DNS - Outline

- Overview
  - What is DNS
  - Structure
  - Zones
  - Resolution process
  - Record types
- BIND
  - What is BIND
  - Installation
  - General configuration
  - Recursive configuration
  - Authoritative configuration
  - Views
  - Zone files
- Practical example
  - Home router
  - Registrar settings
  - DHCPD auto update DNS
- Questions, resources

DNS – What is DNS

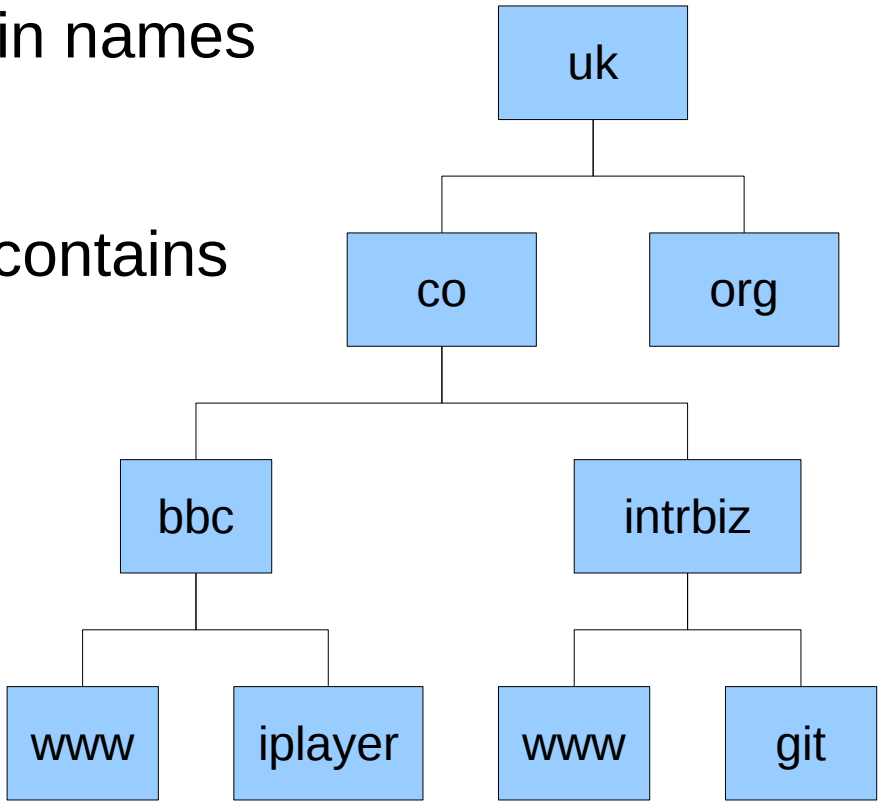
- The Domain Name System is a hierarchical, distributed naming database for networked computer systems.

- DNS is critical to the Internet and underpins practically all Internet applications.

- DNS stores a variety of information
  - Name to IP address mappings
  - Mail routing information
  - Authority information

DNS – Structure

- Data in DNS is identified by domain names
- Each node in the tree (a domain) contains a label
- At any point the domain name is the concatenation of all labels to the root of the tree



DNS – Structure

- Resolvers

  The DNS client which initiates a query which ultimately results in translation of the resource sought. Queries can be either recursive or non-recursive.

