[Q]: README от dnswalk'a - рекомендации по настройке DNS

[A]: Dave Barr (barr@pop.psu.edu)

```
      Here's some tips I've come up with in my months of running DNS, as
      well as in development of dnswalk:
```

* Every Internet host should have a name. Enough said.

* Allowable characters in a name are ONLY letters, digits, and

```
the '-' character (separated by '.' of course).  Domain names
may not be all numbers, but may have a leading digit.  (e.g. 3com.com)
(See RFC 1035 and 1123)
```

* You shouldn't have any A records in an in-addr.arpa zone file.

```
This includes NS glue records.  Just put the nameserver name in
there and be done with it.  Why?  It's unnecessary, and just makes
things harder when that nameserver changes its IP address.  You'll
spend hours trying to figure out why random people still see the old
address for some machine.  BIND 4.9.x handles this better, however.
```

* Verify the data you just entered or changed by querying the

```
resolver with 'dig' (or your favorite DNS tool) after a change.  A
few seconds spent double checking can save hours of trouble, lost
mail, and headaches.  Also be sure to check syslog output when you
reload the nameserver.
```

* Don't forget to change the serial number. Also, even though BIND

```
allows you to use a decimal in a serial number, don't use them.  If you
want to know why, read "DNS & BIND" (see below).
```

* Always remember your $ORIGIN. If you don't put a '.' at the end

```
of an FQDN, it's not an FQDN.  Double check, triple check, those dots.
```

* BE CONSISTENT! If your $ORIGIN is “foo.org.”, don't have entries

```
like:
```

tron in a 1.2.3.1 mcp.foo.org. in a 1.2.3.2

or even:

mcp in a 1.2.3.2

```
              in      mx      flynn.foo.org.  ; why not just "flynn"?
```

Either use all FQDNs everywhere or used unqualified names everywhere. Don't mix the two. It just adds confusion and needless typing. (Of course this can't be avoided for RRs of hosts outside $ORIGIN)

* Be a good net.neighbor. Use HINFO records. Don't believe what you

```
hear about the security concerns.  If you're too busy to worry about
fixing known vendor security holes, then you shouldn't be on the
Internet.  Don't forget that HINFO _requires_ two tokens, the machine
type, and the operating system.  BIND won't complain if the second is
missing, but will result in garbage and will confuse resolvers.
```

* On the other hand, don't use WKS records. They're useless and obsolete.

* Pick friendly, easy to remember hostnames. “rm5ws3” may tell you

```
that it's the 3rd workstation in room 5, but what if you move rm5ws1
and rm5ws2 to another room?  Also, don't succumb to the "Bond,
James Bond" naming scheme.  "psuvm.psu.edu" is no more informative
than "vm.psu.edu".  (Perpetuated by inferior networks like BITNET)
```

* Have a secondary outside your network. If the secondary isn't under

```
your control, periodically check up on them and make sure they're
properly set up to secondary for you.  (queries to their nameserver
about your machines should result in an "authoritative" response, etc)
Use the 'doc' program for this one.
```

* make sure your parent domain has the same NS records for your zone

```
as you do.  (Don't forget the in-addr.arpa domain too!).  Use the
'doc' program if you're not sure how to check.
```

* If a site plans to receive mail, give it an MX record, EVEN IF IT

```
POINTS TO ITSELF!  Some mailers will cache MX records, but will
ALWAYS query to find an MX before sending mail.  If a site does not
have an MX, then EVERY piece of mail will result in one more resolver
query.  (most mailers do not implement negative caching)  If you put
in an MX, then this data can be cached.  (Yes, Virginia, Internet
SMTP mailers are REQUIRED BY RFCs to support the "MX" mechanism.
Pound on sites that refuse to comply.)
```

* Wildcard MX's are only useful for non IP-connected sites. If

```
a site has any other records, a wildcard MX won't apply to it.
```

e.g. *.podunk.edu. in mx mail.podunk.edu. mary.podunk.edu. in A 1.2.3.4

```
Mail for "mary.podunk.edu" will be sent to mary, while mail for
```

```
"jane.podunk.edu" will be sent to mail.podunk.edu.  Really.
```

```
Wildcard MX's can also be quite harmful, because they make some
operations succeed when they should fail instead.  Consider the case
where people try to send mail to "joe@larry" over in the accounting
department of "your.domain.com".  Unfortunately, the host "larry"
doesn't actually exist anymore, so the address should in fact
bounce.  But because of domain searching, the address gets resolved
to larry.your.domain.com, and because of the wildcard MX this is a
valid address according to DNS.  The mail message then gets routed to
the mail host, which proceeds to barf with strange error messages
like "I refuse to talk to myself!" or "Local configuration error!".
```

```
Now, it is possible to tweak your mailer configuration to account
for such problems, but why would you want to?
```

* Wildcards can be used on other RR's too, but are generally a bad

```
idea.   They are confusing to users because resolver queries for
unknown hosts in a wildcarded domain give _emtpy_ responses instead
of NXDOMAIN.
```

```
Wildcard A's and CNAME's are especially confusing to users.  I really
can't think of a valid reason for wildcard records other than MX.
```

* Don't go overboard with CNAMEs. Use them when moving/renaming machines,

```
but plan to get rid of them.  (And inform your users)  CNAMEs ARE useful
(and encouraged) for generalized names for servers - "ftp" for your ftp
server, "www" for your Web server, "gopher" for your gopher server,
"news" for your news server, etc.
```

* Do NOT use CNAMEs with ANY other data. Especially do NOT try to do

```
the following!:
```

```
podunk.edu.   in      ns      mary.podunk.edu.
podunk.edu.   in      ns      sue.podunk.edu.
podunk.edu.   in      cname   mary.podunk.edu.
```

```
DNS servers like BIND will see the CNAME and refuse to add any
more records to the zone.  More importantly, since "podunk.edu"
is now a CNAME only, all the entries under podunk.edu are ignored!
```

* If a host is multi-homed, (more than on A record) make sure that all

```
its IP addresses have a corresponding PTR record.  (not just the first
one)
```

* As more useful RRs come into existence, use them. (Like TXT, RP, etc).

* And of course, above all, use my dnswalk program.