COMPUTER NETWORKS

ASSIGNMENT 7

Custom Lightweight Discovery Protocol (CLDP) using Raw Sockets

Overview:

Raw sockets allow applications to access the network layer (IP) and data-link layer (Ethernet) directly, bypassing the standard TCP/UDP protocols, enabling the creation and parsing of custom headers and protocols.

CLDP is one such custom protocol (numbered 253) that operates over raw sockets and is used for node discovery and system information exchange. It supports 3 message types: HELLO, QUERY and RESPONSE.

Different servers periodically send a HELLO message indicating that they are an “active node” in a closed network environment. A client node listens for the HELLO messages and maintains a list of active nodes. It then periodically sends a QUERY message to all the active nodes, asking for some system metadata from the servers. The server receives this QUERY and sends a RESPONSE message containing the system metadata as a payload (character string).

The CLDP protocol constructs the packets in the following structure:

CLDP Header - 16 bytes, 4 bytes for each of the following:

type	: signifies packet type - HELLO, QUERY, or RESPONSE
payload_length	: length of the payload sent along with the packet*
transaction_id	: a randomly generated ID to allow QUERY-RESPONSE matching
reserved	: extra bytes to fix header size.

Payload (only for RESPONSE type message (Max Size: 512 bytes)

string : contains the metadata in the following format:

Time: YYYY-MM-DD HH:MM:SS | Host: <name> | Free RAM: <size> MB | CPU Load: 0.xx

Client Output: Uses non-blocking socket to receive the packets

```
CLDP Client started. Listening for HELLO messages...
Querying all active nodes...

--- Active Nodes ---
No active nodes

Received HELLO from 192.168.137.87
Received HELLO from 192.168.137.90
Received HELLO from 192.168.137.90
Received HELLO from 192.168.137.87
Querying all active nodes...
Sent QUERY to 192.168.137.87
Sent QUERY to 192.168.137.90

--- Active Nodes ---
1. 192.168.137.87
2. 192.168.137.90
------------------

Received RESPONSE from 192.168.137.90:
Time: 2025-03-31 23:02:43 | Host: nived-Inspiron-14-5420 | Free RAM: 4841 MB | CPU Load: 0.19

Received RESPONSE from 192.168.137.87:
Time: 2025-03-31 23:02:43 | Host: acer-aspire-lite-52 | Free RAM: 597 MB | CPU Load: 0.86
```

Server Output: Uses child process for sending HELLO and parent for responding to QUERY

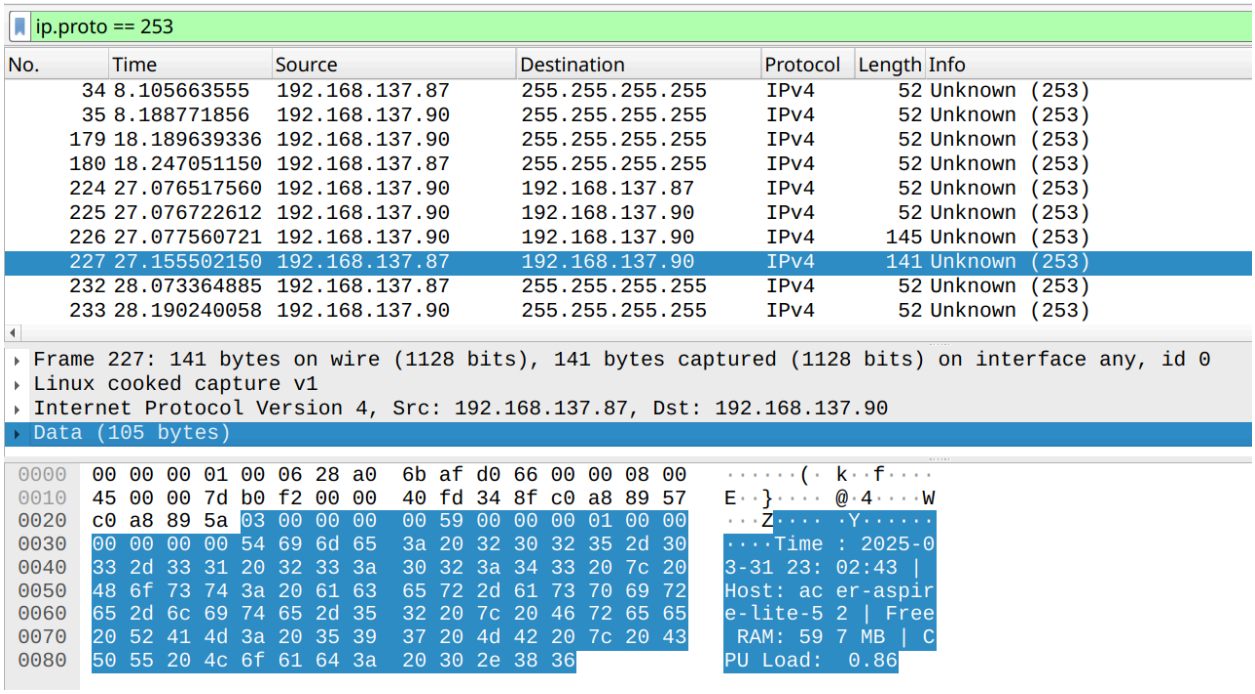
```
HELLO announcement broadcasted
HELLO announcement broadcasted
Received QUERY from 192.168.137.90
Sent RESPONSE to 192.168.137.90
HELLO announcement broadcasted
```