- Recursive name servers

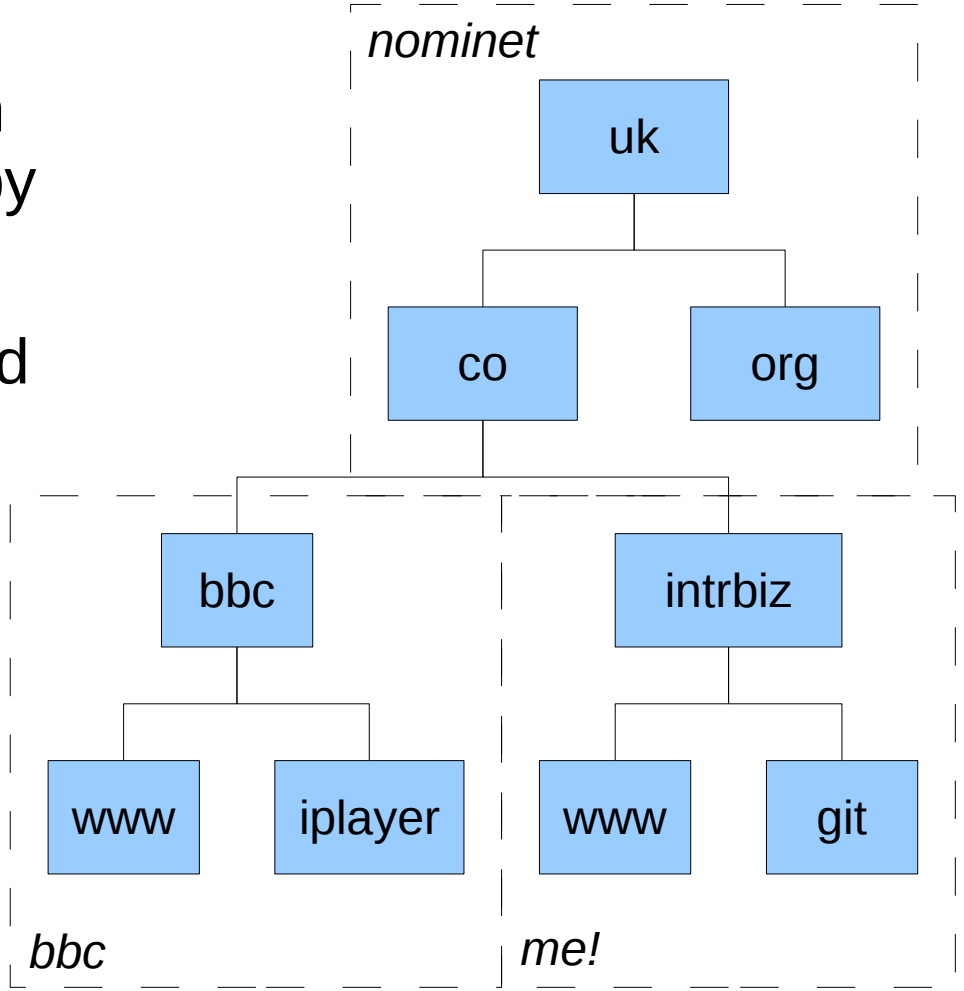
  A recursive name server handles recursive queries, looking up a resources on-behalf of a resolver.

- Authoritative name servers

  An authoritative name server holds actual data and responds to non-recursive queries with the information it holds. An authoritative server may response with the answer or with another name server who should know the answer.

