LUCRAREA NR. 7
DNS: SISTEMUL NUMELOR DE DOMENII

1. Obiective

Obiectivele acestui laborator sînt: întelegerea noțiunilor de rezoluție de nume, spațiu de nume DNS, familiarizarea cu componentele DNS: servere, zone, resolvere, înregistrări de resurse, prezentarea procesului de interogare: metode de rezoluție, paşii unei interogări, caching, configurarea serverelor şi clienților DNS.

2. Consideraţii teoretice

2.1 Introducere

Fiecare host pe care este instalată stiva TCP/IP trebuie să aibă asignată o adresa IP unică pentru a comunica cu alte hosturi. Hosturile dintr-o rețea operează cu adrese IP dar utilizatorilor le este mai uşor să identifice un host printr-un nume.

La începutul rețelei ARPANET exista un număr redus de hosturi. NIC (Network Information Center) era locul în care se menținea un fişier de configurație, HOSTS.TXT, cu numele şi adresele tuturor hosturilor din rețea. Adminsitratorii actualizau via e-mail fişierul HOSTS.TXT, iar utilizatorii rețelei ARPANET descărcau prin ftp acest fişier.

În timp, rețeaua ARPANET s-a dezvoltat şi au apărut: problemele de scalabilitate - lățimea de bandă necesară pentru transferul versiunile actualizate ale HOSTS.TXT era proporțională cu pătratul numărului de hosturi din ARPANET, probleme legate de natura statică şi flat a fişierului - imposibil ca două hosturi din rețea să aibă acelaşi nume, probleme generate de modificarea caracteristicilor rețelei. Pe masură ce rețeaua ARPANET evolua s-a renunțat la soluția fişierului centralizat şi s-a adoptat o soluție bazată pe serviciul de nume distribuit şi pe un spațiu de nume ierarhic. RFC 882 şi 883 descriu sistemul numelor de domenii, RFC 1034 şi 1035 conțin proiectarea acestui sistem.

În esență, sistemul numelor de domenii conține tot o listă de nume şi adrese IP dar aceasta nu este stocată într-un singur loc ci distribuită pe mai multe servere din Internet.
DNS reprezintă serviciul ce gestionează numele de domenii şi rezolvă solicitările clienților de translatare a numelor în adrese IP şi reciproc.

2.2 Sistemul numelor de domenii (DNS – Domain Name System)

2.2.1 Spațiul de nume DNS. Nume de domenii

Sistemul de nume DNS are o organizare ierarhică, sub formă de arbore. Spațiul de nume are o rădăcină unică (root) care are subdomenii, fiecare nod şi frunză a arborelui spațiului de nume reprezentînd un nume de domeniu. Fiecare domeniu poate avea subdomenii.

