DHCP Rework in Bro 2.6

Seth Hall
Corelight
Why Tackled?

Extend DHCP protocol analyzer with new options. #121

Mr-Click commented on Jan 8

Add the following option types:

- 55 Parameters Request List;
- 58 Renewal time;
- 59 Rebinding time;
- 61 Client Identifier;
- 82 Relay Agent Information.

 Extend the following events with new parameters, specifically:

- dhcp_discover exports client identifier and parameters request list;
- dhcp_request exports client_identifier and parameters request list;
- dhcp_ack exports rebinding time, renewal time and list of suboptions value of dhcp relay agent information option;
- dhcp_inform exports parameters request list.
Why Tackled?

• Log wasn’t great.
  • Purely based on DHCP ACK messages.
  • No tie together between assigned IP address and MAC address.

• Load balancing issues
  • Mix of broadcast and unicast packets is a nightmare for load balancing.
Design Approach
Novel BinPAC Structure

Define a case with no values up front

type OptionValue(code: uint8, length: uint8) = case code of {
    # This is extended in dhcp-options.pac
    MSG_TYPE_OPTION -> msg_type ::= uint8;
    default -> other ::= bytestring & length = length;
};

Refine and extend case (switch)

# Parse the option
refine casetype OptionValue += {
    ROUTER_OPTION -> router_list ::= uint32[length/4];
};
Design Approach
Simplify Event Structure

- dhcp_discover
- dhcp_offer
- dhcp_request
- dhcp_decline
- dhcp_ack
- dhcp_nak
- dhcp_release
- dhcp_inform

- dhcp_message
Design Approach
Centralize DHCP messages
Design Approach
Log DHCP “Conversation”

Client
- discover
- request

Server
- offer
- ack

One Log Entry!
What's in the log?

```json
{
  "ts": 1439902916.426308,
  "uids": [
    "CPYpdx1vBDR90y5xH",
    "CXCZAGi09NIEyaLOj"
  ],
  "client_addr": "172.17.156.78",
  "server_addr": "172.17.156.65",
  "mac": "a0:88:b4:d9:f4:e0",
  "host_name": "wma-asenm",
  "client_fqdn": "wma-asenm.COPCP.local",
  "requested_addr": "172.17.156.78",
  "assigned_addr": "172.17.156.78",
  "lease_time": 1000,
  "msg_types": [
    "DISCOVER",
    "OFFER",
    "REQUEST",
    "ACK"
  ],
  "duration": 0.10258
}
```
Regrets & Mistakes

- blindly changed the DHCP event structure!
  - Thanks to Vlad Grigorescu for jumping in and writing a compatibility script for scripts that haven’t been updated.
  - @load protocols/dhcp/deprecated_events
- No DHCPv6!
Fun Stuff

IP Forwarding option (19)

*Option length:* 3 bytes.

*Links:* [IANA: BOOTP and DHCP options.](#)

This option specifies whether the client should configure its IP layer for packet forwarding.

<table>
<thead>
<tr>
<th>MAC header</th>
<th>IP header</th>
<th>UDP header</th>
<th>BOOTP</th>
<th>DHCP header</th>
<th>BOOTP/DHCP option 19</th>
</tr>
</thead>
</table>

**BOOTP/DHCP option 19:**

<table>
<thead>
<tr>
<th></th>
<th>Code</th>
<th>Length</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>02</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>03</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>04</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>05</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>07</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>08</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Code.** 8 bits. Always set to 19.
Option code.

**Length.** 8 bits. Always set to 1.
Size of the option data in bytes.

**Value.** 8 bits.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Disable IP forwarding.</td>
</tr>
<tr>
<td>1</td>
<td>Enable IP forwarding.</td>
</tr>
</tbody>
</table>
The Dynamic Host Configuration Protocol (DHCP) Client
Fully Qualified Domain Name (FQDN) Option
Fun Stuff
Client FQDN option (81)

- BAHRxHxxxx.resource.ds.bah.com
- PLxxxxxx-NB.corp.tango.com
- sysxxxxl.meachamapel.com
- ussfmbblxxxxx.na.watson.com
- L01OHxxxxxxxxxxxxQ.cardinalhealth.net
Fun Stuff
Auto Proxy Config option (252)

INTERNET-DRAFT
Expires: December 1999
Category: Standards Track
draft-ietf-wrec-wpad-01.txt

Paul Gauthier
Inktomi Corporation
Josh Cohen
Microsoft Corporation
Martin Dunsmuir
RealNetworks, Inc.
Charles Perkins
Sun Microsystems, Inc.

Web Proxy Auto-Discovery Protocol

Status of This Memo
Thanks!