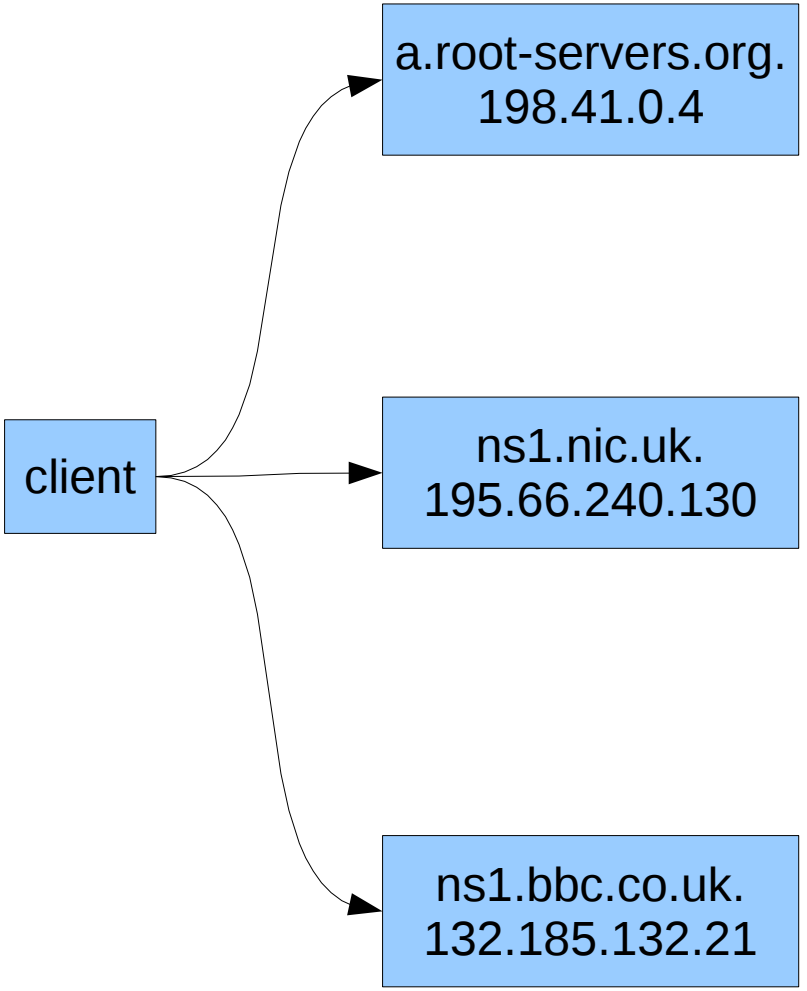
DNS – Zones

- The administration of information stored within DNS is separated by zones.
- Parts of a zone may be delegated to additional name servers.
- Generally a zone has multiple nameservers storing the information.
- Records stored within DNS hold the delegation information.



DNS – Resolution process

- To answer a DNS query multiple servers are queried recursively
- Every recursive server has a static list of 'root servers', these are controlled by ICANN. These servers translate Top Level Domains (TLD), ie: .com .uk
- The chain of delegated zones if followed until a server responds with the answer or no authority information



DNS – Record types

- DNS can store a large variety of information and therefore has a set of record types.

- Below are common record types

Type	Description	Function
A	IPV4 address record	Maps a name to a IPV4 address
AAAA	IPV6 address record	Maps a name to a IPV6 address
CNAME	Canonical name record	Maps a name to a name
MX	Mail exchange record	Maps a domain to a SMTP server
NS	Name server record	Delegates a DNS Zone to a name server
SOA	Start of authority record	Specifies authority information for a zone
TXT	Text Record	Arbitrary text records for this name

DNS – What is BIND

- BIND (Berkeley Internet Name Domain) is the de-facto implementation of a DNS server. It is a fully featured DNS server and is available for most Linux Distributions.

- BIND can act as an Authoritative or Recursive name server or as both.

BIND – General configuration

- Statements are a labeled pair of braces.
- Options are defined within certain statements.

- The options statement defines general settings for the server

```
options {
        directory "/var/lib/named";
        dump-file
"/var/log/named_dump.db";
        statistics-file
"/var/log/named.stats";
        listen-on port 53 { any; };
        listen-on-v6 { any; };
        allow-query { trusted; };
        allow-recursion { trusted; };
        allow-transfer { trusted; };
        notify no;
};
```

- The base directory for data files
- The file to dump the named database
- The file to dump statistics to
- The port to listen on
- The port to listen on
- Where to allow queries from
- Where to allow recursive queries from
- Where to allow zone transfers from
- Notify slave nodes

BIND – General configuration

- Access Controls (ACL) defines a name for a set of hosts, this can then be used to define host permissions.

```
acl acl-name {
    any;                    - Any hosts
    localhost;              - Any host on a local interface
    none;                   - No hosts
    192.168.1.0/24;         - Standard CIDR address range
};

eg.

acl trusted {
        10.0.0.0/8;         - Define the 'trusted' acl
        localhost;          - Allow all machine on my local network, 10.0.0.0 mask 255.0.0.0
};                          - Allow all hosts of a local interface (ie: 127.0.0.1)
```

