Arpwatch – мониторинг соответствие между IP и MAC-адресами

Рано или поздно, любой сетевой администратор сталкивается с необходимостью контролировать смену/появление новых MAC-адресов в сети. Если сеть совсем маленькая – это не сложно, если же сеть на сотни устройств – контролировать подключение устройств к сети становится довольно проблематично. С помощью утилиты ARPWatch можно отслеживать изменения в сети. ARPWatch отслеживает соответствие Ethernet-адресов и IP-адресов. Активность регистрируется в syslog и с помощью почтовых оповещений. Для прослушивания ARP-трафика на локальном ethernet-интерфейсе используется библиотека pcap.

Назначение ARPWatch

- отслеживать появление в сети новых устройств
- отслеживать подмену IP-адресов
- обнаруживать атаки ARP-вирусов

Принцип работы

- ARPWatch запускается на Unix-сервере и работает в фоновом режиме как демон
- ARPWatch слушает на указанном сетевом интерфейсе все широковещательные ARP-уведомления вида “я, устройство с MAC-адресом 11-22-33-44-55-66, имею IP-адрес 77.88.99.111”
- Информация сохраняется во внутренней базе
- При появлении новых устройств или изменении существующих связок MAC-IP отправляется уведомление по электронной почте

Недостатки

- Каждое уведомление отправляется отдельным сообщением.
- Такая отчётность занимает много места, и самое главное — абсолютно лишена наглядности.
- В большой сети не всегда возможно подключить сервер с ARPWatch в каждый сегмент.

Режимы Веб-интерфейса

- Показ сообщений с группировкой по MAC или IP
- Фильтрация за последний день и час
- Показ всех сообщений для выбранного MAC или IP
- Статистика по количеству сообщений для MAC и IP

Устанавливаем arpwatch
Из порта:

```
cd /usr/ports/net-mgmt/arpwatch && make install clean
```

Пакетом:

```
pkg_add -r arpwatch
```

после чего правим rc.conf для запуска arpwatch при загрузке системы:

```
vi /etc/rc.conf
arpwatch_enable="YES" #включаем arpwatch
arpwatch_interfaces="nfe0" #какие интерфейсы слушать
#arpwatch_interfaces="" #слушать все интерфейсы
#arpwatch_nfe0_options="-m admin@mydomain.ru" #отправлять лог себе на мыло
```

Ведение логов

для ведения логов лучше настроить для этого syslog.conf:

```
vi /etc/syslog.conf
!arpwatch
*.notice /var/log/arpwatch.log
```

Мониторинг

Таблица соответствия адресов находится в файле

/usr/local/arpwatch/arp.<интерфейс>.dat и выглядит как обычный текстовый файл, с MAC-адресом, IP-адресом, временем попадения в таблицу, и именем интерфейса, через который пришёл исходный запрос.

```
cat /usr/local/arpwatch/arp.nfe0.dat
0:f:ea:63:e2:d7 192.168.1.31 1265370078 oksen
0:1:29:1b:35:7e 192.168.1.18 1265369952 narman
0:2:b3:b2:26:e4 192.168.1.254 1265370062 ns
0:1d:7d:a6:77:64 192.168.1.67 1265368627 r423-1
0:1d:7d:a6:70:80 192.168.1.84 1265370079 lib5
0:1d:7d:70:6f:28 192.168.1.43 1265370029 tender
0:1d:7d:a6:70:35 192.168.1.82 1265370064 lib3
0:c:76:97:51:e5 192.168.1.48 1265368690 jurist
0:b:6a:6d:fd:81 192.168.1.83 1265370048 lib4
0:e0:4d:2a:cd:68 192.168.1.35 1265369127 matbuh2
0:1d:7d:a6:6a:4b 192.168.1.86 1265370064 lib7
0:1a:4d:dc:db:46 192.168.1.65 1265370078 r421a
0:e:a6:27:5a:59 192.168.1.156 1265370034 lib2-ab1
0:2:44:5a:a4:3d 192.168.1.45 1265369568 ois3
0:f:ea:4f:20:89 192.168.1.24 1265370015 glbuh
0:1a:4d:fb:e:a4 192.168.1.152 1265370059 lib2-4z
0:2:b3:b8:8a:36 192.168.1.38 1265370059 serv3
```

arpwatch формирует события следующих типов:

Важные:

- new activity – Это Ethernet/IP был использован впервые за 6 месяцев.
- new station – Это Ethernet/IP был использована впервые
- flip flop – Замена адреса с одного на другой (оба были в списке).
- changed ethernet address – Замена на новый MAC адрес Ethernet.

