DNS teenus teoorias ja praktikas

Autor Siim Adamson
ITK 2008

Ettekande sisukord

Ettekanne jaotatud 9 peatükiks:

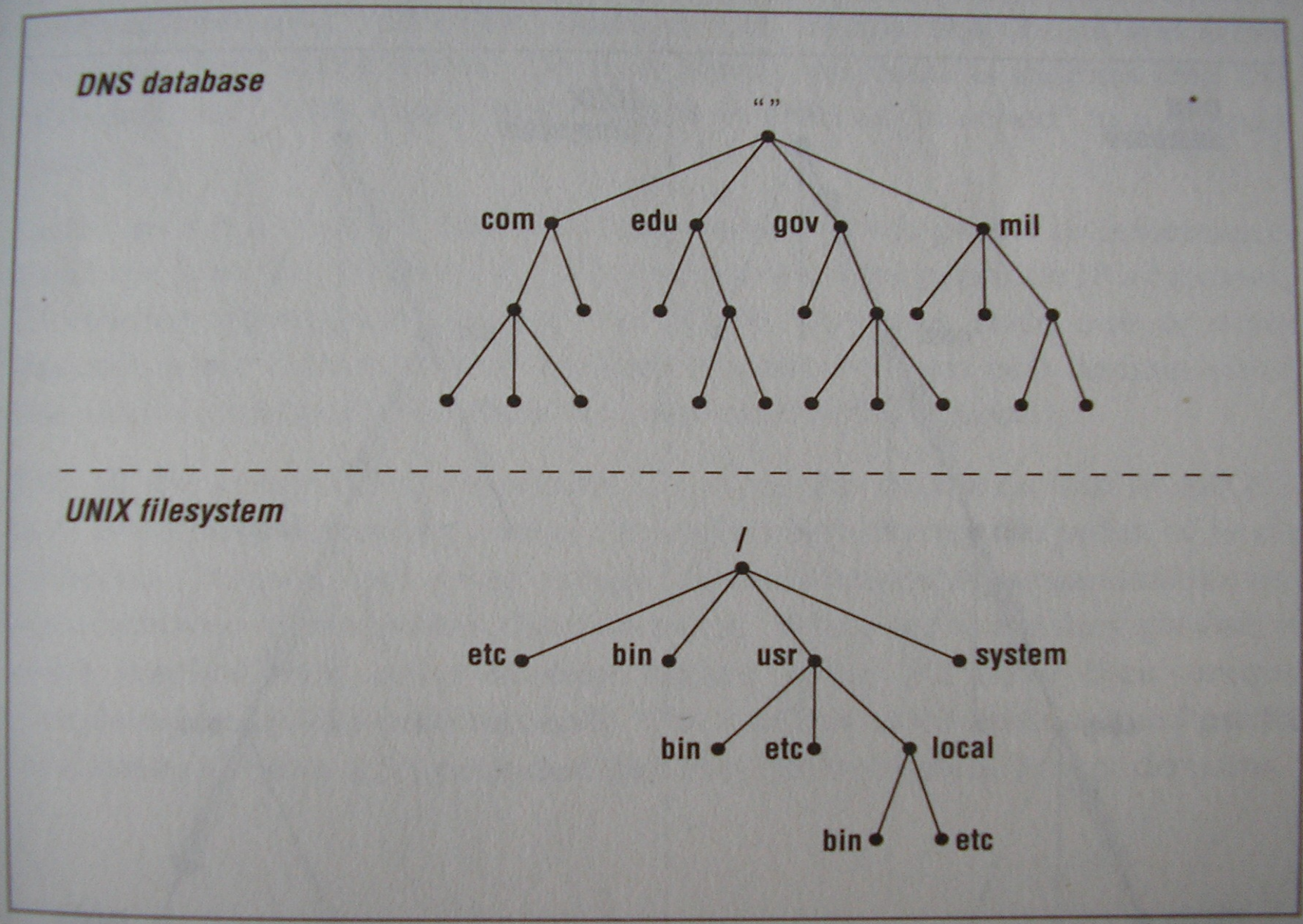
1. DNS süsteemi ajalugu
2. DNS süsteemi struktuur
3. DNS kirjete tüübid
4. DNS serveri seadistamine BIND näitel
5. DNS süsteemi turvalisus
6. Interneti domeeni nime reeglid
7. Domeeni registreerimine .ee alla
8. DNS süsteemi väärkasutus
9. Küsimused

DNS süsteemi ajalugu

- 1960-ndate lõpus U.S. DoD ARPA (hiljem DARPA) – ARPANET
- 1980-ndate alguses TCP/IP protokoll
- 1983 DNS süsteemi väljatöötamine
- 1984 BSD UNIX vaba tarkvara ülikoolidele
- 1988 DARPA lõpp -> NSFNET asutamine
- 1990-ndate algus BIND tugi M$ WinNT-le
- 1980-ndad keskvõrgu kiirus ~45 Kbps
- 1990-ndad keskvõrgu kiirus ~45 Mbps

