bikin satu server VPN, dan saya lebih mudah dalam memaintence dan memonitoring

mawaridz@gmail.com

jaringan yang ada di beberapa warnet tersebut dengan VPN ini saya juga dapat melakukan file sharing antar warnet, ok langsung kita ke inti, yang harus dipersiapan untuk disisi server : disini saya mengunakan Mikrotik router sebagai servernya untuk machine linux yang lain juga sudah pernah berhasil saya lakukan yaitu dengan UBUNTU, tapi untuk topik kali ini saya hanya menggarap khusus untuk Mikrotik router

Persiapan server:

Modem

Modem harus di set port forward atau diset sebagai bridge, disini saya pakai port forward port 1723 ke Mikrotik routernya,

Langkah-langkah

1. Seting IP Address untuk client VPN

Masuk ke mikrotik dengan winbox
masuk ke menu Ip —- Pool
Name = VPN (terserah anda)
address = 192.168.4.2-192.168.4.100 (sesuaikan dengan anda)

2 Aktifin VPN server

masuk ke menu PPP, lihat petunjuk gambar dibawah ini:

3. Berikut membuat Profile VPN Server, Lihat Di Gambar

Masih di menu PPP, klik tab "Profiles".
Name = VPN (atau terserah anda)
Local Address = berfungsi sebagai ip gateway di VPN nantinya
Remote Address = Untuk IP address VPN Client petunjuk langkah nomor 1
DNS Server = masukin DNS ISP

4. Membuat User VPN

Masih di menu PPP, klik tab Secrets
Name = username

mawaridz@gmail.com

Passpword = Password
Service = Pilih pptp
Profile = pilih profile yang kita buat di langkah 3

sekarang test koneksi dari klient di tempat yang terpisa dengan vpn server, bisa di warnet atau pakai speedy personal, saya mengunakan Windows xp,

masuk Ke Control Panel —- Network Connections —- New Conections

Bisa anda lihat dari gambar diabwah ini

di gambar yang terakhir dapat kita lihat client udah mendapatkan ip private dari server VPNnya, sekarang coba ping ke server vpnya (192.168.4.1) anda sudah dapat melakukan file transfer antar warnet atau antar kantor yang berjauhan. Kalau ada yang kurang silahkan di modifikasi sendiri :shock:

Selamat mencoba ***)))
Thanks to http://www.bodsink.net/vpn-speedy.asp
VPN di Speedykomentar (0)VPN di Speedy |

VPN (Virtual Private Network):
Author: Ricky Mahardhika
•20:22
VPN (Virtual Private Network):

Using Mikrotik VPN server in any Local Network of Head office, any folder of Data server can be shared from any branch office of any district / any country.

Most of the company have their Software in Head Office and Data of Branch offices send by Pen drive, floopy disk or CD and they are facing lots of hassle to send this data disk, branch to head office and head office to branch. VPN is the very much suitable solution for those company to escape them from disk sending hassle

* FAQ 1: Is it a costly solution ?

Ans: Not at all, Head office end price will Router + Configuration Charge. And Each remote office connecting costing will be modem price + Dialup connection + Configure.
* FAQ 2: Is it a secured system for Data ?

Ans: VPN is known as 100% secured Data transferred system because in this technology Data transfer with encription. No way of Hacking or Monitoring those Data.

* FAQ 3: Do we need to change existing Local Network Topology ?

Ans: If Client is not interested to do any change then it is possible without changing running network topology. Just one VPN server will be added, one Real IP will be required for VPN server.

* FAQ 4: Do we need any Expert Network Administrator to maintain it ?

Ans: No, Existing network administrator can handle it, necessary training will be provided by us.

* FAQ 5: Do we need Broad Band in all remote office ?

Ans: Dial up is enough for remote offices, Only head office may have Broad Band.

* FAQ 6: Do we need TNT phone line in all remote office ?

Ans: No, Because, GPRS is alternet dial up, where you have no TNT phone line.

* FAQ 7: How much time will take by dial up connection to send one text file from branch ?

Ans: text file takes 1or 2 minutes, larger file may take long time depending on Internet speed.

* FAQ 8: What will be monthly Internet bill per month per remote office ?

Ans: If remote office send text data file every end of the day, may required 50 Taka per month. If remote office remains connected continuously may required 600Taka to 1500Taka depending on transferred Data (Zoom).

* FAQ 9: Can we control bandwidth in same VPN server ?

Ans: Yes, it can be configured as NAT, Proxy, MRTG, http filter, link redundancy,DHCP, PPPoE, Firewall server.

* FAQ 10: Already we have one Mikrotik Router, Do we need to buy one more for VPN server ?

Ans: No, VPN server will be configured in existing MT server.

* FAQ 11: Is it possible to connect all PC of any branch without dialler ?

Ans: Yes, it is possible but Broad band, Real IP and one more MT router required for that branch.

* FAQ 12: Is VPN possible through Intranet ?

Yes, VPN is possible through Intranet of any nationwide data connectivity provider.

* FAQ 13: What about self security of VPN Router ?

We can ensure Satisfactory four layer (99.99%) Self security of VPN Router in the following ways:

a) User Name "admin" will be disabled, administrative user will created with any other name.

b) Administrative user will be restricted from Local IP of Administrator's PC.

c) VPN User's IP will be restricted as no one can connect from others IP of the world. It is one of the Important feature of Mikrotik Router which is not available in all router.

d) Top most strong firewall is input filter, this rule will filter all IP of the world except our (allowed) IP. This is master filter, because all source IP with all source port for all protocal is blocked for this router access. We can see how much packets droped by this rule.

We can also monitor how much attempt failed to access from log of the server.
Thanks to http://www.bijoy.net/mikrotik/virtual.html
VPN (Virtual Private Network):komentar (3)VPN (Virtual Private Network): |

Menu : Mikrotik Bumbu VPN / PPTP
Author: Ricky Mahardhika
•20:17
Menu : Mikrotik Bumbu VPN / PPTP

Bahan - Bahan :
Firewall DEVICE and PACKAGE :
- Redhat / Other Distro

mawaridz@gmail.com

- Install SNMP for Traffic monitoring
- Install Shorewall for Powerfull Firewall Protection
- Install HTTPD for Web Page to display MRTG Graph
- Install MRTG for Real Time Traffic Monitoring with Graphical Interface

PPTP Server :
- Mikrotik OS 2.9.0 Stable (Latest Version)

SERVER REDHAT :
ALL KIND OF SERVER AND PROCESSOR AND HARD DISK

SERVER MIKROTIK :
- CPU and motherboard : advanced 4th generation (core frequency 100MHz or more), 5th generation (Intel Pentium, Cyrix 6X86, AMD K5 or comparable) or newer uniprocessor Intel IA-32 (i386) compatible (multiple processors are not supported)
- RAM :minimum 32 MiB, maximum 1 GiB; 64 MiB or more recommended
- STORAGE medium :standard ATA/IDE interface controller and drive (not supported SCSI, USB controllers n drives, RAID controllers that require additional drivers) minimum of 64 Mb space; Flash and Microdrive devices may be connected using an adapted with ATA interface.

NOTE : If your machine have SATA Drive, ensure that your Machine BIOS, support COMBINED / LEGACY mode at SATA CONTROLLER (ini pengalaman pribadi), klo enggak coba tukerin tu mesin ma yang support aja hehehe .. ato jual ato anggurin dan minta maap hihihi tapi tetep usaha dulu ampe mentok n kringetan sapa tau ada ide.

Cara Memasak :

MIKROTIK OS (untuk VPN / PPTP USE)
1. Install Mikrotik OS
- Siapkan bumbu dapur .. hehe ... bukan dink .. beli mesin dulu .. server / PC minimal Pentium II juga gak papa RAM 64
- Di server / PC kudu ada minimal 2 ethernet, 1 ke arah Firewall dan 1 lagi ke Network yang akan dituju dr Internet via VPN.
- Siapkan CDROM untuk install (ini salah satu cara selain lewat Net Install dan Flashdisk belajar ndiri buat PR)
- Burn Source CD Mikrotik OS masukan ke CDROM
- Boot dari CDROM

mawaridz@gmail.com

- Ikuti petunjuk yang ada, jangan ragu2 hehehehe, klo salah ya .. coba lagi .. rusak Purchased lagi ^_^
- Install paket2 utama : System, PPP (untuk PPTP), Advanced Tools, Routing, Security.
- Setelah semua paket y6ang dibutuhkan diinstall maka untuk menginstallnya tekan "I"
- Lama Install jika PC / Server Sehat sekitar 5 menit lebih dr itu .. buang aja servernya ganti yang baru ..
- Setelah diinstall beres .. maka klo normal semuanya .. saat system restart .. maka akan kluar halaman login Mikrotik.

2. Configure Mikrotik OS (untuk VPN / PPTP)
- Login dengan Default User : Username : admin
Password : gak usah diisi langsung ENTER saja
- ketik "/setup"
- pilih untuk setup networknya .. ikuti petunjuk yang ada .. coba aja jangan takut .. gak hamil kok
- Sesuaikan IP addressnya dengan Network ID IP PC / Server tempat backup konfigurasi Mikrotik Sebelumnya agar bisa di-FTP (ini klo udah pernah install dan di-backup configurasinya)
- test ping ke IP PC / Server backup bila normal .. maka siap melakukan restore.

3. Restore Configurasi :
- FTP dulu ke mikrotik dengan IP, User dan password sesuai configurasi sebelumnya.
- setelah masuk ketik "bin" trus ENTER untuk mode binary
- kemudian ketik "put FILE_BACKUP_MIKROTIK" trus enter .. kuduna mah sukses (NOTE: sebelum melakukan FTP, harus ada di folder tempat si file backup berada).
- ketik "quit" untuk kluar
- di PC / Server tempat backup-an mikrotik, buka Internet Explorer trus ketikan dah disitu "IP_ADDRESS_MIKROTIK_ELU"
- download program WINBOX.EXE di Web yang terbuka (klik aja gambar Winbox-nya).
- Setelah download kelar .. klik 2 kali tu downloadan .. klo normal akan muncul si WINBOX
- ketikin di WINBOX, IP ADDRESS mikrotik lu, username ma passwordnya trus CONNECT
- Setelah berhasil masuk .. klik di FILE .. kemudian pilih File yang ada .. klik "RESTORE"
- DONE --> reboot MIKROTIk (Klik SYSTEM --> SHUTDOWN --> REBOOT)

4. Backup Configurasi :
- Sebaiknya setiap malam konfigurasi Mikrotik di backup agar tidak bingung bila ada masalah dengan masuk ke FILE di WINBOX

- Hapus backup sebelumnya (pastikan sudah dibackup), dan setelah kosong klik tombol BACKUP.
- buka START --> RUN --> CMD di PC yang akan jadi tempat backup
- masuk ke folder tempat file backup mo ditaruh (contoh "d:" kemudian "cd MikrotikBckup")
- ftp ke Mikrotik (misal :"ftp IP_MIKROTIK_ELU" trus ENTER)
- masukin User dan password
- setelah masuk.. maka masuk ke mode BIN dengan cara ketik "bin" trus ENTER.
- ketik "ls" untuk menampilkan isi backup
- ketik "get NAMA_FILE_BACKUP" Trus ENTER untuk mengambilnya.
- ketik "QUIT" untuk kluar

5. Firewall Rules di Mikrotik :
- Di WINBOX, Klik IP --> Firewall --> SOURCE NAT
- Di tabel Source NAT, add :
Masquerade packet dr SOURCE NETWORK_ID_LAN_ELU/NETMASK_LAN_ELU ke DESTINATION NETWORK_ID_YANG_DITUJU/NETMASK_YANG_DITUJU dengan OUTGOING INTERFACE-nya adalah nama interface yang dipake buat ke DESTINATION(lihat di bagian IP --> ADDRESS)

6. Mengaktifkan PPTP Server :
- di WINBOX, klik INTERFACE --> SETTING --> PPTP Server
- Setelah muncul tabel PPTP Server maka enable-kan, seluruh parameter default, dan check seluruh authentication yang ada (agar tidak ribet nyetting security di client PPTP).
- buat IP POOL yang berperan memberikan IP Dynamic pada setiap koneksi PPTP yang masuk dan berhasil konek dengan cara :
a. klik IP --> POOL, klik tanda "+" dan berikan NAMA serta masukkkan network atau range IP.
b. klik OK, Selesai .. sudah ? belum .. jalan masih panjang kawan heheeh .. terusin baca bawahnya gih .. ^_^
- buat USER PPTP dengan cara :
a. klik PPP --> Profiles, edit profile defaultnya dengan klik 2 kali (mo nambah juga gak papa, cuman biar gak ribet aja hehe)
b. masukkan LOCAL ADDRESS dengan IP ADDRESS yang dipegang oleh interface yang terhubung ke MESIN FIREWALL
c. drop down menu REMOTE ADDRESS dan pilih nama IP POOL yang udah dibuat (makanya IP POOL-nya gw duluin biar gak ditanya hehehe)
d. klik APPLY --> OK

e. klik SECRETS, NAME : isi dengan USERNAME dan PASSWORD untuk CLIENT
f. Masih di SECRETS, bagian SERVICE : pilih PPTP
g. Masih di SECRETS juga, jika diinginkan client hanya dial VPN dr IP public tertentu maka bagian CALLER ID diisi dengan IP PUBLIC Client tersebut (bisanya untuk kasus client adalah ISP atau Corporate Laen, untuk monitoring).
h. Jika ada kasus client menggunakan IP address LOCAL yang sama dengan IP Address yang didapat dari PPTP (biasanya client di Internet gedung atau perusahaan) maka jika koneksi VPN sudah ESTABLISH dan masih belum bisa ping, di bagian REMOTE ADDRESS untuk SECRETS dari user bersangkutan harus diisi dengan IP ADDRESS diluar dr range IP POOL tapi masih dalam satu network, kemudian tambahkan routing DEFAULT di PC CLIENT tersebut.

