Implementare mDNS și DNS-SD. Aplicație demonstrativă.

Proiect realizat de Lemny Erich și Antăluțe Silvia

Introducere:
DNS - Domain Name System - modul în care calculatoarele interpretează un URL (de exemplu “google.com”) și îl transformă în adresa IP la care să se conecteze (în cazul de față, 172.217.23.110).

mDNS - Multicast DNS - modul în care, într-o rețea locală (de obicei, de dimensiuni reduse) se pot efectua operații de tip DNS într-o manieră simplă (cum ar fi asignarea fiecărui calculator și fiecărei adrese din rețea, o adresă tipic celor găzduite, de tipul MyComputer.local.)

DNS-SD - DNS-based Service Discovery - modalitatea în care, în cadrul unei rețele locale, pot fi interogate și identificate dispozitive ce acceptă comenzi/operații specifice. (de exemplu: un telefon mobil poate transmite unei imprimate comanda de a printa ceva, prin simplul fapt că ambele dispozitive sunt conectate la aceeași rețea)

Particularități de implementare:
Adresele IPv4 vor avea prefixul 169.254/16 iar cele IPv6 pe FE80::/10. Orice cerere de tip “.local.” va fi trimisă la adresa locală IPv4 = 224.0.0.251 (echivalentul IPv6 = FF02::FB).

mDNS oferă doua tipuri de cereri: one-shot și continuă/ongoing. Răspunsurile la interogările mDNS nu trebuie să conțină și alte întrebări/interogări (se ignoră dacă sunt). De asemenea, între fiecare interogare trebuie impus un delay de o durată aleatoare (un număr din intervalul 20-120ms selectat folosind distribuția aleatoare, sau 400-500ms dacă setul de biți este “truncated”).

1. Primul pas este de a analiza toate echipamentele ce conțin protocolul mDNS și de a le transmite o interogare pentru a vedea care dintre ele sunt ocupate sau rezervate. Se trimit 3 interogări cu pauză de 250(ms) între ele pentru a vedea care echipamente sunt disponibile.
2. Al doilea pas este de a anunța rețeaua și celelalte dispozitive, de resursele pe care noua componență le are la dispoziție printr-un răspuns forțat către toate celelalte echipamente (în caz de apar orice tip de schimbări în această etapă, se retrimit răspunsuri către toată rețeaua pentru ca fiecare echipament să aibă informația de actualitate).

Un mesaj mDNS trebuie să aibă alocat: 20 bytes pt IPv4/ 40 bytes pt IPv6, 8 bytes pentru header-ul UDP.
Orice pachet mDNS nu trebuie să depășească 9000 bytes (limita teoretică)/ 1500 bytes (limita actuală din motive de bună practică).

Mesajele de tip mDNS:
ID (identifier): 0 la transmisie și ignorat la recepție;
QR (query/response): 0 la interogări, 1 la răspunsuri;
OPCODE: 0 la transmisie. Orice răspuns care are un OPCODE mai mare de 0 va fi ignorat.

AA (authoritative answer):
- pentru interogări: 0 la transmisie, ignorat la recepție;
- pentru răspunsuri: 1 la transmisie, ignorat la recepție;

TC (truncated):
- pentru interogări: dacă este 1, înseamnă că urmează un răspuns deja cunoscut de către rețea;
- pentru răspunsuri: 0 la transmisie, ignorat la recepție;

RD (recursion desired): 0 la transmisie, ignorat la recepție.
RA (recursion available): 0 la transmisie, ignorat la recepție.
Z (zero):
AD (authentic data):
CD (checking disabled):
RCODE (response code): 0 la transmisie, iar orice răspuns care are un RCODE diferit de 0 trebuie ignorat.

Maparea răspunsurilor la interogărirle protocolului DNS-SD de tip PTR de forma <Service>.<Domain> se face astfel:

Service Instance Name = <Instance> . <Service> . <Domain>

Pentru DSN-SD, trebuie să avem înregistrări TXT și SRV, cele TXT având cel mult 200 bytes per înregistrare.

