Dhcpdump - утилита для диагностики и отладки работы DHCP

Опубликовано muff в Чт, 2016-03-17 01:05

При наличии в сети **DHCP**-сервера, иногда возникает необходимость детального анализа содержимого **DHCP** запросов/ответов. В этом случае отличным помощником выступает утилита **dhcpdump**. Указав в качестве параметра сетевой интерфейс, получаем расшифровку всех зафиксированных на нем **DHCP**-пакетов.

Выполним установку утилиты из системы портов:

```
# cd /usr/ports/net/dhcpdump && make install clean && rehash
```

Сложностей с использованием утилиты не возникает. Ключей запуска не так и много:

```
# dhcpdump
Usage: $0 <-i interface> [-h macaddress]
```

По сути, из обязательных ключей запуска - необходимо указать интерфейс, на котором необходимо перехватывать **DHCP** траффик. Также, можно использовать ключ **-h** и регулярные выражения для прослушивания обмена только с определенным хостом/хостами.

Пример запуска утилиты:

```
# dhcpdump -i re0
```

где **re0** - интерфейс, на котором ожидаем DHCP-запросы.

Пример **DHCP**-запроса от клиента:

```
  TIME: 2016-03-15 03:06:19.106    IP: 10.70.1.26 (74:d0:2b:49:8a:b7) > 255.255.255.
255 (ff:ff:ff:ff:ff:ff)    OP: 1 (BOOTPREQUEST) HTYPE: 1 (Ethernet)  HLEN: 6  HOPS:
0   XID: a45b529a  SECS: 0 FLAGS: 7f80CIADDR: 10.70.1.26YIADDR: 0.0.0.0SIADDR: 0.0.0
.0GIADDR: 0.0.0.0CHADDR: 74:d0:2b:49:8a:b7:00:00:00:00:00:00:00:00:00:00 SNAME: . FN
AME: .OPTION:  53 (  1) DHCP message type         8 (DHCPINFORM)OPTION:  61 (  7) Cl
ient-identifier         01:74:d0:2b:49:8a:b7OPTION:  12 (  4) Host name
    ASUSOPTION:  60 (  8) Vendor class identifier   MSFT 5.0OPTION:  55 ( 13) Parame
ter Request List      1 (Subnet mask)                                              15
 (Domainname)                                          3 (Routers)
                                6 (DNS server)
       44 (NetBIOS name server)                                              46 (NetB
IOS node type)                                         47 (NetBIOS scope)
                                     31 (Perform router discovery)
                            33 (Static route)
     121 (Classless Static Route)                                             249 (MS
FT - Classless route)                                       43 (Vendor specifi
c info)                                          252 (MSFT - WinSock Proxy Auto De
tect)
```

Пример **DHCP**-ответа сервера:

```
  TIME: 2016-03-15 03:06:19.106    IP: 10.70.1.1 (00:e0:ed:26:69:d9) > 10.70.1.26 (7
4:d0:2b:49:8a:b7)    OP: 2 (BOOTPREPLY) HTYPE: 1 (Ethernet)  HLEN: 6  HOPS: 0   XID:
 a45b529a  SECS: 0 FLAGS: 7f80CIADDR: 10.70.1.26YIADDR: 0.0.0.0SIADDR: 0.0.0.0GIADDR
: 0.0.0.0CHADDR: 74:d0:2b:49:8a:b7:00:00:00:00:00:00:00:00:00:00 SNAME: . FNAME: .OP
TION:  53 (  1) DHCP message type         5 (DHCPACK)OPTION:  54 (  4) Server identi
fier         10.70.1.1OPTION:   1 (  4) Subnet mask              255.255.255.0OPTIO
```

```
N:  15 ( 22) Domainname                 example.comOPTION:   3 (  4) Routers
          10.70.1.1OPTION:   6 (  8) DNS server                 10.10.10.10,8.8.8.8
```

Если в сети много запросов, можно воспользоваться ключем **-h** и указать в качестве значения **MAC**-адрес устройства, от которого ожидаем запрос:

```
# dhcpdump -i re0 -h 6c:70:9f:d2:e2:2a
```

В результате перехватываем следующие данные:

```
  TIME: 2016-03-15 16:44:45.293     IP: 10.34.21.5 (6c:70:9f:d2:e2:2a
) > 10.34.21.1 (00:1b:21:ba:ea:b4)    OP: 1 (BOOTPREQUEST) HTYPE: 1 (Ethernet)  HLEN: 6  HOPS: 0
  XID: 68d02651  SECS: 0 FLAGS: 0CIADDR: 10.34.21.5YIADDR: 0.0.0.0SIADDR: 0.0.0.0GIADDR: 0.0.
0.0CHADDR: 6c:70:9f:d2:e2:2a:00:00:00:00:00:00:00:00:00:00 SNAME: . FNAME: .OPTION:  53 (  1)
DHCP message type         3 (DHCPREQUEST)OPTION:  51 (  4) IP address leasetime      86400 (24h)O
PTION:  12 ( 15) Host name                airport-extremeOPTION:  55 (  7) Parameter Request List      1
(Subnet mask)                          2 (Time offset)                          3 (Routers)
                                15 (Domainname)                          6 (DNS server)
                    12 (Host name)                          44 (NetBIOS name server)OPTION:  57 (
  2) Maximum DHCP message size 1500OPTION:  61 (  7) Client-identifier         01:6c:70:9f:d2:e2:2a
OPTION:  82 ( 18) Relay Agent Information                Circuit-ID    00:04:0d:5d:01:0a                Circu
it-ID    02:08:00:06:00:12:cf:82:7d:00---------------------------------------------------------------------------- TIME: 2
016-03-15 16:44:45.293    IP: 10.227.180.224 (00:1b:21:ba:ea:b4) > 10.34.21.5 (6c:70:9f:d2:e2:2a
)    OP: 2 (BOOTPREPLY) HTYPE: 1 (Ethernet)  HLEN: 6  HOPS: 0   XID: 68d02651  SECS: 0 FLAGS: 0CI
ADDR: 10.34.21.5YIADDR: 10.34.21.5SIADDR: 0.0.0.0GIADDR: 0.0.0.0CHADDR: 6c:70:9f:d2:e2:2a:00
:00:00:00:00:00:00:00:00:00 SNAME: . FNAME: .OPTION:  53 (  1) DHCP message type         5 (DHCP
ACK)OPTION:  54 (  4) Server identifier         10.34.21.1OPTION:  51 (  4) IP address leasetime      180
0 (30m)OPTION:   1 (  4) Subnet mask              255.255.255.0OPTION:   3 (  4) Routers                1
0.34.21.1OPTION:  15 ( 12) Domainname               example.comOPTION:   6 (  8) DNS server
   10.227.180.2,10.227.180.3OPTION:  82 ( 18) Relay Agent Information                Circuit-ID    00:0
4:0d:5d:01:0a                Circuit-ID    02:08:00:06:00:12:cf:82:7d:00----------------------------------------------
------------------------------
```

Источник (получено *2025-03-14 10:54*):
http://muff.kiev.ua/content/dhcpdump-utilita-dlya-diagnostiki-i-otladki-raboty-dhcp