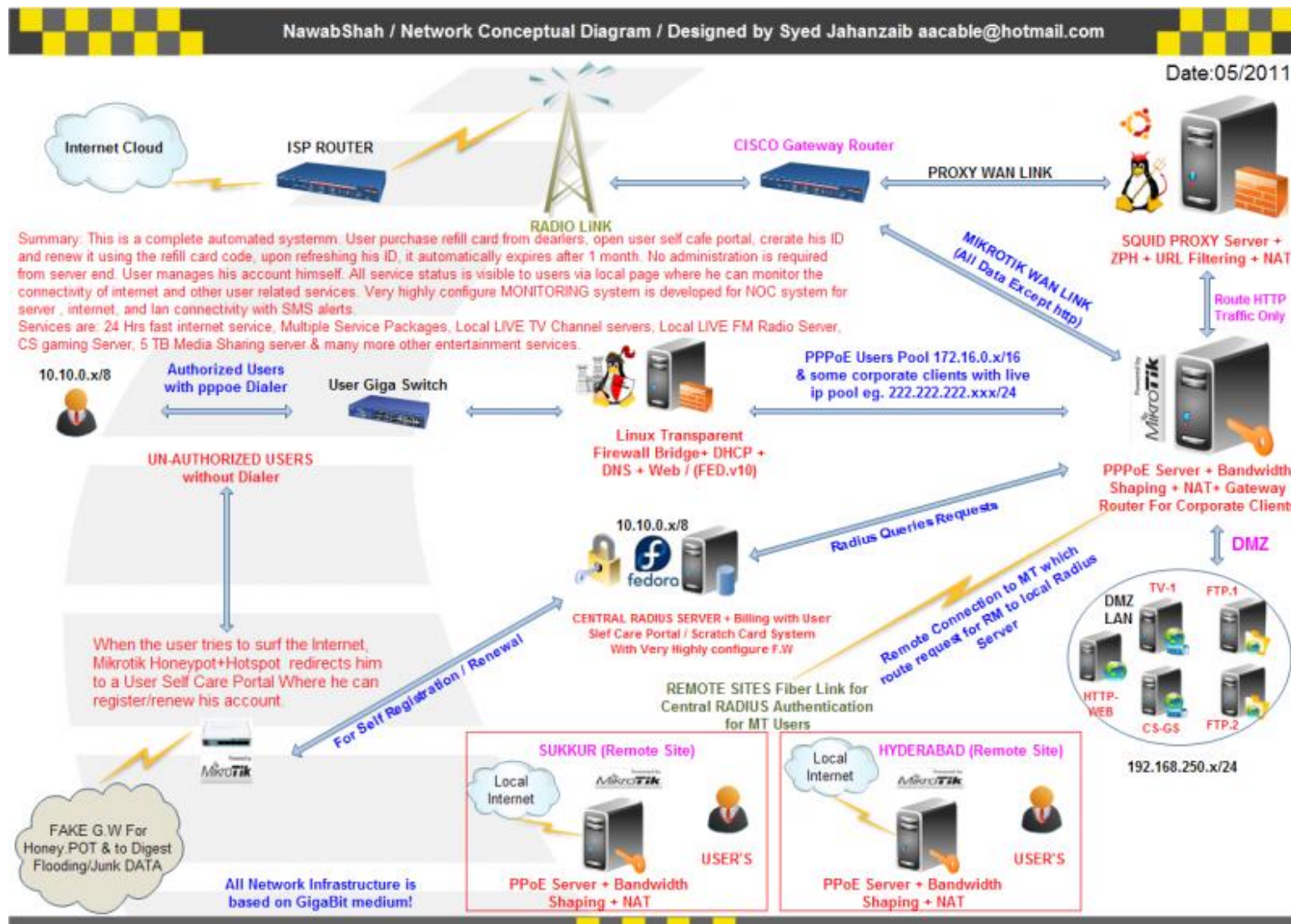


# **Howto setup Mini ISP using Mikrotik as PPPoE Server + DMASOFTLAB Radius Manager Scratch Card Billing System+ Linux Transparent Firewall Bridge + Ubuntu SQUID 2.7 Proxy Server**

Following is a my personnel experience / Guide on

Howto configure a **mini ISP** type Network using following scenario



Recently I was contacted by a friend who was really passionate in starting a **mini-ISP** type network setup for about **3000** users in the interior area of city. (soon it may expand up to **5000+** users). He asked my help to setup a scratch card base fully automatic system where user purchase scratch card, & using User self care portal web site, user may create his new **ID** or refresh his previous **ID** or change the service package

according to the card package offers. I had previously setup this kind of scenario in a cable.net environment using **Mikrotik** built-in radius server called '**User Manager**', but it have very limited basic features and all it can offer was a **pre-paid** type option and it doesn't have many accounting features. So I thought I should give a try to more rich feature radius server and after a lot of googling i decided to go with (**FREERADIUS** base ) **DMASOFTLAB RADIUS MANAGER**. A very famous radius server with all the option that a **mini-ISP** would required at unbelievably low price.

The hardware that I have used for this setup.

\***Main Mikrotik** = v4.17 x86 / Xeon 3.6Ghz Dual / 2 GB Ram / WD 500 GB Sata Hdd , This MT is serving as a PPPoE Server + NAT + bandwidth shaping. It also redirects **HTTP** traffic to **Proxy** server.

\* **Mikrotik RB750** = Just for **HOTSPOT** to redirect users to self care portal.  
(This can be done on Main **MT** also, but I prefer it this way)

\* **Radius Server** = DMAsoftlab RM v3.9 installed on Fedora v10 / Xeon 3.6Ghz Dual / 4 GB Ram / WD 500 GB x2 Sata Hdd

\* **SQUID PROXY GW** = SQUID v2.7 on UBUNTU Karmic Koala v9.10 / Xeon 3.6Ghz Dual / 8 GB Ram / WD 500 GB x3 SATA HDD (2 HDD reserved for Cache), This server acts as a proxy + Gateway machine for the **Mikrotik**, It also do **URL Filtering** blocking ads, it also have **ZPH** enabled so content available in squid cache should be downloaded at full speed (without package limitation) at user end.

\* **Linux Transparent BRIDGE firewall + DHCP + DNS + MRTG + WEB** Server on **FEDORA V10** / Xeon 3.6Ghz Dual / 4 GB Ram / WD 500 GB SATA HDD, This server sits between **Mikrotik** and Users , filtering unwanted traffic, ports and do some other stuff like lightweight **DNSMASQ** DNS Server, **DHCP** server providing ips to users , Web Site with **MRTG** , **Psychostats** ranking system for **Counter Strike Game**, Server **Monitoring** Scripts and Alerts, **PHPBB** Forums for Users, and some other cool stuff. **DNS+DHCP** is hosted on this server to minimize load on main **mikrotik** machine, alos this machine filters unwanted traffic from passing by to main mikrotik.

In this setup , I have configured **HOTSPOT** on extra **RB750** only to redirect user to my advertisement page, where he is informed that he is not logged in via dialer, either create / refresh his ID from **RM User Self Care Portal**, or if he already have an id, connect it via dialer. I don't prefer **HotSpot** authentication due to various security reasons, mainly due to I had a very bad experience having **HOTSPOT** hit by **ARP-POISONING** and many virus flooder that requires default gateway.

When user first login , his PC MAC address is **binded** with his **ID** to prevent accessing it from different pcs. Multiple session of same **ID** is **NOT** allowed , I provide user with scratch card (with refill code) , which he can use to refill his account according to card amount/package from RM User self care portal. **RM** demo can be viewed at <http://www.dmasoftlab.com/cont/radman>

When users with **pppoe** dialer tries to connect to main **Mikrotik**, MT verifies its credentials by asking Radius Server for the account validity, if the **ID** is valid, user connects okay and can use internet , otherwise he gets disconnected. When the User account is expired, he still can login via **dialer**, but then he is redirect to my local web server page where he is informed that his account is expired and he should visit billing.local page to renew his account using the card.

Please find along with attachment is my Network Diagram (This was initially designed, I made few changes afterward, I removed **FTP** from **MT DMZ** to user subnet lan to avoid load on **MT** , I moved **ftp OS** from **windows** to **Linux** and integrate it with **radius** authentication using **APACHE**.

Some other entertainment services that I setup here were:

**2** FTP Media Sharing Servers ( **4** TB of data ) based on Linux Apache with radius as back-end authentication

**2** Live TV Channel streaming over LAN using VLC Media Player Broadcasting

**1** Counter Strike 1.6 Dedicated Server with Psychostats Ranking System and adminmod/amxmod

**1** Web Server (Ubunut) hosting site u-dear . com , an entertainment portal and hosting other features. It also features monitoring system with MRTG / SMS Alerts via attached Mobile.

About RM: Radius Manager uses a nice web interface for administering the users and the whole system (traffic accounting, tracking of online users, display statistics, maintenance ,account management etc.) and to add that DMAsoftlab customer support guys (specially Mr. Viktor.K) have excellent support and respond instantly even to the dumbest of questions. It is real value for money especially for those who do not have big budgets.

We will distribute this article in following sections.

### 1) MIKROTIK ROUTEROS CONFIGURATION [x86 v4.17]

### 2) SQUID SERVER CONFIGURATION [using UBUNTU 9.1]

### 3) RADIUS MANGER CONFIGURATION [using FEDORA 10] + Adding Service Plans & Generating Refill Cards

### 4) LINUX TRANSPARENT FIREWALL BRIDGE CONFIGURATION [using FEDORA 10]

### 5) USER / CLIENT SIDE CONFIGURATION [using WINXP/WIN7]

I will focus only **Radius Manager** configuration here because it was a little tricky to setup at the first time, Rest of configs like mikrotik , squid and others are well describd in my other articles which i have mentioned in this post)

Now we will start from **Mikrotik** 😊

## 1) MIKROTIK ROUTEROS CONFIGURATION [x86 v4.17]

In this scenario , **Mikrotik** have **FOUR** interface card. Description is as follows

- 1) **LAN** interface = Connected with user switch
- 2) **WAN** interface = Connected with ISP WAN
- 3) **DMZ** interface = Connected with FTP Server's Switch or via Crossover cable if there is only single ftp server.
- 4) **Proxy** interface = Connected with SQUID PROXY Server via Crossover cable

