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:

Vo.		Time			Sour	ce				Des	tinati	on		P	rotocol	Length	Info			
	34	8.105	6635	55	192	. 168	3.137	87		255	. 255	5.255	. 255	I	Pv4	52	Unknown	(253)		
	35	8.188	7718	56	192	.168	3.137	90		255	. 255	5.255	. 255	I	Pv4	52	Unknown	(253)		
	179	18.18	96393	336	192	. 168	3.137	90		255	. 255	5.255	. 255	I	Pv4	52	Unknown	(253)		
	180	18.24	7051	150	192	.168	3.137	87		255	. 255	5.255	. 255	I	Pv4	52	Unknown	(253)		
	224	27.07	65175	560	192	.168	3.137	90		192	2.168	3.137	.87	I	Pv4	52	Unknown	(253)		
	225	27.07	67226	312	192	. 168	3.137	90		192	2.168	3.137	. 90	I	Pv4	52	Unknown	(253)		
	226	27.07	7560	721	192	. 168	3.137	90		192	2.168	3.137	. 90	I	Pv4	145	Unknown	(253)		
	227	27.15	55021	150	192	.168	3.137	.87		192	2.168	3.137	.90	I	Pv4	141	Unknown	(253)		
	232	28.07	33648	385	192	.168	3.137	.87		255	. 255	5.255	. 255	I	Pv4	52	Unknown	(253)		
	233	28.19	02400	958	192	.168	3.137	90		255	. 255	5.255	. 255	I	Pv4	52	Unknown	(253)		
⊦ Fr							re (1	128	bits	s),	141	bytes	s сар	tured	(1128	B bits)	on inte	rface	any,	id (
→ Fr → Li	nux (cooke	d cap	tur	e v1												on inte	erface	any,	id (
Fr Li	nux (cooke et Pr	d cap otoco	tur l V	e v1										(1128 68.13		on inte	erface	any,	id (
Fr Li	nux (cooke	d cap otoco	tur l V	e v1												on inte	erface	any,	id (
→ Fr → Li → In	nux (terno ta (:	cooke et Pr 105 b	d cap otoco ytes)	tur l V	e v1 ersi	on 4	4, Sr	c: 1	92.3	168.	137.	87, [Ost:	192.1	68.13	7.90		erface	any,	id (
Fr Li In	nux (terno ta (:	cooke et Pr 105 b	d cap otoco ytes) 00 01	tur l V	e v1 ersi 06	.on 4 28 a	4, Sr a0 6	c: 1	92.1 d0	168. 66 (137. 00 0	87, [0 08	Ost:	192.1	68.13	7.90		erface	any,	id (
→ Fr → Li → In → Da	nux (terno ta (:	cooke et Pr 105 b 0 00 (d cap otoco ytes) 00 01 00 7d	tur l V 00 b0	e v1 ersi 06 f2	on 4 28 a	4, Sr a0 6	c: 1 o af o fd	92.1 d0 34	168. 66 (137. 00 0	87, [0 08 8 89	00 57	192.1 	68.13	7.90 (···f····)·4·····	 W	erface	any,	id (
Fr Li In Da 000 001 002	nux (ita (:	cooke et Pr 105 b 0 00 (5 00 (d cap otoco ytes) 00 01 00 7d 39 5a	00 00 00	e v1 ersi 06 f2	28 a 6 0 0 0	4, Sr a0 6 00 4	c: 1 o af o fd	92.1 d0 34 00	168. 66 (8f (137. 00 0 c0 a	87, [0 08 8 89 1 00	00 57	192.1 E··}	68.13	7.90 (··f···)·4····	W	rface	any,	id (
Fr Li In 000 001 002 003	nux (ita (:	cooke et Pr 105 b 0 00 (5 00 (0 a8 8	d cap otoco ytes) 00 01 00 7d 39 5a 00 00	00 00 03 54	06 f2 00 69	28 a 60 0 66d 6	4, Sr a0 6 00 4 00 0 65 3	c: 1 o af o fd o 59 a 20	92.3 d0 34 00 32	168. 66 (8f (00 (30)	137. 00 0 c0 a 00 0 32 3	87, [0 08 8 89 1 00 5 2d	00 57 00 30	192.1 E··}	68.13	7.90 f 9.4 2025-	W	erface	any,	id (
Fr Li In 000 001 002 003 004	nux (ita (i	cooke et Pr 105 b 0 00 (5 00 (d cap otoco ytes) 00 01 00 7d 39 5a 00 00 33 31	00 00 03 54 20	06 f2 00 69 32	28 a 60 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	4, Sr a0 6 00 4 00 0 65 3 3a 3	c: 1 o af o fd o 59 a 20	92.3 d0 34 00 32 3a	168. 66 (8f (90 (30 : 34 : 34 :	137. 00 0 c0 a 00 0 32 3 33 2	87, [0 08 8 89 1 00	00 57 00 30 20	192.1 E··} ···Z ···3	68.13 ··(· k ···· @ ···· & Time : 23: @	7.90 (··f····)·4····· 2025-)2:43	W	erface	any,	id (
⊦ Li ⊦ In	nux (ternota (:	cooke et Pro 105 b 0 00 (5 00 (0 a8 8 0 00 (3 2d (d cap otoco ytes) 00 01 00 7d 39 5a 00 00 33 31 73 74	00 00 03 54 20 3a	06 f2 00 69 32 20	28 a 60 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	4, Sr a0 6 00 4 00 0 65 3 38 3 63 6	c: 1 o af o fd o 59 a 20 o 32 o 72	92.3 d0 34 00 32 3a 2d	168. 66 (8f (00 (30 (34 (61 (41 (41 (41 (41 (41 (41 (41 (41 (41 (4	137. 00 0 c0 a 00 0 32 3 33 2 73 7	87, [0 08 8 89 1 00 5 2d 0 7c	00 57 00 30 20 72	192.1 E··} ···Z 3-31 Host	68.13 ··(· k ···· @ ···· & Time : 23: @ : ac @	7.90 (f) () 7 2025- 02:43 er-aspi	W 0	erface	any,	id (
Fr Li In 000 001 002 003 004 005	nux (ternota) (ta (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	cooke et Pr 105 b 0 00 (5 00 (0 a8 8 0 00 (3 2d 3 3 6f	d cap otoco ytes) 00 01 00 7d 39 5a 00 00 33 31 73 74 6c 69	00 b0 03 54 20 3a 74	06 f2 00 69 32 20 65	28 a 60 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	4, Sr a0 6 00 4 00 0 65 3 33 6 33 6 35 3	c: 1 o af o fd o 59 a 20 o 32 o 72 o 20	92.3 d0 34 00 32 3a 2d 7c	66 (8f (90 (30 (34 (34 (34 (34 (34 (34 (34 (34 (34 (34	137. 00 0 c0 a 00 0 32 3 33 2 73 7 46 7	87, [0 08 8 89 1 00 5 2d 0 7c 0 69	00 57 00 30 20 72 65	192.1 E··} ···Z 3-31 Host e-li	68.13 ··(· k ··· @ ··· Time : 23: @ : ac @ te-5 2	7.90 (··f····)·4····· 2025-)2:43		erface	any,	id (