INSTALASI LINUX REDHAT UNTUK FIREWALL YANG BERADA DI DEPAN SERVER VPN / PPTP
1. Boot dr CD dengan CD Linux bersangkutan di dalamnya.
2. Selanjutnya seperti install OS biasa hehehe .. coba tanya mbah google untuk ini ato STTers yang laen pada jago2 tuh .. banyak kok source-nya.
3. Package yang dipilih saat install untuk keperluan ini gak usah semua .. banyak euy dan gak manfaat, contohnya X-Window, gak manfaat itu, khan buat server, Command line aja. Package yang perlu :
- KERNEL DEVELOPMENT : ini agar kita saat install RPM tertentu atau Source TGZ gak perlu compile macem2.
- EDITORS : buat ngedit mbah .. klo gak diinstal .. mo configure-nya gimana ? hehehe
- FIREWALL : butuh IPTABLESnya doank
- hmm .. lupa heheh .. kayanya masih ada yang laen .. sesuaiin aja dah sambil liat2 keterangan ma baca2 n belajar.
4. bila udah sukses install LINUX-nya maka tinggal install RPM tambahan seperti :
a. SHOREWALL : download dari http://www.shorewall.net dan baca juga dokumentasinya
b. SNMP : udah ada di CD linux REDHAT tinggal di RPM-kan, caranya ? baca google, hehehe gampang kok
c. MRTG : download dan baca dokumentasinya di http://people.ee.ethz.ch/~oetiker/webtools/mrtg/
d. HTTP : udah ada di CD LINUX REDHAT tinggal di RPM-in dan configure, caranya ? sama .. baca google lagi
e. WEBMIN : download dan baca dokumentasinya di http://www.webmin.com, gampang cari aja package RPM yang buat REDHAT.
5. RULES di SHOREWALL :
- DNAT TCP 1723 ke IP server PPTP

mawaridz@gmail.com

- DNAT Protocol 47 ke IP server PPTP
- RULES yang laen, sesuaikan dengan kebutuhan.
- DEFAULT RULES harus close all klo gak mao ada traffic2 maling hehehe.

PPTP SIAP DISAJIKAN ... INSTALL CLIENTNYA BIASA SAJA .. CUMAN DI BAGIAN SECURITY (Windows 2000 keatas) kudu dipilih ADVANCED trus SETTING .. pilih OPTIONAL ENCRYPTION ma PAP, CHAP, MSCHAPv2 udeh ...
Thanks to http://www.ikast3.org/modules/newbb/viewtopic.php?forum=9&post_id=57&topic_id=12
Menu : Mikrotik Bumbu VPN / PPTPkomentar (0)Menu : Mikrotik Bumbu VPN / PPTP |

Point to Point Tunnel Protocol (PPTP)
Author: Ricky Mahardhika
•20:15
Point to Point Tunnel Protocol (PPTP)
Document revision 1.8 (27-Mar-2003)
This document applies to MikroTik RouterOS v2.7

Table of Contents

mawaridz@gmail.com

Summary
PPTP (Point to Point Tunnel Protocol) supports encrypted tunnels over IP. The MikroTik RouterOS implementation includes support fot PPTP client and server.

General applications of PPTP tunnels:

* For secure router-to-router tunnels over the Internet
* To link (bridge) local Intranets or LANs (when EoIP is also used)
* For mobile or remote clients to remotely access an Intranet/LAN of a company (see PPTP setup for Windows for more information)

Each PPTP connection is composed of a server and a client. The MikroTik RouterOS may function as a server or client – or, for various configurations, it may be the server for some connections and client for other connections. For example, the client created below could connect to a Windows 2000 server, another MikroTik Router, or another router which supports a PPTP server.
Specifications
Packages required : ppp
License required : Basic (DEMO license is limited to 4 tunnels)
Home menu level : /interface pptp-server, /interface pptp-client
Protocols utilized : PPTP (RFC2637)
Hardware usage: not significant
Related Documents
Software Package Installation and Upgrading
IP Addresses and Address Resolution Protocol (ARP)
Authentication, Authorization and Accounting
Ethernet over IP (EoIP) Tunnel Interface

mawaridz@gmail.com

Description
PPTP is a secure tunnel for transporting IP traffic using PPP. PPTP encapsulates PPP in virtual lines that run over IP. PPTP incorporates PPP and MPPE (Microsoft Point to Point Encryption) to make encrypted links. The purpose of this protocol is to make well-managed secure connections between routers as well as between routers and PPTP clients (clients are available for and/or included in almost all OSs including Windows).

PPTP includes PPP authentication and accounting for each PPTP connection. Full authentication and accounting of each connection may be done through a RADIUS client or locally.

MPPE 40bit RC4 and MPPE 128bit RC4 encryption are supported.

PPTP traffic uses TCP port 1723 and IP protocol GRE (Generic Routing Encapsulation, IP protocol ID 47), as assigned by the Internet Assigned Numbers Authority (IANA). PPTP can be used with most firewalls and routers by enabling traffic destined for TCP port 1723 and protocol 47 traffic to be routed through the firewall or router.

PPTP connections may be limited or impossible to setup though a masqueraded/NAT IP connection. Please see the Microsoft and RFC links at the end of this section for more information.
PPTP Client Setup
Submenu level : /interface pptp-client
Property Description
name (name; default: pptp-out1) - interface name for reference
mtu (integer; default: 1460) - Maximum Transmit Unit. The optimal value is the MTU of the interface the tunnel is working over decreased by 40 (so, for 1500-byte ethernet link, set the MTU to 1460 to avoid fragmentation of packets)
mru (integer; default: 1460) - Maximum Receive Unit. The optimal value is the MTU of the interface the tunnel is working over decreased by 40 (so, for 1500-byte ethernet link, set the MRU to 1460 to avoid fragmentation of packets)
connect-to (IP address)- the IP address of the PPTP server to connect to
user (string)- user name to use when logging on to the remote server
password (string; default: "")- user password to use when logging to the remote server
profile (name; default: default) - profile to use when connecting to the remote server
add-default-route (yes | no; default: no) - whether to use the server which this client is connected to as its default router (gateway)
Example

mawaridz@gmail.com

To set up PPTP client named test2 using username john with password john to connect to the 10.1.1.12 PPTP server and use it as the default gateway:

```
[admin@MikroTik] interface pptp-client> add name=test2 connect-to=10.1.1.12 \
\... user=john add-default-route=yes password=john
[admin@MikroTik] interface pptp-client> print
Flags: X - disabled, R - running
0 X name="test2" mtu=1460 mru=1460 connect-to=10.1.1.12 user="john"
password="john" profile=default add-default-route=yes


[admin@MikroTik] interface pptp-client> enable 0
```

Monitoring PPTP Client
Command name : /interface pptp-client monitor
Property Description
Statistics:

uptime (time) - connection time displayed in days, hours, minutes, and seconds
encoding (string) - encryption and encoding (if asymmetric, separated with '/') being used in this connection
status (string) - status of the client:
Dialing – attempting to make a connection
Verifying password... - connection has been established to the server, password verification in progress
Connected – self-explanatory
Terminated – interface is not enabled or the other side will not establish a connection

Example
Example of an established connection:

```
[admin@MikroTik] interface pptp-client> monitor test2
uptime: 4h35s
encoding: MPPE 128 bit, stateless
status: Connected
[admin@MikroTik] interface pptp-client>
```

PPTP Server Setup

mawaridz@gmail.com

Submenu level : /interface pptp-server server

```
[admin@MikroTik] interface pptp-server server> print
enabled: no
mtu: 1460
mru: 1460
authentication: mschap2
default-profile: default
[admin@MikroTik] interface pptp-server server>
```

Description
The PPTP server supports unlimited connections from clients. For each current connection, a dynamic interface is created.
Property Description
enabled (yes | no; default: no) - defines whether PPTP server is enabled or not
mtu (integer; default: 1460) - Maximum Transmit Unit. The optimal value is the MTU of the interface the tunnel is working over decreased by 40 (so, for 1500-byte ethernet link, set the MTU to 1460 to avoid fragmentation of packets)
mru (integer; default: 1460) - Maximum Receive Unit. The optimal value is the MTU of the interface the tunnel is working over decreased by 40 (so, for 1500-byte ethernet link, set the MTU to 1460 to avoid fragmentation of packets)
authentication (multiple choice: pap | chap | mschap1 | mschap2; default: mschap2) - authentication algorithm
default-profile (name; default: default) - default profile to use
Example
To enable PPTP server:

```
[admin@MikroTik] interface pptp-server server> set enabled=yes
[admin@MikroTik] interface pptp-server server> print
enabled: yes
mtu: 1460
mru: 1460
authentication: mschap2
default-profile: default
[admin@MikroTik] interface pptp-server server>
```

PPTP Server Users
Submenu level : /interface pptp-server

mawaridz@gmail.com

Description
There are two types of items in PPTP server configuration - static users and dynamic connections. A dynamic connection can be established if the user database or the default-profile has its local-address and remote-address set correctly. When static users are added, the default profile may be left with its default values and only P2P user (in /ppp secret) should be configured. Note that in both cases P2P users must be configured properly.
Property Description
name - interface name
user - the name of the user that is configured statically or added dynamically

Statistics:

mtu - shows (cannot be set here) client's MTU
client-address - shows (cannot be set here) the IP of the connected client
uptime - shows how long the client is connected
encoding (string) - encryption and encoding (if asymmetric, separated with '/') being used in this connection
Example
To add a static entry for ex1 user:

```
[admin@MikroTik] interface pptp-server> add user=ex1
[admin@MikroTik] interface pptp-server> print
Flags: X - disabled, D - dynamic, R - running
# NAME USER MTU CLIENT-ADDRESS UPTIME ENC...
0 DR  ex 1460 10.0.0.202 6m32s none
1 pptp-in1 ex1
[admin@MikroTik] interface pptp-server>
```

In this example an already connected user ex is shown besides the one we just added.
PPTP Router-to-Router Secure Tunnel Example
The following is an example of connecting two Intranets using an encrypted PPTP tunnel over the Internet.

There are two routers in this example:

* [HomeOffice]
Interface LocalHomeOffice 10.150.2.254/24

mawaridz@gmail.com

Interface ToInternet 192.168.80.1/24

* [RemoteOffice]
Interface ToInternet 192.168.81.1/24
Interface LocalRemoteOffice 10.150.1.254/24

Each router is connected to a different ISP. One router can access another router through the Internet.

On the PPTP server a user must be set up for the client:

```
[admin@HomeOffice] ppp secret> add name=ex service=pptp password=lkjrht
local-address=10.0.103.1 remote-address=10.0.103.2
[admin@HomeOffice] ppp secret> print detail
Flags: X - disabled
0 name="ex" service=pptp caller-id="" password="lkjrht" profile=default
local-address=10.0.103.1 remote-address=10.0.103.2 routes==""

[admin@HomeOffice] ppp secret>
```

Then the user should be added in the PPTP server list:

```
[admin@HomeOffice] interface pptp-server> add user=ex
[admin@HomeOffice] interface pptp-server> print
Flags: X - disabled, D - dynamic, R - running
# NAME USER MTU CLIENT-ADDRESS UPTIME ENC...
0 pptp-in1 ex
[admin@HomeOffice] interface pptp-server>
```

And finally, the server must be enabled:

```
[admin@HomeOffice] interface pptp-server server> set enabled=yes
[admin@HomeOffice] interface pptp-server server> print
enabled: yes
mtu: 1460
mru: 1460
authentication: mschap2
default-profile: default
```

[admin@HomeOffice] interface pptp-server server>

Add a PPTP client to the RemoteOffice router:

[admin@RemoteOffice] interface pptp-client> add connect-to=192.168.80.1 user=ex \
\... password=lkjrht disabled=no
[admin@RemoteOffice] interface pptp-client> print
Flags: X - disabled, R - running
0 R name="pptp-out1" mtu=1460 mru=1460 connect-to=192.168.80.1 user="ex"
password="lkjrht" profile=default add-default-route=no

[admin@RemoteOffice] interface pptp-client>

Thus, a PPTP tunnel is created between the routers. This tunnel is like an Ethernet point-to-point connection between the routers with IP addresses 10.0.103.1 and 10.0.103.2 at each router. It enables 'direct' communication between the routers over third party networks.

To route the local Intranets over the PPTP tunnel – add these routes:

[admin@HomeOffice] > ip route add dst-address 10.150.1.0/24 gateway 10.0.103.2
[admin@RemoteOffice] > ip route add dst-address 10.150.2.0/24 gateway 10.0.103.1

On the PPTP server it can alternatively be done using routes parameter of the user configuration:

[admin@HomeOffice] ppp secret> print detail
Flags: X - disabled
0 name="ex" service=pptp caller-id="" password="lkjrht" profile=default
local-address=10.0.103.1 remote-address=10.0.103.2 routes==""

[admin@HomeOffice] ppp secret> set 0 routes="10.150.1.0/24 10.0.103.2 1"
[admin@HomeOffice] ppp secret> print detail
Flags: X - disabled
0 name="ex" service=pptp caller-id="" password="lkjrht" profile=default
local-address=10.0.103.1 remote-address=10.0.103.2
routes="10.150.1.0/24 10.0.103.2 1"

[admin@HomeOffice] ppp secret>

Test the PPTP tunnel connection:

[admin@RemoteOffice]> /ping 10.0.103.1
10.0.103.1 pong: ttl=255 time=3 ms
10.0.103.1 pong: ttl=255 time=3 ms
10.0.103.1 pong: ttl=255 time=3 ms
ping interrupted
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 3/3.0/3 ms

Test the connection through the PPTP tunnel to the LocalHomeOffice interface:

[admin@RemoteOffice]> /ping 10.150.2.254
10.150.2.254 pong: ttl=255 time=3 ms
10.150.2.254 pong: ttl=255 time=3 ms
10.150.2.254 pong: ttl=255 time=3 ms
ping interrupted
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 3/3.0/3 ms

To bridge a LAN over this secure tunnel, please see the example in the 'EoIP' section of the manual. To set the maximum speed for traffic over this tunnel, please consult the 'Queues' section.

Connecting a Remote Client via PPTP Tunnel
The following example shows how to connect a computer to a remote office network over PPTP encrypted tunnel giving that computer an IP address from the same network as the remote office has (without need of bridging over eoip tunnels)

Please, consult the respective manual on how to set up a PPTP client with the software You are using.