For various reasons, I am not sharing exact Mikrotik Configuration. Just a basic modified version.

```
001 # apr/01/2006 02:35:02 by RouterOS 4.17
002 # software id =
003 #
004
005 /interface ethernet
006 set 0 arp=enabled auto-negotiation=yes cable-settings=default comment="" \
007 disable-running-check=yes disabled=no full-duplex=yes mac-address=\
008 00:0E:0C:06:7C:96 mtu=1500 name=lan speed=100Mbps
009 set 1 arp=enabled auto-negotiation=yes cable-settings=default comment="" \
010 disable-running-check=yes disabled=no full-duplex=yes mac-address=\
011 00:0E:0C:06:5B:BE mtu=1500 name=proxy speed=100Mbps
012 set 2 arp=enabled auto-negotiation=yes cable-settings=default comment="" \
013 disable-running-check=yes disabled=no full-duplex=yes mac-address=\
014 00:13:72:93:4B:C0 mtu=1500 name=wan speed=100Mbps
015 set 3 arp=enabled auto-negotiation=yes cable-settings=default comment="" \
016 disable-running-check=yes disabled=no full-duplex=yes mac-address=\
017 00:0E:0C:06:62:54 mtu=1500 name=dmz speed=100Mbps
018
019 # Setting IP Addresses for interfaces
```

```

020 /ip address
021 add address=10.10.0.1/8 broadcast=10.255.255.255 comment="" disabled=no \
022 interface=lan network=10.0.0.0
023 add address=111.1111.111.111/29 broadcast=111.1111.111.111 comment="" disabled=no \
024 interface=wan network=203.101.173.0
025 add address=192.168.20.1/24 broadcast=192.168.20.255 comment="" disabled=no \
026 interface=proxy network=192.168.20.0
027 add address=192.168.2.1/24 broadcast=192.168.2.255 comment="" disabled=no \
028 interface=dmz network=192.168.2.0
029
030 # Adding PPPoE Profile , Change DNS accordingly to your network
031 /ppp profile
032 set default change-tcp-mss=default comment="" dns-server=10.10.0.1 name=\
033 default only-one=default use-compression=default use-encryption=default \
034 use-vj-compression=default
035 add change-tcp-mss=default comment="" dns-server=192.168.20.2 local-address=\
036 10.10.0.1 name=ppoe-profile only-one=default remote-address=256k \
037 use-compression=default use-encryption=default use-vj-compression=default
038 set default-encryption change-tcp-mss=yes comment="" name=default-encryption \
039 only-one=default use-compression=default use-encryption=yes \
040 use-vj-compression=default
041
042 # Setting PPPoE Server configuration
043 /interface pppoe-server server
044 add authentication=pap default-profile=ppoe-profile disabled=no interface=lan \
045 keepalive-timeout=10 max-mru=1480 max-mtu=1480 max-sessions=1 mrru=\
046 disabled one-session-per-host=yes service-name=glassline1
047 add authentication=pap,chap,mschap1,mschap2 default-profile=ppoe-profile \
048 disabled=yes interface=lan keepalive-timeout=10 max-mru=1480 max-mtu=1480 \
049 max-sessions=1 mrru=disabled one-session-per-host=yes service-name=\
050 servicel

```

```
051
052 # Setting DNS Server for LOCAL LAN users
053 /ip dns
054 set allow-remote-requests=yes cache-max-ttl=1w cache-size=250000KiB \
055 max-udp-packet-size=512 servers=221.132.112.8,8.8.8.8
056
057 # User gets ip from these pools as per there packages, Just to locate and for some record purpose.
058 /ip pool
059 add name=256k ranges=172.16.2.1-172.16.4.250
060 add name=512k ranges=172.16.5.1-172.16.7.250
061 add name=1mb ranges=172.16.8.1-172.16.9.250
062 add name=2mb ranges=172.16.10.1-172.16.10.250
063 add name=expired-pool ranges=172.16.99.1-172.16.101.250
064
065 /queue type
066 set default kind=pfifo name=default pfifo-limit=50
067 set ethernet-default kind=pfifo name=ethernet-default pfifo-limit=50
068 set wireless-default kind=sfq name=wireless-default sfq-allot=1514 \
069 sfq-perturb=5
070 set synchronous-default kind=red name=synchronous-default red-avg-packet=1000 \
071 red-burst=20 red-limit=60 red-max-threshold=50 red-min-threshold=10
072 set hotspot-default kind=sfq name=hotspot-default sfq-allot=1514 sfq-perturb=\
073 5
074 add kind=sfq name=exempt sfq-allot=1514 sfq-perturb=5
075 set default-small kind=pfifo name=default-small pfifo-limit=10
076
077 # Unlimited Speed for CACHE content to be delivered to users at LAN speed regardless of there pcakge.
078 /queue simple
079 add burst-limit=0/0 burst-threshold=0/0 burst-time=0s/0s comment="" \
080 direction=both disabled=no dst-address=0.0.0.0/0 interface=all limit-at=\
081 0/0 max-limit=0/0 name=Proxy-HITTING packet-marks=proxy-hit parent=none \
```

```

082 priority=1 queue=default-small/default-small total-queue=default-small
083
084 ## Unlimited Speed for CACHE content to be delivered to users at LAN speed regardless of there pcakge.
085 ## Unlimited Speed for FTP SERVER's in DMZ
086 /queue tree
087 add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=0 \
088 max-limit=1G name=CACHE-HIT packet-mark=proxy-hit parent=global-out \
089 priority=1 queue=default
090 add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=0 \
091 max-limit=1G name=pmark packet-mark=proxy-hit parent=global-out priority=\
092 1 queue=default
093 add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=0 \
094 max-limit=1G name=exempt-up packet-mark=exempt-up parent=global-in \
095 priority=8 queue=exempt
096 add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=0 \
097 max-limit=1G name=exempt-down packet-mark=exempt-down parent=global-out \
098 priority=8 queue=exempt
099
100 # For SNMP Monitoring
101 /snmp
102 set contact=aacable@hotmail.com enabled=yes engine-boots=33 engine-id="" location="Glassline Nawabshah" time-
  window=15 \
103 trap-sink=0.0.0.0 trap-version=1
104 /snmp community
105 set secret_name address=0.0.0.0/0 authentication-password="" authentication-protocol=MD5 encryption-password="" \
106 encryption-protocol=DES name=gl read-access=yes security=none write-access=no
107
108 # Logging features, I used to have 14 lines, with all necessary info written to DISK for record purpose.
109 /system logging action
110 set memory memory-lines=100 memory-stop-on-full=no name=memory target=memory
111 set disk disk-file-count=14 disk-file-name=GLMT-log disk-lines-per-file=10000 disk-stop-on-full=no name=disk
  target=disk

```



```

112 set echo name=echo remember=no target=echo
113
114 /system logging
115 add action=memory disabled=no prefix="" topics=info,!firewall
116 add action=echo disabled=no prefix="" topics=error
117 add action=echo disabled=no prefix="" topics=warning
118 add action=echo disabled=no prefix="" topics=critical
119 add action=remote disabled=no prefix="" topics=firewall
120 add action=disk disabled=no prefix="" topics=pppoe,ppp,info
121 add action=disk disabled=no prefix="" topics=critical
122 add action=disk disabled=no prefix="" topics=system,info
123 add action=disk disabled=no prefix="" topics=pppoe,info
124
125 # Adding rules to block Virus and adding some security
126 /ip firewall filter
127 add action=reject chain=forward comment="" disabled=yes dst-address=\
128 !192.168.20.2 reject-with=icmp-admin-prohibited src-address=\
129 172.16.99.1-172.16.101.250
130 add action=accept chain=input comment="Accept established connections" \
131 connection-state=established disabled=no
132 add action=accept chain=input comment="Accept related connections" \
133 connection-state=related disabled=no
134 add action=drop chain=input comment="Drop invalid connections" \
135 connection-state=invalid disabled=no
136 add action=accept chain=input comment=UDP disabled=no protocol=udp
137 add action=drop chain=virus comment="Drop Blaster Worm" disabled=no dst-port=\
138 135-139 protocol=tcp
139 add action=drop chain=virus comment="Drop Messenger Worm" disabled=no \
140 dst-port=135-139 protocol=udp
141 add action=drop chain=virus comment="Drop Blaster Worm" disabled=no dst-port=\
142 445 protocol=tcp

```

```

143 add action=drop chain=virus comment="Drop Blaster Worm" disabled=no dst-port=\
144 445 protocol=udp
145 add action=add-src-to-address-list address-list="port scanners" \
146 address-list-timeout=2w chain=input comment="Port scanners to list " \
147 disabled=no protocol=tcp psd=21,3s,3,1
148 add action=add-src-to-address-list address-list="port scanners" \
149 address-list-timeout=2w chain=input comment="NMAP FIN Stealth scan" \
150 disabled=no protocol=tcp tcp-flags=fin,!syn,!rst,!psh,!ack,!urg
151 add action=add-src-to-address-list address-list="port scanners" \
152 address-list-timeout=2w chain=input comment="SYN/FIN scan" disabled=no \
153 protocol=tcp tcp-flags=fin,syn
154 add action=add-src-to-address-list address-list="port scanners" \
155 address-list-timeout=2w chain=input comment="SYN/RST scan" disabled=no \
156 protocol=tcp tcp-flags=syn,rst
157 add action=add-src-to-address-list address-list="port scanners" \
158 address-list-timeout=2w chain=input comment="FIN/PSH/URG scan" disabled=\
159 no protocol=tcp tcp-flags=fin,psh,urg,!syn,!rst,!ack
160 add action=add-src-to-address-list address-list="port scanners" \
161 address-list-timeout=2w chain=input comment="ALL/ALL scan" disabled=no \
162 protocol=tcp tcp-flags=fin,syn,rst,psh,ack,urg
163 add action=add-src-to-address-list address-list="port scanners" \
164 address-list-timeout=2w chain=input comment="NMAP NULL scan" disabled=no \
165 protocol=tcp tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg
166 add action=drop chain=input comment="dropping port scanners" disabled=no \
167 src-address-list="port scanners"
168 add action=drop chain=input comment="drop ftp brute forcers" disabled=no \
169 dst-port=21 protocol=tcp src-address-list=ftp_blacklist
170 add action=drop chain=input comment="DROP PING REQUEST - SECURITY" disabled=\
171 no protocol=icmp
172 add action=accept chain=input comment="" disabled=no dst-port=\
173 21,22,23,80,443,8291 protocol=tcp src-address-list=management-servers
174 add action=drop chain=input comment="" disabled=yes dst-port=\