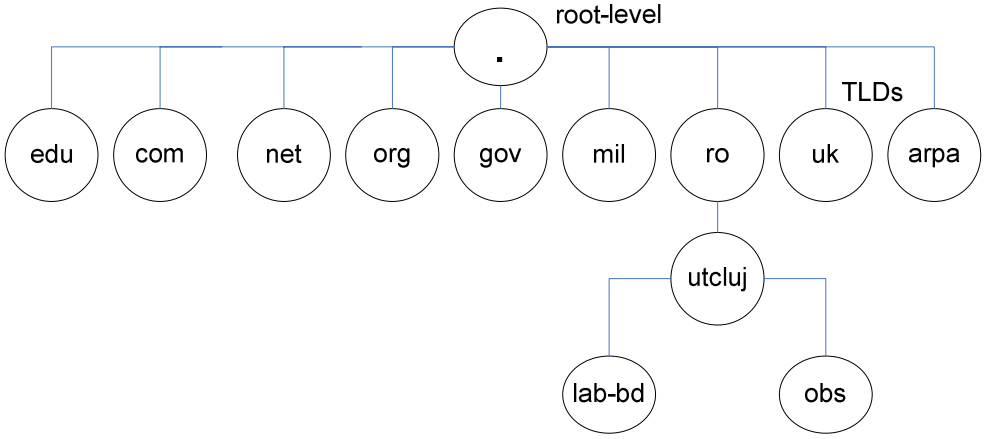

Figura 7.1 *Ierarhia DNS*

Organizarea ierarhică a spațiului de nume DNS face posibil ca un server din Internet să execute un număr cît mai mic de paşi pentru localizarea unei surse autoritative pentru un domeniu de nume. Localizarea este eficientă deoarece fiecare domeniu de la un anumit nivel păstrează informații despre domeniile de pe nivelul inferior.

Fiecare nod din arborele DNS are un nume definit în RFC 1034 ca etichetă. O etichetă are lungimea de 1 pînă la 63 de caractere, numele domeniului rădăcină nu are nici un character. Un nume de domeniu este lista etichetelor din calea de la nod pînă la rădăcina spațiului de nume.

Convenția de citire a etichetelor DNS indică parcurgerea de la stînga la dreapta – de la cel mai specific nume spre rădăcina (de exemplu, host1.design.compania.com). Acest nume complet se numeşte nume de domeniu în formă canonică (FQDN - fully qualified domain name).

Domeniile de sub domeniul rădăcină se numesc domenii de vîrf (TLD - top-level domains). Există trei categorii de domenii de vîrf:

- ARPA: domeniu special pentru mapări adresă_IP-la-nume (căutare inversă - reverse lookup);
- domenii de vîrf generice (domenii organizaționale): domenii cu nume formate din trei caractere care indică funcția sau activitatea pe care o îndeplinesc organizațiile care dețin aceste domenii (de exemplu, com, edu, info, gov, mil, museum, biz, aero, net, org);
- domenii de tări (domenii geografice): domenii cu nume bazate pe standardul ISO de denumire a tărilor (de exemplu, ro, uk, dk, sg).

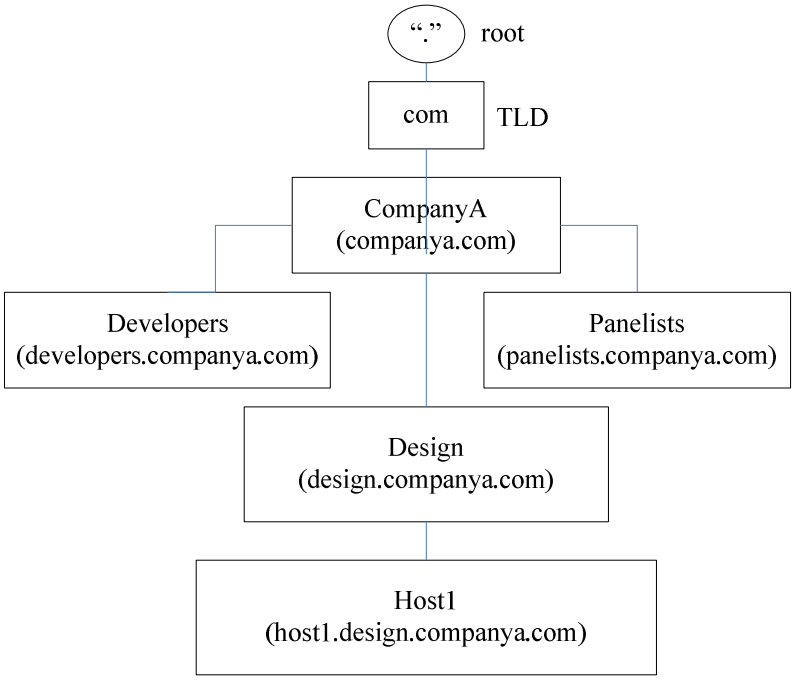

Figura 7.2 *Domenii şi subdomenii*

2.2.2 Componente DNS

Sistemul numelor de domenii are la bază configurarea serverelor DNS, zonelor, rezolverelor şi înregistrărilor de resurse.