BIND – General configuration

- The logging statement configures a variety of logging options
- The channel statement defines output options
- The category statement maps log messages to an output

```
logging {
        category default { log_syslog; };
        channel log_syslog { syslog; };
};
```

- Map default output to system
- output to syslog

BIND – General configuration

- Access Controls (ACL) defines a name for a set of hosts, this can then be used to define host permissions.

```
acl acl-name {
    any;                    - Any hosts
    localhost;              - Any host on a local interface
    none;                   - No hosts
    192.168.1.0/24;         - Standard CIDR address range
};

eg.

acl trusted {               - Define the 'trusted' acl
        10.0.0.0/8;         - Allow all machine on my local network, 10.0.0.0 mask 255.0.0.0
        localhost;          - Allow all hosts of a local interface (ie: 127.0.0.1)
};
```

BIND – General configuration

- Zones define data available within the server

```
zone "." in {
    type hint;
    file "root.hint";
};

zone "intrbiz.com" in {
                allow-transfer
{ trusted; };
                file
"master/internal/intrbiz.com";
                type master;
};
```

- Any hosts
- Any host on a local interface
- No hosts
- Standard CIDR address range

- Define the 'trusted' acl
- Allow all machine on my local network, 10.0.0.0 mask 255.0.0.0
- Allow all hosts of a local interface (ie: 127.0.0.1)

BIND – Recursive configuration

```
acl trusted {
        10.0.0.0/8;
        localhost;
};

options {
        directory "/var/lib/named";
        dump-file "/var/log/named_dump.db";
        statistics-file "/var/log/named.stats";
        listen-on port 53 { any; };
        listen-on-v6 { any; };
        allow-query { trusted; };
        allow-recursion {trusted;};
        recursion yes;
        additional-from-auth yes ;
        additional-from-cache yes ;
};

logging {
        category default { log_syslog; };
        channel log_syslog { syslog; };
};
```

```
zone "." in {
        type hint;
        file "root.hint";
};



#------------------------------------------------------------
# Define an internal master zone
#------------------------------------------------------------

zone "intrbiz.co.uk" in {
                allow-transfer { trusted; };
                file "master/internal/intrbiz.co.uk";
                type master;
};
```

BIND – Authoritative configuration

```
acl trusted {
        10.0.0.0/8;
        localhost;
};

options {
        directory "/var/lib/named";
        dump-file "/var/log/named_dump.db";
        statistics-file "/var/log/named.stats";
        listen-on port 53 { any; };
        listen-on-v6 { any; };
        allow-query { any; };
        allow-recursion { none; };
        recursion no;
        additional-from-auth no ;
        additional-from-cache no ;
};

logging {
        category default { log_syslog; };
        channel log_syslog { syslog; };
};
```

```
zone "intrbiz.com" in {
        allow-transfer { trusted; };
        file "master/external/intrbiz.com";
        type master;
};
zone "intrbiz.net" in {
        allow-transfer { trusted; };
        file "master/external/intrbiz.net";
        type master;
};
zone "intrbiz.co.uk" in {
        allow-transfer { trusted; };
        file "master/external/intrbiz.co.uk";
        type master;
};
```

BIND – Views

```
acl trusted {
        10.0.0.0/8;
        localhost;
};

options {
        directory "/var/lib/named";
        dump-file "/var/log/named_dump.db";
        statistics-file "/var/log/named.stats";
        listen-on port 53 { any; };
        listen-on-v6 { any; };
        allow-query { trusted; };
        allow-recursion { trusted; };
};

logging {
        category default { log_syslog; };
        channel log_syslog { syslog; };
};

view "internal-in" {
                match-clients {trusted;};
                recursion yes;
                additional-from-auth yes ;
                additional-from-cache yes ;
                zone "." in {
                        type hint;
                        file "root.hint";
                };
                zone "intrbiz.com" in {
                        allow-transfer { trusted; };
                        file "master/internal/intrbiz.com";
                        type master;
                };
};

view "external-in" {
                match-clients {any;};
                recursion no;
                additional-from-auth no ;
                additional-from-cache no ;
                allow-query {any;};

                zone "intrbiz.com" in {
                        allow-transfer { trusted; };
                        file "master/external/intrbiz.com";
                        type master;
                };
};
```