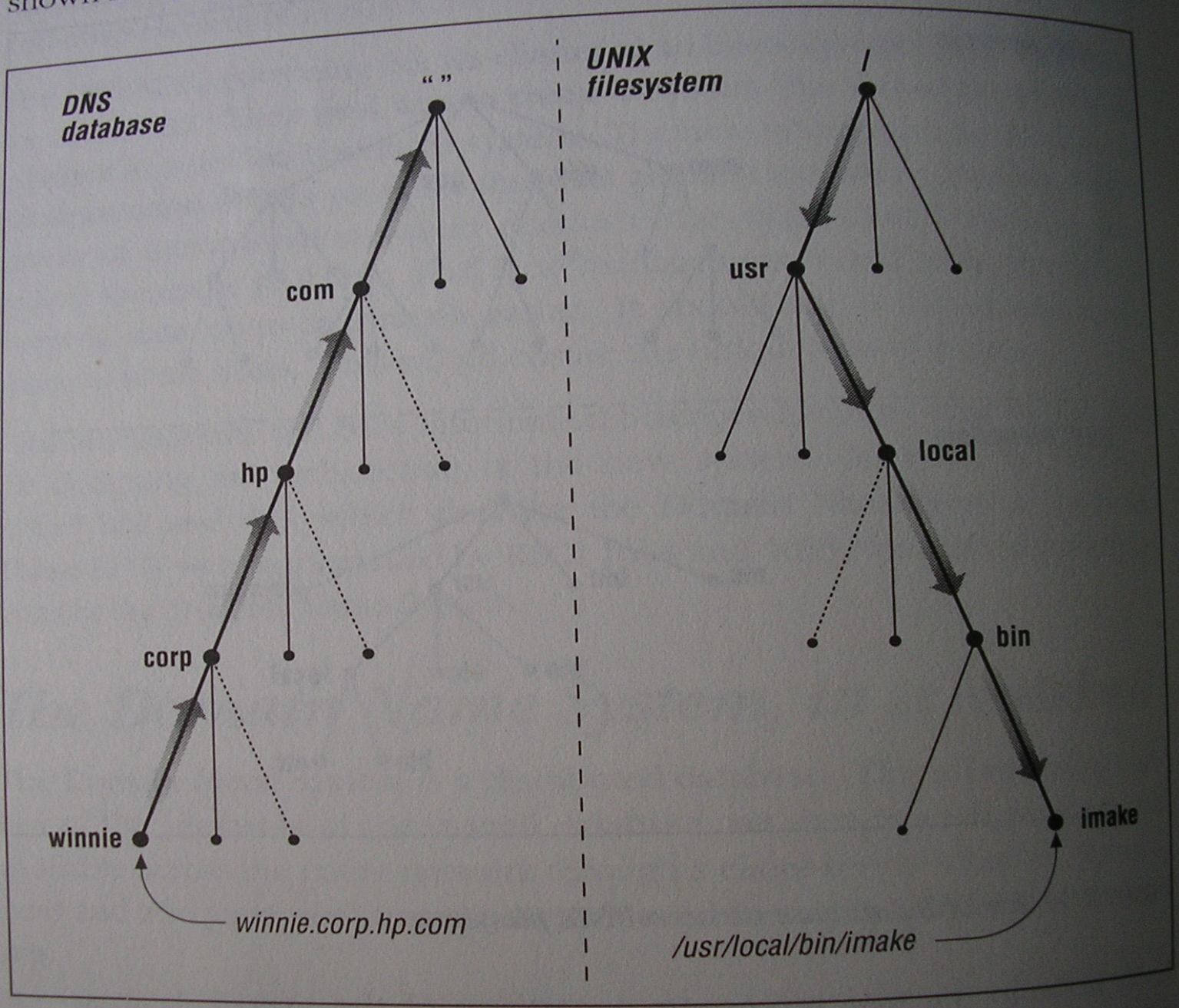
DNS süsteemi struktuur

- Tegemist on OSI L7 protokolliga
- Hierarhilise strutuur
- Tööpõhimõte sarnane telefoniraamatule
- Struktuur on sarnane UNIX failisüsteemi struktuurile
- Tööpõhimõte on päringutele vastamine ja kliendipool peab oskama vastusega midagi edasi teha



Pilt on võetud raamatust „DNS and BIND in a Nutshell" by Paul Albitz & Cricket Liu O´Reilly & Associates, Inc.

shown in Figure 1.2), using



Pilt on võetud raamatust „DNS and BIND in a Nutshell“ by Paul Albitz & Cricket Liu O´Reilly & Associates, Inc.

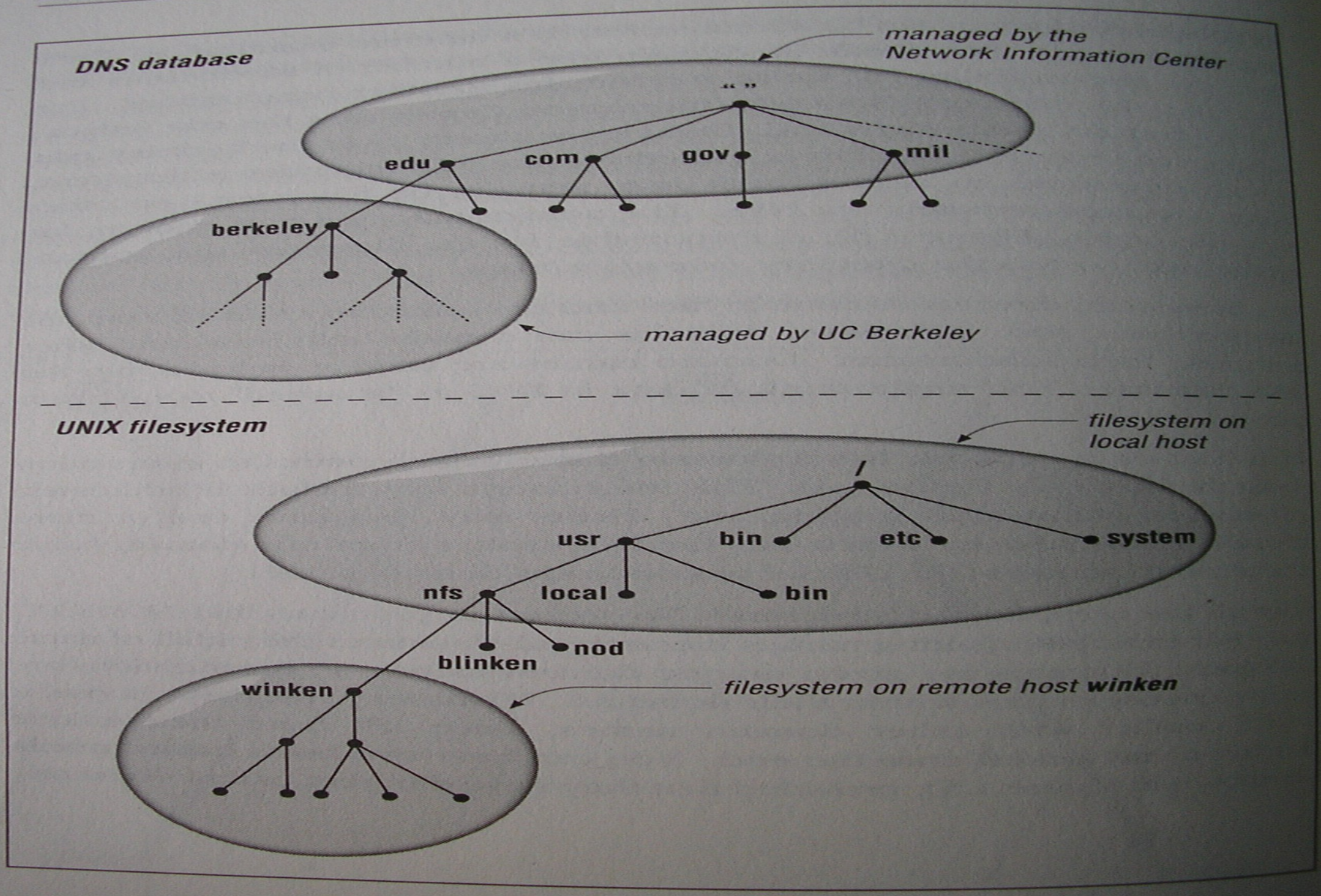


Figure 1.3: Remote management of subdomains and of filesystems

Pilt on võetud raamatust „DNS and BIND in a Nutshell“ by Paul Albitz & Cricket Liu O´Reilly & Associates, Inc.