2.2.2.1 Servere DNS

Un server DNS este un host pe care rulează un program de server DNS, de exmplu serviciul DNS Server sau BIND (Berkley Internet Name Domain). Serverele DNS stochează informații despre o porțiune din structura ierarhică a spațiului de nume şi rezolvă interogări de rezoluție de nume pentru clienții DNS. Cînd sînt interogate, serverele DNS răspund cu informația cerută dacă aceasta este disponibilă sau generează un referal către alt server DNS care poate rezolva interogarea.

Serverele de nume rădăcină (root name servers) sînt situate pe cel mai înalt nivel al ierarhiei de nume şi stochează informaţii despre domeniile de vîrf (TLD). Dezvoltatorii de software preconfigurează implementarile de servere DNS cu adresele IP ale serverelor de nume rădăcina.

Serverele de nume care conțin informatii despre toate hosturile dintr-o zonă se numesc servere de nume master. Orice interogare dintr-o zonă ajunge la un server de nume master. Administratorul de rețea poate configura unul din servere ca server primar – acesta îşi încarcă informația despre zonă din fişierul de date, iar celelalte servere ca servere secundare – acestea îşi actualizează informația despre zonă de la serverul primar la intervale regulate de timp.

2.2.2.2 Zone DNS

O zonă DNS este un spațiu continuu de nume din spațiul de nume DNS pentru care un server DNS are autoritatea să rezolve interogările. O zonă poate conține unul sau mai multe domenii DNS. Pentru fiecare domeniu DNS inclus in zona, zona devine sursă autoritativă de informații despre acel doemniu.

În majoritatea implementărilor de server DNS, datele dintr-o zona sînt stocate în baze de date flat sau în fişiere text. Fişierele din zonă conțin informații pe care serverele DNS le acceseaza pentru a rezolva rezoluția de nume în adresă şi rezoluția de adresă în nume. Informatia din fişiere e stocată sub forma unor înregistrări de resurse (resource records).

2.2.2.3 Resolvere DNS

Resolverul DNS este un serviciu care utilizează protocolul DNS pentru a transmite interogari serverelor DNS. În majoritatea implementarilor, resolverul este parte a serviciului de client DNS.

Un host care comunică regulat cu un alt host trebuie să trimită interogări de rezoluție de nume de mai multe ori (de exemplu, numele serverului de mail). Pentru a evita transmiterea unei interogări DNS de fiecare dată cînd hostul vrea să rezolve numele celuilalt host, serviciul de client DNS implementează un cache local pentru informații DNS.

Serviciul client DNS memorează înregistrări de resurse din răspunsurile la interogări. Resolverul stochează în cache aceste înregistrări în limita spațiului de memori alocat şi a timpului de valabilitate specificat prin TTL-ul aferent înregistrării. Pentru a afișa informația din cache-ul resolverului se execută comanda `ipconfig` cu opțiunea `/displaydns`.

2.2.2.4 Înregistrări de resurse (RR - resource records)

Baza de date DNS conține înregistrări de resurse. Aceste înregistrări provin din mapările între nume şi obiecte din rețea. Fiecare server DNS păstrează înregistrările de resurse din porțiunea de spațiu de nume peste care este autoritativ.

Un server DNS conține următoarele tipuri de înregistrări de resurse:

- A – nume de host: stochează adresa unui host;
- NS – nume de server: defineşte serverul autoritativ pentru o zonă sau serverul care conține fişierul de zona dintr-un domeniu;
- CNAME – nume canonic: crează unui alias pentru un host care are deja o înregistrare;
- MX – mail exchanger: specifică serverul către care aplicațiile de e-mail să trimită mesajele;
- SOA – start of authority: stochează numele serverului DNS care este server primar pentru o zonă DNS; înregistrarea SOA este prima înregistrare creată în momentul definirii unei zone;
- PTR – pointer: pentru interogări inverse – rezolvare de IP în nume de domeniu cu ajutorul domeniul in-addr.arpa.

