

WIRELESS HACKS™

2nd
Edition

*Tips & Tools for Building, Extending,
and Securing Your Network*



O'REILLY®

Rob Flickenger & Roger Weeks



HACK

#51

Track Wireless Users

Automatically keep a database of MAC address to IP address mappings.

MAC address filters on access points are easily circumvented using commonly available tools. If your APs are bridged to the Ethernet segment [Hack #64], there are a couple of utilities you can use to look for people spoofing their MAC addresses. One such tool is *arpwatch*, available from <http://www-nrg.ee.lbl.gov/nrg.html>.

arpwatch runs as a daemon on any machine and keeps track of the MAC address/IP address pairs as ARP replies pass through the network. When it notices something out of the ordinary, it logs the activity to *syslog* and sends an email to the address of your choice. Aside from looking for suspicious activity, this also gives you a nice log of every new user on your wireless network. This can be fun to watch over time, particularly if you are running an open wireless network.

After you unpack the *arpwatch* archive, take a look at *addresses.h*. This is where the email address is set, so be sure to update it before you compile *arpwatch*. Set *WATCHER* to whatever you like. The default is *root*, which sends it to *root* at the machine that is running *arpwatch*.

You should be able to build and install the binaries with the usual commands:

```
/arpwatch-2.1a11# ./configure; make; make install
```

Unfortunately, this doesn't install all of the necessary pieces. In particular, *arpwatch* expects */usr/local/arpwatch* to exist by default and to contain the *arp.dat* database file. It also looks in this directory for an Ethernet OUI to manufacturer a list to give more informative information about the machines it sees.



Check out “Find Radio Manufacturers by MAC” [Hack #39] for more details about the OUI portion of MAC addresses.

Create the necessary directory and files with the following commands:

```
/arpwatch-2.1a11# mkdir /usr/local/arpwatch  
/arpwatch-2.1a11# cp ethercodes.dat /usr/local/arpwatch  
/arpwatch-2.1a11# touch /usr/local/arpwatch/arp.dat
```

Finally, if you have sufficient space, you should install the manpages as well:

```
/arpwatch-2.1a11# cp *.8 /usr/local/man/man8
```

Now you can start *arpwatch* as a daemon. Use the *-i* switch to specify the interface you would like to watch:

```
# arpwatch -i eth0
```

If it doesn't seem to be running, it will log any problems to *syslog*, so take a look at your system logs (particularly */var/log/messages* and */var/log/syslog*).

Now, as machines ARP for each other on the network, *arpwatch* keeps track of them. Every time there is new activity, you should get an email that looks something like this:

```
From: arpwatch@florian.rob.swn (Arpwatch)
Date: Mon Jun 23, 2003 2:16:51 PM US/Pacific
To: root@florian.rob.swn
Subject: new station (dhcp-68)

      hostname: dhcp-68
      ip address: 10.15.6.68
      ethernet address: 0:30:65:03:e7:8a
      ethernet vendor: APPLE COMPUTER, INC.
      timestamp: Monday, June 23, 2003 14:16:51 -0700
```

You will be notified by email whenever a new client is detected, when an already logged MAC address is seen in use with a new IP address, and when the MAC address associated with a particular IP changes. There are a number of legitimate reasons why IP-to-MAC address mappings might change, particularly if you are running a busy network with an insufficient number of available DHCP leases.

Regardless of the cause, *arpwatch* keeps a nice historical log of the traffic it sees, which can be valuable when tracking down potential miscreants. Since *arpwatch* logs to *syslog* as well as email, you can easily generate reports or graphs by processing these logs whenever you like.

While *arpwatch* faithfully logs everything it sees, it doesn't actually take any corrective action on its own. If you need an automated method for reacting to suspicious ARP or other activity on your network, take a look at Snort (<http://www.snort.org>).