

# Services:

## DNS – domain name system

David Morgan

© David Morgan 2003

## Buying numbers and names

- numbers are IP addresses
  - you buy them from an ISP
  - the ISP makes sure those addresses go to your place
- the names are domain names
  - you buy them from a name registrar
  - if you can connect the names to the addresses, those names will go to your place

© David Morgan 2003

## Grouping numbers and names

- grouping IP addresses is called subnetting
  - you buy 164.67.\*.\* from an ISP
  - you define subgroups 164.67.78.\* 164.67.79.\* etc
- grouping names is called creating zones
  - you buy mycompany.com from a name registrar
  - you define machine names like vp.mycompany.com
  - you define subgroups like sales.mycompany.com
    - you define machine names like  
manny.sales.mycompany.com, moe.sales.mycompany.com,  
jack.sales.mycompany.com

© David Morgan 2003

## DNS job 1:

Assigning your numbers to your names by a cross-correlation of your choosing, and making the assignments accessible to the world by dynamic software lookup. Then, the world can use your names and forget about your numbers.

© David Morgan 2003

## A poor-man's, non-DNS alternative: /etc/hosts

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1      hostz hostz.linnet.edu localhost.localdomain localhost

164.67.79.150  hostz.linnet.edu
164.67.79.151  hosta.linnet.edu
164.67.79.152  hostb.linnet.edu
164.67.79.153  hostc.linnet.edu
164.67.79.154  hostd.linnet.edu
164.67.79.155  hoste.linnet.edu