```

```

175 21,22,23,443,8291 protocol=tcp
176
177 # Marking various packets like http, cache content, ftp etc . . .
178 /ip firewall mangle
179 add action=mark-packet chain=prerouting comment=squid disabled=no dscp=12 \
180 new-packet-mark=proxy-hit passthrough=no
181 add action=mark-packet chain=postrouting comment="" disabled=no dscp=12 \
182 new-packet-mark=proxy-hit passthrough=no
183 add action=mark-routing chain=prerouting comment="" disabled=no dst-port=80 \
184 new-routing-mark=http passthrough=yes protocol=tcp
185 add action=mark-packet chain=prerouting comment="UNLIMITED SPEED FOR FTP" disabled=no dst-address=\
186 192.168.2.0/24 new-packet-mark=exempt-up passthrough=yes src-address=\
187 172.16.0.0/16
188 add action=mark-packet chain=postrouting comment="UNLIMITED SPEED FOR FTP" disabled=no dst-address=\
189 172.16.0.0/16 new-packet-mark=exempt-down passthrough=yes src-address=\
190 192.168.2.0/24
191
192 # NAT rule for pppoe users pool only
193 /ip firewall nat
194 add action=accept chain=srcnat comment="ACCEPT PORT 80 FOR ROUTING" disabled=no dst-port=80 protocol=tcp
195 add action=masquerade chain=srcnat comment="NAT FOR 172.16.0.0/16 SERIES" disabled=no out-interface=wan src-
  address=\
196 172.16.0.0/16
197
198 # Adding default route for HTTP to be routed to SQUID and all other traffic to Mikrotik WAN
199 # Also adding route for DMZ / FTP
200 /ip route
201 add comment="" disabled=no distance=1 dst-address=0.0.0.0/0 gateway=\
202 192.168.20.2 routing-mark=http scope=30 target-scope=10
203 add comment="" disabled=yes distance=1 dst-address=0.0.0.0/0 gateway=\
204 192.168.2.1 routing-mark=ftp scope=30 target-scope=10

```

```
205 add comment="" disabled=no distance=1 dst-address=0.0.0.0/0 gateway=\
206 111.1111.111.111 scope=30 target-scope=10
207
208 # Adding RADIUS SUPPORT
209 /ppp aaa
210 set accounting=yes interim-update=1m use-radius=yes
211
212 /radius
213 add accounting-backup=no accounting-port=1813 address=10.10.0.2 \
214 authentication-port=1812 called-id="" comment="" disabled=no domain="" \
215 realm="" secret=immiarro9 service=ppp timeout=2s
216
217 /radius incoming
218 set accept=yes port=1700
219 /system logging
220 add action=memory disabled=no prefix="" topics=info
221 add action=memory disabled=no prefix="" topics=error
222 add action=memory disabled=no prefix="" topics=warning
223 add action=echo disabled=no prefix="" topics=critical
224 add action=disk disabled=no prefix="" topics=info
225 add action=disk disabled=no prefix="" topics=warning
```

For General Mikrotik configuration, Please read the following post.

<http://aacable.wordpress.com/2011/08/09/mikrotik-pppoe-server-with-user-manager-pre-paid-billing-system/>

For User ip redirection to SQUID configuration in Mikrotik, Please read the following post.

<http://aacable.wordpress.com/2011/07/21/mikrotik-howto-redirect-http-traffic-to-squid-with-original-source-client-ip/>

For FTP queue exemption in Mikrotik, Please read the following post.

<http://aacable.wordpress.com/2011/08/04/howto-exempt-rate-limit-for-ftp-server-behind-mt-dmz-in-placment-of-dynamic-queues/>

## **2) SQUID SERVER CONFIGURATION [using UBUNTU 9.1 Karmic Koala]**

**SQUID** Server have two lan cards.

One is connected with ISP WAN

Other is connected directly with Mikrotik with cross over cable.

I used the following script to share the basic internet. just copy all contents in any file , for example `/etc/squid/fw.sh` and paste the following content in it.

```
01 #!/bin/sh
02 # -----
03 # See URL: http://www.cyberciti.biz/tips/linux-setup-transparent-proxy-squid-howto.html
04 # (c) 2006, nixCraft under GNU/GPL v2.0+
05 # -----
06 # squid server IP
07 SQUID_SERVER="192.168.20.2"
08 # Interface connected to Internet
09 INTERNET="eth1"
10 # Interface connected to LAN
11 LAN_IN="eth0"
12 # Squid port
13 SQUID_PORT="8080"
14
15 # DO NOT MODIFY BELOW
16 # Clean old firewall
17 iptables -F
18 iptables -X
19 iptables -t nat -F
20 iptables -t nat -X
21 iptables -t mangle -F
```

```

22 iptables -t mangle -X
23 # Load IPTABLES modules for NAT and IP conntrack support
24 modprobe ip_conntrack
25 modprobe ip_conntrack_ftp
26 # For win xp ftp client
27 modprobe ip_nat_ftp
28 echo 1 > /proc/sys/net/ipv4/ip_forward
29 # Setting default filter policy
30 #iptables -P INPUT DROP
31 iptables -P OUTPUT ACCEPT
32 # Unlimited access to loop back
33 iptables -A INPUT -i lo -j ACCEPT
34 iptables -A OUTPUT -o lo -j ACCEPT
35 # Allow UDP, DNS and Passive FTP
36 iptables -A INPUT -i $INTERNET -m state --state ESTABLISHED,RELATED -j ACCEPT
37 # set this system as a router for Rest of LAN
38 iptables --table nat --append POSTROUTING --out-interface $INTERNET -j MASQUERADE
39 iptables --append FORWARD --in-interface $LAN_IN -j ACCEPT
40 # unlimited access to LAN
41 iptables -A INPUT -i $LAN_IN -j ACCEPT
42 iptables -A OUTPUT -o $LAN_IN -j ACCEPT
43 # DNAT port 80 request coming from LAN systems to squid 8080 ($SQUID_PORT) aka transparent proxy
44 iptables -t nat -A PREROUTING -i $LAN_IN -p tcp --dport 80 -j DNAT --to $SQUID_SERVER:$SQUID_PORT
45 # if it is same system
46 iptables -t nat -A PREROUTING -i $INTERNET -p tcp --dport 80 -j REDIRECT --to-port $SQUID_PORT
47 # DROP everything and Log it
48 iptables -A INPUT -j LOG
49 #iptables -A INPUT -j DROP
50 route add -net 172.16.0.0 netmask 255.255.0.0 gw 192.168.20.1 dev eth0
51 route add -net 10.0.0.0 netmask 255.0.0.0 gw 192.168.20.1 dev eth0

```

The above script will share internet connection on this **BOX**. add it in **/etc/rc.local** so it may run every time system restarts.

For fine tuned **squid.conf** , I used the following modified version.  
**/etc/squid/squid.conf** with the following data.

```
001 # PORT and Transparent Option
002 http_port 8080 transparent
003
004 # Cache Directory , modify it according to your system.
005 # but first create directory in root by mkdir /cache1
006 # and then issue this command chown proxy:proxy /cache1
007 # [for ubuntu user is proxy, in Fedora user is SQUID]
008 # I have set 400 GB for caching in secondary hdd reserved just for caching ,
009 # adjust it according to your need.
010 # My recommendation is to have one cache_dir per drive. zzz
011 store_dir_select_algorithm round-robin
012 cache_replacement_policy heap GDSF
013 memory_replacement_policy heap GDSF
014 cache_dir ufs /cache1 400000 16 256
015
016 # If you want to enable DATE time n SQUID Logs,use following
017 emulate_httpd_log on
018 logformat squid %tl %6tr %>a %Ss/%03Hs %<st %rm %ru %un %Sh/%<A %mt
019 log_fqdn off
020
021 logfile_rotate 8
022 debug_options ALL,1
023 cache_access_log /var/log/squid/access.log
024 cache_log /var/log/squid/cache.log
025 cache_store_log /var/log/squid/store.log
026
027 #I used DNSAMSQ service for fast dns resolving
028 #so install by using "apt-get install dnsmasq" first
```

```
029 dns_nameservers 127.0.0.1 221.132.112.8
030 ftp_user anonymous@
031 ftp_list_width 32
032 ftp_passive on
033 ftp_sanitycheck on
034
035 # To Deny ads and show my company ads instead.
036 # view this link for more info http://aacable.wordpress.com/2011/06/01/squid-howto-block-ads/
037
038 #acl adsites dstdomain url_regex "/etc/squid/adslist.txt"
039 #http_access deny adsites
040 #deny_info http://192.168.2.1/psb.htm adsites
041
042 # If you want to exclude some site from Cache, use following
043
044 #acl NoCache1 urlpath_regex u-dear.com
045 #no_cache deny NoCache1
046
047 # If you want to deny some users or ip series, Use following
048
049 # acl expiredu src 172.16.99.0/24
050 # http_access deny expiredu
051 # deny_info http://10.10.0.4/policy/expired.htm expiredu
052
053 #ACL Section
054 acl all src 0.0.0.0/0.0.0.0
055 acl manager proto cache_object
056 acl localhost src 127.0.0.1/255.255.255.255
057 acl to_localhost dst 127.0.0.0/8
058 acl SSL_ports port 443 563 # https, snews
```



```
059 acl SSL_ports port 873 # rsync
060 acl Safe_ports port 80 # http
061 acl Safe_ports port 21 # ftp
062 acl Safe_ports port 443 563 # https, snews
063 acl Safe_ports port 70 # gopher
064 acl Safe_ports port 210 # wais
065 acl Safe_ports port 1025-65535 # unregistered ports
066 acl Safe_ports port 280 # http-mgmt
067 acl Safe_ports port 488 # gss-http
068 acl Safe_ports port 591 # filemaker
069 acl Safe_ports port 777 # multiling http
070 acl Safe_ports port 631 # cups
071 acl Safe_ports port 873 # rsync
072 acl Safe_ports port 901 # SWAT
073 acl purge method PURGE
074 acl CONNECT method CONNECT
075 http_access allow manager localhost
076 http_access deny manager
077 http_access allow purge localhost
078 http_access deny purge
079 http_access deny !Safe_ports
080 http_access deny CONNECT !SSL_ports
081 http_access allow localhost
082 http_access allow all
083 http_reply_access allow all
084 icp_access allow all
085
086 #=====
087 # Administrative Parameters
088 #=====
089
```

```

090 # I used UBUNTU so user is proxy, in FEDORA you may use use squid
091 cache_effective_user proxy
092 cache_effective_group proxy
093 cache_mgr aacable@hotmail.com
094 visible_hostname proxy.aacable.net
095 unique_hostname aacable@hotmail.com
096
097 #=====
098 # ACCELERATOR
099 #=====
100 memory_pools off
101 forwarded_for off
102 log_icp_queries off
103 # If you want to hide your proxy machine from being detected at various site use following
104 via off
105
106 #=====
107 # OPTIONS WHICH AFFECT THE CACHE SIZE
108 #=====
109 # If you have 4GB memory in Squid box, we will use formula of 1/3
110 # You can adjust it according to your need. I used 2GB however :D
111 cache_mem 2 GB
112 maximum_object_size 1500 MB
113 maximum_object_size_in_memory 5000 KB
114
115 #=====
116 # SNMP , if you want to generate graphs for SQUID via MRTG
117 #=====
118 #acl snmppublic snmp_community gl
119 #snmp_port 3401
120 #snmp_access allow snmppublic all