BIND – Zone files

```
$TTL 5h
@               IN SOA   ns1 dns.intrbiz.com (
                         2009071200; serial
                         3H;  refresh
                         1H;  retry
                         2H;  expiry
                         1H); minimum

intrbiz.com.    IN NS    ns1.intrbiz.com.
intrbiz.com.    IN NS    ns2.intrbiz.com.
ns1             IN A     82.152.34.222
ns2             IN A     82.152.34.222
intrbiz.com.    IN A     82.152.34.222
intrbiz.com.    IN MX    0 mx1
www             IN CNAME saturn
saturn          IN A     82.152.34.222
*               IN A     82.152.34.222
```

- define the zone Time To Live
- SOA record define the authoritative name server, email contact
- zone serial number
- time between the slave server checking the master server
- time between zone transfer retries if a transfer fails
- time after which the slave will stop responding to queries
- minimum record TTL time

- NS record for the primary authoritative server
- NS record for the secondary authoritative server
- A record for the primary NS record
- A record for the secondary NS record
- A record for the root of the zone
- MX (email routing) record for the zone
- CNAME record for www → saturn
- A record for saturn
- A record with wildcard, this will match anything .intrbiz.com and will break the above two records, use with caution

Example – Home router

- DNS server running on a single server.
- Acting as a recursive caching name server for internal clients.
- Acting as an authoritative name server for for external clients, ie the Internet.
- The DHCP server updates DNS with the host name and IP assigned by DHCP.

Example – The config !

```
key routel {
    algorithm hmac-md5 ;
    secret VppMy3bLmtx5SY7VPWW5D0wyrLdYh8MVhwmVKfVsdvsvUtPGClLSY65Bj4E9 ;
};

controls {
    inet 127.0.0.1 port 953
    allow { 127.0.0.1; } keys { "routel"; };
};

acl "trusted_networks" {
    127.0.0.1;
    192.168.1.0/24;
};

statistics-channels {
    inet 127.0.0.1 port 5380 allow { 127.0.0.1; };
};
```

Example – The config !

```
logging {
        channel security_channel {
                file "/var/log/security.log" versions 4 size 10m;
                print-category yes;
                print-severity yes;
                print-time yes;
                severity info;
        };
        channel default_channel {
                file "/var/log/default.log" versions 4 size 10m;
         severity info;
                print-category yes;
                print-severity yes;
                print-time yes;
        };
        channel xfer-in_channel {
                file "/var/log/xfer-in.log" versions 4 size 10m;
                severity info;
                print-category yes;
                print-severity yes;
                print-time yes;
        };
        channel xfer-out_channel {
                file "/var/log/xfer-out.log" versions 4 size 10m;
                severity info;
                print-category yes;
                print-severity yes;
                print-time yes;
        };
```

Example – The config !

```
channel update_debug {
                file "/var/log/update.log" versions 4 size 10m;
                severity debug 3;
                print-category yes;
                print-severity yes;
                print-time yes;
        };
        channel notify_channel {
                file "/var/log/notify.log" versions 4 size 10m;
                severity info;
                print-category yes;
                print-severity yes;
                print-time yes;
        };
    channel "querylog" {
                file "/var/log/query.log" versions 4 size 10m;
         print-time yes;
        };

    category queries { querylog; };
        category security { security_channel; };
        category default { default_channel; };
        category xfer-in { xfer-in_channel; };
        category xfer-out { xfer-out_channel; };
        category notify { notify_channel; };
        category update { update_debug; };
        category lame-servers { null; };
        category "delegation-only" { "null" ; };

};
```