The router in this example:

* [RemoteOffice]

mawaridz@gmail.com

Interface ToInternet 192.168.81.1/24
Interface Office 10.150.1.254/24

The client computer can access the router through the Internet.

On the PPTP server a user must be set up for the client:

```
[admin@RemoteOffice] ppp secret> add name=ex service=pptp password=lkjrht
local-address=10.150.1.254 remote-address=10.150.1.2
[admin@RemoteOffice] ppp secret> print detail
Flags: X - disabled
0 name="ex" service=pptp caller-id="" password="lkjrht" profile=default
local-address=10.150.1.254 remote-address=10.150.1.2 routes==""

[admin@RemoteOffice] ppp secret>
```

Then the user should be added in the PPTP server list:

```
[admin@RemoteOffice] interface pptp-server> add name=FromLaptop user=ex
[admin@RemoteOffice] interface pptp-server> print
Flags: X - disabled, D - dynamic, R - running
# NAME USER MTU CLIENT-ADDRESS UPTIME ENC...
0 FromLaptop ex
[admin@RemoteOffice] interface pptp-server>
```

And the server must be enabled:

```
[admin@RemoteOffice] interface pptp-server server> set enabled=yes
[admin@RemoteOffice] interface pptp-server server> print
enabled: yes
mtu: 1460
mru: 1460
authentication: mschap2
default-profile: default
[admin@RemoteOffice] interface pptp-server server>
```

Finally, the proxy APR must be enabled on the 'Office' interface:

```
[admin@RemoteOffice] interface ethernet> set Office arp=proxy-arp
[admin@RemoteOffice] interface ethernet> print
Flags: X - disabled, R - running
# NAME MTU MAC-ADDRESS ARP
0 R ToInternet 1500 00:30:4F:0B:7B:C1 enabled
1 R Office 1500 00:30:4F:06:62:12 proxy-arp
[admin@RemoteOffice] interface ethernet>
```

PPTP Setup for Windows
Microsoft provides PPTP client support for Windows NT, 2000, ME, 98se, and 98. Windows 98se, 2000, and ME include support in the Windows setup or automatically install PPTP. For 95, NT, and 98, installation requires a download from Microsoft. Many ISPs have made help pages to assist clients with Windows PPTP installation.

http://www.real-time.com/Customer_Support/PPTP_Config/pptp_config.html
http://www.microsoft.com/windows95/downloads/contents/WUAdminTools/S_WUNetworkingTools/W95WinsockUpgrade/Default.asp

Sample instructions for PPTP (VPN) installation and client setup – Windows 98se

If the VPN (PPTP) support is installed, select 'Dial-up Networking' and 'Create a new connection'. The option to create a 'VPN' should be selected. If there is no 'VPN' options, then follow the installation instructions below. When asked for the 'Host name or IP address of the VPN server', type the IP address of the router. Double-click on the 'new' icon and type the correct user name and password (must also be in the user database on the router or RADIUS server used for authentication).

The setup of the connections takes nine seconds after selection the 'connect' button. It is suggested that the connection properties be edited so that 'NetBEUI', 'IPX/SPX compatible', and 'Log on to network' are unselected. The setup time for the connection will then be two seconds after the 'connect' button is selected.

To install the 'Virtual Private Networking' support for Windows 98se, go to the 'Setting' menu from the main 'Start' menu. Select 'Control Panel', select 'Add/Remove Program', select the 'Windows setup' tab, select the 'Communications' software for installation and 'Details'. Go to the bottom of the list of software and select 'Virtual Private Networking' to be installed.
Troubleshooting

mawaridz@gmail.com

* I use firewall and I cannot establish PPTP connection
Make sure the TCP connections to port 1723 can pass through both directions between your sites. Also, IP protocol 47 should be passed through.

Additional Resources
Links for PPTP documentation:

http://msdn.microsoft.com/library/backgrnd/html/understanding_pptp.htm
http://support.microsoft.com/support/kb/articles/q162/8/47.asp
http://www.ietf.org/rfc/rfc2637.txt?number=2637
http://www.ietf.org/rfc/rfc3078.txt?number=3078
http://www.ietf.org/rfc/rfc3079.txt?number=3079

Thanks to http://www.mikrotik.com/documentation//manual_2.7/Interface/PPTP.html
Point to Point Tunnel Protocol (PPTP)komentar (0)Point to Point Tunnel Protocol (PPTP) |

VPN menggunakan PPTP Server Mikrotik
Author: Ricky Mahardhika
•20:13

```
/ interface ethernet
set ether1 name="ether1"

/ interface bridge
add name="lan" arp=proxy-arp

/ interface bridge port
add interface=ether1 bridge=lan

/ ip address
add address=192.168.0.1/24 interface=lan

/ ip dns
allow-remote-requests=yes

/ ip firewall service-port
set gre disabled=no
```

mawaridz@gmail.com

```
set pptp disabled=no

/ ip pool
add name="pptp" ranges=192.168.0.200-192.168.0.229

/ ppp profile
add name="pptp-in" local-address=192.168.0.1 remote-address=pptp \

use-encryption=required only-one=yes change-tcp-mss=yes \

dns-server=192.168.0.1

/ interface pptp-server server
set enabled=yes max-mtu=1460 max-mru=1460 \

authentication=chap,mschap1,mschap2 default-profile=pptp-in

/ ppp secret
add name="sony1" service=pptp password="cape_d" profile=pptp-in
add name="sony2" service=pptp password="cape_d" profile=pptp-in


# done
```

Thanks to www.sony.web.id
VPN menggunakan PPTP Server Mikrotikkomentar (0)VPN menggunakan PPTP Server Mikrotik |

MIKROTIK SEBAGAI ACCESS CONSENTRATOR VPN
Author: Ricky Mahardhika
•20:07
MIKROTIK SEBAGAI ACCESS CONSENTRATOR VPN

Mikrotik VPN

VPN merupakan singkatan dari Virtual Private Network, sekarang VPN mulai digunakan sebagai salah satu layanan ISP di Indonesia, sebagai contoh Indosat Mega Media (IM2), dan beberapa ISP besar lainnya. VPN memungkinkan kita untuk masuk kedalam jaringan internal perusahaan kita, ataupun ISP kita dari provider internet yang lainnya. VPN terdiri atas dua macam yaitu PPTP dan L2TP. PPTP sering digunakan untuk membangun

mawaridz@gmail.com

VPN yang relatif sederhana jika dibandingkan dengan L2TP, karena L2TP memungkinkan enkripsi data sehingga data yang dikirimkan dapat dijamin keamanannya saat melewati jaringan yang tidak kita kenal

Namun, pada kesempatan kali ini saya akan mencoba memberikan penjelasan tentang PPTP. Tingkat lisensi minimal yang diperlukan untuk membuat mikrotik sebagai AC (Access Concentrators) adalah level 4 dengan user aktif sebanyak 200 pengguna, saya rasa jumlah pengguna sekian itu sudah cukup untuk ISP atau kantor-kantor yang ukurannya tidak terlalu besar. Cara setting mikrotik dasar sudah banyak dibahas di internet, saya tidak akan membahasnya di blog saya ini.Untuk mengaktifkan mikrotik sebagai Access Concentrator bagi VPN anda, masukkan ke menu PPP, kemudian masuk pada tab Interface cari bagian PPTP Server, setelah anda klik pada bagian tersebut, aktifkan PPTP Server dengan memberikan tanda centang pada "Enable", kemudian klik OK.

Mikrotik VPN Server

Setelah anda mengaktifkan PPTP Server sekarang masuklah kedalam tab secret, kemudian buat user baru, dengan rincian
Name :
Pass :
Service :
Service pada PPP ini ada berbagai macam seperti PPP (Menggunakan analog modem), L2TP, PPPoE (Seperti Speedy), dan lainnya. Jika diset ke "Any" maka username tersebut dapat digunakan untuk login melalui media di atas.
Profile :

Mikrotik UserMikrotik User

Setelah anda selesai membuat user baru, sekarang kita berpindah ke tab profile, disini kita dapat mengatur berbagai parameter tentang server kita ini. Yang perlu dirubah disini adalah local address, remote address, dan DNS Server. Untuk local address kita isi dengan alamat server PPTP kita, sedangkan remote address dapat ditentukan melalui static allocation atau dynamic allocation, penggunaan dynamic allocation lebih fleksibel dibandingkan dengan statik. Untuk menggunakan dynamic allocation kita harus melakukan pengalokasian IP address space melalui menu IP>Pool. Setelah anda membuat pool, silakan masukkan nama pool tersebut kedalam kolom remote-address. Sehingga user yang terkoneksi ke server kita akan mendapatkan IP Address secara otomatis. PPTP tidak

dapat menggunakan DHCP server, harus menggunakan alokasi yang telah ditentukan sebenarnya.

Server Profile

Silakan anda coba dengan membuat koneksi menggunakan VPN ke server anda, setting VPN untuk Windows XP akan saya bahas pada kesempatan mendatang. Koneksi akan segera terjalin dengan server VPN, anda pun dapat menggunakannya untuk keperluan anda.
Thanks to http://indramgl.wordpress.com
MIKROTIK SEBAGAI ACCESS CONSENTRATOR VPNkomentar (0)MIKROTIK SEBAGAI ACCESS CONSENTRATOR VPN |

Dynamic DNS Update Script for ChangeIP.com
Author: Ricky Mahardhika
•04:57
Dynamic DNS Update Script for ChangeIP.com

The following script should be created when you wish to update your ChangeIP.com Dynamic DNS account. Once created you should schedule this to run once in a while. The :global variables should be edited to include your unique username and password, interface name, etc.

The script below is RouterOS 3.0 Compatible!

An updated script here (01/20/08) should allow auto-detection of the default gateways interface name. This script below can be used if you have more than 1 WAN connection, but only 1 is active at a time

```
# Define User Variables
:global ddnsuser "CHANGEIPUSERID"
:global ddnspass "CHANGEIPPASSWORD"
:global ddnshost "FREEHOSTNAME.TOUPDATE.TLD"

# Define Global Variables
:global ddnsip
:global ddnslastip
:if ([ :typeof $ddnslastip ] = nil ) do={ :global ddnslastip "0" }
```

mawaridz@gmail.com

```
:global ddnsinterface
:global ddnssystem ("mt-" . [/system package get system version] )

# Define Local Variables
:local int

# Loop thru interfaces and look for ones containing
# default gateways without routing-marks
:foreach int in=[/ip route find dst-address=0.0.0.0/0 active=yes ] do={
:if ([:typeof [/ip route get $int routing-mark ]] != str ) do={
:global ddnsinterface [/ip route get $int interface]
}
}

# Grab the current IP address on that interface.
:global ddnsip [ /ip address get [/ip address find interface=$ddnsinterface ] address ]

# Did we get an IP address to compare?
:if ([ :typeof $ddnsip ] = nil ) do={
:log info ("DDNS: No ip address present on " . $ddnsinterface . ", please check.")
} else={

:if ($ddnsip != $ddnslastip) do={

:log info "DDNS: Sending UPDATE!"
:log info [ :put [/tool dns-update name=$ddnshost address=[:pick $ddnsip 0 [:find
$ddnsip "/"] ] key-name=$ddnsuser key=$ddnspass ] ]
:global ddnslastip $ddnsip

} else={
:log info "DDNS: No update required."
}

}

# End of script
```

mawaridz@gmail.com

If errors or problems occur with the above scripts please check to see if we are even receiving any updates. https://www.changeip.com/Reports/DDNSUpdates.asp will show you current updates on your account. Feel free to contact Support at ChangeIP.com if you are having problems.

2.9 Series: (Please use the above for the newer 3.0 version - this version is left here for archival reasons.)

```
:log info "DDNS: Begin"

:global ddns-user "YOURUSERID"
:global ddns-pass "YOURPASSWORD"
:global ddns-host "*1"
:global ddns-interface "EXACTINTERFACENAME"

:global ddns-ip [ /ip address get [/ip address find interface=$ddns-interface] address ]

:if ([ :typeof $ddns-lastip ] = nil ) do={ :global ddns-lastip 0.0.0.0/0 }

:if ([ :typeof $ddns-ip ] = nil ) do={

:log info ("DDNS: No ip address present on " . $ddns-interface . ", please check.")

} else={

:if ($ddns-ip != $ddns-lastip) do={

:log info "DDNS: Sending UPDATE!"
:log info [ /tool dns-update name=$ddns-host address=[:pick $ddns-ip 0 [:find $ddns-ip
"/"] ] key-name=$ddns-user key=$ddns-pass ]
:global ddns-lastip $ddns-ip

} else={

:log info "DDNS: No change"

}

}
```

```
:log info "DDNS: End"
```

For those of you that like to use the CLI, and want to make sure you get a very clean import with no line breaks, etc, you can run this script to create it for you:

```
/system script
add name=HomingBeaconDynamicDNSUpdater policy=\
ftp,reboot,read,write,policy,test,winbox,password,sniff \
source="# Define User Variables\r\
\n:global ddnsuser \"CHANGEIPUSERID\"\r\
\n:global ddnspass \"CHANGEIPPASSWORD\"\r\
\n:global ddnshost \"FREEHOSTNAME.TOUPDATE.TLD\"\r\
\n\r\
\n# Define Global Variables\r\
\n:global ddnsip\r\
\n:global ddnslastip\r\
\n:if ([ :typeof \$ddnslastip ] = nil ) do={ :global ddnslas\
tip \"0\" }\r\
\n\r\
\n:global ddnsinterface\r\
\n:global ddnssystem (\"mt-\" . [/system package get system \
version] )\r\
\n\r\
\n# Define Local Variables\r\
\n:local int\r\
\n\r\
\n# Loop thru interfaces and look for ones containing\r\
\n# default gateways without routing-marks\r\
\n:foreach int in=[/ip route find dst-address=0.0.0.0/0 acti\
ve=yes ] do={ \r\
\n :if ([:typeof [/ip route get \$int routing-mark ]] != st\
r ) do={\r\
\n :global ddnsinterface [/ip route get \$int interface]\
\r\
\n } \r\
\n}\r\
\n\r\
\n# Grab the current IP address on that interface.\r\
```

mawaridz@gmail.com

```
\n:global ddnsip [ /ip address get [/ip address find interfa\
ce=\$ddnsinterface ] address ]\r\
\n\r\
\n# Did we get an IP address to compare\?\r\
\n:if ([ :typeof \$ddnsip ] = nil ) do={\r\
\n :log info (\"DDNS: No ip address present on \" . \$ddns\
interface . \", please check.\")\r\
\n} else={\r\
\n\r\
\n :if (\$ddnsip != \$ddnslastip) do={\r\
\n\r\
\n :log info \"DDNS: Sending UPDATE!\"\r\
\n :log info [ :put [/tool dns-update name=\$ddnshost add\
ress=[:pick \$ddnsip 0 [:find \$ddnsip \"/\"] ] key-name=\$d\
dnsuser key=\$ddnspass ] ]\r\
\n :global ddnslastip \$ddnsip\r\
\n\r\
\n } else={ \r\
\n :log info \"DDNS: No update required.\"\r\
\n }\r\
\n\r\
\n}\r\
\n\r\
\n# End of script"
```

Dynamic DNS Update Script for ChangeIP.comkomentar (0)Dynamic DNS Update Script for ChangeIP.com |

_

Tutorial Mikrotik VPN : Point to Point Tunnel Protocol (PPTP)

Author: Ricky Mahardhika

•04:55

Tutorial Mikrotik VPN : Point to Point Tunnel Protocol (PPTP)

Summary

PPTP (Point to Point Tunnel Protocol) supports encrypted tunnels over IP. The MikroTik RouterOS implementation includes support fot PPTP client and server.

