Mittuniversitetet
MID SWEDEN UNIVERSITY

Administration of UNIX-like systems

Lennart Franked

3 december 2024

Institutionen för data- och elektroteknik
Mid Sweden University

Mittuniversitetet
MID SWEDEN UNIVERSITY

Domain Name System

1. Domain Name System

2. Konfigurering av BIND

Intro

Vad är DNS?

I [3, chapter 17.1] kan man läsa följande om DNS:

- En hierarkisk namnrymd för värdnamn (hosts) och IP-adresser.
- En distribuerad databas över värdnamn och adressinformation.
- En ‘resolver’ / Uppslagningstjänst används för att fråga denna databas
- Möjliggör förbättrar routing
- Används för authenticering vid e-post.
- Tillhandahåller också en mekanism för att hitta tjänster på ett nätverk.
- Ett protokoll som används av namnservern för att utbyta information.

Hierarkisk namnrymd

- Namnrymden som används i DNS har en hierarkisk trädstruktur.
- Används för att identifiera värdar eller domäner.
- En delmängd av detta träd kallas för domän.
- En huvuddomän kan vara fristående, men också ha underdomäner.
- En domän innehåller också värdar (hosts).
- Ett namn som pekar på en specifik nod i ett träd kallas för värdens fullständiga domännamn (’Fully Qualified Domain Name’ (FQDN)).
- Visar vägen genom trädet för att hitta noden.

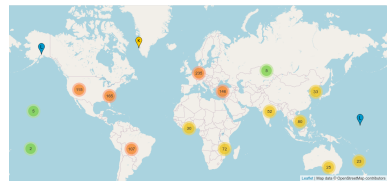
Hierarkisk namnrymd 2

Varje nivå i trädet namnges enligt följande:

- Rot
- top eller landsdomän (Top Level Domain)
- Huvuddomän
- Underdomän
- Nod

Hierarkisk namnrymd 2

- 13 Rotservrar
  - Namngivna A - M
  - Sverige har 11 spegelservrar.
  - Finns en i Sundsvall (1 Luleå, 5 Sthlm, 3 Gbg, 1 Malmö)



Figur: Hämtad från [4]

Hierarkiska namnrymden 4

IANA är den organisation som har det slutgiltiga ansvaret för att hantera namnrymden.

- **Registry:** Förvaltar topdomäner (TLD), till exempel Internetstiftelsen för .se
- **Registrator (Registrar):** Organisation som har rätten att sälja domännamn åt en registry. Exempelvis Loopia eller One.
- **Registrant:** En person eller organisation som äger ett registrerat domännamn. Exempelvis Mittuniversitetet.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Begränsningar i namngivning

- Begränsas praktiskt till ASCII
- Total begränsning på 255 tecken
- [2] Begränsar tecken till a — z, 0 — 9 samt -
- Sedan [1, s. 2.1] är det tillåtet att börja domännamn med en siffra.
- Namn får dock aldrig ha samma format som en IP-adress.

Begränsningar i namngivning

Internationalized Domain Names in Applications (IDNA)

- Kom 2003 för att tillåta domännamn med icke-ASCII tecken.
- Ett speciellt ascii-format används för att representera icke-ASCII-tecken.
- Ascii-tecknet har formatet <prefix><ascii kod>
- prefixet för IDNA är “xn–”
- För användaren ser det dock korrekt ut.
- Har öppnat upp för attacker (IDN homograph attack) där bokstäver byts ut mot liknande tecken från exempelvis grekiska, latin eller cyrilliska alfabetet (confusables).

Mittuniversitetet
MID SWEDEN UNIVERSITY

Distribuerad databas

- I och med den hierarkiska designed av databasen, så kan man låta denna vara helt distribuerad.
- Varje nivå är bara ansvarig för sig själv och att förse en koppling mot domäner som är underordnade dem.
- Tillåter en organisation att hantera sin egen namnrymd.

Resolver

- En resolver är ett program som skickar förfrågan till en DNS-server, rörande Namn, IP eller annan information som finns lagrad.
- Detta kallas för att den gör ett uppslag.
- Liknande funktion som ARP, där vi har en adress från ett högre lager och önskar en adress från ett nedre lager.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Uppslagstekniker

- Iterativ förfrågan
- Rekursiv förfrågan
- Inverterad förfrågan

Mittuniversitetet
MID SWEDEN UNIVERSITY

DIG — DNS lookup utility

- Verktyg för att fråga DNS-servrar
- Utför DNS-uppslag och visar dess resultat.
- Värdefullt verktyg för felsökning och verifiering

DIG-användning

```
dig @<server> <namn> <typ>
dig @10.2.1.3 remote.netlab.miun.se A
```

DIG exempel

```
lenfra@remote:~$ dig @10.2.1.3 remote.netlab.miun.se A

; <<>> DiG 9.11.5-P4-5.1+deb10u11-Debian <<>> @10.2.1.3 remote.netlab.miun.se A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60598
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;remote.netlab.miun.se.          IN      A

;; ANSWER SECTION:
remote.netlab.miun.se.  3600    IN      A       10.14.14.21

;; Query time: 1 msec
;; SERVER: 10.2.1.3#53(10.2.1.3)
;; WHEN: tis dec 03 09:12:52 CET 2024
;; MSG SIZE  rcvd: 66

lenfra@remote:~$
```

Figur: Exempel på ett dig-uppslag, med svar rödmarkerat

Routing och avsändarauthentisering för e-post

- Då DNS förser oss med en namn till adresskoppling, kan vi använda detta för att identifiera vilken e-post server som ett e-post skall levereras till.
- $$\underbrace{lennart.franked}_{anvndare}@\underbrace{miun}_{\text{huvuddomän}}.\underbrace{se}_{TLD}.\underbrace{}_{Rot} \quad (1)$$
- Vi kan också använda detta system för att inkludera information om godkända e-post servrar för en domän (SPF, DKIM). Återkommer til detta.