```

```

121 #snmp_access allow all
122
123 #=====
124 #ZPH , To enable cache content to be delivered at full lan speed, bypass the queue at MT.
125 #=====
126 tcp_outgoing_tos 0x30 all
127 zph_mode tos
128 zph_local 0x30
129 zph_parent 0
130 zph_option 136
131
132 #=====
133 # Refresh Rate Patterns : zaib
134 #=====
135
136 #=====
137 #image
138 #=====
139 refresh_pattern -i \.(ico|swf|png|jpg|jpeg|bmp|tiff|png|gif) 43200 100% 129600 override-expire override-lastmod
    reload-into-ims
140
141 #=====
142 #documents
143 #=====
144 refresh_pattern -i \.(doc|xls|ppt|ods|odt|odp|pdf|pptx|xlsx|docs|txt) 43200 100% 129600 override-expire override-
    lastmod reload-into-ims
145
146 #=====
147 #multimedia
148 #=====
149 refresh_pattern -i \.(mov|mpg|mpeg|flv|avi|mp3|3gp|sis|wma|3gp|mp4|dat|wmv|rm|rmv|rma|) 43200 100% 129600
    override-expire override-lastmod reload-into-ims

```

```

150
151 #=====
152 #compression
153 #=====
154 refresh_pattern -i \.(zip|rar|ace|bz|bz2|tar|gz|exe|rpm|deb|bin|cab) 43200 100% 129600 override-expire override-
lastmod reload-into-ims
155
156 #=====
157 #web default
158 #=====
159 refresh_pattern -i (.html$|.htm|.shtml|.aspx|.asp|.php) 180 100% 4320 override-expire override-lastmod
reload-into-ims
160 refresh_pattern http://office\microsoft\com/ 0 100% 20160 reload-into-ims
161 refresh_pattern http://windowsupdate\microsoft\com/ 0 100% 20160 reload-into-ims
162 refresh_pattern ^ftp: 14440 80% 10080 override-expire override-lastmod reload-into-ims
163
164 refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
165 refresh_pattern . 0 50% 4320

```

For Basic Internet Sharing on Linux , please read the following post.

<http://aacable.wordpress.com/2011/06/01/linux-simple-internet-sharing-script/>

For basic SQUID configuration , Please read the following post.

<http://aacable.wordpress.com/2011/08/08/linux-transparent-squid-proxy-server-guide/>

For fine tuned squid.conf, Please read the following post.

<http://aacable.wordpress.com/2011/06/01/working-squid-conf-example-fil/>

For ZPH configuration in squid, Please read the following post. (To deliver cache content to user in full lan speed, exempt cache content from queue)

<http://aacable.wordpress.com/2011/07/21/mikrotik-with-squidzph-unlimited-speed-for-cache-content-traffic/>

### 3) RADIUS MANGER CONFIGURATION [using FEDORA 10] The Real Giant :p



#### **MANAGER Version 3.9 INSTALLATION MANUAL © DMA Softlab LLC**

[This RM installation guide is a shorter version, copied from DMASOFTLAB RM original manual. I edited it and cut off all un-necessary paragraphs which are not required for basic installation and added some info of my personnel experience.](#)

For RM Screenshot gallery, please visit following link.

**<http://www.dmasoftlab.com/cont/screenshots>**

This document describes the installation procedure of Radius Manager billing system on a Linux host using **FEDORA 10**. For beginners I recommend the usage of Fedora Core 10. Fedora Core is the easiest and the most comfortable Linux system for RM isntallation (Although I have tested in Ubuntu also, but still FED wins in few aspects) It comes with all required packages to install and run Radius Manager. The packages are available on the installation media and they are also down-loadable from the official online repositories using the Yum tool.

In this document You will also find guidelines on how to set up your NAS (mikrotik) to integrate with Radius Manager system.

To successfully install Radius Manager on your host, You have to complete the following steps:

1. Install ionCube runtime libraries
2. Build and configure FreeRadius server
3. Configure MySQL database and credentials
4. Install Radius Manager WEB components
5. Install Radius Manager binaries
6. Complete the post installation steps and fine tuning

## INSTALLATION Prerequisites:

To successfully install and run Radius Manager, You need the following components installed on the Linux host, If they are not installed already, dont worry 😊 we will install them in next step 😊

## Software Requirements:

- FreeRadius 2.1.8 DMA mod 2 (downloadable from [www.dmasoftlab.com](http://www.dmasoftlab.com))
- PHP 5 or better
- MySQL 5 or better
- MySQL development libraries
- php-mysql
- php-mcrypt
- curl, php-curl
- glibc 2.4 or better
- GNU C/C++ compiler
- IonCube runtime libraries. They are downloadable freely from [www.ioncube.com](http://www.ioncube.com) and [www.dmasoftlab.com](http://www.dmasoftlab.com)
- Javascript enabled browser on running on client machines

## Preparing the Linux system Fedora 10

Install the necessary components on your Linux host before You begin the installation of Radius Manager.

1. Disable SeLinux in **/etc/sysconfig/selinux** and reboot your host:

```
1 SELINUX=disabled
```

2. On Fedora Core 10 install the required packages in one step:

```
1 yum install make php php-mysql php-mcrypt mysql-devel mysql-server gcc libtool-ltdl
```

[ Note: This will download and install about **60-70 mb** of packages depends on you FED installation. Be patience if you have slow internet connection ]

## Installation procedure of ionCube runtime system

Radius Manager requires ionCube runtime libraries. You can download them from: <http://www.dmasoftlab.com/downloads>

Before installing ionCube, You have to know the following:

1. The architecture of your Linux system (32 or 64 bit) (usually 32bit pc is used in most cases, I will use 32bit only as example)
2. Which PHP version are You using (use `php -v` to view version info, hopefully you will get v5.2.9)
3. Where is your `php.ini` file located (On fedora its usually `/etc/php.ini`)

## Example ionCube installation

1. First create a temp folder in root

```
1 mkdir /temp
2 cd /temp
```

Now download ionCube by issuing following command

```
1 wget http://www.dmasoftlab.com/cont/download/ioncube\_loaders\_lin\_x86.tar.gz
```

UNTAR the ionCube runtime libraries to `/usr/ local/ioncube` by using following command

```
1 tar zxvf ioncube_loaders_lin_x86.tar.gz
```

Now copy the **ioncube** folder to `/usr/ local/ioncube` by using following command

```
1 cp /temp/ioncube/* /usr/local/ioncube/
```

2. Add the appropriate ionCube loader to your `php.ini`. You have to add the following line in **`/etc/php.ini`**

```
1 zend_extension=/usr/local/ioncube/ioncube_loader_lin_5.2.so
```

3. Test the ionCube loader from shell:

```
1 [root@localhost]# php -v
2
3 You have to see the ionCube PHP Loader version displayed correctly.
4
5 PHP 5.2.9 (cli) (built: Apr 17 2009 03:29:12)
6 Copyright (c) 1997-2009 The PHP Group
7 Zend Engine v2.2.0, Copyright (c) 1998-2009 Zend Technologies
8 with the ionCube PHP Loader v3.3.14, Copyright (c) 2002-2010, by ionCube Ltd.
```

4. Restart the web server by following command:

#### **sevice httpd restart**

5. Run **ifconfig** command from shell to determine the MAC address of the network interface card (NIC):

```
1 [root@localhost]# ifconfig
2
3 eth0      Link encap:Ethernet  HWaddr 00:00:E8:EC:8A:E8
```

6. Now it's time to request a license for your server. If this is first time, Ask support@dmsoftlab.com to grant you id passwrod for customer portal. after getting Id, Log on to DMA Softlab customer's portal (<https://customers.dmasoftlab.com>) and request a trial license for the hardware address (MAC address) of your network interface card.

Radius Manager will run only on the specified host and the license is binding to the MAC address of the network interface card. You can migrate Radius Manager to another host if You also move the same network interface card with it.

It is strongly recommended to request a license for a removable networking interface to allow migration to new host without loosing the license.

7. When a license file is issued (You will get a notification about it in email), download and copy the lic.txt and mod.txt to radiusmanager web directory (read the "Installation procedure of Radius Manager" chapter of this manual) to enable licensing of your Radius Manager installation.

#### **Troubleshooting the ionCube loader system**



If encoded files fail to run, you can test ionCube runtime by using the helper PHP script `ioncubeloader-helper.php`, which is included in the loader download archive.

1. Copy the `ioncube-encoded-file.php` PHP script to your http root (on Redhat-based system it is `/var/www/html`).
2. Try to access the `ioncube-encoded-file.php` script using your favorite web browser:

1 <http://yourhost/ioncube-encoded-file.php>

3. If You can see the message “This file has been successfully decoded. ionCube Loaders are correctly installed”, it means You have successfully installed ionCube runtime on your host and it is ready to use. If You can’t decode the file via a HTTP call, check the `php.ini` and be sure `SeLinux` is disabled.

### **Installation procedure of FreeRadius**

Follow the installation steps to successfully build, install and configure FreeRadius RADIUS server on your host. Use only FreeRadius 2.1.8 DMA mod 2 source archive (downloadable from our site). It is prepared and tested by our team and it is 100% compatible with Radius Manager.

Other versions and builds will not function properly with Radius Manager. If your host already has a different FreeRadius version installed, remove it completely including it’s configuration files (`/etc/raddb` or `/usr/local/etc/raddb`).

Execute the following actions as super user (root user):

1. Download FreeRadius archive in `/temp` folder from the following URL: <http://www.dmasoftlab.com/downloads> by issuing following command

```
1 cd /temp
2 wget http://www.dmasoftlab.com/cont/download/freeradius-server-2.1.8-dmamod-2.tar.gz
```

2. Build FreeRadius server from sources. Do it in the following way. Ungzip and untar the FreeRadius archive:

```
1 gzip -d freeradius-server-2.1.8-dmamod-2.tar.gz
2 tar xvf freeradius-server-2.1.8-dmamod-2.tar
```

Create the makefile:

```
1 cd freeradius-server-2.1.8
2 ./configure
3 make
4 make install
```

By default, FreeRadius will be installed in **/usr/local** directory.

3. Now You can test FreeRadius in debug mode. Start it with parameter -X

```
1 radiusd -X
2
3 Listening on authentication address * port 1812 Listening on accounting address * port 1813
4 Listening on command file /usr/local/var/run/radiusd/radiusd.sock Listening on proxy address * port 1814
5
6 Ready to process requests.
```

It must answer with ***“Ready to process requests”***.

If radiusd cannot find the required libraries, issue ldconfig from shell to refresh the ld linker’s cache.

```
1 ldconfig
```

4. Set the correct permissions on FreeRadius configuration files (Fedora):

```
1 chown apache /usr/local/etc/raddb
2 chown apache /usr/local/etc/raddb/clients.conf
```

Radius Manager updates the clients.conf automatically, so it is necessary to set the correct permission on it. Do not modify the **clients.conf** by hand. Don’t forget to define all **NASes** in **ACP** with the correct secret and restart FreeRadius (from **ACP** or from shell) after modifying the **NASes** in the system.