General applications of PPTP tunnels:

* For secure router-to-router tunnels over the Internet
* To link (bridge) local Intranets or LANs (when EoIP is also used)

mawaridz@gmail.com

* For mobile or remote clients to remotely access an Intranet/LAN of a company (see PPTP setup for Windows for more information)
Each PPTP connection is composed of a server and a client. The MikroTik RouterOS may function as a server or client – or, for various configurations, it may be the server for some connections and client for other connections. For example, the client created below could connect to a Windows 2000 server, another MikroTik Router, or another router which supports a PPTP server.

Description
PPTP is a secure tunnel for transporting IP traffic using PPP. PPTP encapsulates PPP in virtual lines that run over IP. PPTP incorporates PPP and MPPE (Microsoft Point to Point Encryption) to make encrypted links. The purpose of this protocol is to make well-managed secure connections between routers as well as between routers and PPTP clients (clients are available for and/or included in almost all OSs including Windows).

PPTP includes PPP authentication and accounting for each PPTP connection. Full authentication and accounting of each connection may be done through a RADIUS client or locally.

MPPE 40bit RC4 and MPPE 128bit RC4 encryption are supported.

PPTP traffic uses TCP port 1723 and IP protocol GRE (Generic Routing Encapsulation, IP protocol ID 47), as assigned by the Internet Assigned Numbers Authority (IANA). PPTP can be used with most firewalls and routers by enabling traffic destined for TCP port 1723 and protocol 47 traffic to be routed through the firewall or router.

PPTP connections may be limited or impossible to setup though a masqueraded/NAT IP connection. Please see the Microsoft and RFC links at the end of this section for more information.
PPTP Client Setup
Submenu level : /interface pptp-client
Property Description
name (name; default: pptp-out1) - interface name for reference
mtu (integer; default: 1460) - Maximum Transmit Unit. The optimal value is the MTU of the interface the tunnel is working over decreased by 40 (so, for 1500-byte ethernet link, set the MTU to 1460 to avoid fragmentation of packets)
mru (integer; default: 1460) - Maximum Receive Unit. The optimal value is the MTU of the interface the tunnel is working over decreased by 40 (so, for 1500-byte ethernet

link, set the MRU to 1460 to avoid fragmentation of packets)
connect-to (IP address)- the IP address of the PPTP server to connect to
user (string)- user name to use when logging on to the remote server
password (string; default: "")- user password to use when logging to the remote server
profile (name; default: default) - profile to use when connecting to the remote server
add-default-route (yes | no; default: no) - whether to use the server which this client is connected to as its default router (gateway)
Example
To set up PPTP client named test2 using username john with password john to connect to the 10.1.1.12 PPTP server and use it as the default gateway:

```
[admin@MikroTik] interface pptp-client> add name=test2 connect-to=10.1.1.12 \
\... user=john add-default-route=yes password=john
[admin@MikroTik] interface pptp-client> print
Flags: X - disabled, R - running
0 X name="test2" mtu=1460 mru=1460 connect-to=10.1.1.12 user="john"
password="john" profile=default add-default-route=yes

[admin@MikroTik] interface pptp-client> enable 0
```

Monitoring PPTP Client
Command name : /interface pptp-client monitor
Property Description
Statistics:

uptime (time) - connection time displayed in days, hours, minutes, and seconds
encoding (string) - encryption and encoding (if asymmetric, separated with '/') being used in this connection
status (string) - status of the client:
Dialing – attempting to make a connection
Verifying password... - connection has been established to the server, password verification in progress
Connected – self-explanatory
Terminated – interface is not enabled or the other side will not establish a connection

Example
Example of an established connection:

```
[admin@MikroTik] interface pptp-client> monitor test2
uptime: 4h35s
encoding: MPPE 128 bit, stateless
status: Connected
[admin@MikroTik] interface pptp-client>
```

PPTP Server Setup
Submenu level : /interface pptp-server server

```
[admin@MikroTik] interface pptp-server server> print
enabled: no
mtu: 1460
mru: 1460
authentication: mschap2
default-profile: default
[admin@MikroTik] interface pptp-server server>
```

Description
The PPTP server supports unlimited connections from clients. For each current connection, a dynamic interface is created.
Property Description
enabled (yes | no; default: no) - defines whether PPTP server is enabled or not
mtu (integer; default: 1460) - Maximum Transmit Unit. The optimal value is the MTU of the interface the tunnel is working over decreased by 40 (so, for 1500-byte ethernet link, set the MTU to 1460 to avoid fragmentation of packets)
mru (integer; default: 1460) - Maximum Receive Unit. The optimal value is the MTU of the interface the tunnel is working over decreased by 40 (so, for 1500-byte ethernet link, set the MTU to 1460 to avoid fragmentation of packets)
authentication (multiple choice: pap | chap | mschap1 | mschap2; default: mschap2) - authentication algorithm
default-profile (name; default: default) - default profile to use
Example
To enable PPTP server:

```
[admin@MikroTik] interface pptp-server server> set enabled=yes
[admin@MikroTik] interface pptp-server server> print
enabled: yes
mtu: 1460
```

mru: 1460
authentication: mschap2
default-profile: default
[admin@MikroTik] interface pptp-server server>

PPTP Server Users
Submenu level : /interface pptp-server
Description
There are two types of items in PPTP server configuration - static users and dynamic connections. A dynamic connection can be established if the user database or the default-profile has its local-address and remote-address set correctly. When static users are added, the default profile may be left with its default values and only P2P user (in /ppp secret) should be configured. Note that in both cases P2P users must be configured properly.
Property Description
name - interface name
user - the name of the user that is configured statically or added dynamically

Statistics:

mtu - shows (cannot be set here) client's MTU
client-address - shows (cannot be set here) the IP of the connected client
uptime - shows how long the client is connected
encoding (string) - encryption and encoding (if asymmetric, separated with '/') being used in this connection
Example
To add a static entry for ex1 user:

[admin@MikroTik] interface pptp-server> add user=ex1
[admin@MikroTik] interface pptp-server> print
Flags: X - disabled, D - dynamic, R - running
NAME USER MTU CLIENT-ADDRESS UPTIME ENC…
0 DR ex 1460 10.0.0.202 6m32s none
1 pptp-in1 ex1
[admin@MikroTik] interface pptp-server>

In this example an already connected user ex is shown besides the one we just added.
PPTP Router-to-Router Secure Tunnel Example

mawaridz@gmail.com

The following is an example of connecting two Intranets using an encrypted PPTP tunnel over the Internet.

There are two routers in this example:

* [HomeOffice]
Interface LocalHomeOffice 10.150.2.254/24
Interface ToInternet 192.168.80.1/24

* [RemoteOffice]
Interface ToInternet 192.168.81.1/24
Interface LocalRemoteOffice 10.150.1.254/24

Each router is connected to a different ISP. One router can access another router through the Internet.

On the PPTP server a user must be set up for the client:

```
[admin@HomeOffice] ppp secret> add name=ex service=pptp password=lkjrht
local-address=10.0.103.1 remote-address=10.0.103.2
[admin@HomeOffice] ppp secret> print detail
Flags: X - disabled
0 name="ex" service=pptp caller-id="" password="lkjrht" profile=default
local-address=10.0.103.1 remote-address=10.0.103.2 routes=""

[admin@HomeOffice] ppp secret>
```

Then the user should be added in the PPTP server list:

```
[admin@HomeOffice] interface pptp-server> add user=ex
[admin@HomeOffice] interface pptp-server> print
Flags: X - disabled, D - dynamic, R - running
# NAME USER MTU CLIENT-ADDRESS UPTIME ENC…
0 pptp-in1 ex
[admin@HomeOffice] interface pptp-server>
```

And finally, the server must be enabled:

```
[admin@HomeOffice] interface pptp-server server> set enabled=yes
[admin@HomeOffice] interface pptp-server server> print
enabled: yes
mtu: 1460
mru: 1460
authentication: mschap2
default-profile: default
[admin@HomeOffice] interface pptp-server server>
```

Add a PPTP client to the RemoteOffice router:

```
[admin@RemoteOffice] interface pptp-client> add connect-to=192.168.80.1 user=ex \
\… password=lkjrht disabled=no
[admin@RemoteOffice] interface pptp-client> print
Flags: X - disabled, R - running
0 R name="pptp-out1" mtu=1460 mru=1460 connect-to=192.168.80.1 user="ex"
password="lkjrht" profile=default add-default-route=no

[admin@RemoteOffice] interface pptp-client>
```

Thus, a PPTP tunnel is created between the routers. This tunnel is like an Ethernet point-to-point connection between the routers with IP addresses 10.0.103.1 and 10.0.103.2 at each router. It enables 'direct' communication between the routers over third party networks.

To route the local Intranets over the PPTP tunnel – add these routes:

```
[admin@HomeOffice] > ip route add dst-address 10.150.1.0/24 gateway 10.0.103.2
[admin@RemoteOffice] > ip route add dst-address 10.150.2.0/24 gateway 10.0.103.1
```

On the PPTP server it can alternatively be done using routes parameter of the user configuration:

```
[admin@HomeOffice] ppp secret> print detail
Flags: X - disabled
0 name="ex" service=pptp caller-id="" password="lkjrht" profile=default
local-address=10.0.103.1 remote-address=10.0.103.2 routes==""
```

```
[admin@HomeOffice] ppp secret> set 0 routes="10.150.1.0/24 10.0.103.2 1"
[admin@HomeOffice] ppp secret> print detail
Flags: X - disabled
0 name="ex" service=pptp caller-id="" password="lkjrht" profile=default
local-address=10.0.103.1 remote-address=10.0.103.2
routes="10.150.1.0/24 10.0.103.2 1"

[admin@HomeOffice] ppp secret>
```

Test the PPTP tunnel connection:

```
[admin@RemoteOffice]> /ping 10.0.103.1
10.0.103.1 pong: ttl=255 time=3 ms
10.0.103.1 pong: ttl=255 time=3 ms
10.0.103.1 pong: ttl=255 time=3 ms
ping interrupted
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 3/3.0/3 ms
```

Test the connection through the PPTP tunnel to the LocalHomeOffice interface:

```
[admin@RemoteOffice]> /ping 10.150.2.254
10.150.2.254 pong: ttl=255 time=3 ms
10.150.2.254 pong: ttl=255 time=3 ms
10.150.2.254 pong: ttl=255 time=3 ms
ping interrupted
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 3/3.0/3 ms
```

To bridge a LAN over this secure tunnel, please see the example in the 'EoIP' section of the manual. To set the maximum speed for traffic over this tunnel, please consult the 'Queues' section.

Connecting a Remote Client via PPTP Tunnel

The following example shows how to connect a computer to a remote office network over PPTP encrypted tunnel giving that computer an IP address from the same network as the remote office has (without need of bridging over eoip tunnels)

mawaridz@gmail.com

Please, consult the respective manual on how to set up a PPTP client with the software You are using.

The router in this example:

* [RemoteOffice]
Interface ToInternet 192.168.81.1/24
Interface Office 10.150.1.254/24

The client computer can access the router through the Internet.

