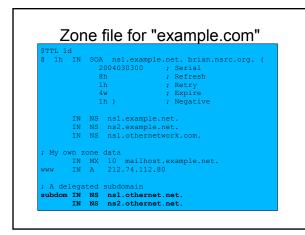


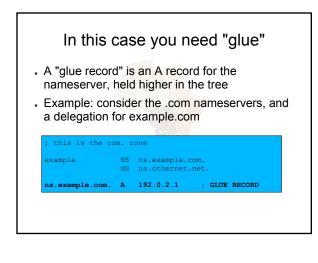
#### How do you delegate a subdomain?

- In principle straightforward: just insert NS
  records for the subdomain, pointing at someone
  else's servers
- If you are being careful, you should first *check* that those servers are authoritative for the subdomain
  - by using "dig +norec" on all the servers
- If the subdomain is managed badly, it reflects badly on you!
  - and you don't want to be fielding problem reports when the problem is somewhere else



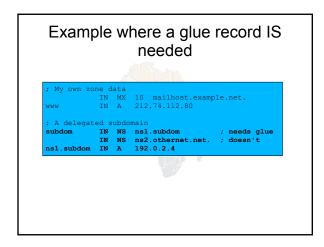
### There is one problem here:

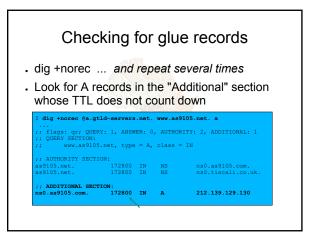
- NS records point to names, not IPs
- What if zone "example.com" is delegated to "ns.example.com"?
- Someone who is in the process of resolving (say) www.example.com first has to resolve ns.example.com
- But in order to resolve ns.example.com they must first resolve ns.example.com !!

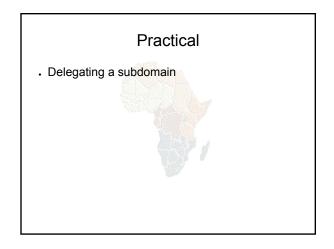


### Don't put in glue records except where necessary

- In the previous example, "ns.othernet.net" is not a subdomain of "example.com". Therefore no glue is needed.
- Out-of-date glue records are a big source of problems
  - e.g. after renumbering a nameserver
  - Results in intermittent problems, difficult to debug

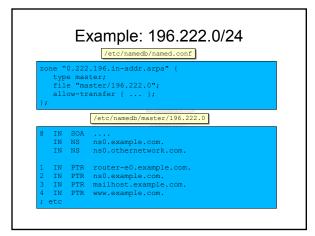


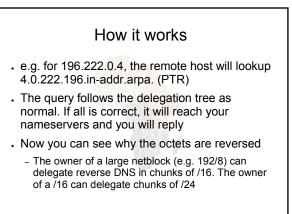




# Loose ends: how to manage reverse DNS

- If you have at least a /24 of address space then your provider will arrange delegation to your nameservers
- e.g. your netblock is 196.222.0.0/24
- Set up zone 0.222.196.in-addr.arpa.
- If you have more than a /24, then each /24 will be a separate zone
- If you a lucky enough to have a /16 then it will be a single zone
  - 196.222.0.0/16 is 222.196.in-addr.arpa.





# There is nothing special about reverse DNS

- . You still need master and slave(s)
- It won't work unless you get delegation from above
- However, DO make sure that if you have a PTR record for an IP address, that the hostname resolves back to the same IP address
  - Otherwise, many sites on the Internet will think you are spoofing reverse DNS and will refuse to let you connect

### What if you have less than /24?

- Reverse DNS for the /24 has been delegated to your upstream provider
- Option 1: ask your provider to insert PTR records into their DNS servers
  - Problem: you have to ask them every time you want to make a change
- Option 2: follow the procedure in RFC 2317
  - Uses a trick with CNAME to redirect PTR requests for your IPs to your nameservers

_		. you own 192.0.2.64/29
64	IN	CNAME 64.64/29.2.0.192.in-addr.arpa.
65	IN	CNAME 65.64/29.2.0.192.in-addr.arpa.
66	IN	CNAME 66.64/29.2.0.192.in-addr.arpa.
67	IN	CNAME 67.64/29.2.0.192.in-addr.arpa.
68	IN	CNAME 68.64/29.2.0.192.in-addr.arpa.
69	IN	CNAME 69.64/29.2.0.192.in-addr.arpa.
70	IN	CNAME 70.64/29.2.0.192.in-addr.arpa.
71	IN	CNAME 71.64/29.2.0.192.in-addr.arpa.
64/29	IN	NS ns0.customer.com.
64/29	IN	NS nsl.customer.com.
Set up	zone	"64/29.2.0.192.in-addr.arpa" on your nameserve:
65 66 ; etc	IN IN	PTR www.customer.com. PTR mailhost.customer.com.

### DNS: Summary

- Distributed database of Resource Records
- e.g. A, MX, PTR, ...Three roles: resolver, cache, authoritative
- Resolver statically configured with nearest caches
   \_ e.g. /etc/resolv.conf
- Caches are seeded with a list of root servers
   zone type "hint", /etc/namedb/named.root
- Authoritative servers contain RRs for certain zones (part of the DNS tree)
  - replicated for resilience and load-sharing

### DNS: Summary (cont)

- Root nameservers contain delegations (NS records) to gTLD or country-level servers (com, uk etc)
- These contain further delegations to subdomains
- Cache finally locates an authoritative server containing the RRs requested
- Errors in delegation or in configuration of authoritative servers result in no answer or inconsistent answers



- RFC 1912, RFC 2182
  - http://www.rfc-editor.org/