Дополнительные:

- ethernet broadcast – MAC-адрес хоста является широковещательным.
- ip broadcast – IP-адрес хоста является

широковещательным.

- bogon – Адрес отправителя IP-пакета не входит в непосредственно подключённую
  сеть (directly connected network) для заданного интерфейса.
- ethernet broadcast – MAC-адрес отправителя состоит из одних нулей или одних
  единиц.
- ethernet mismatch – MAC-адрес отправителя пакета не соответствует MAC-адресу,
  указанному внутри ARP-запроса.
- reused old ethernet address – Ethernet-адрес изменился с известного адреса на
  адрес, который был замечен ранее, но не только
  что. (Похоже на flip flop, но чуть-чуть другое.)
- suppressed DECnet flip flop – Сообщение “flip flop” подавлено в связи с тем,
  что как минимум один из двух адресов является адресом DECnet.

если есть необходимость вести журнал всех событий (не только важных), то меняем (*.*notice*) на (*.*) в syslog.conf

после чего перезагружаем syslog

killall -HUP syslogd

выглядеть это будет примерно так:

cat /var/log/arpwatch.log

```
Feb 5 09:27:20 bsd-9 arpwatch: new station 192.168.1.169
0:13:8f:27:2f:6f
Feb 5 09:30:39 bsd-9 arpwatch: new station 192.168.1.29
0:13:8f:24:a3:a
Feb 5 09:35:39 bsd-9 arpwatch: new station 192.168.1.28
0:2:44:5a:69:65
Feb 5 09:53:28 bsd-9 arpwatch: new station 192.168.1.33
0:2:44:5a:69:6b
Feb 5 09:55:40 bsd-9 arpwatch: new station 192.168.1.8
```

```
0:1d:7d:a6:6a:73
Feb 5 10:17:35 bsd-9 arpwatch: new station 192.168.1.249
0:13:46:65:81:f5
Feb 5 10:17:36 bsd-9 arpwatch: changed ethernet address
192.168.1.249 0:11:95:b8:96:42 (0:13:46:65:81:f5)
Feb 5 10:41:15 bsd-9 arpwatch: new station 192.168.1.146
0:f:ea:63:f8:40
Feb 5 10:49:11 bsd-9 arpwatch: new station 192.168.1.164
0:19:5b:2f:99:b1
Feb 5 10:52:11 bsd-9 arpwatch: new station 192.168.1.124
0:f:ea:63:f8:32
Feb 5 11:00:57 bsd-9 arpwatch: new station 192.168.1.170
0:f:ea:4f:65:d7
```

по желанию можно настроить ротацию:

```
vi /etc/newsyslog.conf
/var/log/arpwatch.log 644 3 100 * JC
```

Перенесена с www.ignix.ru
http://muff.kiev.ua/content/arpwatch-sledim-za-novymi-ustroistvami-v-seti

Web-interface №2

Первым делом необходимо создать базу данных, куда будем записывать данные, полученные от ARPWatch. Создадим базу данных и пользователя с правами на эту базу данных:

```
 mysql> create database arpwatch;
 Query OK, 1 row affected (0.00 sec)
  mysql> grant all on arpwatch.* to arpwatch@localhost
identified by 'VerySecretPassword';
 Query OK, 0 rows affected (0.00 sec)
 mysql> use arpwatch;
 Database changed
```

SQL-запросы для создания структуры таблиц будут следующие:

```
CREATE TABLE flip_flop( hostname VARCHAR( 255 ) ,
ip_address VARCHAR( 15 ) ,
ethernet_address VARCHAR( 17 ) ,
ethernet_vendor VARCHAR( 255 ) ,
```

```
old_ethernet_address VARCHAR( 17 ) ,
old_ethernet_vendor VARCHAR( 255 ) ,
TIMESTAMP VARCHAR( 19 ) ,
previous_timestamp VARCHAR( 19 ) ,
delta VARCHAR( 50 )

);

CREATE TABLE changed_ethernet_address(
hostname VARCHAR( 255 ) ,
ip_address VARCHAR( 15 ) ,
ethernet_address VARCHAR( 17 ) ,
ethernet_vendor VARCHAR( 255 ) ,
old_ethernet_address VARCHAR( 17 ) ,
old_ethernet_vendor VARCHAR( 255 ) ,
TIMESTAMP VARCHAR( 19 ) ,
previous_timestamp VARCHAR( 19 ) ,
delta VARCHAR( 50 )

);

CREATE TABLE new_station(
hostname VARCHAR( 255 ) ,
ip_address VARCHAR( 15 ) ,
ethernet_address VARCHAR( 17 ) ,
ethernet_vendor VARCHAR( 255 ) ,
TIMESTAMP VARCHAR( 19 )

);

CREATE TABLE new_activity(
hostname VARCHAR( 255 ) ,
ip_address VARCHAR( 15 ) ,
ethernet_address VARCHAR( 17 ) ,
ethernet_vendor VARCHAR( 255 ) ,
TIMESTAMP VARCHAR( 19 )

);
```

