Network Monitoring with Arpwatch

Arpwatch allows a system to track IP address pairings. It maps the MAC Addresses on a network by tracking ARP requests to each device on the LAN and recording the response in a database. All network cards are manufactured with a unique MAC address and this allows Arpwatch to identify each device. The main purpose of mapping a network like this is so the system administrator can keep track of the devices on a network and identify when there are networking issues. Arpwatch is commonly used to identify when an ARP Man in the Middle attack is being conducted by notifying the system administrator when a duplicate MAC address is being used on the network. Arpwatch is most commonly ran on routers, but it can also useful on a managed network switch.

Install

Arpwatch is not apart of the standard Slackware Linux distribution. It can be obtained by downloading the SlackBuild from SlackBuilds.org for your desired Slackware release. SlackBuilds.org has a great HOWTO discussing how to install a SlackBuild. The SlackBuilds.org FAQ is also very helpful for Slackware users struggling to install a SlackBuild.

Configuration

The included start up script allows the administrator to configure Arpwatch for one or more network cards. The start up script is also where the administrator can configure the run time settings for Arpwatch. Open up **/etc/rc.d/rc.arpwatch** on your system and edit the **OPTIONS** variable to your satisfaction. By default the **root** account gets all Arpwatch emails. Let's try changing the email account Arpwatch will use for email notifications. Make sure you use a user account or an email address that exists or Arpwatch will not send notifications to you.

The line you are looking for is:

```
OPTIONS="-i $IFACE -f $ARPDIR/arp-$IFACE.dat -u root -e root -s root"
```

The Arpwatch man page indicates that the **-e** switch manages the email account. Let us change it to the user **darkstar**.

```
OPTIONS="-i $IFACE -f $ARPDIR/arp-$IFACE.dat -u root -e darkstar -s root"
```

Or we can use a remote email address if **sendmail** is configured to do so:

```
OPTIONS="-i $IFACE -f $ARPDIR/arp-$IFACE.dat -u root -e
user@randomdomain.com -s root"
```

Update MAC Address Database

The README.ethercodes installed with the Arpwatch SlackBuild indicates that the MAC Address database that comes with the source tarball can be outdated. This database is only updated when there is a new release of Arpwatch, which has not happened in quite a while.

These steps are covered in greater detail if you read /usr/doc/arpwatch-$VERSION/README.ethercodes

```
su -
cd /var/lib/arpwatch
wget http://standards-oui.ieee.org/oui.txt
./massagevendor oui.txt > ethercodes.dat
rm -f oui.txt
```

Start and Stop at Boot

The file **/etc/rc.d/rc.arpwatch** controls start up and shut down of Arpwatch. In order to use this script you need to add a few lines to **/etc/rc.d/rc.local** and **/etc/rc.d/rc.local_shutdown**. Be sure to use the appropriate order if you have any other network services starting or stopping in these scripts. As an example, you should start Arpwatch before you bring up hostapd if you are running a Wireless Access Point, and shutdown Arpwatch after hostapd exits. Using such ordering assures that Arpwatch identifies all ARP requests on your network.

Continuing with the above example lets assume you are running a wireless access point. Add this to **/etc/rc.d/rc.local**

```
if [ -x /etc/rc.d/rc.arpwatch ]; then
  /etc/rc.d/rc.arpwatch start wlan0
fi
```

If you wish to run Arpwatch on multiple network cards adjust **/etc/rc.d/rc.local** like this:

```
# Change eth0 and wlan0 to match your configuration
if [ -x /etc/rc.d/rc.arpwatch ]; then
  /etc/rc.d/rc.arpwatch start eth0
  /etc/rc.d/rc.arpwatch start wlan0
fi
```

It's important that Arpwatch is stopped cleanly when your system is shutdown or rebooted. If you haven't already done so, create **/etc/rc.d/rc.local_shutdown** as root:

```
touch /etc/rc.d/rc.local_shutdown
```

Next you need to edit **rc.local_shutdown** like so:

```
if [ -x /etc/rc.d/rc.arpwatch ]; then
  /etc/rc.d/rc.arpwatch stop
fi
```

Finally, mark **rc.local** and **rc.local_shutdown** as *executable*. This tells Slackware to automatically

execute these scripts during the boot process.

```
chmod +x /etc/rc.d/rc.local
chmod +x /etc/rc.d/rc.local_shutdown
```

Wrap Up

Assuming all steps were followed you should have received an email for each device Arpwatch discovered on your network. If you opted to use the **root** user for notifications, you can view them by using the **mail** command as root user.

```
mail -f /var/spool/mail/root
```

Here is an example of what you may find in your inbox:

```
            hostname: <unknown>
          ip address: 192.168.151.170
   ethernet address: XX:XX:XX:XX:XX:XX
   ethernet address: XX:XX:XX:XX:XX:XX
    ethernet vendor: <unknown>
          timestamp: Monday, April 9, 2018 12:01:39 -0600
```

Sources

* Arpwatch Home

* Originally written by Brenton Earl

howtos, network, monitoring, arpwatch, user mralk3