164.67.79.156  hostf.linnet.edu
164.67.79.157  hostg.linnet.edu
164.67.79.158  hosth.linnet.edu
164.67.79.159  hosti.linnet.edu
164.67.79.160  hostj.linnet.edu
164.67.79.161  hostk.linnet.edu
164.67.79.162  hostl.linnet.edu
164.67.79.163  hostm.linnet.edu
164.67.79.164  hostn.linnet.edu
164.67.79.165  hosto.linnet.edu
164.67.79.166  hostp.linnet.edu
164.67.79.167  hostq.linnet.edu
164.67.79.168  hostr.linnet.edu
```

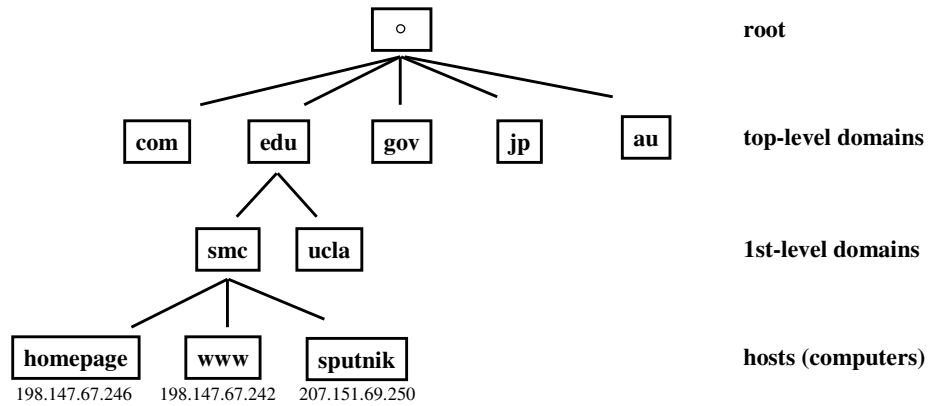
© David Morgan 2003

## Resolvers

- Clients that query name-number databases
- Functions
  - issue query
  - interpret response
  - return response to program that requested it
- Resolvers can query local /etc/hosts file

© David Morgan 2003

# The domain name space



© David Morgan 2003

# Name-address correlation table

Name	Address
homepage.smc.edu	198.147.67.246
www.smc.edu	198.147.67.242
sputnik.smc.edu	207.151.69.250

© David Morgan 2003

## Addresses in a nameserver's database

- Always (permanent, file-based)
  - for the nameserver's own domain
    - the hosts in it
  - for a subdomain of the nameserver's domain
    - the hosts in it, or
    - the nameserver(s) for it
  - hosts in the root zone
- Maybe (transient, cache-based)
  - for other, unrelated domains
    - some of the hosts in those

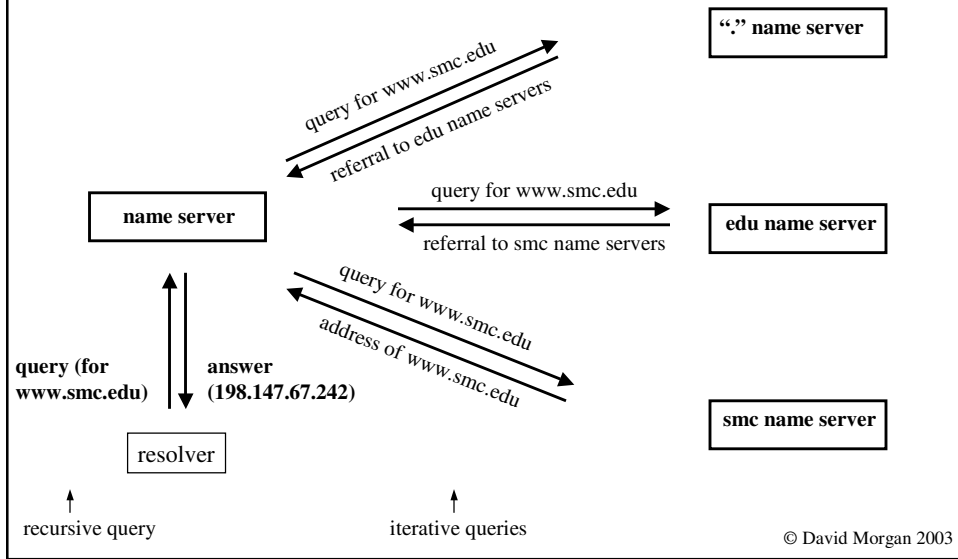
© David Morgan 2003

## Name-resolution process

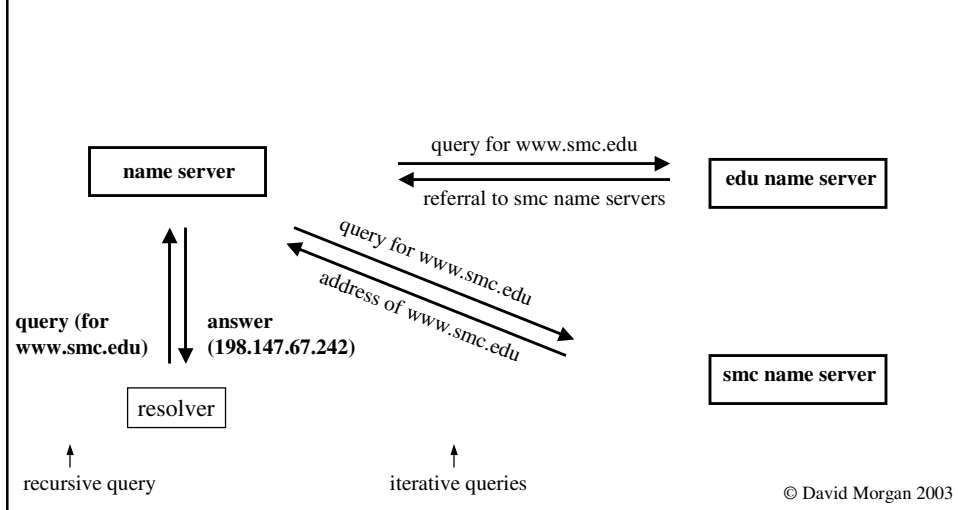
- Computers (including nameservers) query nameservers
- 2 query types
  - recursive
  - iterative