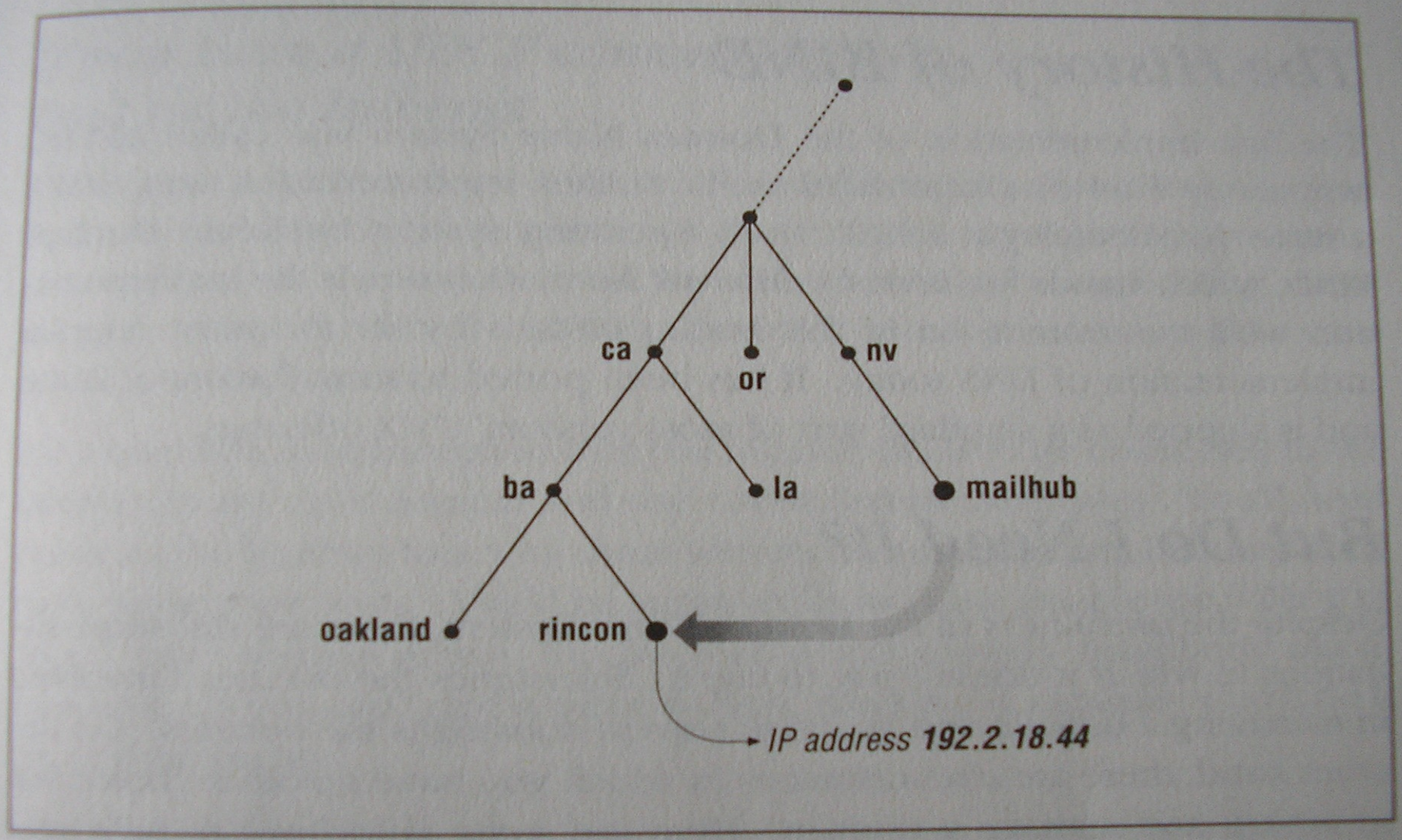


Figure 1.4: An alias in DNS pointing to a canonical name

Pilt on võetud raamatust „DNS and BIND in a Nutshell“ by Paul Albitz & Cricket Liu O´Reilly & Associates, Inc.

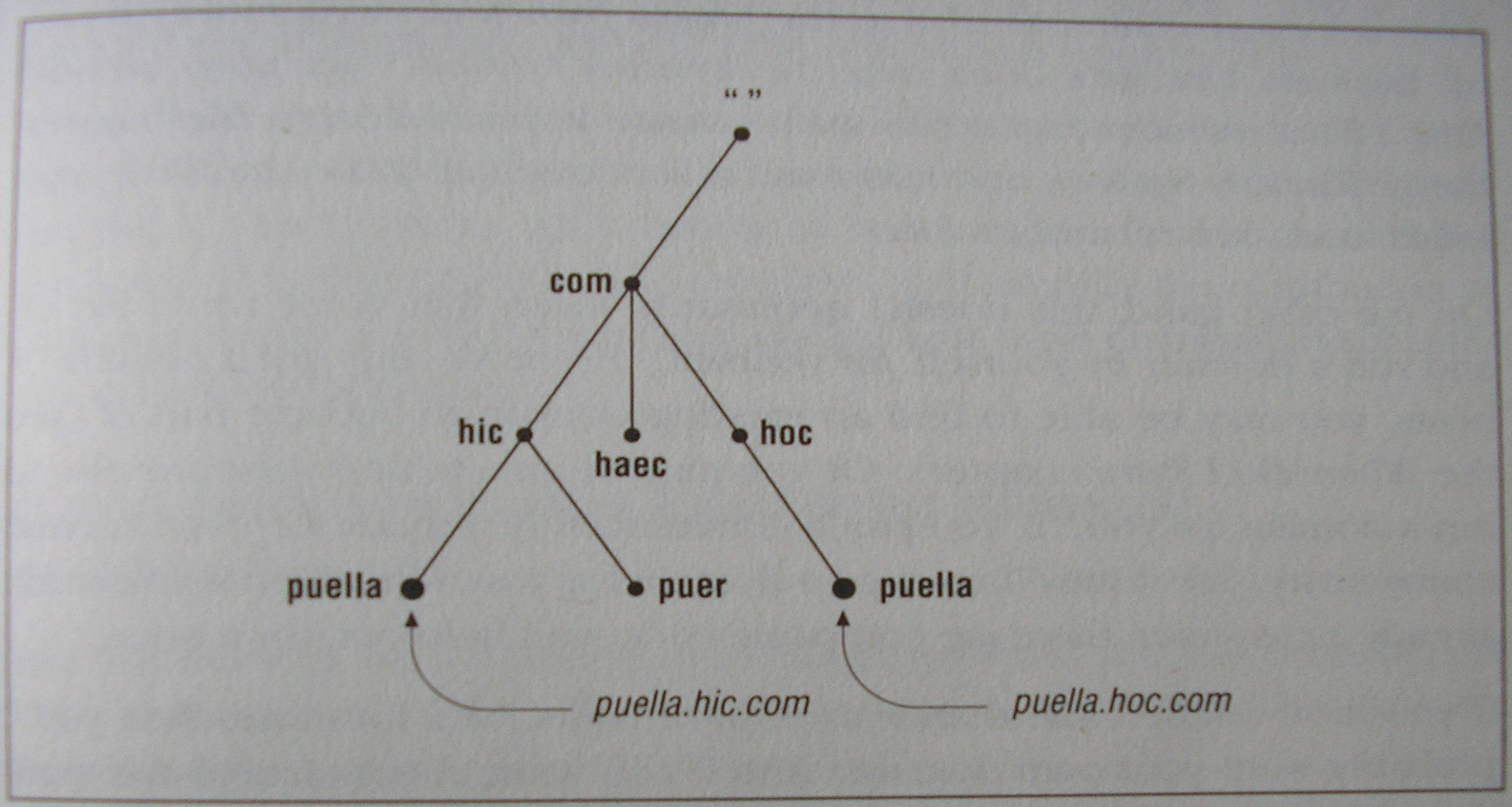
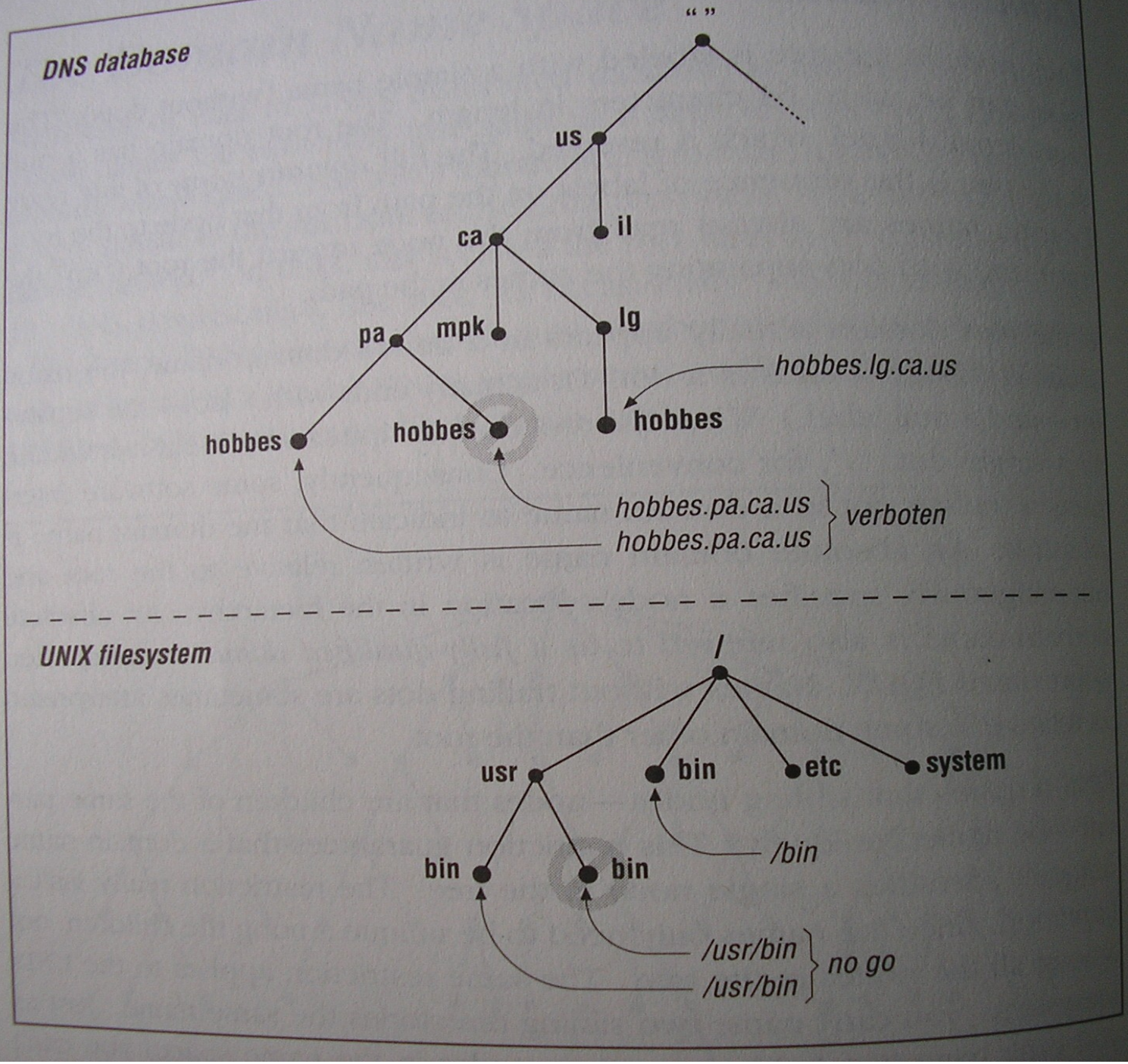