5. Review and modify (if needed) the **MySQL** credentials in **/usr/local/etc/raddb/sql.conf**: by issuing following command

```
1 nano /usr/local/etc/raddb/sql.conf
2
3 # Connection info:
4 server = "localhost" #port = 3306
5 login = "radius"
6 password = "radius123"
```

## Creating MySQL databases with MySQL command line tool

If You are familiar with MySQL command line tool, You can create databases, users and permissions with it easily and much faster. First start MYSQL daemon via

```
1 service mysqld start
```

Now, Log on to **MySQL** server as root:

```
1 mysql -u root -ppassword
```

where password is the MySql root password. If there is no password for root, simply change it via

```
1 mysqladmin -u root password NEWPASSWORD
```

or if you want to change old password, issue this command

```
1 mysqladmin -u root -p'oldpassword' password newpass
```

Execute the following statement from the MySQL command shell:

```
1 CREATE DATABASE radius;
2 CREATE DATABASE conntrack;
3 CREATE USER 'radius'@'localhost' IDENTIFIED BY 'radius123';
4 CREATE USER 'conntrack'@'localhost' IDENTIFIED BY 'conn123'; GRANT ALL ON radius.* TO radius@localhost;
5 GRANT ALL ON conntrack.* TO conntrack@localhost;
```

```
6 exit
```

Completing this step the databases are ready to use.

### Installation procedure of Radius Manager

There are two methods of installation available:

1. Interactive, using the included installer script. (We will focus on this as its easier for newbie)
2. Manual installation, using Unix commands. (We will not discuss it as its already briefly described in RM Manual)

### Interactive installation

The easiest way to install Radius Manager is to use the included install.sh script. It is located in Radius Manager tar archive and can be used on Redhat, Debian and (with slight modification of the environment) on other systems. Before You begin, be sure You have prepared the MySQL database tables and credentials. Radius Manager requires two databases:

1. **RADIUS** – for storing all system data, including users and accounting information.
2. **CONTRACK** – for storing connection tracking system (CTS) data.

Create both databases even on a non-CTS enabled system.

Now download **RM (radiusmanager-3.9.0.tgz)** from dma customer portal in **/temp** folder. Now decompress the Radius Manager tarball using following command.

```
1 tar xf radiusmanager-3.9.0.tgz
2 cd radiusmanager-3.9.0-rel-allpatches-1-5/
```

Now invoke the installer script, but first change its permission to **755**. In the examples below we will use the installer script on Redhat / Fedora system.

```
01 chmod 755 install.sh
02
03 ./install.sh
04
05 Radius Manager installer
06 Copyright 2004-2011, DMA Softlab LLC All right reserved.
07 (Use CTRL+C to abort any time)
08
09 Select the type of your operating system:
10 1. Redhat (Fedora, CentOS etc.)
11 2. Debian (Ubuntu etc.)
12 Choose an option: [1]
```

Select the operating system You have. For Redhat, RHEL, CentOS, Fedora select option **1**.

Now select the installation method:

```
1 Select installation type:
2
3 1. New installation
4 2. Upgrade old system
5 Choose an option: [1]
```

For new installation, use option 1. You can see the default options after every question, so You can just press enter in most cases.

```
1 Choose an option: [1]
2 Selected installation method: NEW INSTALLATION
3 WWW root path: [/var/www/html]
```

Now define the HTTP root folder. The installer will create radiusmanager subfolder in it automatically. On Redhat You can simply press enter.

Now define the MySQL database credentials:

```
1 RADIUS database host: [localhost]
2 RADIUS database username: [radius]
3 RADIUS database password: [radius123]
4 CTS database host: [localhost]
5 CTS database username: [conntrack]
6 CTS database password: [conn123]
```

For the default setup simply press enter and use MySQL user “radius” with password “radius123” for RADIUS database, and conntrack / conn123 for CONNTRACK database.

The host is “localhost” by default. If You have different setup, specify proper values. If You are planning to use the system with hundreds of online users, it is recommended to use separate database host for CONNTRACK database.

In the next step You have to define the FreeRadius user. It must be the correct user to set the permission properly on /etc/radiusmanager.cfg. If there are permission problems on /etc/radiusmanager.cfg, Radius Manager binaries will not function at all.

#### **Freeradius UNIX user: [root]**

On Fedora it is root, so simply press enter.

Now define the HTTP user (the user name under Apache is running). It is required to set the permission on files in radiusmanager/config directory. On Fedora it is the apache user.

#### **Httpd UNIX user: [apache]**

You can now decide to create rmpoller service or not? It is a standard Fedora / Debian compatible service script which invokes rmpoller helper. You can also start rmpoller using alternative ways.

#### **Create rmpoller service: [y]**

In most cases simply press enter. When a service has been created, You can use the command (on Fedora)

**service rmpoller [start | stop]**

to control rmpoller service activity. Also make this service auto starting at boot time together with FreeRadius. Use command `chkconfig -add rmpoller on` or use Webmin to activate the service at boot time.

In the next step select yes if You want to create the rmconntack service. It is a standard Linux service, like rmpoller. It is required for Radius Manager CTS only.

### Create rmconntack service: [y]

When a service has been created, You can use the command

### service rmconntack [start | stop]

to control rmconntack service activity. Also make this service auto starting at boot time.

It is strongly recommended to create a full database backup before You continue. Answer 'yes' to the following question:

### Back up RADIUS database: [y]

Now the system warns You it will overwrite the existing databases if You continue. Press 'y' to continue or 'n' to abort the installation process.

```
01 WARNING! If You continue You will overwrite the existing RADIUS database!
02 Are You sure to start the installation? [n]
03 You can press Ctrl+C any time to abort the installation process.
04
05 Starting installation process...
06 Backing up radiusmanager.cfg Backing up system_cfg.php Backing up netcash_cfg.php Backing up paypal_cfg.php
   Backing up authorizenet_cfg.php Backing up dps_cfg.php Backing up 2co_cfg.php
07 Copying web content to /var/www/html/radiusmanager Copying binaries to /usr/local/bin
08 Copying rootexec to /usr/local/sbin Copying radiusmanager.cfg to /etc
09 Backing up RADIUS database... Creating mysql tables
10 Creating rmpoller service
11 Creating rmconntack service
12 Copying logrotate script
```

```
13 Setting permission on raddb files
14 Copying radiusd init script to /etc/init.d
15
16 Installation finished!
```

the installation process is finished, You can begin configuring the system with [/etc/radiusmanager.cfg](#) and radiusmanager/config files.

Add the following line to [/etc/crontab](#) to execute rmscheduler.php every day after midnight by issuing following command:

```
1 crontab -e
```

Now press **i** and add the the following entry.

```
1 02 0 * * * root /usr/bin/php /var/www/html/radiusmanager/rmscheduler.php 12345
```

Now press **ESC** button, now press **SHIFT+:** , now press **wq**  
it will save the crontab and exit.

**12345** is the default password, as it is defined in [system\\_cfg.php](#). Always specify the full path of the PHP interpreter. If You are not sure, check it's location before You add the crontab record. The password has to match the predefined one in [system\\_cfg.php](#).

Now download the the license files (**lic.txt** and **mod.txt**) and copy them in in radiusmanager web folder

```
1 cp lic.txt /var/www/html/radiusmanager
2 cp mod.txt /var/www/html/radiusmanager
```

Now Try to access the **ACP (Administration Control Panel)** by pointing your browser to **http://localhost/radiusmanager/admin.php**.



Reboot your system to check if helper services are starting properly (radiusd, rmpoller and optionally rmconnttrack). By default few services donot run at Fed startup, See the last paragraph of this guide on **Starting daemons at boot time so that required services automatically starts at boot. You can use the following commands to make sure the services starts at boot time.**

```
1 chkconfig --add radiusd
2  chkconfig --add rmpoller
3  chkconfig --add rmconnttrack
4  chkconfig --add mysqld
5  chkconfig --add httpd
6  chkconfig --add dnsmasq
```

To test RADIUS communication, be sure MySQL server is running. Start FreeRadius in debug mode:

```
1 radiusd -X
2
3 Listening on authentication address * port 1812 Listening on accounting address * port 1813
4  Listening on command file /usr/local/var/run/radiusd/radiusd.sock Listening on proxy address * port 1814
5  Ready to process requests.
```

On the second terminal issue the radtest command:

```
1 radtest user 1111 localhost 1812 testing123
2
3 Sending Access-Request of id 57 to 127.0.0.1 port 1812
4  User-Name = "user"
5  User-Password = "1111" NAS-IP-Address = 127.0.0.1 NAS-Port = 1812
6  rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=57, length=50
7  WISPr-Bandwidth-Max-Up = 262144
8  WISPr-Bandwidth-Max-Down = 262144 Acct-Interim-Interval = 60
```

You have to see Access-Accept answer. If You see an error message, check the following:

- Is MySQL server running?
- Are MySQL credentials correct? • Are MySQL table permissions correct? • Can FreeRadius connect to MySQL database?
- Have You created the RADIUS and CONNTRACK databases and tables?
- Is the NAS defined in ACP? In this case it is 127.0.0.1 ?( NAS-IP-Address = 127.0.0.1).
- If the hostname is different than localhost, You have to substitute the localhost with the IP address of the Linux server. You have to update the NAS list in RM ACP in this case.

Now access the **ACP (Administration Control Panel)** by pointing your browser to **<http://localhost/radiusmanager/admin.php>** and First add Mikrotik NAS device in ACP.

Enter the ip address of Mikrotik. In Secret , type the secret that you will set in Mikrotik RADIUS (See below section / screenshot)

The screenshot shows the 'New NAS' form in the RADIUS Manager 3 interface. The form is titled 'New NAS' and has a navigation bar with 'System', 'Users', 'Services', 'Managers', 'NAS', 'Financials', 'Card system', and 'IAS'. The 'NAS' tab is selected. The form contains several fields: 'NAS name' (Mikrotik), 'IP address' (192.168.2.2), 'Type' (Mikrotik), 'Secret' (12345), 'Password' (empty), 'Enable Mikrotik API' (checkbox), 'API user name' (empty), 'API password' (empty), 'Cisco bandwidth support' (radio buttons for None, Rate limit, Policy map), and 'Description' (My Mikrotik Test Box ! zaib). The 'Secret' field is highlighted with a red circle. The 'Add NAS' button is at the bottom right.

Also test the functionality of the User Control Panel (UCP):

1 <http://yourhost/radiusmanager/user.php>

The initial username and password are:

```
1 Username: user
2 Password: 1111
```

To be able to log on to **UCP** as another user, create the user in **ACP** first.

## System optimization Tips

The performance of the entire Radius Manager system mainly depends on the speed of the hard disks and the MySQL subsystem. If You encounter performance problems, check the following:

1. Check radacct table size. If it is large (> 300-500 MB), delete the old years from it using the deloldyears.sql script (included in the RM tar archive in doc directory).
2. Add more RAM to the system. Adding 2-4 GB of RAM doesn't mean any problem nowadays.
3. Use RAID 0 or RAID 5 array MySQL db storage devices.
4. Optimize the MySQL server via my.cnf file.

key\_buffer=1024M

myisam\_sort\_buffer\_size=512M sort\_buffer\_size=32M

Set key\_buffer = RAM size / 2, myisam\_sort\_buffer\_size = RAM size / 4, sort\_buffer\_size = RAM size / 64.