- Resolvers can query nameservers
  - configured with addresses of a few known nameservers

© David Morgan 2003

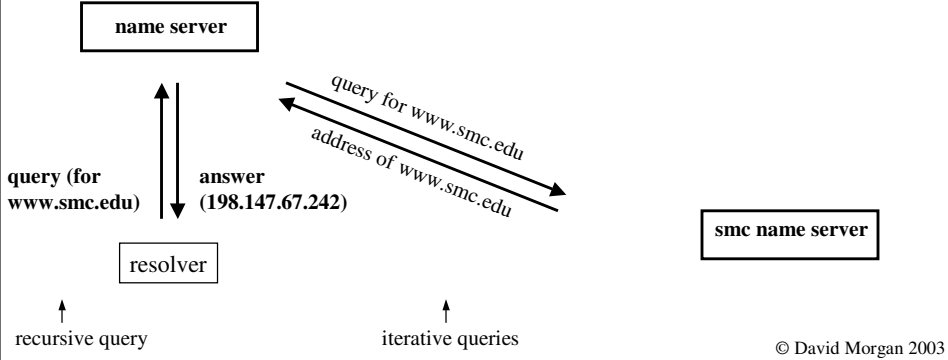
# Name-resolution process



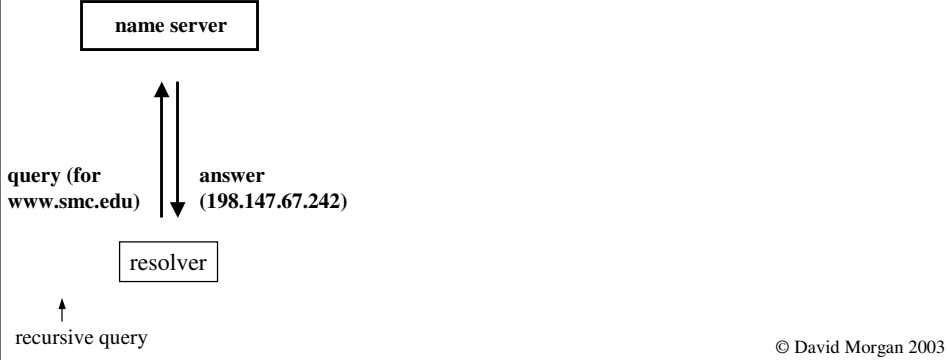
# Or maybe just...



# Or maybe just...



# Or maybe just...



## DNS mechanism

A decentralized, distributed database for the internet as a whole. You keep the part internal to your company on your own nameserver for others to access. They do the same for you.

Software on linux to integrate your name-number list into the global database is Berkeley Internet Name Daemon (BIND). You supply your name-number list to BIND and BIND makes it available to outsiders.

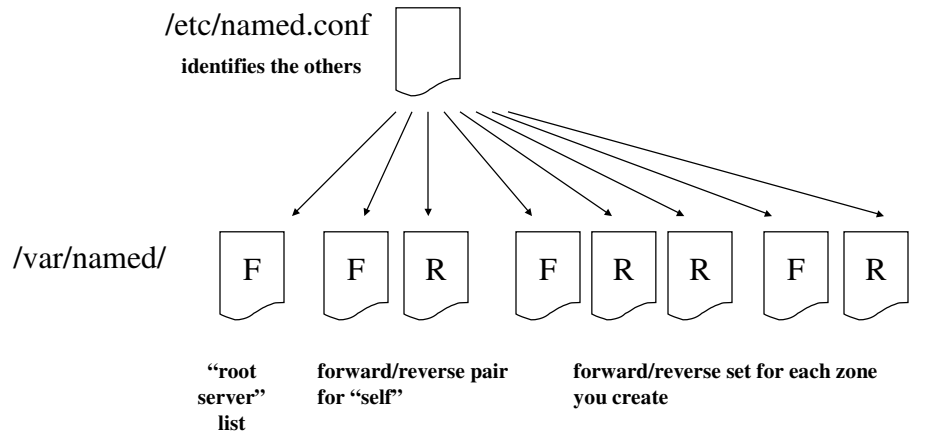
© David Morgan 2003

## DNS implements 2 lookup types

- Forward lookup – given a name provides a number
- Reverse lookup – give a number provides a name

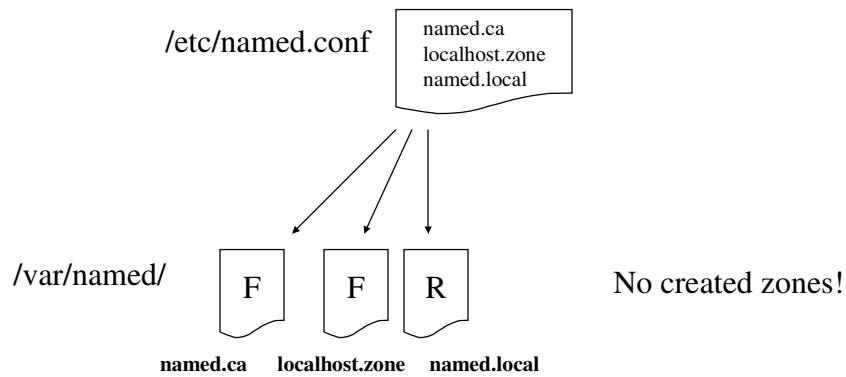
© David Morgan 2003

# BIND's files



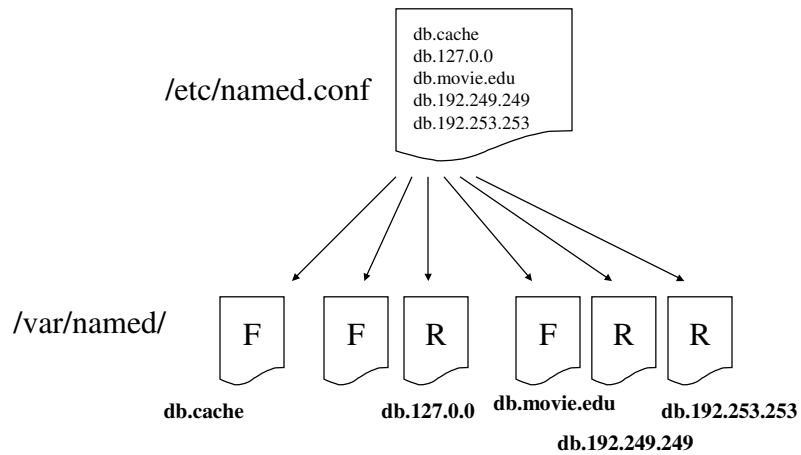
© David Morgan 2003

# RedHat 8 default fileset



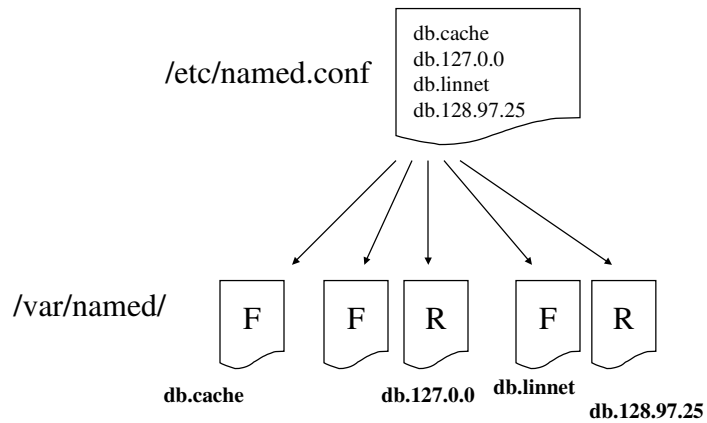
© David Morgan 2003

## DNS and BIND's example fileset



© David Morgan 2003

## Homegrown fileset



© David Morgan 2003

## Zone data files have resource records of several types

- SOA – indicates authority for this zone
- NS – lists name server for this zone
- A – name-to-address mapping
- PTR – address-to-name mapping
- ... others

© David Morgan 2003

## SOA record – start of authority