Figure 1.5: Solving the name collision problem

Pilt on võetud raamatust „DNS and BIND in a Nutshell" by Paul Albitz & Cricket Liu O´Reilly & Associates, Inc.



Pilt on võetud raamatust „DNS and BIND in a Nutshell" by Paul Albitz & Cricket Liu O´Reilly & Associates, Inc.

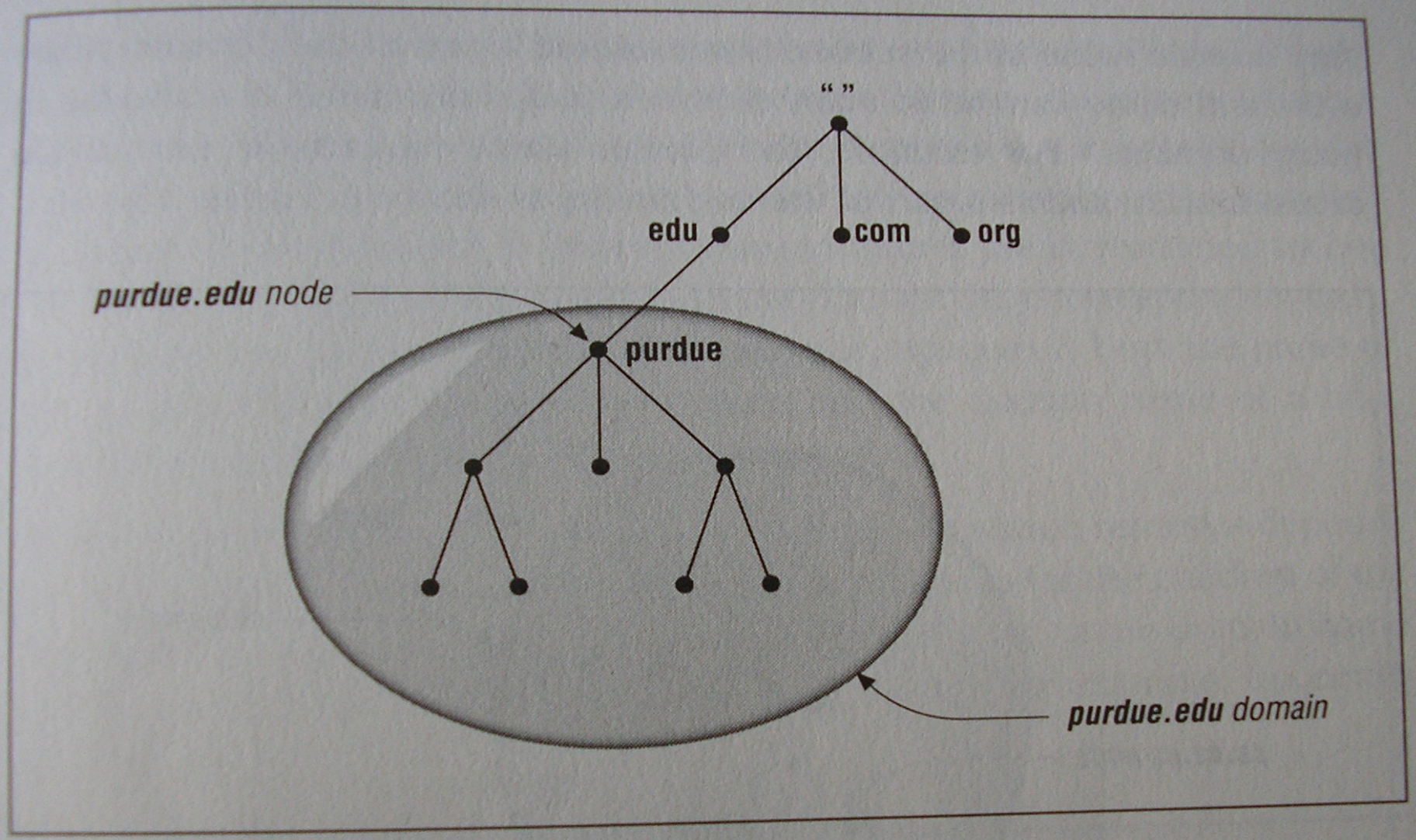


Figure 2.3: The purdue.edu domain

Likewise, in a filesystem, at the top of the */usr* directory, you'd expect to

Pilt on võetud raamatust „DNS and BIND in a Nutshell" by Paul Albitz & Cricket Liu O´Reilly & Associates, Inc.