On the PPTP server a user must be set up for the client:

[admin@RemoteOffice] ppp secret> add name=ex service=pptp password=lkjrht
local-address=10.150.1.254 remote-address=10.150.1.2
[admin@RemoteOffice] ppp secret> print detail
Flags: X - disabled
0 name="ex" service=pptp caller-id="" password="lkjrht" profile=default
local-address=10.150.1.254 remote-address=10.150.1.2 routes=""

[admin@RemoteOffice] ppp secret>

Then the user should be added in the PPTP server list:

[admin@RemoteOffice] interface pptp-server> add name=FromLaptop user=ex
[admin@RemoteOffice] interface pptp-server> print
Flags: X - disabled, D - dynamic, R - running
NAME USER MTU CLIENT-ADDRESS UPTIME ENC…
0 FromLaptop ex
[admin@RemoteOffice] interface pptp-server>

And the server must be enabled:

[admin@RemoteOffice] interface pptp-server server> set enabled=yes
[admin@RemoteOffice] interface pptp-server server> print
enabled: yes
mtu: 1460
mru: 1460

authentication: mschap2
default-profile: default
[admin@RemoteOffice] interface pptp-server server>

Finally, the proxy APR must be enabled on the 'Office' interface:

[admin@RemoteOffice] interface ethernet> set Office arp=proxy-arp
[admin@RemoteOffice] interface ethernet> print
Flags: X - disabled, R - running
NAME MTU MAC-ADDRESS ARP
0 R ToInternet 1500 00:30:4F:0B:7B:C1 enabled
1 R Office 1500 00:30:4F:06:62:12 proxy-arp
[admin@RemoteOffice] interface ethernet>

ref: http://www.mikrotik.com/documentation//manual_2.7/Interface/PPTP.html
Entri ini ditulis oleh Yoyok Riawan dan dikirimkan oleh Agustus 21, 2007 at 2:32 am dan disimpan di bawah Mikrotik
Tutorial Mikrotik VPN : Point to Point Tunnel Protocol (PPTP)komentar (0)Tutorial Mikrotik VPN : Point to Point Tunnel Protocol (PPTP) |

caching youtube squid 2.6.STABLE14
Author: Ricky Mahardhika
•04:44
caching youtube squid 2.6.STABLE14 (xubuntu 7.10)

browsing2 akhirnya dapat link buat cache youtube dengan squid 2.6 http://fedora.co.in/content/youtube-cache-version-03-available, tapi ini buat fedora.....mumpung ada waktu kosong iseng-iseng dicoba di xubuntu 7.10, dan ternyata proses tersulit adalah pada saat compile python-iniparse karena paket ini tidak tersedia buat debian base, kita mulai ya

download
http://kulbirsaini.fedorapeople.org/stuff/youtube_cache/youtube_cache-0.3-1.tar.gz
dan ekstrak

pastikan sebelumnya paket-paket dibawah ini sudah terinstall
python
python-urlgrabber

mawaridz@gmail.com

python-iniparse
squid

dari keempat paket tersebut sudah tersedia semua di repo ubuntu, tapi untuk python-iniparse gak ada dan kita harus install dari source, caranya download paketnya di http://code.google.com/p/iniparse/

ekstrak, kemudian dari hasil ekstrak tersebut copy folder iniparse ke dalam /usr/lib/python2.5/site-packages/

gitu aja installnya..he..he, padaha; tadi ada satu jam cari lewat google, gak ketemu….

setelah itu ekstark file youtube_cache-0.3-1.tar.gz

[root@localhost root]# tar -xvzf youtube_cache-0-3-1.tar.gz

masuk ke youtube_cache-0-3-1 directory

[root@localhost youtube_cache-x.x-x]# cd youtube_cache-0.3-1

Copy youtube_cache.conf ke /etc/youtube_cache.conf

[root@localhost youtube_cache-0.3-1]# cp youtube_cache.conf /etc/youtube_cache.conf

Copy youtube_cache directory to /etc/squid/

[root@localhost youtube_cache-0.3-1]# cp -r youtube_cache /etc/squid/

Buat directories untuk cache youtube videos

[root@localhost root]# cd /var/spool/
[root@localhost spool]# chmod 751 squid
[root@localhost spool]# cd squid
[root@localhost squid]# mkdir youtube
[root@localhost squid]# chown squid:squid youtube
[root@localhost squid]# chmod 755 youtube
[root@localhost squid]# cd youtube

mawaridz@gmail.com

[root@localhost youtube]# mkdir temp
[root@localhost youtube]# chown squid:squid temp
[root@localhost youtube]# chmod 755 temp

setelah itu, masukkan baris di bawah ini ke squid.conf di /etc/squid/squid.conf .

BEGIN Add to squid.conf
redirect_program /usr/bin/python /etc/squid/youtube_cache/youtube_cache.py
redirect_children 20
END Add to squid.conf

buat file youtube_cache.log di /var/log/squid/youtube_cache.log dan set permission buat squid

pastikan konfigurasi pada /etc/youtube_cache.conf, sesuai dengan mesin proxy anda

Save squid.conf dan reload squid service menggunakan perintah
[root@proxy root]# /etc/init.d/squid restart

sekarang tinggal di test…dan tempatku berhasil dengan baik….hemat bandwith mas, masalahnya sekarang harus nyediain berapa giga untuk cache youtube ini….?
Ditulis oleh poerwo2211 @ http://poerwo2211.wordpress.com
caching youtube squid 2.6.STABLE14komentar (1)caching youtube squid 2.6.STABLE14 |

Handle Virus Trojan Port with Mikrotik
Author: Ricky Mahardhika
•04:37
Handle Virus Trojan Port with Mikrotik
Berbagi pengalaman dengan teman2 nih.
Berpedoman pada info di http://www.glocksoft.com/trojan_port.htm, saya membuat di filter mikrotik agar mudah diadmin oleh kita.
Trojan port ini dipisahkan antara yang tcp port and udp port dengan tujuan jika ada penambahan atau pengurangan akan memudahkan untuk mencari dan menemukannya.. apalagi kalau yang bikin sudah check-out :-D
Dan juga didefinisikan dari arah mana kita mau ngeblok dari arah LAN atau internet.

Sebelumnya, harap diperhatikan bahwa buka tutup port sangat ditentukan kebutuhan kita akan port yang kita pakai. Jadi tutorial ini bukan harga mati untuk menutup port2 jika ada

mawaridz@gmail.com

port yang dibutuhkan.. tinggal di adjust on purpose lah.