Adding more RAM will drastically speed up the MySQL system. Indexes must be fit in the RAM for optimal performance.

## Notes

By default, many web servers can list the contents of the directory where Radius Manager files are stored. To prevent this there are several methods available:

1. Use .htaccess file. Enable the Options -Indexes directive In .htaccess file (example file is included in radiusmanager directory in the installation archive). Be sure to enable the htaccess support in order to use this feature (set AllowOverride All directive in httpd.conf).
2. Disable the directory listing in httpd configuration files.

## HOWTO REPLACE/MODIFY DMASOFTLAB RM LOGO and TEXT !!!

You can Replace/Edit the default **DMASOFTLAB** logo files. by default, Images are available where you have installed the radiusmanager. Look into the images folder of radiusmanager.

For example I installed RM in /var/www/html/radiusmanager. There will be a folder name 'images' Look for these files.

[dmalogo\\_small.gif](#)  
[radmanlogo\\_small.gif](#)  
[main1\\_01.gif](#)  
[main1\\_02.gif](#)  
[main1\\_03.gif](#)  
[emailheader.gif](#)

You can also edit the texts/descriptions in language description files in **radiusmanager/lang/english** folder.  
look for **texts.txt** and **strings.txt**

To add logo in prepaid cards , you can modify its base image at **radiusmanager/lang/english/card** folder.  
look for **classic\_bg.png** and **refill\_bg.png**

Some Example:

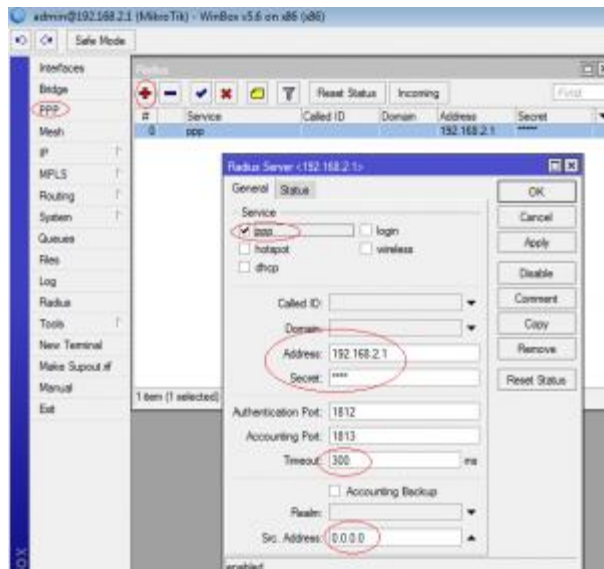


## **MIKROTIK NAS CONFIGURATION**

### **Setting up RADIUS authentication and accounting**

To send authentication and accounting requests to Radius server, You have to configure your Mikrotik NAS. Use Winbox to view and edit the configuration. Follow these steps:

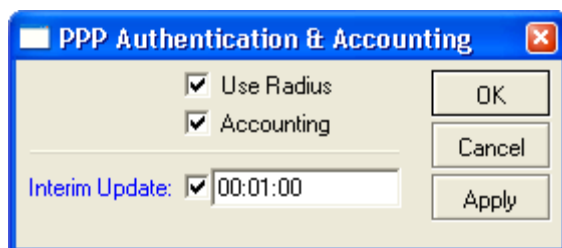
1. Connect to your Mikrotik router using Winbox.
2. Select Radius from the main menu.
3. Click on the + to create a new RADIUS server description:  
(see the attached screenshot)



### Description of fields:

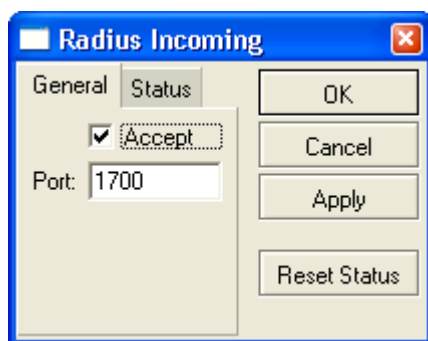
- Service:
- PPP: for PPP RADIUS authentication
- Address is your RADIUS server host. eg 192.168.2.1
- Secret is the NAS secret from /usr/local/etc/raddb/clients.conf e.g 12345
- Authentication and Accounting ports are the standard RADIUS ports.
- Timeout defines how much milliseconds can elapse while the answer arrives from the RADIUS server. If You are using slower connection to RADIUS server or the accounting tables are large, set this timeout higher (3000-5000 ms).

**Now Set the AAA options of PPP service (PPPoE): Goto PPP / Secrets / click on PPP Authentication & Accounting Button, and see the following.**



Turn on RADIUS authentication (Use Radius) and RADIUS accounting (Accounting). Interim update is the time interval when RADIUS client (Mikrotik NAS) sends the accounting information to the RADIUS server. If You have more than 200 online users, use higher values (5-8 minutes) to avoid MySQL overload.

**Now Enable incoming RADIUS requests (POD packets).** It is required to use the REMOTE disconnection method in Radius Manager: Don't forget to open the UDP port 1700 in firewall on Mikrotik and Linux server.



To Test the database connectivity: use the following command from RADIUS CLI.

```
1 rmauth 192.168.2.9 user 1
2
3 Mikrotik-Xmit-Limit=1028,Mikrotik-Rate-Limit="262144/262144"
```

(Where 192.168.2.1 is the MT IP) You have to see similar output to this. If there is a MySQL socket error, define the correct socket location in /etc/radiusmanager.cfg. The default socket file on Redhat is /var/lib/mysql/mysql.sock. On Debian systems the proper socket path is /var/run/mysqld/mysqld.sock.

To successfully test rauth, You have to create NAS entries in ACP. In this example, the NAS IP

You have to restart FreeRadius every time when You modify the NAS devices. Unfortunately FreeRadius doesn't read the configuration files dynamically.

## ADDITIONAL SETUP

### Starting daemons at boot time

Radius Manager system supports automatic startup of daemons: radiusd, rmpoller and rmconntack. The automatic installer copies all the required scripts to /etc/init.d directory and sets the required permissions on them.

The following methods are available to set up automatic service startup:

- Use Webmin to start services at boot time or
- Use command `chkconfig --add [service_name]` (Fedora only)

A chkconfig example follows:

```
1 chkconfig --add radiusd
2  chkconfig --add rmpoller
3  chkconfig --add rmconntack
4  chkconfig --add mysqld
5  chkconfig --add httpd
6  chkconfig --add dnsmasq
```

## **ADDED SECURITY: (My Suggestion, zaib)**

I placed this RADIUS Server on user subnet, which is not suitable, place it on behind Mikrotik DMZ, then create a user in Mikrotik For example 'user' with restricted ip pool, and using FIREWALL rules, Restrict this id/ip to access only RADIUS Server , block all other access for this id / pass. This way user have to first dialin to open RM User Self Care Portal.



## **HOWTO ADD Service Plans in RM ACP & Generate Prepaid/Refill Cards:**

### **256Kbps Monthly Service Plan**

Following is an example on howto add New Service and assosicate it with new user.

**Package = 256Kb**

**Expiry = 30 Days**

Login to **RM ACP** , Goto **Services** and click on **New Service**.

In **Service Name\*** tpye '**256Kbps Monthly**'

Click on '**Available in UCP**'

Click on '**Limit Expiration**'

on '**Set data rates**' (DL/UL) type **256 / 256**

Now goto Bottom and in '**Expiration Date Unit**' Select **1** , Initial **0**, and

Finally, Click on Store Service Bottom in the End.

Done Your new service is created with 256Kbps Speed Limitation with 1 Month Up-Time Limitaion.

Following are screenshot for the above created Service.

**RADIUS MANAGER 3**

System Users **Services** Managers RAS Financials Card system IAS

**New service**

**Basic parameters**

Service name: 256Kbps Monthly

Enable service: ☒

Available in UCP: ☒

Prepaid regular ☒ Prepaid card or IAS ☒

Type of service: ☐ Postpaid ☐ Email only ☐ Access list entry

Limit download Bytes: ☐

Limit upload Bytes: ☐

Limit total traffic: ☐

Limit expiration: ☒

Limit online time: ☐

Set data rates (DL / UL): 256 / 256 kbps

Expiration date unit: 1 Initial: 0 month(s)

Online time unit: 0 Initial: 0 minute(s)

Download traffic unit: 0 Initial: 0 MB

Upload traffic unit: 0 Initial: 0 MB

Total traffic unit: 0 Initial: 0 MB

Minimal base amount: 1 unit(s)

Minimal additional amount: 1 unit(s)

\* Fields are mandatory!

Store service

Add Service – Image 2 [aacable@hotmail.com](mailto:aacable@hotmail.com)

Now we have created the new service , its time to create new user or generate pre-paid cards and assosciate them with this new service plan.

rm-add-pre-paid-cards / aacable@hotmail.com

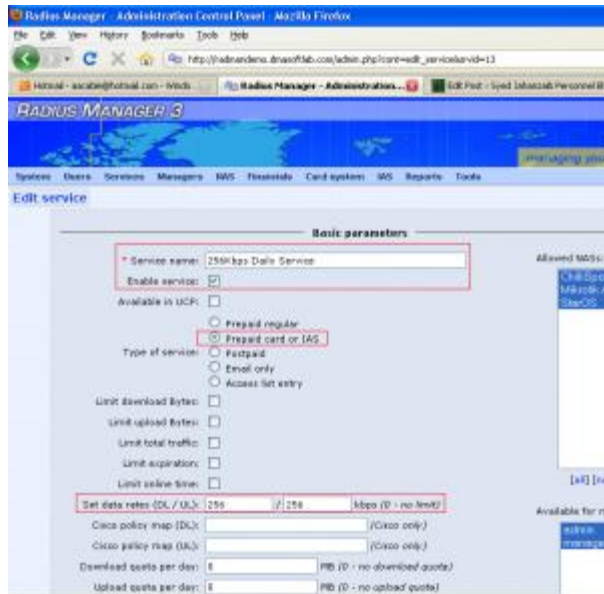
Service is ready to be used. 😊

## HOWTO ADD QUOTA BASE SERVICE IN RM:

Now we will Add Quota Base Service Plan. For example User is allowed to use **1GB @ 1mbps** per Day, After using his **1 GB** Quota, his service plan should auto switch to **256Kbps** speed plan for the rest of the day. . . We have to use **DAILY SERVICE** option in **RM** for this purpose. First create **Daily service** with **256Kbps** limitation, and then create the **1Mbps / 1Gb** Daily Quota limit service and use the next daily service option in **1mb** service plan to point it to **256k**.

First we will create **256Kbps** service plan. This will be very simple basic plan.