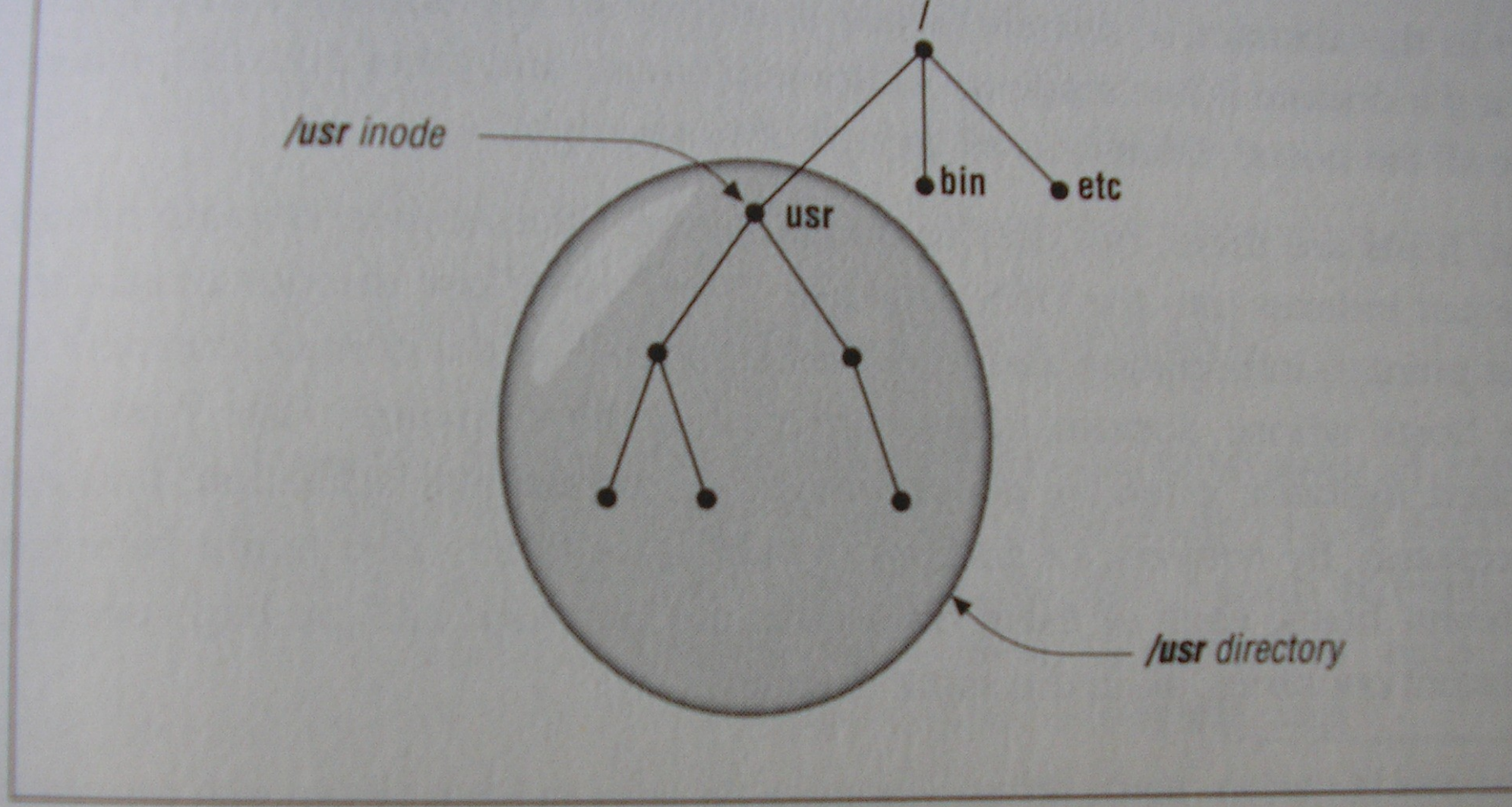


Figure 2.4: The /usr directory

Pilt on võetud raamatust „DNS and BIND in a Nutshell“ by Paul Albitz & Cricket Liu O´Reilly & Associates, Inc.

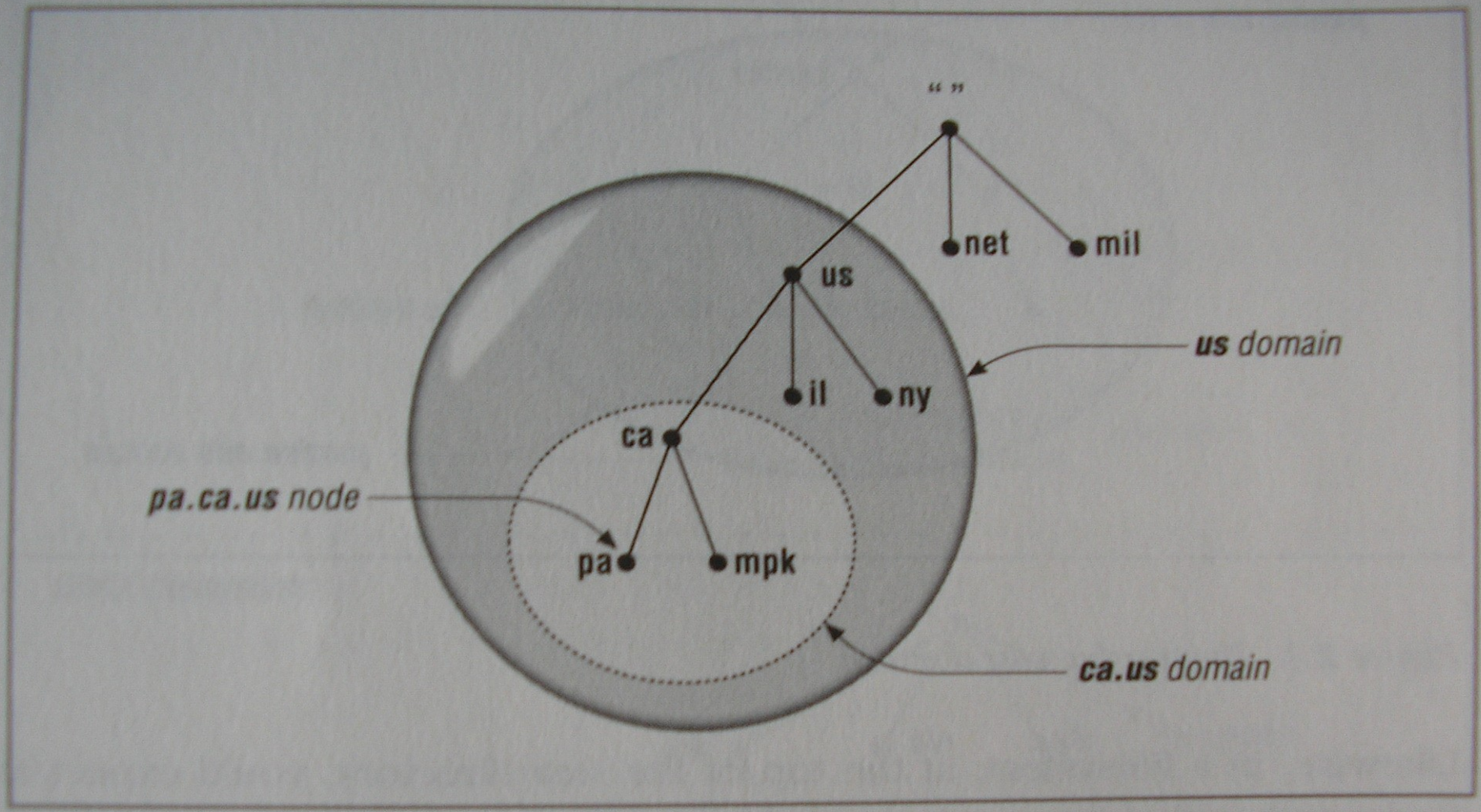


Figure 2.5: A node in multiple domains

So in the abstract, a domain is just a subtree of the domain name space.

Pilt on võetud raamatust „DNS and BIND in a Nutshell“ by Paul Albitz & Cricket Liu O´Reilly & Associates, Inc.