Pertama2 kita mendefinisikan untuk yang TCP port

```
/ip firewall filter
add action=drop chain=tcp-viruses comment="Socks Des Troie, Death" disabled=\
no dst-port=1-2 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"Agent 31, Hacker's Paradise, Agent 40421" disabled=no dst-port=30-31 \
protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
37 protocol=tcp
add action=drop chain=tcp-viruses comment="Deep Throat Fore play" disabled=no \
dst-port=41 protocol=tcp
add action=drop chain=tcp-viruses comment=DRAT disabled=no dst-port=48 \
protocol=tcp
add action=drop chain=tcp-viruses comment=DRAT disabled=no dst-port=50 \
protocol=tcp
add action=drop chain=tcp-viruses comment="DM Setup" disabled=no dst-port=\
58-59 protocol=tcp
add action=drop chain=tcp-viruses comment=W32.Evala.Worm disabled=no \
dst-port=69-70 protocol=tcp
add action=drop chain=tcp-viruses comment="CDK, Firehotcker" disabled=no \
dst-port=79 protocol=tcp
add action=drop chain=tcp-viruses comment="Beagle.S RemoconChubo" disabled=no \
dst-port=81 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
85-90 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"Common Port for phishing scam sites, Hiddenport, NCX" disabled=no \
dst-port=99 protocol=tcp
add action=drop chain=tcp-viruses comment="More than 3 known worms and trojans\
usethis port , Invisible Identd Deamon, Kazimas" disabled=no dst-port=\
113 protocol=tcp
add action=drop chain=tcp-viruses comment=Happy99 disabled=no dst-port=119 \
protocol=tcp
```

```
add action=drop chain=tcp-viruses comment=\
"Jammer Killah, Attack Bot, God Message" disabled=no dst-port=121 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Password Generator Protocol" \
disabled=no dst-port=129 protocol=tcp
add action=drop chain=tcp-viruses comment=Farnaz disabled=no dst-port=133 \
protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
135-139 protocol=tcp
add action=drop chain=tcp-viruses comment=NetTaxi disabled=no dst-port=142 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Infector 1.3" disabled=no \
dst-port=146 protocol=tcp
add action=drop chain=tcp-viruses comment=A.Trojan disabled=no dst-port=170 \
protocol=tcp
add action=drop chain=tcp-viruses comment=W32.Rotor disabled=no dst-port=382 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Backage disabled=no dst-port=334 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Backage disabled=no dst-port=411 \
protocol=tcp
add action=drop chain=tcp-viruses comment=\
"W32.kibuv.b, Breach, Incognito, tcp Wrappers" disabled=no dst-port=\
420-421 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
445 in-interface=!ether-local protocol=tcp src-address-list=!pura-local
add action=drop chain=tcp-viruses comment=\
"Fatal Connections - Hacker's Paradise" disabled=no dst-port=455-456 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Hacker's Paradise" disabled=no \
dst-port=456 protocol=tcp
add action=drop chain=tcp-viruses comment="Grlogin, RPC backDoor" disabled=no \
dst-port=513-514 protocol=tcp
add action=drop chain=tcp-viruses comment=W32.kibuv.worm disabled=no \
dst-port=530 protocol=tcp
add action=drop chain=tcp-viruses comment="Rasmin, Net666" disabled=no \
```

```
dst-port=531 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"Stealth Spy, Phaze, 7-11 Trojan, Ini-Killer, Phase Zero, Phase-0" \
disabled=no dst-port=555 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
559 protocol=tcp
add action=drop chain=tcp-viruses comment="Sober worm Variants" disabled=no \
dst-port=587 protocol=tcp
add action=drop chain=tcp-viruses comment="W.32.Sasser worm" disabled=no \
dst-port=593 protocol=tcp
add action=drop chain=tcp-viruses comment="Secret Service" disabled=no \
dst-port=605 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"Attack FTP, Back Construction, BLA Trojan, NokNok, satans" disabled=no \
dst-port=666 protocol=tcp
add action=drop chain=tcp-viruses comment=SnipperNet disabled=no dst-port=667 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Dp Trojan" disabled=no dst-port=\
669 protocol=tcp
add action=drop chain=tcp-viruses comment=GayOL disabled=no dst-port=692 \
protocol=tcp
add action=drop chain=tcp-viruses comment="BackDoor.Netcrack.B - AimSpy" \
disabled=no dst-port=777-778 protocol=tcp
add action=drop chain=tcp-viruses comment=WinHole disabled=no dst-port=808 \
protocol=tcp
add action=drop chain=tcp-viruses comment=\
"Common Port for phishing scam sites" disabled=no dst-port=880 protocol=\
tcp
add action=drop chain=tcp-viruses comment=Backdoor.Devil disabled=no \
dst-port=901-902 protocol=tcp
add action=drop chain=tcp-viruses comment="Dark Shadow" disabled=no dst-port=\
911 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
999-1001 protocol=tcp
add action=drop chain=tcp-viruses comment="Doly Trojan" disabled=no dst-port=\
1011-1016 protocol=tcp
```

```
add action=drop chain=tcp-viruses comment=Vampire disabled=no dst-port=1020 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.lingosky disabled=no \
dst-port=1024-1025 protocol=tcp
add action=drop chain=tcp-viruses comment="NetSpy, Multidropper" disabled=no \
dst-port=1033-1035 protocol=tcp
add action=drop chain=tcp-viruses comment=Bla disabled=no dst-port=1042 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Rasmin disabled=no dst-port=1045 \
protocol=tcp
add action=drop chain=tcp-viruses comment="/sbin/initd - MiniCommand" \
disabled=no dst-port=1049-1050 protocol=tcp
add action=drop chain=tcp-viruses comment="The Thief, AckCmd" disabled=no \
dst-port=1053-1054 protocol=tcp
add action=drop chain=tcp-viruses comment="Backdoor.Zagaban, WinHole" \
disabled=no dst-port=1080-1083 protocol=tcp
add action=drop chain=tcp-viruses comment=Xtreme disabled=no dst-port=1090 \
protocol=tcp
add action=drop chain=tcp-viruses comment="RAT, Blood Fest Evoltion" \
disabled=no dst-port=1095-1099 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
1111 protocol=tcp
add action=drop chain=tcp-viruses comment=Orion disabled=no dst-port=\
1150-1151 protocol=tcp
add action=drop chain=tcp-viruses comment="Psyber Stream Server" disabled=no \
dst-port=1170 protocol=tcp
add action=drop chain=tcp-viruses comment=SoftWAR,Infector disabled=no \
dst-port=1207-1208 protocol=tcp
add action=drop chain=tcp-viruses comment=Kaos disabled=no dst-port=1212 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Sazo disabled=no dst-port=\
1218 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
1234 protocol=tcp
add action=drop chain=tcp-viruses comment="Sub Seven" disabled=no dst-port=\
1243 protocol=tcp
```

```
add action=drop chain=tcp-viruses comment="VooDoo Doll" disabled=no dst-port=\
1245 protocol=tcp
add action=drop chain=tcp-viruses comment="Scarab, Project next" disabled=no \
dst-port=1255-1256 protocol=tcp
add action=drop chain=tcp-viruses comment="Maverick's Matrix" disabled=no \
dst-port=1269 protocol=tcp
add action=drop chain=tcp-viruses comment="The Matrix" disabled=no dst-port=\
1272 protocol=tcp
add action=drop chain=tcp-viruses comment=NETrojan disabled=no dst-port=1313 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Millenium Worm" disabled=no \
dst-port=1338 protocol=tcp
add action=drop chain=tcp-viruses comment="Bo dll" disabled=no dst-port=1349 \
protocol=tcp
add action=drop chain=tcp-viruses comment="GoFriller, Backdoor G-1" disabled=\
no dst-port=1394 protocol=tcp
add action=drop chain=tcp-viruses comment=w32.spybot.ofn disabled=no \
dst-port=1433 protocol=tcp
add action=drop chain=tcp-viruses comment="remote Storm" disabled=no \
dst-port=1441 protocol=tcp
add action=drop chain=tcp-viruses comment=FTP99CMP disabled=no dst-port=1492 \
protocol=tcp
add action=drop chain=tcp-viruses comment="FunkProxy " disabled=no dst-port=\
1505 protocol=tcp
add action=drop chain=tcp-viruses comment="Psyber Streaming server" disabled=\
no dst-port=1509 protocol=tcp
add action=drop chain=tcp-viruses comment=Trinoo disabled=no dst-port=1524 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Remote Hack" disabled=no dst-port=\
1568 protocol=tcp
add action=drop chain=tcp-viruses comment="Backdoor.Miffice, Bize.Worm" \
disabled=no dst-port=1533-1534 protocol=tcp
add action=drop chain=tcp-viruses comment="Shivka-Burka, Direct Connection" \
disabled=no dst-port=1600 protocol=tcp
add action=drop chain=tcp-viruses comment="ICA Browser" disabled=no dst-port=\
1604 protocol=tcp
add action=drop chain=tcp-viruses comment=Exploiter disabled=no dst-port=1703 \
protocol=tcp
```

```
add action=drop chain=tcp-viruses comment=Scarab disabled=no dst-port=1777 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Loxbot.d disabled=no dst-port=1751 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.NetControle disabled=no \
dst-port=1772 protocol=tcp
add action=drop chain=tcp-viruses comment=SpySender disabled=no dst-port=1807 \
protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
1863 protocol=tcp
add action=drop chain=tcp-viruses comment="Fake FTP. WM FTP Server" disabled=\
no dst-port=1966-1967 protocol=tcp
add action=drop chain=tcp-viruses comment="Shockrave, Bowl" disabled=no \
dst-port=1981 protocol=tcp
add action=drop chain=tcp-viruses comment="OpC BO" disabled=no dst-port=1969 \
protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
1999-2005 protocol=tcp
add action=drop chain=tcp-viruses comment=Ripper disabled=no dst-port=2023 \
protocol=tcp
add action=drop chain=tcp-viruses comment=W32.korgo.a disabled=no dst-port=\
2041 protocol=tcp
add action=drop chain=tcp-viruses comment="Backdoor.TJServ - WinHole" \
disabled=no dst-port=2080 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Expjan disabled=no \
dst-port=2090 protocol=tcp
add action=drop chain=tcp-viruses comment=Bugs disabled=no dst-port=2115 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Deep Throat" disabled=no dst-port=\
2140 protocol=tcp
add action=drop chain=tcp-viruses comment="Illusion Mailer" disabled=no \
dst-port=2155 protocol=tcp
add action=drop chain=tcp-viruses comment=Nirvana disabled=no dst-port=2255 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Hvl RAT, Dumaru" disabled=no \
dst-port=2283 protocol=tcp
```

```
add action=drop chain=tcp-viruses comment=Xplorer disabled=no dst-port=2300 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Studio 54" disabled=no dst-port=\
2311 protocol=tcp
add action=drop chain=tcp-viruses comment=backdoor.shellbot disabled=no \
dst-port=2322 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"backdoor.shellbot, Eyeveg.worm.c, contact" disabled=no dst-port=\
2330-2339 protocol=tcp
add action=drop chain=tcp-viruses comment=vbs.shania disabled=no dst-port=\
2414 protocol=tcp
add action=drop chain=tcp-viruses comment=Beagle.N disabled=no dst-port=2556 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Striker disabled=no dst-port=2565 \
protocol=tcp
add action=drop chain=tcp-viruses comment=WinCrash disabled=no dst-port=2583 \
protocol=tcp
add action=drop chain=tcp-viruses comment="The Prayer 1.2 -1.3" disabled=no \
dst-port=2716 protocol=tcp
add action=drop chain=tcp-viruses comment="Phase Zero" disabled=no dst-port=\
2721 protocol=tcp
add action=drop chain=tcp-viruses comment=Beagle.J disabled=no dst-port=2745 \
protocol=tcp
add action=drop chain=tcp-viruses comment=W32.hllw.deadhat.b disabled=no \
dst-port=2766 protocol=tcp
add action=drop chain=tcp-viruses comment=SubSeven disabled=no dst-port=\
2773-2774 protocol=tcp
add action=drop chain=tcp-viruses comment="Phineas Phucker" disabled=no \
dst-port=2801 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Brador.A disabled=no \
dst-port=2989 protocol=tcp
add action=drop chain=tcp-viruses comment="Remote Shut" disabled=no dst-port=\
3000 protocol=tcp
add action=drop chain=tcp-viruses comment=WinCrash disabled=no dst-port=3024 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Wortbot disabled=no \
dst-port=3028 protocol=tcp
add action=drop chain=tcp-viruses comment="W32.Mytob.cz@mm, MicroSpy" \
```

```
disabled=no dst-port=3030-3031 protocol=tcp
add action=drop chain=tcp-viruses comment=W32.korgo.a disabled=no dst-port=\
3067 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
3127-3198 protocol=tcp
add action=drop chain=tcp-viruses comment=W32.HLLW.Dax disabled=no dst-port=\
3256 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Nemog.D disabled=no \
dst-port=3306 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
3332 protocol=tcp
add action=drop chain=tcp-viruses comment=w32.Mytob.kp@MM disabled=no \
dst-port=3385 protocol=tcp
add action=drop chain=tcp-viruses comment=W32.mockbot.a.worm disabled=no \
dst-port=3410 protocol=tcp
add action=drop chain=tcp-viruses comment="Backdoor.Fearic, Terror Trojan" \
disabled=no dst-port=3456 protocol=tcp
add action=drop chain=tcp-viruses comment="Eclipse 2000" disabled=no \
dst-port=3459 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Amitis.B disabled=no \
dst-port=3547 protocol=tcp
add action=drop chain=tcp-viruses comment="Portal of Doom" disabled=no \
dst-port=3700 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.helios disabled=no \
dst-port=3737 protocol=tcp
add action=drop chain=tcp-viruses comment=PsychWard disabled=no dst-port=3777 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Eclypse disabled=no dst-port=3791 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Eclypse disabled=no dst-port=3801 \
protocol=tcp
add action=drop chain=tcp-viruses comment=SkyDance,Backdoor.OptixPro.13.C \
disabled=no dst-port=4000-4001 protocol=tcp
add action=drop chain=tcp-viruses comment=WinCrash disabled=no dst-port=4092 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.rcserv disabled=no \
```

```
dst-port=4128 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"Backdoor.Nemog.D - Virtual Hacking Machine" disabled=no dst-port=4242 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.smokodoor disabled=no \
dst-port=4300 protocol=tcp
add action=drop chain=tcp-viruses comment=BoBo disabled=no dst-port=4321 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Phatbot disabled=no dst-port=4387 \
protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
4444 protocol=tcp
add action=drop chain=tcp-viruses comment=W32.mytob.db disabled=no dst-port=\
4512 protocol=tcp
add action=drop chain=tcp-viruses comment="File Nail" disabled=no dst-port=\
4567 protocol=tcp
add action=drop chain=tcp-viruses comment="ICQ Trojan" disabled=no dst-port=\
4590 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Nemog.D disabled=no \
dst-port=4646 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Nemog.D disabled=no \
dst-port=4661 protocol=tcp
add action=drop chain=tcp-viruses comment=Beagle.U disabled=no dst-port=4751 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.tuxder disabled=no \
dst-port=4820 protocol=tcp
add action=drop chain=tcp-viruses comment=W32.Opanki disabled=no dst-port=\
4888 protocol=tcp
add action=drop chain=tcp-viruses comment=W32.RaHack disabled=no dst-port=\
4899 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"Common Port for phishing scam sites" disabled=no dst-port=4903 protocol=\
tcp
add action=drop chain=tcp-viruses comment="ICQ Trogen" disabled=no dst-port=\
4950 protocol=tcp
add action=drop chain=tcp-viruses comment="Sokets de Trois v1./Bubbel, cd00r" \
disabled=no dst-port=5000-5002 protocol=tcp
```

```
add action=drop chain=tcp-viruses comment=Solo,Ootlt disabled=no dst-port=\
5010-5011 protocol=tcp
add action=drop chain=tcp-viruses comment="WM Remote Keylogger" disabled=no \
dst-port=5025 protocol=tcp
add action=drop chain=tcp-viruses comment="Net Metropolitan 1.0" disabled=no \
dst-port=5031-5032 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.laphex.client disabled=no \
dst-port=5152 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
5190 protocol=tcp
add action=drop chain=tcp-viruses comment=Firehotcker disabled=no dst-port=\
5321 protocol=tcp
add action=drop chain=tcp-viruses comment=Baackage,NetDemon disabled=no \
dst-port=5333 protocol=tcp
add action=drop chain=tcp-viruses comment="WC Remote Administration Tool" \
disabled=no dst-port=5343 protocol=tcp
add action=drop chain=tcp-viruses comment="Blade Runner" disabled=no \
dst-port=5400-5402 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"Backdoor.DarkSky.B, Backconstruction" disabled=no dst-port=5418-5419 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Xtcp, Illusion Mailer" disabled=no \