Open **RM ACP**, Goto **Services**, and create new service, and name it **256Mbps – Daily Service**, rest of options can be set by seeing the image below.



256k-daily-image-1

256k-daily-image-2

Click on Store Service. Now **256Kbps** daily service is ready, its time to create your regular **1Mbps / 1GB** daily Quota Service Plan. Open RM ACP, Goto **Services**, and create new service, and name it **256Mbps – Monthly**, rest of options can be set by seeing the image below.

Radius Manager - Administration Control Panel - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://radmandemo.dnsoftlab.com/admin.php?cont=edit\_service&id=12

Radius Manager - Administration...

Radius Manager 3

System Users Services Managers NAS Financials Card updates SMS Reports Tools

Edit service: Create new Service with 1Mb/1Gb quota

Basic parameters

Service name: 1Mbps - Monthly

Enable service: ☒

Available in UCF: ☒

Prepaid regular: ☐

Prepaid postpaid or LBS: ☒

Type of service: Postpaid: ☐ Prepaid only: ☐ Access list entry: ☐

Limit download bytes: ☒

Limit upload bytes: ☐

Limit total traffic: ☐

Limit expiration: ☒

Limit online time: ☐

Set data rates (DL / UL): 1024 / 256 kbps (0 - no limit)

Cisco policy map (DL): (Cisco only)

Cisco policy map (UL): (Cisco only)

Download quota per day: 1024 MB (0 - no download quota)

Upload quota per day: 0 MB (0 - no upload quota)

Allowed NAS:

Available for management:

1mb-1gb-quota-image-1

Radius Manager - Administration Control Panel - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://radmandemo.dnsoftlab.com/admin.php?cont=edit\_service&id=12

Radius Manager - Administration...

Limit upload bytes: ☐

Limit total traffic: ☐

Limit expiration: ☒

Limit online time: ☐

Set data rates (DL / UL): 1024 / 256 kbps (0 - no limit)

Cisco policy map (DL): (Cisco only)

Cisco policy map (UL): (Cisco only)

Download quota per day: 1024 MB (0 - no download quota)

Upload quota per day: 0 MB (0 - no upload quota)

Total quota per day: 0 MB (0 - no total quota)

Time quota per day: 00:00:00 (HH:MM:SS) (00:00:00 - no time quota)

Enable burst mode: ☐

Burst limit (DL / UL): 0 / 0 kbps

Burst threshold (DL / UL): 0 / 0 kbps

Burst time (DL / UL): 0 / 0 seconds

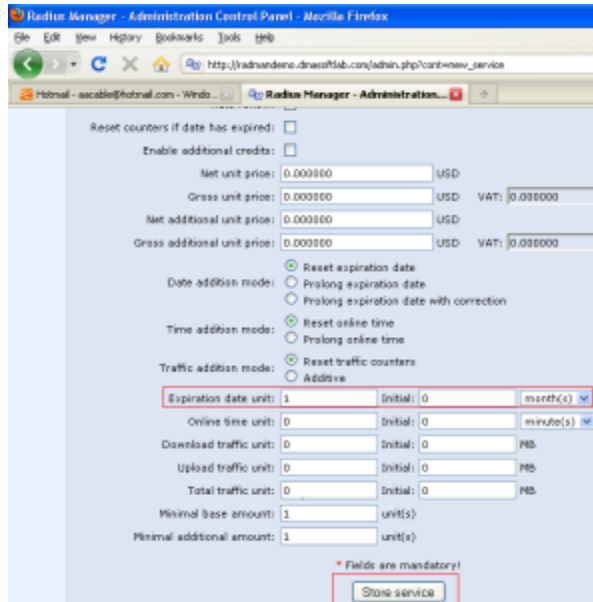
Priority: 0

IP pool name:

Next master service: None

Next daily service: 256Kbps Daily Service

1mb-1gb-quota-image-2



The screenshot shows the 'Radix Manager - Administration Control Panel' in a web browser. The page is titled 'cont-new\_service'. It contains several configuration sections:

- Reset counters if date has expired:** ☐
- Enable additional credits:** ☐
- Net unit price:** 0.000000 USD
- Gross unit price:** 0.000000 USD VAT: 0.000000
- Net additional unit price:** 0.000000 USD
- Gross additional unit price:** 0.000000 USD VAT: 0.000000
- Date addition mode:** ☒ Reset expiration date, ☐ Prolong expiration date, ☐ Prolong expiration date with correction
- Time addition mode:** ☒ Reset online time, ☐ Prolong online time
- Traffic addition mode:** ☒ Reset traffic counters, ☐ Additive
- Expiration date unit:** 1 Initial: 0 month(s) (highlighted with a red box)
- Online time unit:** 0 Initial: 0 minute(s)
- Download traffic unit:** 0 Initial: 0 MB
- Upload traffic unit:** 0 Initial: 0 MB
- Total traffic unit:** 0 Initial: 0 MB
- Minimal base amount:** 1 unit(s)
- Minimal additional amount:** 1 unit(s)

At the bottom, there is a red box containing the text '\* Fields are mandatory!' and a button labeled 'Stop service'.

1mb-1gb-quota-image-3

All Done. Now Simply generate cards or user ids and associate it with the 1mbps service.

## HOWTO SEND EMAIL NOTIFICATIONS / WARNING TO USERS BEFORE THERE ACCOUNT EXPIRE

Goto **Home / system settings** , here you can set it.

**Email notifications**

Send email notifications: ☐

Send email warnings: ☐

Warning level: ☒ Fixed value ☐ Percentage

Download warning:  MB  %

Upload warning:  MB  %

Total traffic warning:  MB  %

Online time warning:  (HH:MM:SS)  %

Expiry warning:  days

\* Fields are mandatory!

#### 4) LINUX TRANSPARENT FIREWALL BRIDGE CONFIGURATION [using FEDORA 10]

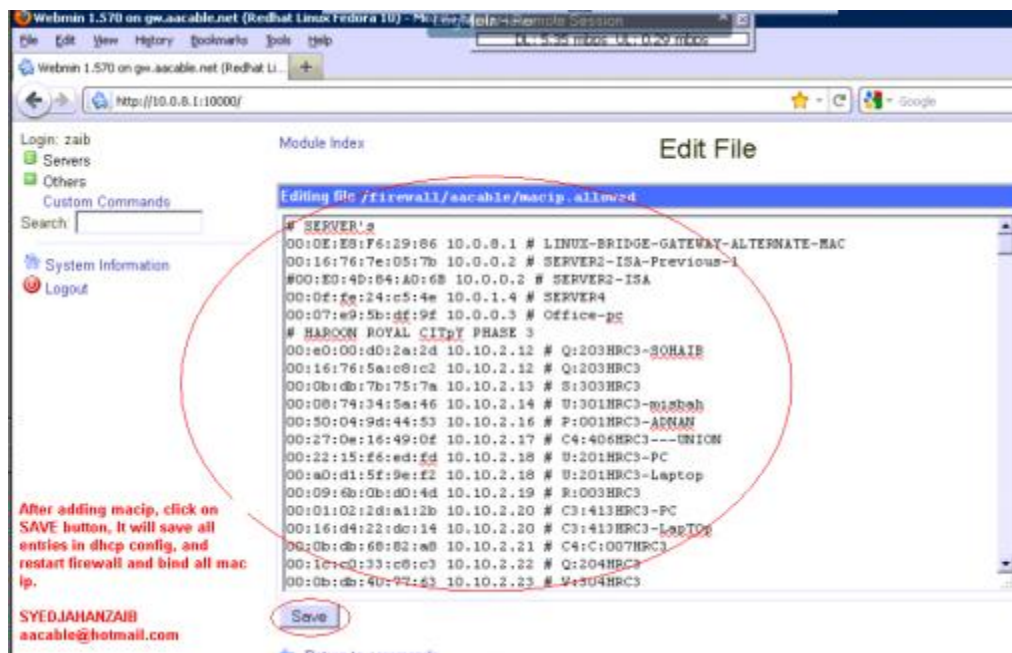
## Linux Transparent Firewall + Bridge

06/2011



In this scenario, Linux is acting as Transparent Bridge also acting as firewall. It is sitting between Users and Server end transparently. User will know nothing about it. It will filter all unwanted traffic. It is also acting as DHCP server with MAC to IP bind restriction. DHCP will read user mac address and ip from a file, and put it in its configuration file and iptables will lock the specific MAC to specific IP address (that we define in the file). So the user will get fix ip every time, if the user changes his ip or mac, he will not be able to pass from this bridge, any user mac/ip which is not defined in this file, will get invalid ip. valid user will get ips from the file and only these users will be able to communicate with the other end.





Following is a comprehensive guide on how you can setup Linux base Transparent bridge with advance firewall capabilities like **DHCP Server** **MACto IP** binding restriction, Easily add remove clients via single file using text editor or **WEBMIN**, Also you can **Port Filtering** to block unwanted traffic from passing through.

A **bridge** is a way to connect two Ethernet segments together in a protocol independent way. Packets are forwarded based on Ethernet address, rather than IP address (like a router). Since forwarding is done at Layer 2, all protocols can go transparently through a bridge. You can think of a bridge like a advance manageable network switch/firewall/router. We will be using this Linux Transparent bridge according to the network diagram shown at the start of this article.

The job of the bridge is to examine the destination of the data packets one at a time and decide whether or not to pass the packets to the other side of the Ethernet segment. The result is a faster, quieter network with less collisions.

You don't need to change your existing network layout. You just plug in the bridge and you start working. If for some reasons, your Linux bridge box should go down, reconnect the cables from your bridge to your switch, and nobody will even notice that something was not working!

The placement of the bridge would be something like.