Diverse:

Inregistrarile TXT sunt de forma "key=value".
Exemplu:

| 0x09 | key=value | 0x08 | paper=A4 | 0x07 | passreq |

Observație:
- Dacă lipsește cheia, se ignoră;
- Dacă lipsește valoarea, se consideră tip de dată boolean, implicit 1;

De preferat să se introducă la început și un "txtvers=1" sau "txtvers=8" pentru a facilita procesul de interpretare a datelor(în special dacă se folosesc anumite versiuni de ASCII).
Pentru ca o înregistrare TXT să fie considerată goală/nulă, ea trebuie să aibă:
- Un singur octet de 0 (string gol);
- Un string de lungime 0;
- Să nu fie primită;

PTR mapează numele mașinii de un IP.
O înregistrare de tip PTR este de forma:
_service._proto.name. ttl PTR type CNAME

Exemplu:

_printer._tcp.local. 28800 PTR PrintsAlot._printer._tcp.local.

- service: (domeniul de forma <Service Type>.<Domain>) (variabil, 255 bytes);
- proto: (2 bytes);
- name: (variabil, 255 bytes);
- ttl: time to live, (32 biți = 4 bytes);
- type: 16 biți (2 bytes);
- CNAME: (variabil , 255 bytes);

O înregistrare de tip SRV este de tipul:
_service._proto.name. ttl IN SRV priority weight port target.

- *service*: un nume simbolic al serviciului oferit. (în cazul nostru, PTR de forma instance.service.domain) (variabil, maxim 255 bytes);
- *proto*: protocolul de transport (în cazul nostru, UDP) (2 bytes);
- *name*: numele domeniului valid. (variabil, maxim 255 bytes);
- *ttl*: time-to-live, durata de viață standard. (32 biți = 4 bytes);
- *IN*: standard DNS class field (mereu *IN*). (15 biți).
- *SRV*: tipul de înregistrare (mereu *SRV*) (2 bytes).
- *priority*: prioritatea gazdei, valoare mică înseamnă prioritate înaltă; (16 biti)
- *weight*: greutatea unei înregistrări în caz de se află conflict de prioritate, cu cât are valoarea mai mare cu atât șansa să fie aleasă e mai mare. (16 biți = 2 bytes)
- *port*: portul folosit. (16 biți = 2 bytes)
- *target*: numele gazdei care oferă respectivul serviciu. (variabil, maxim 255 bytes)

Exemplu:

_sip._tcp.example.com. 86400 IN SRV 0 5 5060 sip server.example.com.

Folosim UDP pentru configurație, mai specific, portul 5353.

Conversia SRV -> PTR -> A ->TXT

- Înregistrarea SRV: definește un serviciu și gazdă care furnizează acel serviciu.
- Înregistrarea PTR (Pointer Record): în mDNS, înregistrarea PTR este folosită pentru căutări DNS inverse pentru servicii. Pentru a crea o înregistrare PTR pentru o înregistrare SRV, trebuie să inversezi numele țintă al înregistrării SRV și să creezi o înregistrare PTR cu un nume precum "_service._protocol.local." De exemplu, dacă ai o înregistrare SRV precum "_http._tcp.local" îndreptată către "myserver.local," trebuie să creezi o înregistrare PTR cu numele "_http._tcp.local" și un tip de PTR îndreptat către "myserver.local."
- Înregistrarea A (Address Record): mapează un nume de gazdă la o adresă IPv4. Pentru a converti o înregistrare PTR într-o înregistrare A, trebuie să creezi o înregistrare A

pentru numele de gazdă (de exemplu, "myserver.local") și să specifici adresa IPv4 corespunzătoare.

- Înregistrarea TXT (Text Record): înregistrarea TXT poate stoca date text arbitrare asociate unui nume de gazdă. Pentru a converti o înregistrare PTR într-o înregistrare TXT, trebuie să creezi o înregistrare TXT pentru numele de gazdă (de exemplu “myserver.local”) și să furnizezi datele text relevante asociate serviciului,cum ar fi metadatele serviciului.

Pașii de implementat:

- Clientul caută în rețea și se conectează la server-ul gazdă;
- Server-ul gazdă dispune de un host-name anume;
- Clientul selectează serviciul dorit, folosind o interfață simplă;
- Gazda înregistrează acțiunile într-un jurnal;

Surse:

RFC 6762 - Multicast DNS
RFC 6763 - DNS-Based Service Discovery
RFC 1035 - Domain names - implementation and specification
RFC 2782 - A DNS RR for specifying the location of services (DNS SRV)
Iotespresso.com
socket - Python 3.12.0 documentation
https://github.com/TUIASI-AC-IoT/proiectrcp2023-echipa1
https://github.com/nicolaebotezatu/RC-P
https://grouper.ieee.org/groups/1722/contributions/2009/Bonjour%20Device%20Discovery.pdf
Ethical Hacking - A Hands-on Introduction to Breaking In (Daniel Graham)