2.3 Procesul de interogare

DNS are la bază modelul client-server, serverul stochează informații despre porțiuni din spațiul de nume DNS şi pune la dispoziția clienților aceste informații, clientul DNS transmite o interogare legată de spațiul de nume unui server DNS. Serverul DNS poate, la rîndul lui, să transmită interogarea altui server DNS.

Cînd un server DNS primeşte o interogare încearca să localizeze informația cerută în fişierul din zonă. Deasemenea, serverul poate să caute şi în memoria cache. Dacă nu se gaseşte un raspuns la interogare nici în zona nici în cache, se interoghează alt server DNS.

2.3.1 Tipuri de interogări

Exista două tipuri de interogări DNS:

- iterative: interogări transmise de un client DNS unui server DNS la care serverul răspunde în baza informației din zonă sau cache. Dacă serverul interogat nu gaseşte informația trimite clientului un pointer către alt server DNS din ierarhie. Clientul interoghează serverul repectiv. Procesul continuă pînă cînd clientul localizează un server autoritativ pentru numele pe care l-a cerut, se generează o eroare sau expiră timpul de aşteptare a unui răspuns.
- recursive: interogări transmise de un client unui server DNS pentru care serverul îşi asumă responsabilitatea găsirii unui răspuns. Dacă serverul interogat nu gaseşte informația în zonă sau în cache, serverul va transmite interogari iterative altor servere DNS în numele clientului.

În general, se utilizează interogarile recursive. Hostul client presupune că serverul DNS deține informația sau poate afla informația iar serverul execută interogari iterative către alte servere dacă nu deține informația în zonă sau în cache.

2.3.2 Tipuri de rezoluții

Majoritatea interogărilor primite de serverelor DNS implică rezolvarea unui nume. Acest tip de interogare aşteaptă ca răspuns o adresă IP şi se numeşte interogare de tip forward.

DNS suportă şi procesul invers de rezolvare a unei adrese IP într-un nume de host. Pentru aceasta s-a definit domeniul in-addr.arpa. Subdomeniile domeniului in-addr.arpa sint nume ce utilizează ordinea inversă a numerelor din notația zecimală cu punct a adreselor IP. De exemplu, zona pentru subrețeau 192.168.100.0 este 100.168.192.in-addr.arpa.

2.3.3 Paşii unei interogari DNS

Următorul exemplu ilustrează procesul de interogare DNS. Un client DNS interoghează un server DNS care contactează la rîndul lui servere DNS superioare în ierarhie. Se presupune că memoria cache a clientului şi a serverului nu conțin înregistrări.