Sserver's >> switch >>eth0>> **LINUX BRIDGE with 2 interfaces >>eth1>> User Switch >>User Pc's**

Now there are few scripts involved in engaging the bridge, If any one requires them, email me and I will send him my script copies, File Name: [firewall.rar](#)

**SIMPLE STEP BY STEP instructions on howto copy and execute the scripts:**

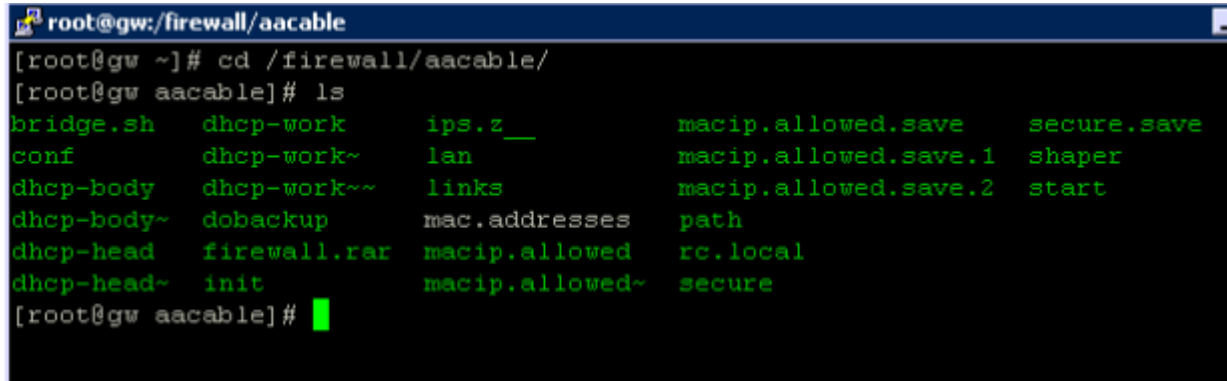
### **HAWRDWARE REQUIREMENTS:**

Any adequate P4 / Xeon Dual Core with at least 1 GB RAM , 2 Lan Cards (preferably Gigabit)

### **SOFTWARE REQUIREMENTS:**

Any Linux flavor, preferably **FEDORA CORE 10 or likewise** (Full installation with all packages selected at them time of installation, specially bridge utilities)

After successfull installation of **FEDORA**, copy **firewall.rar** , unrar them, and copy all scripts in a folder **/firewall/aacable**



```
root@gw:/firewall/aacable
[root@gw ~]# cd /firewall/aacable/
[root@gw aacable]# ls
bridge.sh  dhcp-work  ips.z__  macip.allowed.save  secure.save
conf       dhcp-work~  lan      macip.allowed.save.1  shaper
dhcp-body  dhcp-work~~ links    macip.allowed.save.2  start
dhcp-body~ dobackup   mac.addresses  path
dhcp-head  firewall.rar macip.allowed  rc.local
dhcp-head~ init       macip.allowed~ secure
[root@gw aacable]#
```

Now goto **/firewall/aacable** folder, make all scripts executable by issuing command **chmod +x \*.\***

If required, convert them using **dos2unix** command, as sometimes copying it from windows generates some problems.

Now copy **rc.local** to **/etc/** (overwrite older one) & restart the system.

Now after booting , **rc.local** will execute following files . . .

1)

**/firewall/aacable/bridge.sh**

(It will remove ip address from **eth0** n **eth1** and create bridge interface **br0** with following ip: **10.0.8.1** for remote access and management of local bridge system, also **dhcpcd** will be bind to this interface)

2)

**/firewall/aacable/conf**

(This is some custom configuration to prevent timeouts / delays, Latency and some other stuff)

3)

**/firewall/aacable/start**

(This is the main firewall script , It will execute All **DHCP** n Firewall related Scripts one by one. It will add all **mac/ ip** found in **macip.allowed** file in **dhcp** configuration file and then bind them using **iptables** so that user mac ip must be matched with the file accordingly otherwise user access will not be granted. Any user whose entry will not be found in **macip.allowed** file, will get off subnet ip like **192.168.100.x**

You can view the '**start**' file and see the related actions defined in there.

**Your BRIDGE is ready & Following restrictions will be in place.**

1)

If a user **MAC n IP** is found in **/firewall/aacable/macip.allowed** file, User will be granted valid ip as you entered in the macip.allowed file, for example

**00:19:d1:fd:83:b1 10.10.2.13 # ZAIB-PC**

The user with above mac address will always get the **10.10.2.13** ip, if he manually tries to change the ip or mac, he will not be able to pass the bridge. MAC n IP combination matching is required in order to pass the bridge.

If a user **MAC n IP** is not found in **/firewall/aacable/macip.allowed** file, User will be granted **INVALID ip** series from following off subnet **192.168.100.10-192.168.100.200** and thus will be completely isolated from the local valid network.

You can change all ip series in DHCP related files.

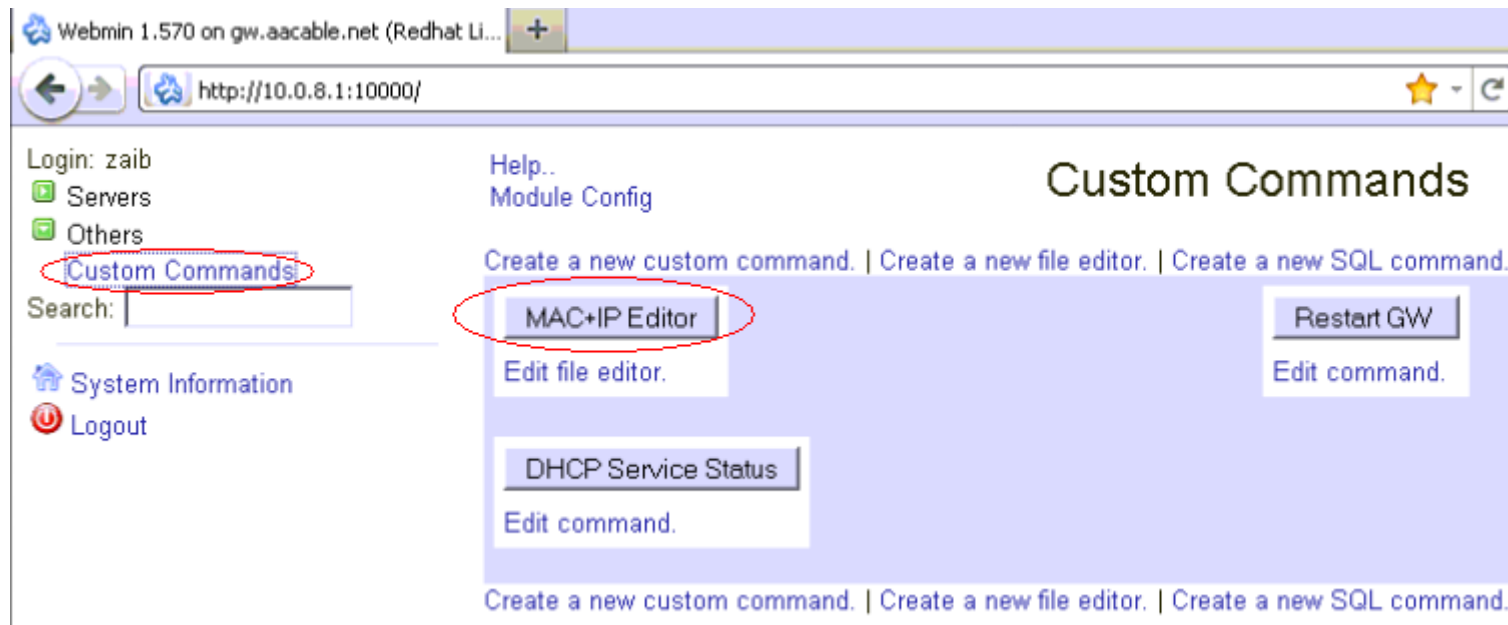
To add user , you can manually edit **/firewall/aacable/macip.allowed** file and add entry in following format

**00:16:76:7E:05:7B 10.0.0.1 # SERVER1-ISA**

**00:06:5b:62:71:0a 10.10.2.12 # JOHN-LAPTOP**

and the run **start** file which will add entry in macip.allowed file and add dhcp entry and run the security script.

OR the easiest way is to setup **WEBMIN** and link the file with webmin, so you can add/remove files easily via webmin GUI.I have done some advance customization of **webmin**, I added support user in **webmin** for support personnel , and grant him only right of editing this file, after the support personnel edit this file and click on **save**, it automatically execute the start script which add / remove all entries again in firewall. See the below images for example.



Webmin 1.570 on gw.aacable.net (Redhat Linux Fedora 10) - Mozilla Remote Session

DL: 5.35 mbps UL: 0.29 mbps

Webmin 1.570 on gw.aacable.net (Redhat Li... +

http://10.0.8.1:10000/

Google

Login: zaib

Servers

Others

Custom Commands

Search:

System Information

Logout

Module Index

Edit File

Editing file /firewall/aacable/macip.allowed

```
# SERVER's
00:0E:E8:F6:29:86 10.0.8.1 # LINUX-BRIDGE-GATEWAY-ALTERNATE-MAC
00:16:76:7e:05:7b 10.0.0.2 # SERVER2-ISA-Previous-1
#00:E0:4D:84:A0:6B 10.0.0.2 # SERVER2-ISA
00:0f:fe:24:c5:4e 10.0.1.4 # SERVER4
00:07:e9:5b:df:9f 10.0.0.3 # Office-pc
# HAROON ROYAL CITpY PHASE 3
00:e0:00:d0:2a:2d 10.10.2.12 # Q:203HRC3-SOHAIB
00:16:76:5a:c8:c2 10.10.2.12 # Q:203HRC3
00:0b:db:7b:75:7a 10.10.2.13 # S:303HRC3
00:08:74:34:5a:46 10.10.2.14 # U:301HRC3-misbah
00:50:04:9d:44:53 10.10.2.16 # P:001HRC3-ADNAN
00:27:0e:16:49:0f 10.10.2.17 # C4:406HRC3---UNION
00:22:15:f6:ed:fd 10.10.2.18 # U:201HRC3-PC
00:a0:d1:5f:9e:f2 10.10.2.18 # U:201HRC3-Laptop
00:09:6b:0b:d0:4d 10.10.2.19 # R:003HRC3
00:01:02:2d:a1:2b 10.10.2.20 # C3:413HRC3-PC
00:16:d4:22:dc:14 10.10.2.20 # C3:413HRC3-LapTop
00:0b:db:68:82:a8 10.10.2.21 # C4:C:007HRC3
00:1e:c0:33:c8:c3 10.10.2.22 # Q:204HRC3
00:0b:db:40:77:63 10.10.2.23 # V:304HRC3
```

Save

Return to commands

After adding macip, click on SAVE button, It will save all entries in dhcp config, and restart firewall and bind all mac ip.

SYEDJAHANZAIB  
aacable@hotmail.com

This firewall script also blocks few ports which are commonly used in virus flooding, thus saving junk traffic from passing by from one end to other end.

You can do many interesting things using this bridge :~)

**BRIDGE SETUP DONE.**

X=X=X=X=X=XX=X=X=X=X=X=X=X=X=X=X=X=X=X=X=X=X=X

Note: Later on, I moved FTP servers from Mikrotik DMZ to User Subnet, I also changed FTP operating system from Microsoft Windows 2003 R2 Server to Ubuntu Linux and set all sharing via Apache and linked apache authentication with Radius Manager , This step was done because there was unnecessary junk load of FTP data going through Mikrotik router , so I placed them on user subnet and put radius authenticaiton on it, so only valid account holder can access it. I have also posted an article on my blog website on how I achieved it.

**So guys, this is a very shorten version of how I completed this project. It was a very good project for me. I learned many new techniques on howto handle various issues. It took me many days n nights in googling, and I must say GOOGLE was my best friend and I consider google my teacher 😊**

**If you need any assistance , Do let me know**



Regard's

**SYED JAHANZAIB**

Email: aacable [at] hotmail.com

Source:

<http://aacable.wordpress.com/2011/07/19/mikrotik-dmasoftlab-rm-squid-zph-linux-bridgecomplete-guide/>