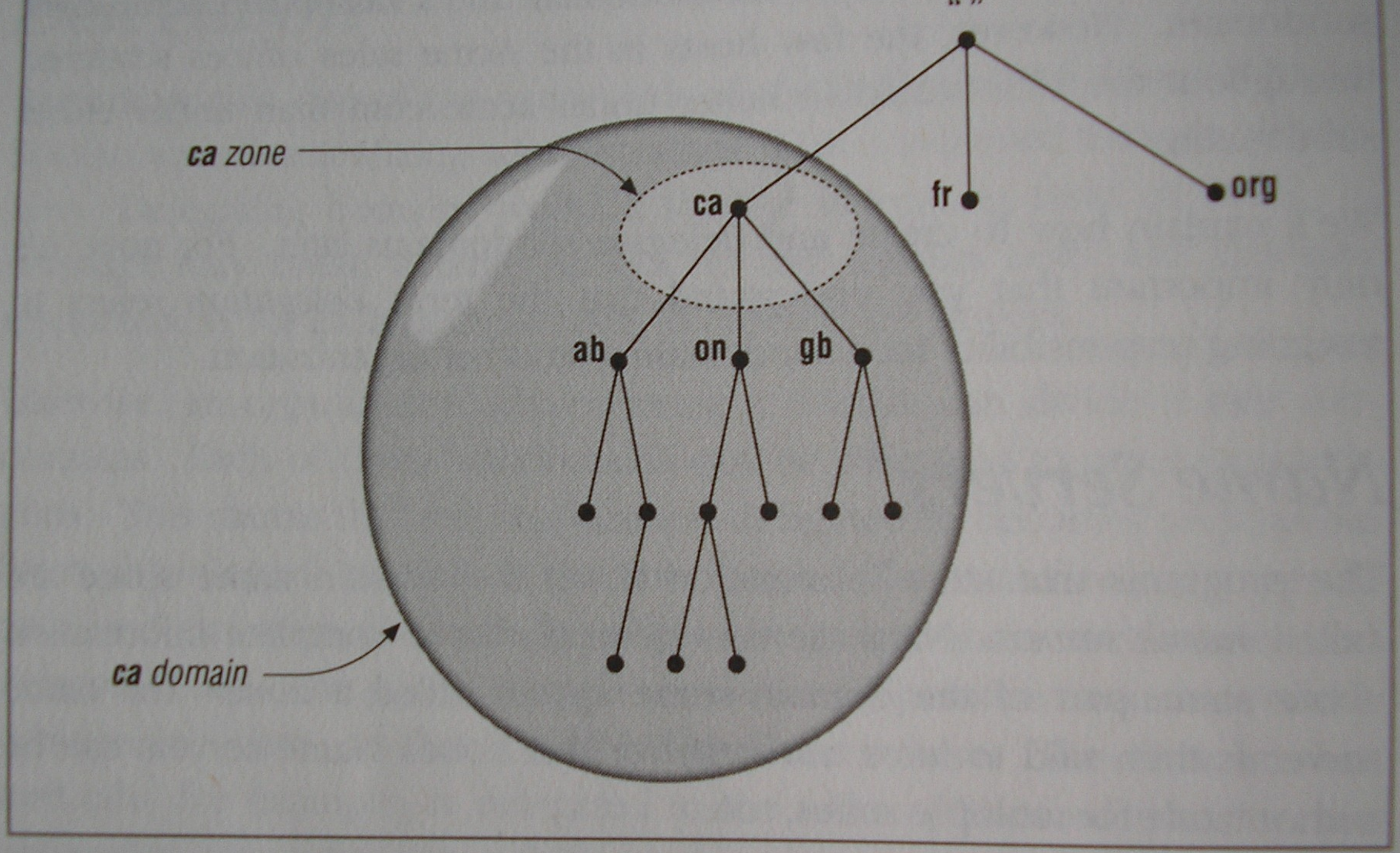


Figure 2.8: The domain ca versus the zone ca

Pilt on võetud raamatust „DNS and BIND in a Nutshell“ by Paul Albitz & Cricket Liu O´Reilly & Associates, Inc.

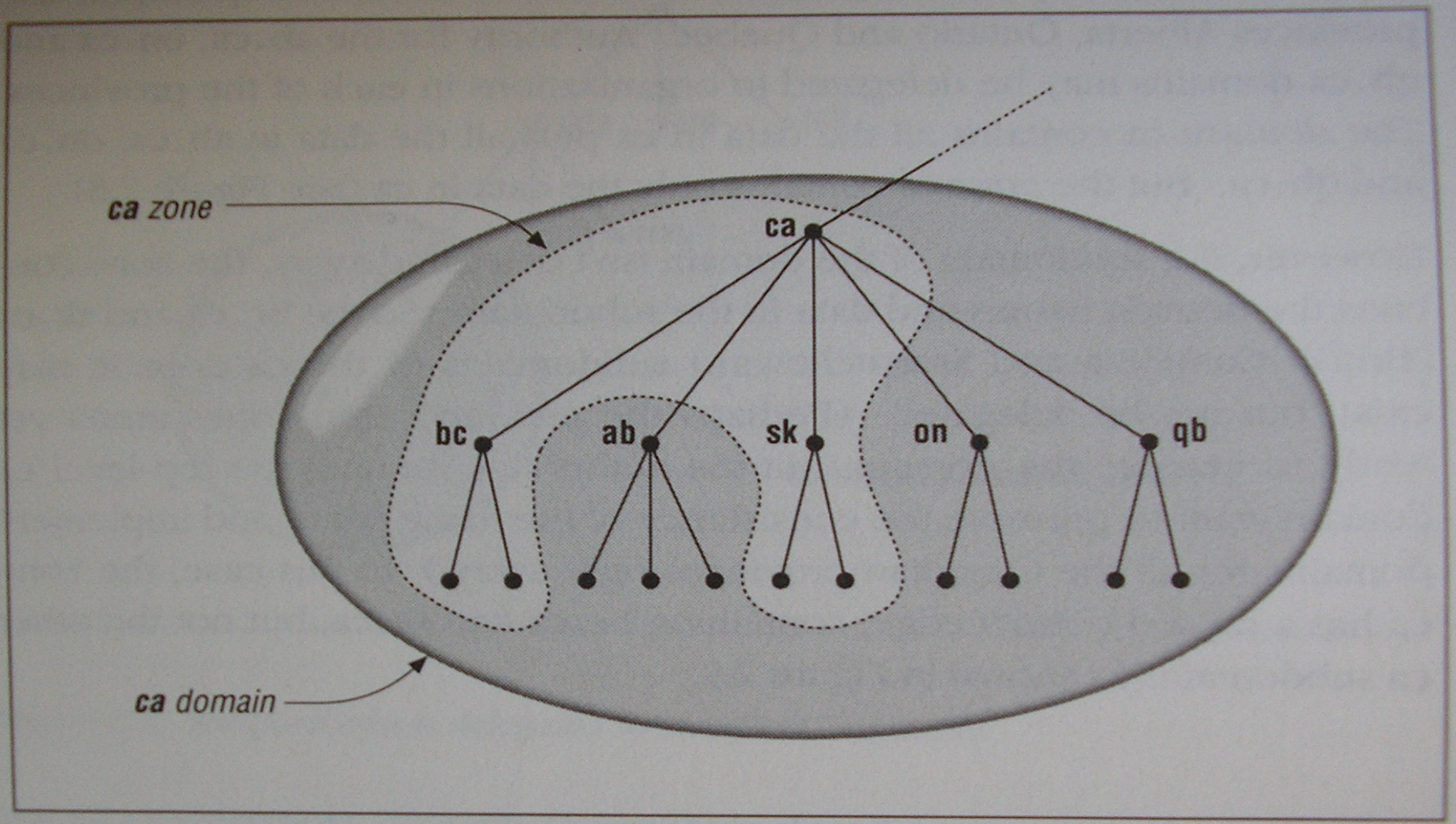


Figure 2.9: The domain ca vs. the zone ca

Pilt on võetud raamatust „DNS and BIND in a Nutshell“ by Paul Albitz & Cricket Liu O´Reilly & Associates, Inc.