Example – The config !

```
options {
    version "";
    directory "/var/named";
    dump-file "/var/tmp/named_dump.db";
    pid-file "/var/run/named.pid";
    statistics-file "/var/tmp/named.stats";
    zone-statistics yes;
    coresize 100M;
    auth-nxdomain yes;
    query-source address * port *;
    listen-on port 53 { any; };
    cleaning-interval 120;
    transfers-in 20;
    transfers-per-ns 2;
    lame-ttl 0;
    max-ncache-ttl 10800;
    allow-query { none; };
    allow-recursion {none;};
    allow-transfer {none;};
    notify no;
    //also-notify { secondary_name_server };
    transfer-format many-answers;
    max-transfer-time-in 60;
    interface-interval 0;
};
```

Example – The config !

```
view "internal-in" {
  match-clients {trusted_networks;};
  allow-query { trusted_networks; };
  allow-recursion {trusted_networks;};
  allow-transfer {trusted_networks;};
  allow-update {127.0.0.1;};
  recursion yes;
  additional-from-auth yes ;
  additional-from-cache yes ;
  zone "." in {
    type hint;
    file "named.ca";
  };
  // fixes verisign patch
  zone "ac" { type delegation-only; };
  zone "cc" { type delegation-only; };
  zone "com" { type delegation-only; };
  zone "cx" { type delegation-only; };
  zone "lv" { type delegation-only; };
  zone "museum" { type delegation-
only; };
  zone "net" { type delegation-only; };
  zone "nu" { type delegation-only; };
  zone "ph" { type delegation-only; };
  zone "sh" { type delegation-only; };
  zone "tm" { type delegation-only; };
  zone "ws" { type delegation-only; };
```

```
zone "1.168.192.in-addr.arpa" in {
    type master;
    file "internal/reverse/192.168.1";
    allow-update {key "routel";};
    notify yes;
  };
  zone "internal.intrbiz.co.uk" in {
    allow-transfer { trusted_networks; };
    file
"internal/master/internal.intrbiz.co.uk";
    type master;
    allow-update {key "routel";};
  notify yes;
  };
  zone "intrbiz.co.uk" in {
    allow-transfer { trusted_networks; };
    file "internal/master/intrbiz.co.uk";
    type master;
  };
  zone "intrbiz.com" in {
    allow-transfer { trusted_networks; };
    file "internal/master/intrbiz.com";
    type master;
  };
  zone "intrbiz.net" in {
    allow-transfer { trusted_networks; };
    file "internal/master/intrbiz.net";
    type master;
  };
};
```

Example – The config !

```
view "external-in" {
  match-clients {any;};
  allow-recursion {none;};
  recursion no;
  additional-from-auth no ;
  additional-from-cache no ;
  allow-query {any;};
  zone "intrbiz.com" in {
    allow-transfer
{ trusted_networks; };
    file "external/master/intrbiz.com";
    type master;
  };
  zone "intrbiz.net" in {
    allow-transfer
{ trusted_networks; };
    file "external/master/intrbiz.net";
    type master;
  };
  zone "intrbiz.co.uk" in {
    allow-transfer
{ trusted_networks; };
    file
"external/master/intrbiz.co.uk";
    type master;
  };
};
```

Example – Registrar settings

Is your domain a .com or .net?

If so, please make sure the domain is unlocked. To check this, just go to our locking page and click **Unlock domain**. If you don't see that option, the domain's already unlocked.

Remember to lock the domain again afterwards. More about domain locking.