dst-port=5512 protocol=tcp
add action=drop chain=tcp-viruses comment="The Flu" disabled=no dst-port=5534 \
protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port " disabled=no \
dst-port=5550-5558 protocol=tcp
add action=drop chain=tcp-viruses comment=Robo-Hack disabled=no dst-port=5569 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.EasyServ disabled=no \
dst-port=5588 protocol=tcp
add action=drop chain=tcp-viruses comment="PC Crasher" disabled=no dst-port=\
5637-5638 protocol=tcp
add action=drop chain=tcp-viruses comment=WinCrash disabled=no dst-port=5714 \
protocol=tcp
add action=drop chain=tcp-viruses comment=WinCrash disabled=no dst-port=\
```

```
5741-5742 protocol=tcp
add action=drop chain=tcp-viruses comment="Portmap Remote Root Linux Exploit" \
disabled=no dst-port=5760 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Evivinc disabled=no \
dst-port=5800 protocol=tcp
add action=drop chain=tcp-viruses comment="Y3K RAT" disabled=no dst-port=5880 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Y3K RAT" disabled=no dst-port=5882 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Y3K RAT" disabled=no dst-port=\
5888-5889 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Evivinc disabled=no \
dst-port=5900 protocol=tcp
add action=drop chain=tcp-viruses comment=LovGate.ak disabled=no dst-port=\
6000 protocol=tcp
add action=drop chain=tcp-viruses comment="Bad Blood" disabled=no dst-port=\
6006 protocol=tcp
add action=drop chain=tcp-viruses comment=W32.mockbot.a.worm disabled=no \
dst-port=6129 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"Common Port for phishing scam sites" disabled=no dst-port=6180 protocol=\
tcp
add action=drop chain=tcp-viruses comment=Trojan.Tilser disabled=no dst-port=\
6187 protocol=tcp
add action=drop chain=tcp-viruses comment="Secret Service" disabled=no \
dst-port=6272 protocol=tcp
add action=drop chain=tcp-viruses comment="The Thing" disabled=no dst-port=\
6400 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Nemog.D disabled=no \
dst-port=6565 protocol=tcp
add action=drop chain=tcp-viruses comment=backdoor.sdbot.ag disabled=no \
dst-port=6631 protocol=tcp
add action=drop chain=tcp-viruses comment="TEMan, Weia-Meia" disabled=no \
dst-port=6661 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"Netbus Worm, winSATAN, Dark FTP, Schedule Agent" disabled=no dst-port=\
6666-6667 protocol=tcp
add action=drop chain=tcp-viruses comment="Vampyre, Deep Throat" disabled=no \
```

```
dst-port=6669-6671 protocol=tcp
add action=drop chain=tcp-viruses comment="Sub Seven, Backdoor.G" disabled=no \
dst-port=6711-6713 protocol=tcp
add action=drop chain=tcp-viruses comment="Mstream attack-handler" disabled=\
no dst-port=6723 protocol=tcp
add action=drop chain=tcp-viruses comment="Deep Throat" disabled=no dst-port=\
6771 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"Sub Seven, Backdoor.G, W32/Bagle@MM" disabled=no dst-port=6776-6777 \
protocol=tcp
add action=drop chain=tcp-viruses comment=NetSky.U disabled=no dst-port=6789 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Delta source DarkStar" disabled=no \
dst-port=6883 protocol=tcp
add action=drop chain=tcp-viruses comment="Shxt Heap " disabled=no dst-port=\
6912 protocol=tcp
add action=drop chain=tcp-viruses comment=Indoctrination disabled=no \
dst-port=6939 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
6969 protocol=tcp
add action=drop chain=tcp-viruses comment="Gate Crasher" disabled=no \
dst-port=6970 protocol=tcp
add action=drop chain=tcp-viruses comment="w32.mytob.mx@mm, Remote Grab, explo\
it translation server, kazimas, remote grab" disabled=no dst-port=\
7000-7001 protocol=tcp
add action=drop chain=tcp-viruses comment="Unknown Trojan" disabled=no \
dst-port=7028 protocol=tcp
add action=drop chain=tcp-viruses comment=W32.Spybot.ycl disabled=no \
dst-port=7043 protocol=tcp
add action=drop chain=tcp-viruses comment=SubSeven disabled=no dst-port=7215 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Net Monitor" disabled=no dst-port=\
7300-7308 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.netshadow disabled=no \
dst-port=7329 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.phoenix disabled=no \
dst-port=7410 protocol=tcp
```

```
add action=drop chain=tcp-viruses comment="Host Control" disabled=no \
dst-port=7424 protocol=tcp
add action=drop chain=tcp-viruses comment="QaZ -Remote Access Trojan" \
disabled=no dst-port=7597 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.GRM disabled=no dst-port=\
7614 protocol=tcp
add action=drop chain=tcp-viruses comment=Glacier disabled=no dst-port=7626 \
protocol=tcp
add action=drop chain=tcp-viruses comment=backdoor.nodelm disabled=no \
dst-port=7740-7749 protocol=tcp
add action=drop chain=tcp-viruses comment="GodMessaage, Tini" disabled=no \
dst-port=7777 protocol=tcp
add action=drop chain=tcp-viruses comment=ICKiller disabled=no dst-port=7789 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Amitis.B disabled=no \
dst-port=7823 protocol=tcp
add action=drop chain=tcp-viruses comment="The ReVeNgEr" disabled=no \
dst-port=7891 protocol=tcp
add action=drop chain=tcp-viruses comment=W32.kibuv.b disabled=no dst-port=\
7955 protocol=tcp
add action=drop chain=tcp-viruses comment=Mstream disabled=no dst-port=7983 \
protocol=tcp
add action=drop chain=tcp-viruses comment=w32.mytob.lz@mm disabled=no \
dst-port=7999-8000 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Ptakks.b disabled=no \
dst-port=8012 protocol=tcp
add action=drop chain=tcp-viruses comment="W32.Spybot.pen " disabled=no \
dst-port=8076 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
8081 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Asniffer disabled=no \
dst-port=8090 protocol=tcp
add action=drop chain=tcp-viruses comment=W32.PejayBot disabled=no dst-port=\
8126 protocol=tcp
add action=drop chain=tcp-viruses comment="BackOrifice 2000" disabled=no \
dst-port=8787 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Monator disabled=no \
```

```
dst-port=8811 protocol=tcp
add action=drop chain=tcp-viruses comment=Beagle.B@mm disabled=no dst-port=\
8866 protocol=tcp
add action=drop chain=tcp-viruses comment="BackOrifice 2000" disabled=no \
dst-port=8879 protocol=tcp
add action=drop chain=tcp-viruses comment=W32.Axatak disabled=no dst-port=\
8888-8889 protocol=tcp
add action=drop chain=tcp-viruses comment="BackHack - Rcon, Recon, Xcon" \
disabled=no dst-port=8988-8989 protocol=tcp
add action=drop chain=tcp-viruses comment="W32.randex.ccf - netministrator" \
disabled=no dst-port=9000 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.nibu.k disabled=no \
dst-port=9125 protocol=tcp
add action=drop chain=tcp-viruses comment=InCommand disabled=no dst-port=9400 \
protocol=tcp
add action=drop chain=tcp-viruses comment=W32.kibuv.worm disabled=no \
dst-port=9604 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.gholame disabled=no \
dst-port=9696-9697 protocol=tcp
add action=drop chain=tcp-viruses comment="BackDoor.RC3.B, Portal of Doom" \
disabled=no dst-port=9872-9878 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
9898-10002 protocol=tcp
add action=drop chain=tcp-viruses comment=iNi-Killer disabled=no dst-port=\
9989 protocol=tcp
add action=drop chain=tcp-viruses comment="W.32.Sasser Worm" disabled=no \
dst-port=9996 protocol=tcp
add action=drop chain=tcp-viruses comment="The Prayer" disabled=no dst-port=\
9999 protocol=tcp
add action=drop chain=tcp-viruses comment=OpwinTRojan disabled=no dst-port=\
10000 protocol=tcp
add action=drop chain=tcp-viruses comment=OpwinTRojan disabled=no dst-port=\
10005 protocol=tcp
add action=drop chain=tcp-viruses comment="Cheese worm" disabled=no dst-port=\
10008 protocol=tcp
add action=drop chain=tcp-viruses comment=w32.mytob.jw@mm disabled=no \
dst-port=10027 protocol=tcp
```

```
add action=drop chain=tcp-viruses comment="Portal of Doom" disabled=no \
dst-port=10067 protocol=tcp
add action=drop chain=tcp-viruses comment=Mydoom.B disabled=no dst-port=10080 \
protocol=tcp
add action=drop chain=tcp-viruses comment="backdoor.ranky.o, backdoor.staprew,\
backdoor.tuimer, gift trojan, brainspy, silencer" disabled=no dst-port=\
10100-10103 protocol=tcp
add action=drop chain=tcp-viruses comment="Acid Shivers" disabled=no \
dst-port=10520 protocol=tcp
add action=drop chain=tcp-viruses comment=Coma disabled=no dst-port=10607 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Ambush disabled=no dst-port=10666 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Senna Spy" disabled=no dst-port=\
11000 protocol=tcp
add action=drop chain=tcp-viruses comment="Host Control" disabled=no \
dst-port=11050-11051 protocol=tcp
add action=drop chain=tcp-viruses comment="Progenic Trojan - Secret Agent" \
disabled=no dst-port=11223 protocol=tcp
add action=drop chain=tcp-viruses comment="Dipnet / oddBob Trojan" disabled=\
no dst-port=11768 protocol=tcp
add action=drop chain=tcp-viruses comment="Latinus Server" disabled=no \
dst-port=11831 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Satancrew disabled=no \
dst-port=12000 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Berbew.j disabled=no \
dst-port=12065 protocol=tcp
add action=drop chain=tcp-viruses comment=GJamer disabled=no dst-port=12076 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Hack'99, KeyLogger" disabled=no \
dst-port=12223 protocol=tcp
add action=drop chain=tcp-viruses comment="Netbus, Ultor's Trojan" disabled=\
no dst-port=12345-12346 protocol=tcp
add action=drop chain=tcp-viruses comment=Whack-a-Mole disabled=no dst-port=\
12361-12363 protocol=tcp
add action=drop chain=tcp-viruses comment=NetBus disabled=no dst-port=12456 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Whack Job" disabled=no dst-port=\
```

```
12631 protocol=tcp
add action=drop chain=tcp-viruses comment="Eclypse 2000" disabled=no \
dst-port=12701 protocol=tcp
add action=drop chain=tcp-viruses comment="Mstream attack-handler" disabled=\
no dst-port=12754 protocol=tcp
add action=drop chain=tcp-viruses comment="Senna Spy" disabled=no dst-port=\
13000 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Amitis.B disabled=no \
dst-port=13173 protocol=tcp
add action=drop chain=tcp-viruses comment=W32.Sober.D disabled=no dst-port=\
13468 protocol=tcp
add action=drop chain=tcp-viruses comment="Kuang2 the Virus" disabled=no \
dst-port=13700 protocol=tcp
add action=drop chain=tcp-viruses comment=Trojan.Mitglieder.h disabled=no \
dst-port=14247 protocol=tcp
add action=drop chain=tcp-viruses comment="Mstream attack-handler" disabled=\
no dst-port=15104 protocol=tcp
add action=drop chain=tcp-viruses comment="Dipnet / oddBob Trojan" disabled=\
no dst-port=15118 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Cyn disabled=no dst-port=\
15432 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Lastdoor disabled=no \
dst-port=16322 protocol=tcp
add action=drop chain=tcp-viruses comment=Mosucker disabled=no dst-port=16484 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Backdoor.Haxdoor.D - Stacheldraht" \
disabled=no dst-port=16660-16661 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
16959 protocol=tcp
add action=drop chain=tcp-viruses comment="Kuang2.B Trojan" disabled=no \
dst-port=17300 protocol=tcp
add action=drop chain=tcp-viruses comment=W32.Imav.a disabled=no dst-port=\
17940 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Gaster disabled=no \
dst-port=19937 protocol=tcp
add action=drop chain=tcp-viruses comment="Millennium - AcidkoR" disabled=no \
dst-port=20000-20002 protocol=tcp
```

```
add action=drop chain=tcp-viruses comment="NetBus 2 Pro" disabled=no \
dst-port=20034 protocol=tcp
add action=drop chain=tcp-viruses comment=Chupacabra disabled=no dst-port=\
20203 protocol=tcp
add action=drop chain=tcp-viruses comment="Bla Trojan" disabled=no dst-port=\
20331 protocol=tcp
add action=drop chain=tcp-viruses comment="Shaft Client to handlers" \
disabled=no dst-port=20432-20433 protocol=tcp
add action=drop chain=tcp-viruses comment=Trojan.Adnap disabled=no dst-port=\
20480 protocol=tcp
add action=drop chain=tcp-viruses comment=Trojan.Mitglieder.E disabled=no \
dst-port=20742 protocol=tcp
add action=drop chain=tcp-viruses comment=W32.dasher.b disabled=no dst-port=\
21211 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"Exploiter - Kid Terror - Schwndler - Winsp00fer" disabled=no dst-port=\
21554 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"Prosiak - Ruler - Donald Dick - RUX The TIc.K" disabled=no dst-port=\
22222 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Simali disabled=no \
dst-port=22311 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor-ADM disabled=no dst-port=\
22784 protocol=tcp
add action=drop chain=tcp-viruses comment=W32.hllw.nettrash disabled=no \
dst-port=23005-23006 protocol=tcp
add action=drop chain=tcp-viruses comment=backdoor.berbew.j disabled=no \
dst-port=23232 protocol=tcp
add action=drop chain=tcp-viruses comment=Trojan.Framar disabled=no dst-port=\
23435 protocol=tcp
add action=drop chain=tcp-viruses comment="Donald Dick" disabled=no dst-port=\
23476-23477 protocol=tcp
add action=drop chain=tcp-viruses comment=w32.mytob.km@mm disabled=no \
dst-port=23523 protocol=tcp
add action=drop chain=tcp-viruses comment="Delta Source" disabled=no \
dst-port=26274 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.optix.04 disabled=no \
dst-port=27379 protocol=tcp
```

```
add action=drop chain=tcp-viruses comment="Sub-7 2.1" disabled=no dst-port=\
27573 protocol=tcp
add action=drop chain=tcp-viruses comment="Trin00 DoS Attack" disabled=no \
dst-port=27665 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Sdbot.ai disabled=no \
dst-port=29147 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.NTHack disabled=no \
dst-port=29292 protocol=tcp
add action=drop chain=tcp-viruses comment="Latinus Server" disabled=no \
dst-port=29559 protocol=tcp
add action=drop chain=tcp-viruses comment="The Unexplained" disabled=no \
dst-port=29891 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Antilam.20 disabled=no \
dst-port=29999 protocol=tcp
add action=drop chain=tcp-viruses comment="AOL Trojan" disabled=no dst-port=\
30029 protocol=tcp
add action=drop chain=tcp-viruses comment=NetSphere disabled=no dst-port=\
30100-30103 protocol=tcp
add action=drop chain=tcp-viruses comment="NetSphere Final" disabled=no \
dst-port=30133 protocol=tcp
add action=drop chain=tcp-viruses comment="Sockets de Troi" disabled=no \
dst-port=30303 protocol=tcp
add action=drop chain=tcp-viruses comment=Kuang2 disabled=no dst-port=30999 \
protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
31335-31339 protocol=tcp
add action=drop chain=tcp-viruses comment=BOWhack disabled=no dst-port=31666 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Hack'a'Tack" disabled=no dst-port=\
31785-31792 protocol=tcp
add action=drop chain=tcp-viruses comment=backdoor.berbew.j disabled=no \
dst-port=32121 protocol=tcp
add action=drop chain=tcp-viruses comment="Acid Battery" disabled=no \
dst-port=32418 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Alets.B disabled=no \
dst-port=32440 protocol=tcp
add action=drop chain=tcp-viruses comment="Trinity Trojan" disabled=no \
```

```
dst-port=33270 protocol=tcp
add action=drop chain=tcp-viruses comment=trojan.lodeight.b disabled=no \
dst-port=33322 protocol=tcp
add action=drop chain=tcp-viruses comment=Prosiak disabled=no dst-port=33333 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Spirit 2001 a" disabled=no \
dst-port=33911 protocol=tcp
add action=drop chain=tcp-viruses comment="BigGluck, TN" disabled=no \
dst-port=34324 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Lifefournow disabled=no \
dst-port=36183 protocol=tcp
add action=drop chain=tcp-viruses comment="Yet Another Trojan" disabled=no \
dst-port=37651 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
39999 protocol=tcp
add action=drop chain=tcp-viruses comment="The Spy" disabled=no dst-port=\
40412 protocol=tcp
add action=drop chain=tcp-viruses comment="Agent 40421 - Masters Paradise" \
disabled=no dst-port=40421-40426 protocol=tcp
