

DNS and BIND

Jeremy Lunn

jeremy@austux.net

<http://www.austux.net/>

Introduction

What this talk will cover:

- History
- Theory on how DNS works
- Installation
- Basic Configuration
- Security tips

Originally it was HOSTS.TXT

- Each machine has a numeric IP address
- The HOSTS.TXT file listed nearly every single host on ARPAnet
- Every single host on ARPAnet had to download this file
- The UNIX file /etc/hosts was updated from HOSTS.TXT

The weaknesses of HOSTS.TXT

- Traffic
- Name collisions
- Consistency

So DNS was born

DNS was designed to:

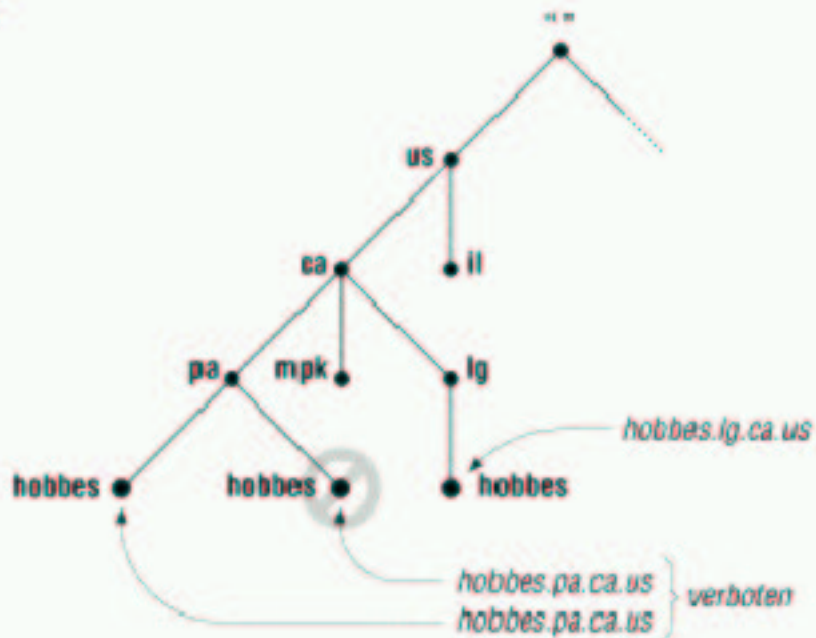
- Be a decentralised database
- Allow each Administrator to make changes to their zone
without having to contact a central point
- This system would of course be scaleable

Nameservers

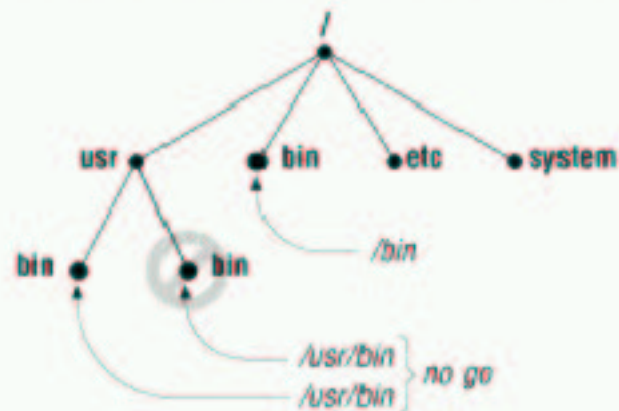
- Provide information to Resolvers (clients)
- Provide information to other Nameservers