All set? Change name servers here

Enter new nameserver information:

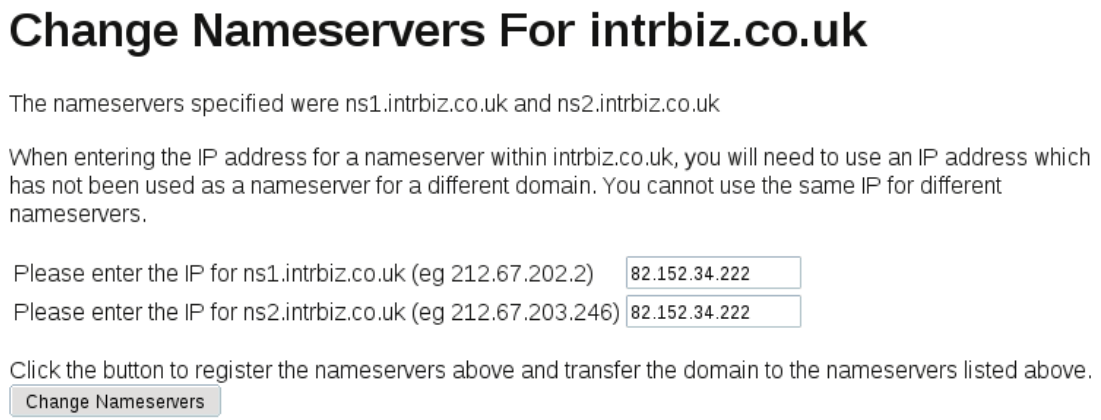
Required
Nameserver 1: ns1.intrbiz.co.uk
Nameserver 2: ns2.intrbiz.co.uk

Optional:
Nameserver 3:
Nameserver 4:

Change Nameservers

- **I've forgotten my current name servers**
  No problem. See them here.
- **I need some help with name servers**
  Read the name server information on our support site.

Back to Control Panel



Change Nameservers For intrbiz.co.uk

The nameservers specified were ns1.intrbiz.co.uk and ns2.intrbiz.co.uk

When entering the IP address for a nameserver within intrbiz.co.uk, you will need to use an IP address which has not been used as a nameserver for a different domain. You cannot use the same IP for different nameservers.

Please enter the IP for ns1.intrbiz.co.uk (eg 212.67.202.2) 82.152.34.222
Please enter the IP for ns2.intrbiz.co.uk (eg 212.67.203.246) 82.152.34.222

Click the button to register the nameservers above and transfer the domain to the nameservers listed above.
Change Nameservers

How do I run my own name server?

- Set the name server of your domain to the IP address of your connection
- Ensure you are on a static IP address, if you use DDNS then you cannot run your own DNS server.
- If you use 123-reg.co.uk then the settings are shown to the left
- Changes will take a day or so to propigate

Example – DHCPD DDNS

```
ddns-domainname
"internal.intrbiz.co.uk.";
ddns-rev-domainname "in-addr.arpa.";
ignore  client-updates;

include "/etc/rndc.key";

zone internal.intrbiz.co.uk. {
    primary 127.0.0.1;
    key routel;
}
zone 1.168.192.in-addr.arpa. {
    primary 127.0.0.1;
    key routel;
}

ddns-update-style interim;
update-static-leases on;
ddns-updates on;
```

```
default-lease-time 600;
max-lease-time 600;
authoritative;

log-facility daemon;

subnet 192.168.1.0 netmask 255.255.255.0 {
    # basic settings
    option routers 192.168.1.1;
    option subnet-mask 255.255.255.0;
    option domain-name
"internal.intrbiz.co.uk.";
    option ntp-servers 192.168.1.1;
    option domain-name-servers 192.168.1.1;
    # the range and lease times
    range dynamic-bootp 192.168.1.128
192.168.1.254;
}

# reservations
host jupiter {
    hardware ethernet 12:34:56:78:AB:CD;
    fixed-address 192.168.1.5;
}
```

Example – Questions, resources

- Questions

- Resources
  - http://www.bind9.net/manuals
  - http://www.bind9.net/manuals-dhcp
  - http://iptools.com/
  - http://en.wikipedia.org/wiki/Domain_Name_System