```
<zone> IN SOA <zone's nameserver> <mail address>  
<numeric data for slaves>
```

```
movie.edu. IN SOA terminator.movie.edu. al.robocop.movie.edu. (  
    1          ; serial  
    3h        ; Refresh after 3 hours  
    1h        ; Retry after 1 hour  
    1w        ; Expire after 1 week  
    1h)       ; Negative caching TTL of 1 day
```

© David Morgan 2003

## NS record – name server

<name> IN NS <zone's nameserver>

movie.edu. IN NS terminator.movie.edu.  
movie.edu. IN NS wormhole.movie.edu.

© David Morgan 2003

## A record – address

<name> IN A <address>

terminator.movie.edu. IN A 192.249.249.3  
diehard.movie.edu. IN A 192.249.249.4

© David Morgan 2003

## PTR record – pointer

<address in a name form> IN PTR <name>

3.249.249.192.in-addr.arpa. IN PTR terminator.movie.edu.  
4.249.249.192.in-addr.arpa. IN PTR wormhole.movie.edu.

© David Morgan 2003

## Notation shortcuts

- Appending domain names
- @ notation
- Repetition of name from last resource record

© David Morgan 2003

## Appending domain names

- 2<sup>nd</sup> field of named.conf's "zone" statement is a domain name
- Serves as "origin" of corresponding zone file's data
- Gets auto-appended to all names in zone file that don't end with a .

© David Morgan 2003

## @ notation

- found in a zone file
- abbreviates that zone file's origin/domain name (from named.conf), with trailing dot
- most common in SOA records

© David Morgan 2003

## Name repetition

- for lines that begin with space or tab
- name from last resource record is implied at beginning of such lines

© David Morgan 2003

## Running the nameserver

- conventional, as other servers
- `/etc/rc.d/init.d/named { start, stop, restart, status }`
- `service named { start, stop, restart, status }`

© David Morgan 2003

## Client side – resolver configuration

- `/etc/resolv.conf` and `/etc/host.conf`
- `resolv.conf` contains directives of type
  - `nameserver`
  - `domain`
  - `search`
- `host.conf` contains directives of type
  - `order`
  - `trim`
  - `multi`
- `man resolv.conf` `man host.conf`

© David Morgan 2003

## tools

- `dig`
- `nslookup`
- `h2n` – converts `/etc/hosts` to DNS fileset

```
ftp://ftp.oreilly.com/published/oreilly/nutshell/dnsbind/dns.  
4ed.tar.Z
```

```
$ zcat dns.tar.Z | tar xf -
```

- `webmin`
- `redhat-config-bind`

© David Morgan 2003

## Biblio

- DNS and BIND, Albitz and Liu, O'Reilly, 4<sup>th</sup> ed. 2001
- [http://www.ibiblio.org/pub/Linux/docs/HOWTO/other-formats/html\\_single/DNS-HOWTO.html#ss5.1](http://www.ibiblio.org/pub/Linux/docs/HOWTO/other-formats/html_single/DNS-HOWTO.html#ss5.1)

© David Morgan 2003