Similarities with a file system

DNS database



UNIX filesystem



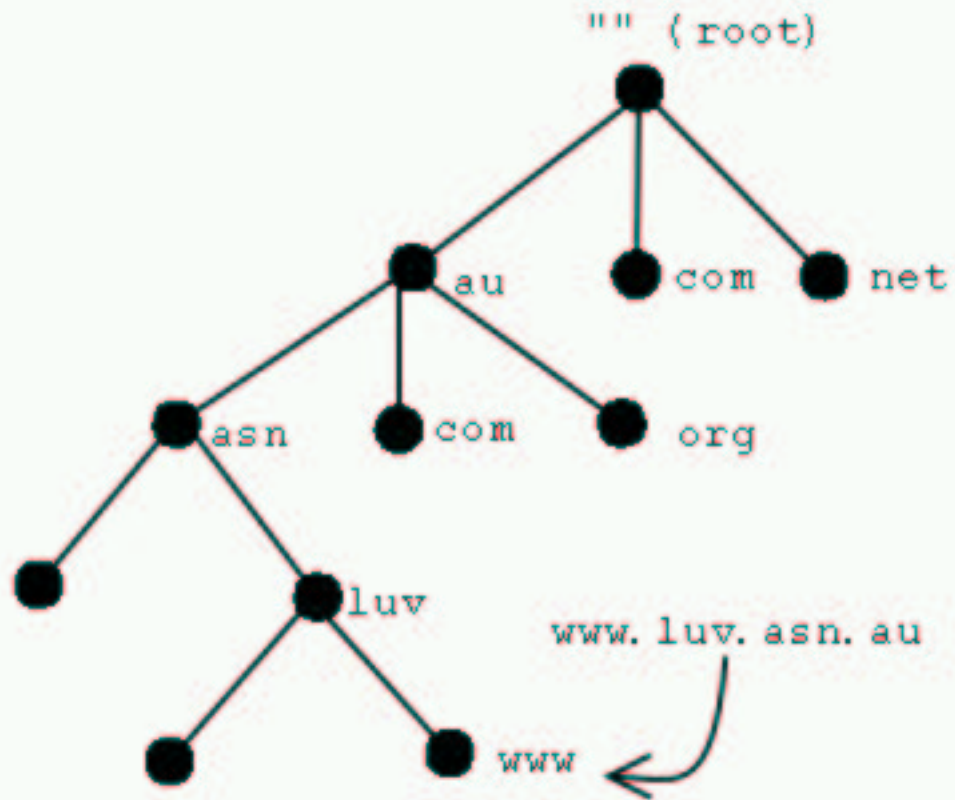
Other characteristics of DNS

- Each domain has to be unique
- Each organisation can administrate their domain (zone)
- The domain name points to information about the host
- This information comes in what is known as resource records

Resource records

SOA - Start of Authority
NS - Name Server
A - Address (Name-to-Address)
PTR - Pointer (Address-to-Name)
CNAME - Canonical Name (Alias)
MX - Mail Exchange
Other records

How DNS works



What might you need DNS for?

- Caching nameserver
- Host your own domain name
- Internal host information for your LAN

Types of Name Servers

- Master (or Primary)
- Slave (or Secondary)
- Caching only

Choosing a domain

Anyone can register (\$30-70/year):

- com
- net
- org

You'll need a business for (\$140/year):

- com.au
- net.au

Incorporated organisations can register for free:

