ARPWatch

ARPWatch, arp bilgilerine bakarak ethernet arayüzlerini kontrol eden programdır.

California Üniversitesi Lawrence Berkeley National Laboratory Network Research Group'unda çalışmakta olan Craig Leres tarafından yazılmıştır.

California Üniversitesi'ne ait özel bir açık kaynak kod lisansına sahiptir.

Gelen ARP bilgilerini kendi veritabanında tutar. PCap kütüphanesini kullanmaktadır.

ARPWatch'u şu şekilde kurabilirsiniz :

```
# wget ftp://ftp.ee.lbl.gov/arpwatch.tar.gz
# tar -zxvf arpwatch.tar.gz
# cd arpwatch-2.1a13/
#./configure
#make
#make install
```

make install komutundan sonra arpwatch ikilileri sisteminize kurulacaktır.

arpwatch çalıştırma parametrelerine bakarsak;

```
# /usr/local/sbin/arpwatch --help
Version 2.1a13
usage: arpwatch [-dN] [-f datafile] [-i interface] [-n net[/width]] [-r
file]
```

- d : debug seçeneğini aktif eder.
- f : MAC/IP adres veritabanının tutulduğu dosyayı belirler. Öntanımlı arp.dat dosyasıdır.
- i : arpwatch'un öntanımlı dinleyeceği ağ arayüzünü belirler.
- n : Dinlenecek ağı belirtir.
- N : bogon hatalarının mail ile raporlanmasını engeller.
- r : Önceden oluşmuş bir arp veritabanını kullanmak için kullanılır.

ARPWatch, gelen arp bilgileri veritabanında tutarak bunlar hakkında çeşitli yorumlar ve karşılaştırmalar yapar.

SYSLOG MESAJLARI

Arpwatch tüm kayıtlarını syslog ile tutmaktadır:

```
# tail -f /var/log/messages
Apr 26 09:20:26 gcknw073 arpwatch: ethernet mismatch 192.168.192.1
0:12:1:3:90:1c (0:0:5e:0:1:c9)
Apr 26 09:20:32 gcknw073 arpwatch: new station 192.168.2.36
0:c:f1:5e:1d:cb
Apr 26 09:20:54 gcknw073 arpwatch: ethernet mismatch 192.168.192.1
0:12:1:4:90:1c (0:0:5e:0:1:c9)
Apr 26 09:21:09 gcknw073 arpwatch: ethernet mismatch 192.168.203.1
0:12:1:4:90:1a (0:0:f4:0:1:cb)
```

Syslog mesajlarının anlamlarına bakarsak:

MAC broadcast

Makinenin ağa MAC Adresini broadcast yaydığını gösterir.

ip broadcast

Makinenin IP adresini ağa broadcast yaydığını belirtir.

bogon

Kaynak IP adresinin yerel ağa ait bir IP bloğundan olmadığını belirtir.

MAC broadcast

Kaynak MAC adresinin hepsinin 0 ya da hepsinin 1 lerden oluştuğunu bildirir.

MAC mismatch

Kaynak MAC adresinin adres veritabanını ile uyuşmadığını bildirir.

reused old MAC address

KAynak makinenin daha once görüldüğü bir MAC adresini tekrar aldığını gösterir. (flip-flop mesajları oluşturur.)

suppressed DECnet flip flop

flip flop mesajlarını oluşturur. Bir MAC adresi iki ayrı IP'de görüldüğü zaman oluşur.

HATA MESAJLARI

Arpwatch syslog ile tuttuğu tüm kayıtları mail ile bildirmez. Arpwatch'un bildirdiği 4 çeşit mesaj vardır:

new activity

Bu MAC/IP adresi 6 aydan bu yana ilk defa ağda anons edilmektedir.

new station

MAC adresi ilk defa ağa dahil olmuştur.

flip flop

Kaynak makinenin MAC adresi değiştiğinde ya da bir MAC adresini birden fazla IP kullandığında oluşur.

changed MAC address

Makine (host) yeni bir MAC adresi ile ağa dahil olmuştur.

ARPWatch'u çalıştırmadan önce arp veritabanı olarak kullanılmak üzere arp.dat isimli bir dosya oluşturmalısınız. Daha sonra;

```
# /usr/local/sbin/arpwatch –N
```

Komutu ile arpwatch'u çalıştırabilirsiniz. arp veritabanını daha sonra kullanmak için arp.dat dosyanızı yedekleyebilirsiniz.

KAYNAKLAR:

[1] man arpwatch

İlk güncelleme: 26.04.2006
Son güncelleme: 28.04.2006

Afşin TAŞKIRAN
EnderUNIX Yazılım Geliştirme Takımı @ Türkiye
afsin ~ enderunix.org
www.enderunix.org/afsin