add action=drop chain=tcp-viruses comment="Master's Paradise" disabled=no \
dst-port=43210 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Amitis.B disabled=no \
dst-port=44280 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Amitis.B disabled=no \
dst-port=44390 protocol=tcp
add action=drop chain=tcp-viruses comment="Delta Source" disabled=no \
dst-port=47252 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Amitis.B disabled=no \
dst-port=47387 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.antilam.20 disabled=no \
dst-port=47891 protocol=tcp
add action=drop chain=tcp-viruses comment="Sokets de Trois v2." disabled=no \
dst-port=50505 protocol=tcp
add action=drop chain=tcp-viruses comment=Fore disabled=no dst-port=50776 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Cyn disabled=no dst-port=\
51234 protocol=tcp
```

```
add action=drop chain=tcp-viruses comment=W32.kalel.a@mm disabled=no \
dst-port=51435 protocol=tcp
add action=drop chain=tcp-viruses comment="Remote Windows Shutdown" disabled=\
no dst-port=53001 protocol=tcp
add action=drop chain=tcp-viruses comment="subSeven -Subseven 2.1 Gold" \
disabled=no dst-port=54283 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port " disabled=no \
dst-port=54320-54321 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"WM Trojan Generator - File manager Trojan" disabled=no dst-port=\
55165-55166 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Osirdoor disabled=no \
dst-port=56565 protocol=tcp
add action=drop chain=tcp-viruses comment="NetRaider Trojan" disabled=no \
dst-port=57341 protocol=tcp
add action=drop chain=tcp-viruses comment=BackDoor.Tron disabled=no dst-port=\
58008-58009 protocol=tcp
add action=drop chain=tcp-viruses comment="Butt Funnel" disabled=no dst-port=\
58339 protocol=tcp
add action=drop chain=tcp-viruses comment=BackDoor.Redkod disabled=no \
dst-port=58666 protocol=tcp
add action=drop chain=tcp-viruses comment=BackDoor.DuckToy disabled=no \
dst-port=59211 protocol=tcp
add action=drop chain=tcp-viruses comment="Deep Throat" disabled=no dst-port=\
60000 protocol=tcp
add action=drop chain=tcp-viruses comment=Trinity disabled=no dst-port=60001 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Trojan.Fulamer.25 disabled=no \
dst-port=60006 protocol=tcp
add action=drop chain=tcp-viruses comment="Xzip 6000068" disabled=no \
dst-port=60068 protocol=tcp
add action=drop chain=tcp-viruses comment=Connection disabled=no dst-port=\
60411 protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.mite disabled=no dst-port=\
61000 protocol=tcp
add action=drop chain=tcp-viruses comment="Bunker-Hill Trojan" disabled=no \
dst-port=61348 protocol=tcp
```

```
add action=drop chain=tcp-viruses comment=Telecommando disabled=no dst-port=\
61466 protocol=tcp
add action=drop chain=tcp-viruses comment="Bunker-Hill Trojan" disabled=no \
dst-port=61603 protocol=tcp
add action=drop chain=tcp-viruses comment="Bunker-Hill Trojan" disabled=no \
dst-port=63485 protocol=tcp
add action=drop chain=tcp-viruses comment="Phatbot, W32.hllw.gaobot.dk" \
disabled=no dst-port=63808-63809 protocol=tcp
add action=drop chain=tcp-viruses comment=Taskmin disabled=no dst-port=64101 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Backdoor.Amitis.B disabled=no \
dst-port=64429 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
65000 protocol=tcp
add action=drop chain=tcp-viruses comment=Eclypse disabled=no dst-port=65390 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Jade disabled=no dst-port=65421 \
protocol=tcp
add action=drop chain=tcp-viruses comment="The Traitor (th3tr41t0r)" \
disabled=no dst-port=65432 protocol=tcp
add action=drop chain=tcp-viruses comment=Phatbot disabled=no dst-port=65506 \
protocol=tcp
add action=drop chain=tcp-viruses comment=/sbin/init disabled=no dst-port=\
65534 protocol=tcp
add action=drop chain=tcp-viruses comment="Adore Worm/Linux - RC1 Trojan" \
disabled=no dst-port=65535 protocol=tcp
add action=drop chain=tcp-viruses comment=Cafeini disabled=no dst-port=51966 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Acid baterry 2000" disabled=no \
dst-port=52317 protocol=tcp
add action=drop chain=tcp-viruses comment=Enterprise disabled=no dst-port=\
50130 protocol=tcp
add action=drop chain=tcp-viruses comment="Online Keylogger" disabled=no \
dst-port=49301 protocol=tcp
add action=drop chain=tcp-viruses comment=Exploiter disabled=no dst-port=\
44575 protocol=tcp
add action=drop chain=tcp-viruses comment=Prosiak disabled=no dst-port=44444 \
```

```
protocol=tcp
add action=drop chain=tcp-viruses comment="Remote Boot Tool - RBT" disabled=\
no dst-port=41666 protocol=tcp
add action=drop chain=tcp-viruses comment=Storm disabled=no dst-port=41337 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Mantis disabled=no dst-port=37237 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Donald Dick" disabled=no dst-port=\
34444 protocol=tcp
add action=drop chain=tcp-viruses comment="Son of PsychWard" disabled=no \
dst-port=33577 protocol=tcp
add action=drop chain=tcp-viruses comment="Son of PsychWard" disabled=no \
dst-port=33777 protocol=tcp
add action=drop chain=tcp-viruses comment="Peanut Brittle, Project Next" \
disabled=no dst-port=32100 protocol=tcp
add action=drop chain=tcp-viruses comment="Donald Dick" disabled=no dst-port=\
32001 protocol=tcp
add action=drop chain=tcp-viruses comment="Hack'a'Tack" disabled=no dst-port=\
31785 protocol=tcp
add action=drop chain=tcp-viruses comment=Intruse disabled=no dst-port=30947 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Lamers Death" disabled=no \
dst-port=30003 protocol=tcp
add action=drop chain=tcp-viruses comment="Infector - ErrOr32" disabled=no \
dst-port=30000-30001 protocol=tcp
add action=drop chain=tcp-viruses comment=ovasOn disabled=no dst-port=29369 \
protocol=tcp
add action=drop chain=tcp-viruses comment=NetTrojan disabled=no dst-port=\
29104 protocol=tcp
add action=drop chain=tcp-viruses comment=Exploiter disabled=no dst-port=\
28678 protocol=tcp
add action=drop chain=tcp-viruses comment="Bad Blood - Ramen - Seeker - SubSev\
en - SubSeven 2.1 Gold - Subseven 2.14 DefCon8 - SubSeven Muie - Ttfloader\
" disabled=no dst-port=27374 protocol=tcp
add action=drop chain=tcp-viruses comment=VoiceSpy disabled=no dst-port=26681 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Moonpie disabled=no dst-port=25982 \
protocol=tcp
```

```
add action=drop chain=tcp-viruses comment=Moonpie disabled=no dst-port=\
25685-25686 protocol=tcp
add action=drop chain=tcp-viruses comment=Infector disabled=no dst-port=24000 \
protocol=tcp
add action=drop chain=tcp-viruses comment=InetSpy disabled=no dst-port=23777 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Evil FTP - Ugly FTP - Whack Job" \
disabled=no dst-port=23456 protocol=tcp
add action=drop chain=tcp-viruses comment=Asylum disabled=no dst-port=23432 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Amanda disabled=no dst-port=23032 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Logged disabled=no dst-port=23232 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Girl friend - Kid Error" disabled=\
no dst-port=21544 protocol=tcp
add action=drop chain=tcp-viruses comment="VP killer" disabled=no dst-port=\
20023 protocol=tcp
add action=drop chain=tcp-viruses comment=Mosucker disabled=no dst-port=20005 \
protocol=tcp
add action=drop chain=tcp-viruses comment="ICQ Revenge" disabled=no dst-port=\
19864 protocol=tcp
add action=drop chain=tcp-viruses comment=Nephron disabled=no dst-port=17777 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Audiodoor disabled=no dst-port=\
17593 protocol=tcp
add action=drop chain=tcp-viruses comment=Infector disabled=no dst-port=17569 \
protocol=tcp
add action=drop chain=tcp-viruses comment=CrazzyNet disabled=no dst-port=\
17499-17500 protocol=tcp
add action=drop chain=tcp-viruses comment=KidTerror disabled=no dst-port=\
17449 protocol=tcp
add action=drop chain=tcp-viruses comment=Mosaic disabled=no dst-port=17166 \
protocol=tcp
add action=drop chain=tcp-viruses comment=Priority disabled=no dst-port=16969 \
protocol=tcp
add action=drop chain=tcp-viruses comment="ICQ Revenge" disabled=no dst-port=\
16772 protocol=tcp
```

```
add action=drop chain=tcp-viruses comment=CDK disabled=no dst-port=15858 \
protocol=tcp
add action=drop chain=tcp-viruses comment=SubZero disabled=no dst-port=15382 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Host Control" disabled=no \
dst-port=15092 protocol=tcp
add action=drop chain=tcp-viruses comment=NetDemon disabled=no dst-port=15000 \
protocol=tcp
add action=drop chain=tcp-viruses comment="PC Invader" disabled=no dst-port=\
14500-14503 protocol=tcp
add action=drop chain=tcp-viruses comment=Chupacabra disabled=no dst-port=\
13473 protocol=tcp
add action=drop chain=tcp-viruses comment="Hack '99 KeyLogger" disabled=no \
dst-port=13223 protocol=tcp
add action=drop chain=tcp-viruses comment=PsychWard disabled=no dst-port=\
13013-13014 protocol=tcp
add action=drop chain=tcp-viruses comment="Hacker Brasil - HBR" disabled=no \
dst-port=13010 protocol=tcp
add action=drop chain=tcp-viruses comment=Buttman disabled=no dst-port=12624 \
protocol=tcp
add action=drop chain=tcp-viruses comment=BioNet disabled=no dst-port=12349 \
protocol=tcp
add action=drop chain=tcp-viruses comment="Host Control" disabled=no \
dst-port=10528 protocol=tcp
add action=drop chain=tcp-viruses comment=Syphilis disabled=no dst-port=\
10085-10086 protocol=tcp
add action=drop chain=tcp-viruses comment=\
"Brown Orifice - RemoConChubo - Reverse WWW Tunnel Backdoor - RingZero" \
disabled=no dst-port=8080 protocol=tcp
add action=drop chain=tcp-viruses comment=DigitalRootbeer disabled=no \
dst-port=2600 protocol=tcp
add action=drop chain=tcp-viruses comment="Doly Trojan" disabled=no dst-port=\
2345 protocol=tcp
add action=return chain=tcp-viruses comment="Back to previous menu" disabled=\
no
add action=drop chain=udp-viruses comment="Socks Des Troie, Death" disabled=\
no dst-port=1 protocol=udp
add action=drop chain=udp-viruses comment="Netbios - DoS attacks msinit" \
```

```
disabled=no dst-port=135-139 protocol=udp
add action=drop chain=udp-viruses comment=Infector disabled=no dst-port=146 \
protocol=udp
add action=drop chain=udp-viruses comment="N0kN0k Trojan" disabled=no \
dst-port=666 protocol=udp
add action=drop chain=udp-viruses comment=\
"Maverick's Matrix 1.2-2.0 - remote storm" disabled=no dst-port=1025 \
protocol=udp
add action=drop chain=udp-viruses comment=NoBackO disabled=no dst-port=\
1200-1201 protocol=udp
add action=drop chain=udp-viruses comment="BackOrifice DLL Comm" disabled=no \
dst-port=1349 protocol=udp
add action=drop chain=udp-viruses comment="FunkProxy " disabled=no dst-port=\
1505 protocol=udp
add action=drop chain=udp-viruses comment="ICA Browser" disabled=no dst-port=\
1604 protocol=udp
add action=drop chain=udp-viruses comment=BackDoor.Fearic disabled=no \
dst-port=2000 protocol=udp
add action=drop chain=udp-viruses comment="Mini Backlash" disabled=no \
dst-port=2130 protocol=udp
add action=drop chain=udp-viruses comment="Deep Throat" disabled=no dst-port=\
2140 protocol=udp
add action=drop chain=udp-viruses comment=BackDoor.Botex disabled=no \
dst-port=2222 protocol=udp
add action=drop chain=udp-viruses comment=voicespy disabled=no dst-port=2339 \
protocol=udp
add action=drop chain=udp-viruses comment=Rat disabled=no dst-port=2989 \
protocol=udp
add action=drop chain=udp-viruses comment=\
"Deep Throat - Foreplay - Mini Backflash" disabled=no dst-port=3150 \
protocol=udp
add action=drop chain=udp-viruses comment=Backdoor.Fearic disabled=no \
dst-port=3456 protocol=udp
add action=drop chain=udp-viruses comment=Eclypse disabled=no dst-port=3801 \
protocol=udp
add action=drop chain=udp-viruses comment="WityWorm - BlackICE/ISS" disabled=\
no dst-port=4000 protocol=udp
add action=drop chain=udp-viruses comment="Remote Shell Trojan" disabled=no \
```

```
dst-port=5503 protocol=udp
add action=drop chain=udp-viruses comment="Y3K RAT" disabled=no dst-port=5882 \
protocol=udp
add action=drop chain=udp-viruses comment="Y3K RAT" disabled=no dst-port=5888 \
protocol=udp
add action=drop chain=udp-viruses comment="Mstream Agent-handler" disabled=no \
dst-port=6838 protocol=udp
add action=drop chain=udp-viruses comment="Unknown Trojan" disabled=no \
dst-port=7028 protocol=udp
add action=drop chain=udp-viruses comment="Host Control" disabled=no \
dst-port=7424 protocol=udp
add action=drop chain=udp-viruses comment="MStream handler-agent" disabled=no \
dst-port=7983 protocol=udp
add action=drop chain=udp-viruses comment="BackOrifice 2000" disabled=no \
dst-port=8787 protocol=udp
add action=drop chain=udp-viruses comment="BackOrifice 2000" disabled=no \
dst-port=8879 protocol=udp
add action=drop chain=udp-viruses comment="MStream Agent-handler" disabled=no \
dst-port=9325 protocol=udp
add action=drop chain=udp-viruses comment="Portal of Doom" disabled=no \
dst-port=10067 protocol=udp
add action=drop chain=udp-viruses comment="Portal of Doom" disabled=no \
dst-port=10167 protocol=udp
add action=drop chain=udp-viruses comment="Mstream handler-agent" disabled=no \
dst-port=10498 protocol=udp
add action=drop chain=udp-viruses comment=Ambush disabled=no dst-port=10666 \
protocol=udp
add action=drop chain=udp-viruses comment="DUN Control" disabled=no dst-port=\
12623 protocol=udp
add action=drop chain=udp-viruses comment="Shaft handler to Agent" disabled=\
no dst-port=18753 protocol=udp
add action=drop chain=udp-viruses comment="Shaft handler to Agent" disabled=\
no dst-port=20433 protocol=udp
add action=drop chain=udp-viruses comment=GirlFriend disabled=no dst-port=\
21554 protocol=udp
add action=drop chain=udp-viruses comment="Donald Dick" disabled=no dst-port=\
23476 protocol=udp
add action=drop chain=udp-viruses comment="Delta Source" disabled=no \
```

```
dst-port=26274 protocol=udp
add action=drop chain=udp-viruses comment="Sub-7 2.1" disabled=no dst-port=\
27374 protocol=udp
add action=drop chain=udp-viruses comment=Trin00/TFN2K disabled=no dst-port=\
27444 protocol=udp
add action=drop chain=udp-viruses comment="Sub-7 2.1" disabled=no dst-port=\
27573 protocol=udp
add action=drop chain=udp-viruses comment=NetSphere disabled=no dst-port=\
30103 protocol=udp
add action=drop chain=udp-viruses comment=\
"More than 3 known worms and trojans use this port" disabled=no dst-port=\
31335-31338 protocol=udp
add action=drop chain=udp-viruses comment="Hack`a'Tack" disabled=no dst-port=\
31787-31791 protocol=udp
add action=drop chain=udp-viruses comment="Trin00 for windows" disabled=no \
dst-port=34555 protocol=udp
add action=drop chain=udp-viruses comment="Trin00 for windows" disabled=no \
dst-port=35555 protocol=udp
add action=drop chain=udp-viruses comment="Delta Source" disabled=no \
dst-port=47262 protocol=udp
add action=drop chain=udp-viruses comment="OnLine keyLogger" disabled=no \
dst-port=49301 protocol=udp
add action=drop chain=udp-viruses comment="Back Orifice" disabled=no \
dst-port=54320-54321 protocol=udp
add action=drop chain=udp-viruses comment="NetRaider Trojan" disabled=no \
dst-port=57341 protocol=udp
add action=drop chain=udp-viruses comment="The Traitor - th3tr41t0r" \
disabled=no dst-port=65432 protocol=udp
add action=return chain=udp-viruses comment="Back to previous menu" disabled=\
no
add action=jump chain=forward comment="PREVENT VIRUS COME FROM LOCAL
NETWORK" \
disabled=no in-interface=ether-local jump-target=viruses
add action=jump chain=forward comment=\
"PREVENT VIRUS COME FROM PUBLIC INTERNET NETWORK" disabled=no \
in-interface=ether-public jump-target=viruses
add action=jump chain=input comment="PREVENT VIRUS COME FROM LAN" disabled=no
\
```

mawaridz@gmail.com

```
in-interface=ether-local jump-target=viruses
add action=jump chain=input comment="PREVENT VIRUS COME FROM PUBLIC
INTERNET" \
disabled=no in-interface=ether-public jump-target=viruses
add action=jump chain=viruses comment="Jump to handle virus from TCP port" \
disabled=no jump-target=tcp-viruses protocol=tcp
add action=jump chain=viruses comment="Jump to handle virus from UDP port" \
disabled=no jump-target=udp-viruses protocol=udp
add action=return chain=viruses comment="Back to previous rules" disabled=no
```

Thanks to aagyung @ www.forummikrotik.com