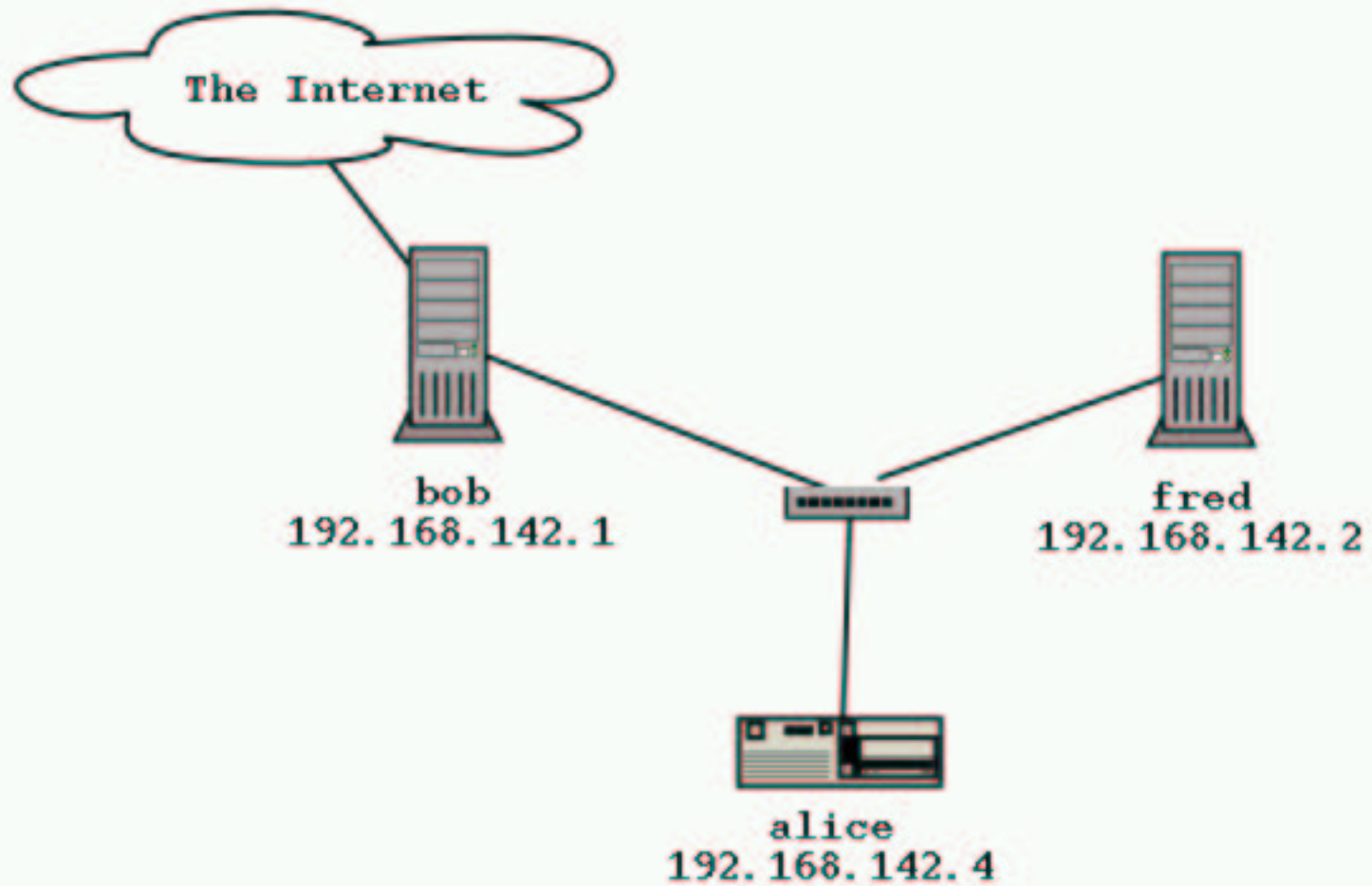
- asn.au
- org.au

What is BIND?

- An Implementation of DNS

- Domain Name System server (named)
- Domain Name System resolver library
- Tools for testing the DNS server

- Maintained by the Internet Software Consortium (ISC)



named.conf

Named.conf is the main configuration file for BIND. Here is a sample:

```
options {
    directory "/var/cache/bind";
    forwarders {
        10.45.45.1;
    };
};

zone "." {
    type hint;
    file "/etc/bind/db.root";
};

zone "example.edu.au" {
    type master;
    file "/etc/bind/db.example.edu.au";
}
```

A look inside a zone file

/etc/bind/db.example.edu.au:

```
example.edu.au. IN SOA bob.example.edu.au. root.example.edu.au. (  
    2001060100 ;serial (version)  
    10800      ;refresh period (3 hours)  
    3600       ;retry interval (1 hour)  
    604800     ;expire time (7 days)  
    86400      ;minimum TTL (24 hours)
```

);

```
example.edu.au. IN NS bob.example.edu.au.  
example.edu.au. IN NS fred.example.edu.au.
```

```
example.edu.au. IN MX 100 alice.example.edu.au.
```

A look inside a zone file

/etc/bind/db.example.edu.au:

```
example.edu.au. IN SOA bob.example.edu.au. root.example.edu.au. (  
    2001060100 ;serial (version)  
    10800      ;refresh period (3 hours)  
    3600       ;retry interval (1 hour)  
    604800    ;expire time (7 days)  
    86400     ;minimum TTL (24 hours)  
);
```

```
example.edu.au. IN NS bob.example.edu.au.  
example.edu.au. IN NS fred.example.edu.au.
```

```
example.edu.au. IN MX 100 alice.example.edu.au.
```

```
bob.example.edu.au. IN A 192.168.142.1  
fred.example.edu.au. IN A 192.168.142.2  
alice.example.edu.au. IN A 192.168.142.4
```

Shortened zone file

/etc/bind/db.example.edu.au:

```
@ IN SOA bob.example.edu.au. root.example.edu.au. (  
    2001060100 ;serial (version)  
    10800      ;refresh period (3 hours)  
    3600       ;retry interval (1 hour)  
    604800    ;expire time (7 days)  
    86400     ;minimum TTL (24 hours)
```

);

```
IN NS bob  
IN NS fred
```

```
IN MX 100 alice
```

```
bob IN A 192.168.142.1  
fred IN A 192.168.142.2  
alice IN A 192.168.142.4
```

Updaing Configuration

Reload the configuration of a running named process

- ndc reload

Starting named

- ndc start

Security

To ensure that your nameserver is secure:

- Run BIND as a non-root user

- Create a user and a group (eg 'bind')
- Make a directory called `/var/run/named` that is owned by the user and group that you created
- Make sure BIND can write to any other directories that it needs to (eg in Debian `/var/cache/bind`)
- Add pid-file `"/var/run/named/named.pid"`; to `named.conf`
- Edit your init script (in Debian `/etc/init.d/bind`) to so that bind is started with with the command line options `'-u bind -g bind'`

- Run BIND in a chroot jail

- Keep up to date with security updates

What's new in BIND version 9

- DNSSEC
- TSIG
- IPv6
- Split Zones

Migrating to BIND 9

- Named won't start with an error in named.conf
- Zone file errors don't cause the server to exit
- ACL names are case sensitive
- New reserved words might conflict with ACLs
- You must now add '\$TTL 86400' to the start of each zone file
- ndc replaced with rndc

resolv.conf in Linux

```
search example.edu.au  
nameserver 192.168.142.1  
nameserver 192.168.142.2
```

Installation

Debian:

- `apt-get install bind`

Red Hat:

- `rpm -i bind-*.rpm`

Other distributions:

- Look for packages or install from source

Alternatives to DNS

On a small network you might be able to :

- Maintain the `/etc/hosts` file on every computer
- or use Sun's NIS (Network Information Service)

For more information

Some places you can go for more information are:

- O'Reilly's book DNS and BIND by Paul Zibitz & Cricket Liu
- The BIND website <http://www.isc.org/products/BIND/>
- BOG (Bind Operators Guide)
- DNS-HOWTO
- My website <http://www.austux.net/> where you'll find this talk

Questions