Additionally, the packets have manually crafted IP headers, which include a standard checksum calculation (similar to RFC 1071).

The manual crafting is possible by using

```
setsockopt(sock, IPPROTO_IP, IP_HDRINCL, &one, sizeof(one))
```

Wireshark Capture:



ip.proto == 253

No.	Time	Source	Destination	Protocol	Length	Info
34	8.105663555	192.168.137.87	255.255.255.255	IPv4	52	Unknown (253)
35	8.188771856	192.168.137.90	255.255.255.255	IPv4	52	Unknown (253)
179	18.189639336	192.168.137.90	255.255.255.255	IPv4	52	Unknown (253)
180	18.247051150	192.168.137.87	255.255.255.255	IPv4	52	Unknown (253)
224	27.076517560	192.168.137.90	192.168.137.87	IPv4	52	Unknown (253)
225	27.076722612	192.168.137.90	192.168.137.90	IPv4	52	Unknown (253)
226	27.077560721	192.168.137.90	192.168.137.90	IPv4	145	Unknown (253)
227	27.155502150	192.168.137.87	192.168.137.90	IPv4	141	Unknown (253)
232	28.073364885	192.168.137.87	255.255.255.255	IPv4	52	Unknown (253)
233	28.190240058	192.168.137.90	255.255.255.255	IPv4	52	Unknown (253)

```
▸ Frame 227: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 192.168.137.87, Dst: 192.168.137.90
▸ Data (105 bytes)
```

```
0000  00 00 00 01 00 06 28 a0  6b af d0 66 00 00 08 00   ......(· k··f····
0010  45 00 00 7d b0 f2 00 00  40 fd 34 8f c0 a8 89 57   E··}···· @·4····W
0020  c0 a8 89 5a 03 00 00 00  00 59 00 00 00 01 00 00   ···Z···· ·Y······
0030  00 00 00 00 54 69 6d 65  3a 20 32 30 32 35 2d 30   ····Time : 2025-0
0040  33 2d 33 31 20 32 33 3a  30 32 3a 34 33 20 7c 20   3-31 23: 02:43 |
0050  48 6f 73 74 3a 20 61 63  65 72 2d 61 73 70 69 72   Host: ac er-aspir
0060  65 2d 6c 69 74 65 2d 35  32 20 7c 20 46 72 65 65   e-lite-5 2 | Free
0070  20 52 41 4d 3a 20 35 39  37 20 4d 42 20 7c 20 43    RAM: 59 7 MB | C
0080  50 55 20 4c 6f 61 64 3a  20 30 2e 38 36            PU Load:  0.86
```