Top-Level Domains

The original top-level domains divided the Internet domain name space organizationally. There were seven main top-level domains:

com	Commercial organizations, like Hewlett-Packard (**hp.com**), Sun Microsystems (**sun.com**) and IBM (**ibm.com**)
edu	Educational organizations, like U.C. Berkeley (**berkeley.edu**) and Purdue University (**purdue.edu**)
gov	Government organizations, like NASA (**nasa.gov**) and the National Science Foundation (**nsf.gov**)
mil	Military organizations, like the U.S. Army (**army.mil**) and Navy (**navy.mil**)
net	Networking organizations, like NSFNET (**nsf.net**)
org	Non-commercial organizations, like the Electronic Frontier Foundation (**eff.org**)
int	International organizations, like NATO (**nato.int**)

There's also a top-level domain called **arpa**, which was originally used during the ARPANET's transition from host tables to DNS. All ARPANET hosts originally had host names under **arpa**, so they were easy to find. Later, they

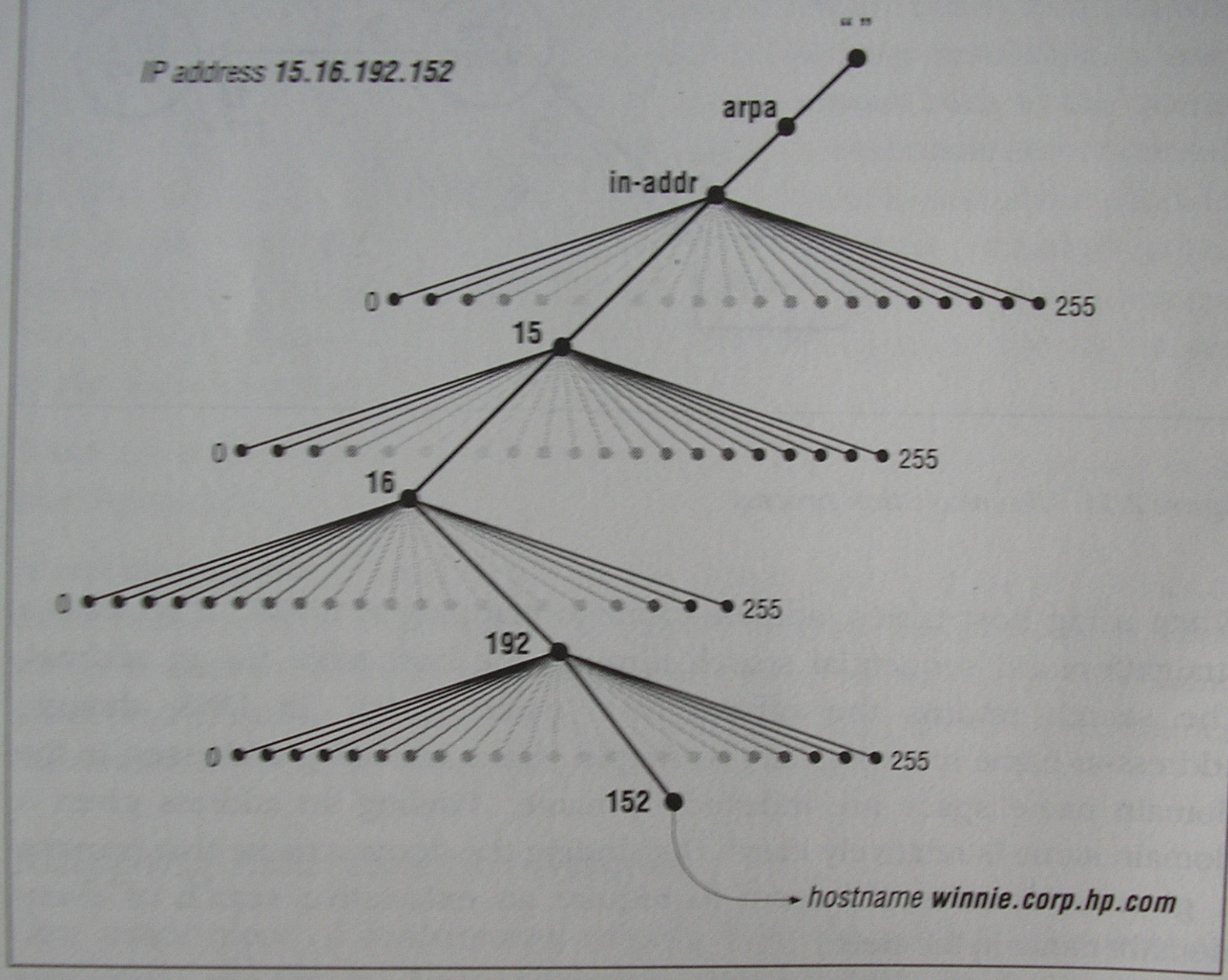
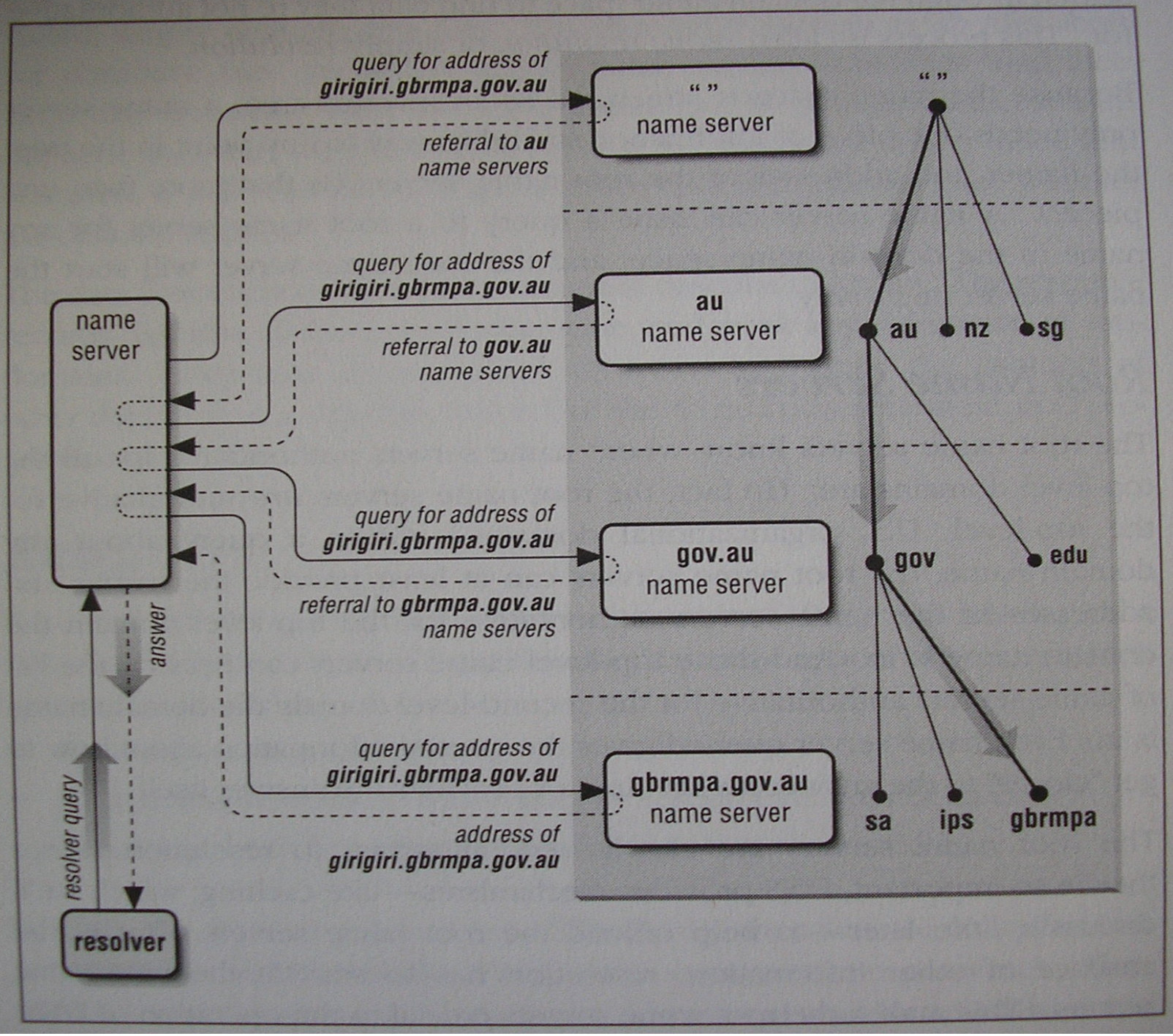


Figure 2.12: The in-addr.arpa Domain

Pilt on võetud raamatust „DNS and BIND in a Nutshell“ by Paul Albitz & Cricket Liu O´Reilly & Associates, Inc.