Скачиваем скрипт **arpwatch.pl** в каталог /usr/local/arpwatch и распакуем его из архива:

```
# cd /usr/local/arpwatch
# fetch http://muff.kiev.ua/files/arpwatch.pl.tar.gz
arpwatch.pl.tar.gz 100% of 1210 B 9 MBps
# tar -xzf arpwatch.pl.tar.gz
```

Этот скрипт будет парсить информацию, получаемую от ARPWatch и раскладывать ее по таблицам базы данных. Для того, чтобы скрипт мог “достучаться” до базы данных, необходимо изменить в нем параметры коннекта к базе данных. Редактируем файл и выставляем переменные в необходимые значения:

```
 $db_user = "arpwatch";
 $db_passwd = "VerySecretPassword";
 $db_name = "arpwatch";
 $db_host = "localhost";
 $db_port = "3306";
```

Для корректной работы скрипта необходима поддержка таких модулей Perl, как DBI, DBD-mysql и Getopt-Long. Если какой-то из модулей не установлен, его необходимо установить. Желательно из системы портов:

```
# cd /usr/ports/databases/p5-DBI && make install clean && rehash
# cd /usr/ports/databases/p5-DBD-mysql && make install clean && rehash
# cd /usr/ports/devel/p5-Getopt-Long && make install clean && rehash
```

Для того, чобы скрипт “скармливал” данные в БД, необходимо в него перенаправить уведомления электронной почты ARPWatch. В моем случае на роутере работает Sendmail в дефолтной конфигурации. Выполним его настройку так, чтобы письма отправленные пользователю arpwatch перенаправлялись в скрипт **arpwatch.pl**.

Создадим пользователя arpwatch, которому и будем доставлять почту (я использовал uid 1005 – проверьте у себя какой uid можно использовать):

```
# pw useradd -n arpwatch -u 1005 -g mailnull -c ARPWatch -d
```

```
/nonexistent -s /usr/sbin/nologin
```

Отредактируем опции запуска ARPWatch в /etc/rc.conf, а именно – получателем уведомлений сделаем локального пользователя arpwatch:

```
# cat /etc/rc.conf | grep arpwatch_flags
arpwatch_flags="-m arpwatch@localhost"
```

Создаем почтовый алиас для пользователя arpwatch с перенаправлением его почты в скрипт arpwatch.pl:

```
#       echo       'arpwatch:       "|/usr/bin/perl
/usr/local/arpwatch/arpwatch.pl"' >> /etc/mail/aliases
```

Чтобы изменения, добавленные в /etc/mail/aliases вступили в силу, необходимо отправить Sendmail-у команду на перечитывание алиасов:

```
# sendmail -bi
/etc/mail/aliases: 29 aliases, longest 40 bytes, 344 bytes
total
```

Запускаем ARPWatch и проверяем, заполняются ли таблицы базы данных. Если заполняются – значит все в норме. Если же нет – смотрите /var/log/maillog и диагностируйте ошибку.

Приступим к настройке веб-интерфейса. Перейдем в каталог /usr/local/www и загрузим туда архив веб-интерфейса:

```
# cd /usr/local/www
# fetch http://muff.kiev.ua/files/arpwatch-www.tar.gz
arpwatch-www.tar.gz 100% of 51 kB 52 MBps
# tar -xzf arpwatch-www.tar.gz
# chown -R www:www /usr/local/www/arpwatch
# rm arpwatch-www.tar.gz
```

Необходимо указать параметры доступа к базе данных в файле /usr/local/www/arpwatch/config.inc.php. Редактируем следующие поля:

```
$dbhost = "localhost"; //Сервер базы данных
$dbuser = "arpwatch"; //Имя пользователя БД
```

```
$dbpassword = "VerySecretPassword"; //Пароль в БД
$dbname = "arpwatch"; //Имя БД
```

Добавим такой блок в httpd.conf – конфигурационный файл веб-сервера Apache:

```
 Alias /arp/ "/usr/local/www/arpwatch/"
 <Directory "/usr/local/www/arpwatch/">
    Options -Indexes
    DirectoryIndex index.php
    AllowOverride None
    Order Deny,Allow
    Allow from all
 </Directory>
```

Отправим Apache команду на перечитывание конфигурации:

```
# apachectl graceful
```

В браузере вводим ссылку **http://ip_servera/arp/** и видим следующий интерфейс: