DHCP Rework in Zeek 2.6

Seth Hall
Corelight

Why Tackled?

Extend DHCP protocol analyzer with new options. #121

Closed **Mr-Click** wants to merge 2 commits into `bro:master` from `Mr-Click:feature/new_dhcp_data`

Conversation 6 | Commits 2 | Checks 0 | Files changed 17

Mr-Click commented on Jan 8 — Contributor

Add the folowing 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

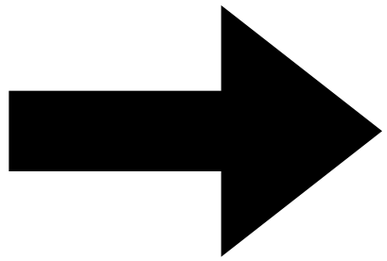
```
type OptionValue(code: uint8, length: uint8) = case code of {
    # This is extended in dhcp-options.pac
    MSG_TYPE_OPTION -> msg_type     : uint8;
    default         -> other        : bytestring &length = length;
};
```

Refine and extend case (switch)

```
# Parse the option
refine casetype OptionValue += {
    ROUTER_OPTION -> router_list : uint32[length/4];
};
```

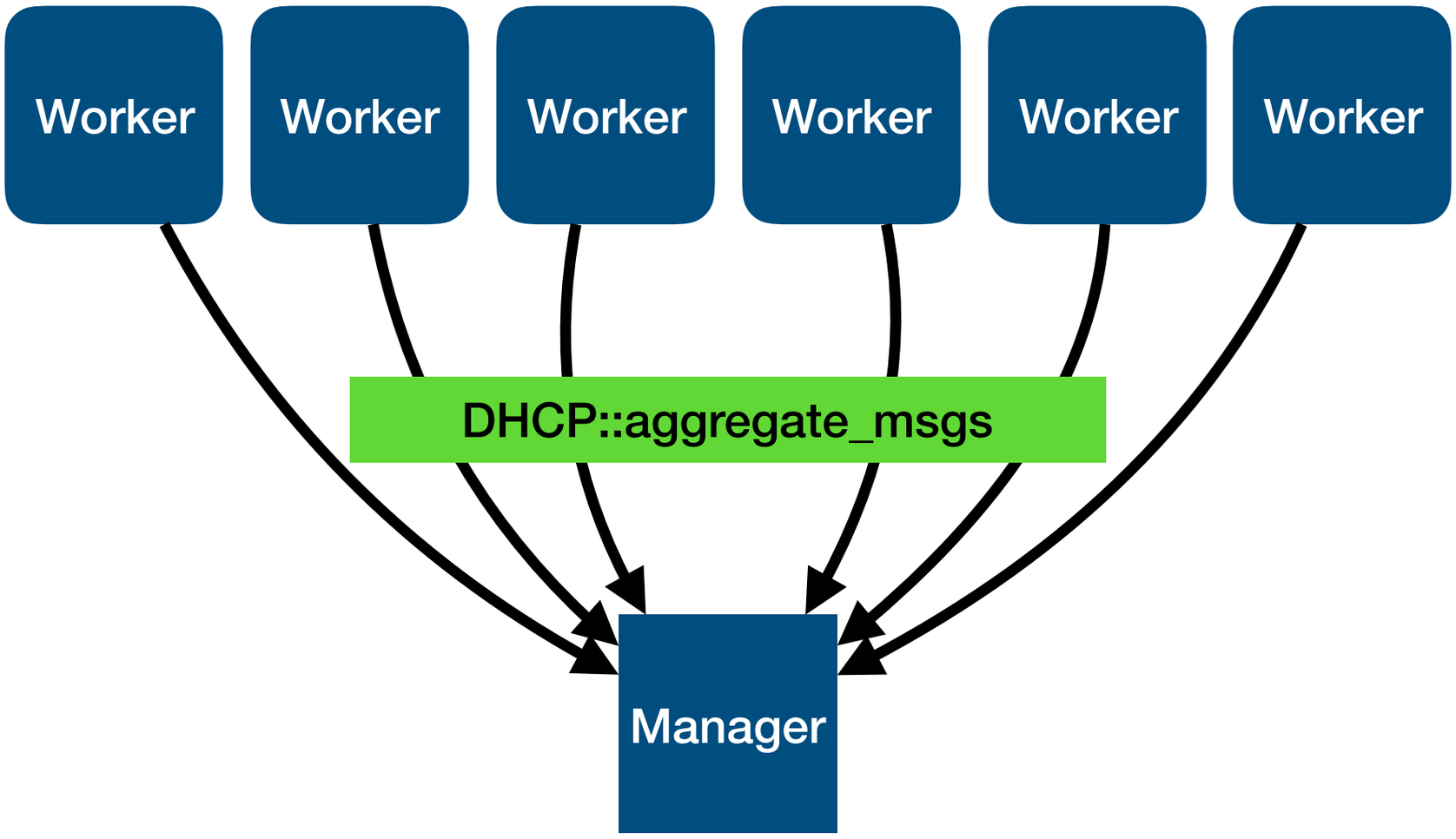
Design Approach
Simplify Event Structure

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

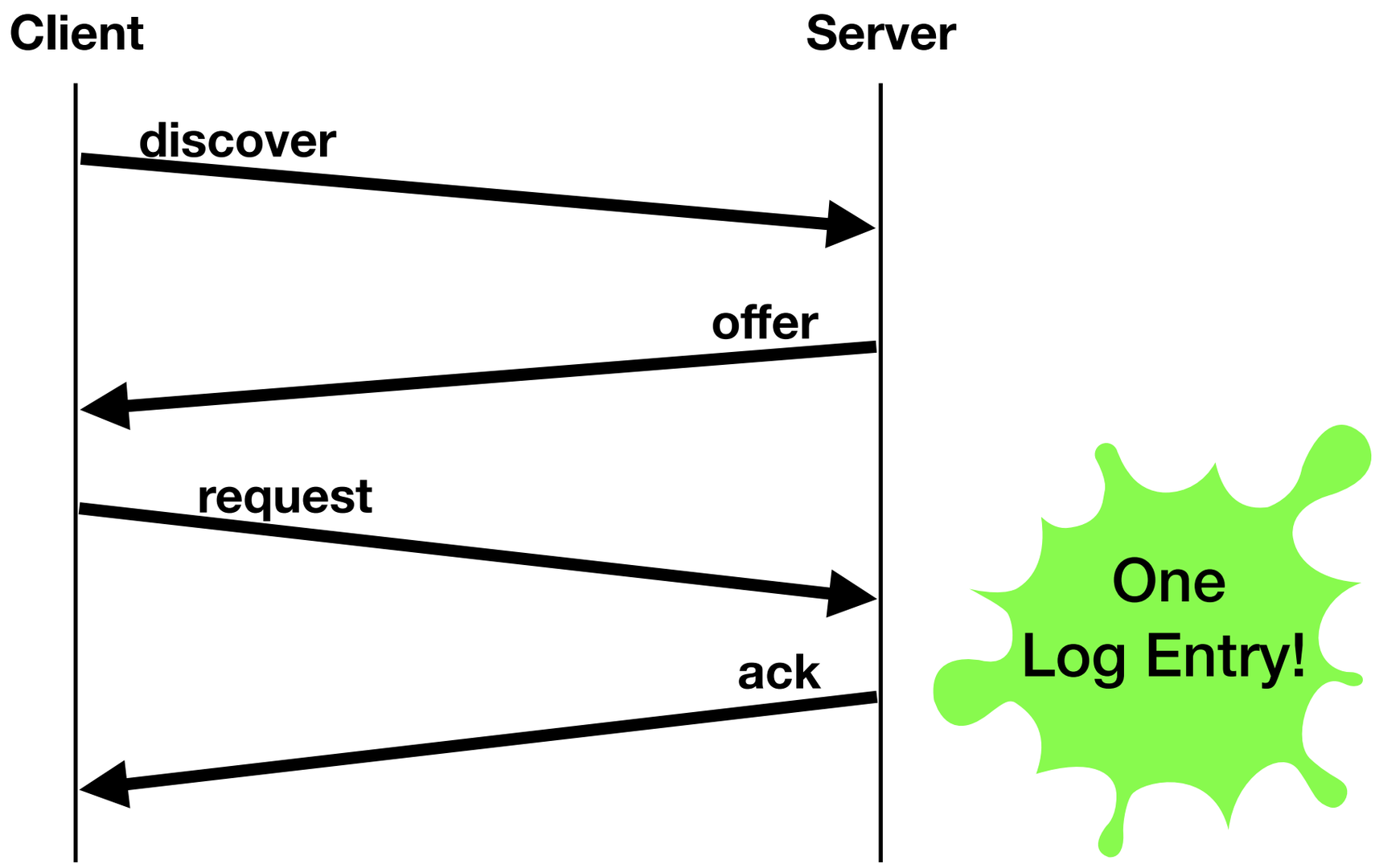


- dhcp_message

Design Approach
Centralize DHCP messages



Design Approach
Log DHCP “Conversation”



What's in the log?


```
{
  "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.

MAC header	IP header	UDP header	BOOTP | DHCP header	BOOTP/DHCP option 19

BOOTP/DHCP option 19:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Code								Length								Value							

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.

Value	Description
0	Disable IP forwarding.
1	Enable IP forwarding.

Fun Stuff
Client FQDN option (81)

[Docs] [txt|pdf] [draft-ietf-dhc-...] [Tracker] [Diff1] [Diff2]

PROPOSED STANDARD

Network Working Group
Request for Comments: 4702
Category: Standards Track

M. Stapp
B. Volz
Cisco Systems, Inc.
Y. Rekhter
Juniper Networks

October 2006

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.tangoe.com
- sysxxxl.meachamapel.com
- ussfmblxxxx.na.watson.com
- L01OHxxxxxxxxxQ.cardinalhealth.net

Fun Stuff
Auto Proxy Config option (252)

[Docs] [txt|pdf] [Tracker] [WG] [Email] [Diff1] [Diff2] [Nits]

Versions: 00 01

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!