Mittuniversitetet
MID SWEDEN UNIVERSITY

DNS för att hitta tjänster i ett nätverk

- DNS används inte enbart för namn <-> IP. Används också för att hitta tjänster som körs i ett nätverk.
- Key-distribution centers, exempelvis Kerberos
- Voice-over-IP
- XMPP
- CalDAV, CardDAV
- DANE (DNS-based Authentication of Named Entities)

Mittuniversitetet
MID SWEDEN UNIVERSITY

DNS-protokollet

- DNS protokollet använder både UDP och TCP.
- UDP för uppslag.
- TCP för zon-överföringar.

DNS-protokollet 2

- UDP-paket har traditionellt varit låsta vid 512 bytes.
- Större paket måste därför använda TCP som transportprotokoll. (DNSSEC, Zone-transfers)

Konfigurering av BIND

1. Domain Name System

2. Konfigurering av BIND

Mittuniversitetet
MID SWEDEN UNIVERSITY

named.conf

```
zone "localhost" {
  type master;
  file "localhost.db";
  allow-update{none;};
};

zone "netlab.miun.se" {
  type master|slave|forward;
  forwarders {ip addr};
  file "netlab.miun.se.db";
  allow-query {ACL};
  allow-transfer {ACL};
  allow-update {ACL};
  zone-statistics yes|no;
};
zone "14.14.10.in-addr.arpa." {
  type master;
  file "14.14.10.db";
};
```

Record types

Tabell: Resource Records [3, Table 17.6]

	Type	Name	Function
Zone	SOA	Start Of Authority	Definierar en DNS-Zon
	NS	Name Server	Identifierar en namnserver, delegerar underdomäner
Basic	A	IPv4 Adress	Översättning Namn-till-adress
	AAAA	IPv6 Adress	Översättning Namn-till-IPv6-adress
	PTR	Pointer	Översättning Adress-till-namn
	MX	Mail Exchanger	Hanterar e-postservrar
Optional	CNAME	Canonical Name	Alias för en nod/värd
	SRV	Services	Pekar till servrar som kör vanliga nätverkstjänster
	TXT	Text	Kommentar eller otypad information

Zon-filer

```
$TTL 30d
$ORIGIN netlab.miun.se
@ IN  SOA ns1.netlab.miun.se.  mail.netlab.miun.se. (
                      2017022000  ;serial
                      3600        ;refresh
                      1800        ;retry
                      604800      ;expiration
                      3600)       ;minimum

@ IN  NS  ns1.netlab.miun.se.
ns1.netlab.miun.se.  IN  A 10.14.14.1

ist IN  A 10.254.20.1
    IN  TXT "IST␣department"

ftp IN  A 10.254.20.24
    IN  TXT "Netlab␣FTP␣server"

subdomain IN  NS  ns1.subdomain.netlab.miun.se.
ns1.subdomain.netlab.miun.se IN A 10.14.15.1

@ IN  MX  10  mailserver1.netlab.miun.se.
@ IN  MX  20  mailserver2.netlab.miun.se.

istweb IN  CNAME  ist

_ftp._tcp SRV 0 1 21 ftp #prio, weight, port
```

Reverse zon-fil

```
$TTL 30d
$ORIGIN 14.14.10.in-addr.arpa.
@ IN  SOA ns1.netlab.miun.se mail.netlab.miun.se. (
                      2017022000  ;serial
                      3600        ;refresh
                      1800        ;retry
                      604800      ;expiration
                      3600)       ;minimum

@ IN  NS  ns1.netlab.miun.se.
ns1.netlab.miun.se.  IN  A 10.14.14.1

1 IN  PTR ns1.netlab.miun.se.
```

Mittuniversitetet
MID SWEDEN UNIVERSITY

Referenser

[1] R. Braden. *Requirements for Internet Hosts - Application and Support*. rfc 1123. IETF, okt. 1989. URL: http://tools.ietf.org/rfc/rfc1123.txt.

[2] K. Harrenstien, M.K. Stahl och E.J. Feinler. *DoD Internet host table specification*. rfc 952. IETF, okt. 1985. URL: http://tools.ietf.org/rfc/rfc0952.txt.

[3] Evi Nemeth m. fl. *UNIX and Linux system administration handbook*. 4th ed. Upper Saddle River, NJ: Prentice Hall, 2011. ISBN: 978-0-13-148005-6 (pbk. : alk. paper).

[4] *Root-servers.org*. 2017. URL: http://www.root-servers.org/index.html.

Mittuniversitetet
MID SWEDEN UNIVERSITY