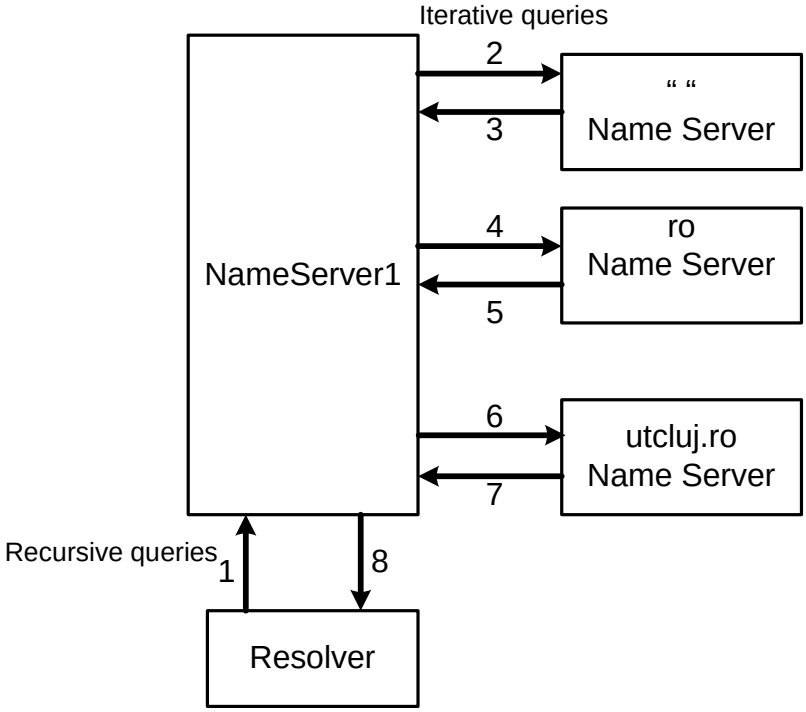

Figura 7.3 *Exemplu de interogare DNS*

1. Hostul client emite o interogare recursivă pentru adresa IP a hostului cu numele *example.utcluj.ro*. Clientul e configurat să interogheze serverul DNS *NameServer1*.
2. *NameServer1* verifică dacă are informația în cache sau zonă dar nu găseşte această informație, deci va contacta un server

autoritativ pentru Internet (un server rădăcină) cu o interogare pentru *example.utcluj.ro*.
3. Serverul rădăcină nu are răspunsul la interogare dar răspunde cu o referință la un server autoritativ pentru domaniul *ro*.
4. *NameServer1* contactează serverul autoritativ pentru domeniul *ro* cu o interogare pentru *example.utcluj.ro*.
5. Serverul autoritativ pentru domeniul *ro* nu are răspunsul la interogare dar răspunde cu o referință la un server autoritativ pentru domeniul *utcluj.ro.*
6. *NameServer1* contactează serverul autoritativ pentru domeniul *utcluj.ro* cu o interogare pentru *example.utcluj.ro*.
7. Serverul autoritativ pentru domeniul *utcluj.ro* deține răpunsul şi transmite adresa IP cerută.
8. *NameServer1* transmite clientului adresa IP corespunzătoare numelui *example.utcluj.ro*.

2.3.4 Caching

Serviciul client DNS şi server DNS au memorie cache. Caching-ul reprezintă o metodă de îmbunătățire a performanțelor DNS si de reducere a traficului de tip DNS din rețea.

Cînd serviciul client DNS porneşte, toate mapările nume_host-adresa_IP din fişierul static Hosts sînt încărcate în memoria cache a resolverului. Pe lîngă informațiile din Hosts, memoria cache conține şi informații primite ca răspuns la interogări precedente. Memoria cache e ştearsă de fiecare dată cînd serviciul client DNS este oprit.
Ca urmare a interogărilor recursive pe care le execută în numele clienților, serverele DNS stochează temporar înregistrări de resurse. Memoria cache a serverului DNS e ştearsă de fiecare dată cînd serviciul server DNS este oprit.

Fiecare înregistrare stocată are asociat un timp de viață în memoria cache. Cît timp acesta nu expiră, informația din cache poate fi utilizată. Implicit, timpul de viață a unei înregistrări din memoria cache este o ora dar acest parametru poate fi ajustat la nivel de zona sau la nivel de înregistrare.

2.3.5 Nslookup

Nslookup este un program utilizat pentru a transmite interogări DNS.

```
Sintaxa: nslookup [ -option ] [ host-to-find | - [ server ]]
```

3. Desfăşurarea lucrării

3.1 Accesați http://www.root-servers.org pentru informații despre serverele de nume rădăcină.
3.2 Instalați serviciul DNS Server pe o stație cu Windows Server.
3.3 Configurați serverul DNS: creați zone şi înregistrări de resurse.
3.4 Configurați clientul DNS.
3.5 Testați configurația printr-o interogare despre o înregistrare de resursa definită în zona de pe server.
3.6 Testați comanda `nslookup` *`nume_domeniu`*.
3.7 Testați comanda `nslookup` *`adresa_IP`*.

Notițe