Pilt on võetud raamatust „DNS and BIND in a Nutshell“ by Paul Albitz & Cricket Liu O´Reilly & Associates, Inc.

1. Name server **A** receives a query from the resolver.
2. **A** queries **B**.
3. **B** refers **A** to other name servers, including **C**.
4. **A** queries **C**.
5. **C** refers **A** to other name servers, including **D**.
6. **A** queries **D**.
7. **D** answers.
8. **A** returns answer to resolver.

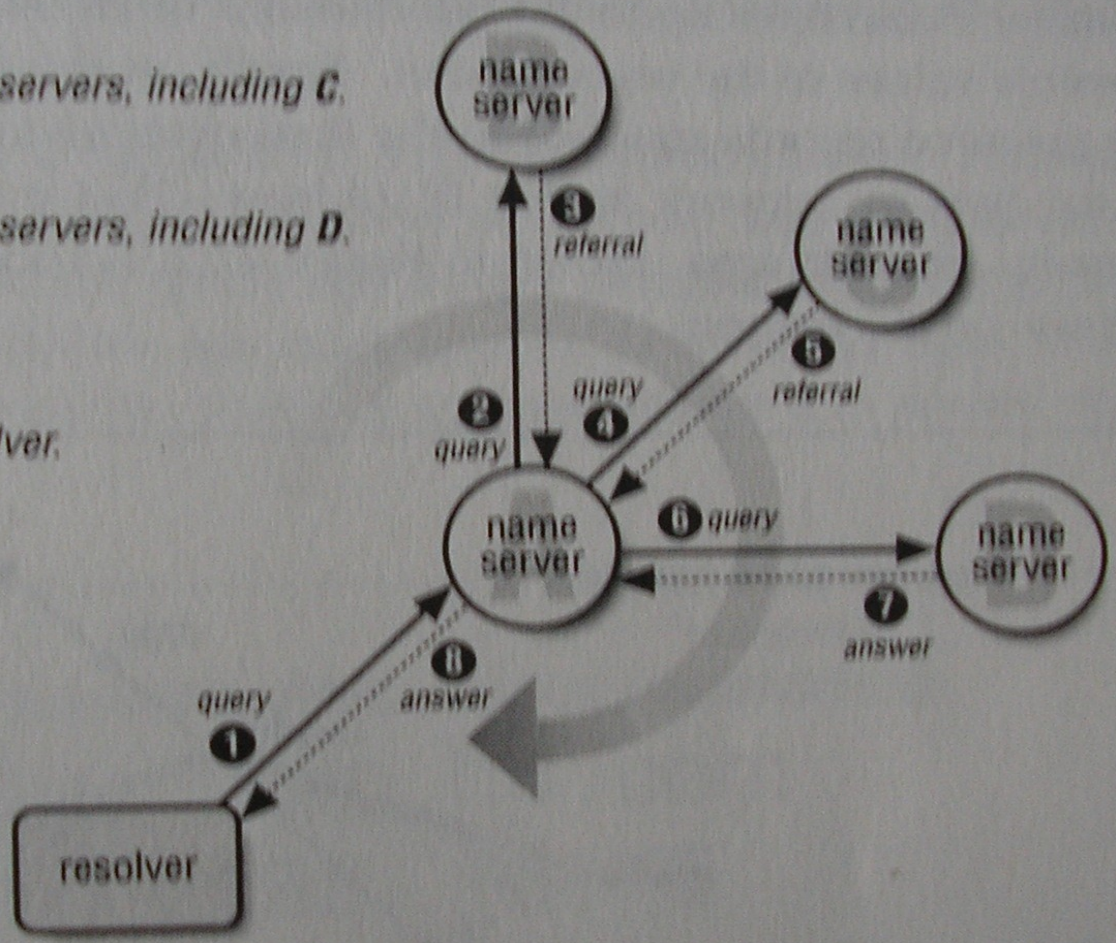


Figure 2.11: The resolution process

DNS kirjete tüübid

- Hetkel kasutusel 33 eritüüpi kirjet
- Olulisemad on:
  - A domeeninimi -> IPv4 aadress
  - AAAA domeeninimi -> IPv6 aadress
  - CNAME domeeni alias -> teine domeen
  - MX domeeni e-posti serveri info
  - NS domeeni nimeserverite info
  - PTR IP-aadress -> domeeninimi
  - SPF info milliselt aadressilt võib e-posti saata. Alternatiiv TXT kirjele.
  - SRV Kirjeldab teenuse pordi,IP võimaldab teenust jooksutada alternatiivportidel
  - TXT võimaldab täiendavat infot nagu SPF, DomainKeys kirjeldada vt. RFC1464
- Lisa info http://en.wikipedia.org/wiki/List_of_DNS_record_types

DNS serveri seadistamine BIND näitel

- Et miks BIND näitel...
- Eestikeelne õpetus LUGi lehel...
- Lisa info KUUTORVAJA.EENET.EE

DNS süsteemi turvalisus

- DNS teenus algselt pole loodud turvalisust silmaspidades.
- Runded DNS süsteemi pihta:
  - DNS cache poisoning
  - Viirus rünnakud (IP, TTL muutus kirjes)
  - Sarnase kirjapildiga domeenide kasutamine
- DNS teenud kuulab UDP porti 53
- Päringud, mis on mahukamad, kui 512 baiti edastatakse TCP abil.
- TCP abil toimub ka zone faili konfiguratsiooni edastamine.
- CHROOT jail BIND teenusele
- Nimeserverite päri ja pöördpäringute vastavuse nõue

Interneti domeeni nime reeglid

- Defineeritud RFC1034, RFC1035 ja RFC 1591 poolt
- Tähestik on piirtud ASCII tähtedega a-z ja lubatud on numbrid 0-9
- IDN Internationalized domain name
- Reserverritud tippdomeeni nimed on kirjeldatud RFC2606 poolt

Domeeni registreerimine .ee alla

- http://www.eenet.ee
- Igal domeenil on vähemalt 2 nimeserverit eri IP aadressidel
- Iga nemeserver lahendub nii IP-aadressi kui nimeserveri FQDN abil
- Samanimelist domeeni uuesti registreerida ei saa.
- 1 domeen.ee per juriidiline isik (oluline, et oleks registreeritud äriregistris)

DNS süsteemi väärkasutus

- news.abc.com asemel abcnews.com
- Domeen avaneb ilma http:// või ftp:// teenuse täpsustuseta
- Typosquatting – sarnase kirjapildi ärakasutamine
- Cybersquatting - üldlevinud kaubamärgi registreerimine domeenina juriidilise isiku poolt, kellele antud kaubamärk ei kuulu
- Alternative DNS root – ICANN'i ametlikud root serverid asendatakse alternatiivsetega, antud tegevuse taunimiseks on koostatud RFC2826

Küsimused?