So You Inherited a DNS Server…

DNS Best Practices from Day One

ISC

How did the DNS find you?

- Because I knew *nix
- No one else would
- It just sort of happened…
- voluntold

The Question

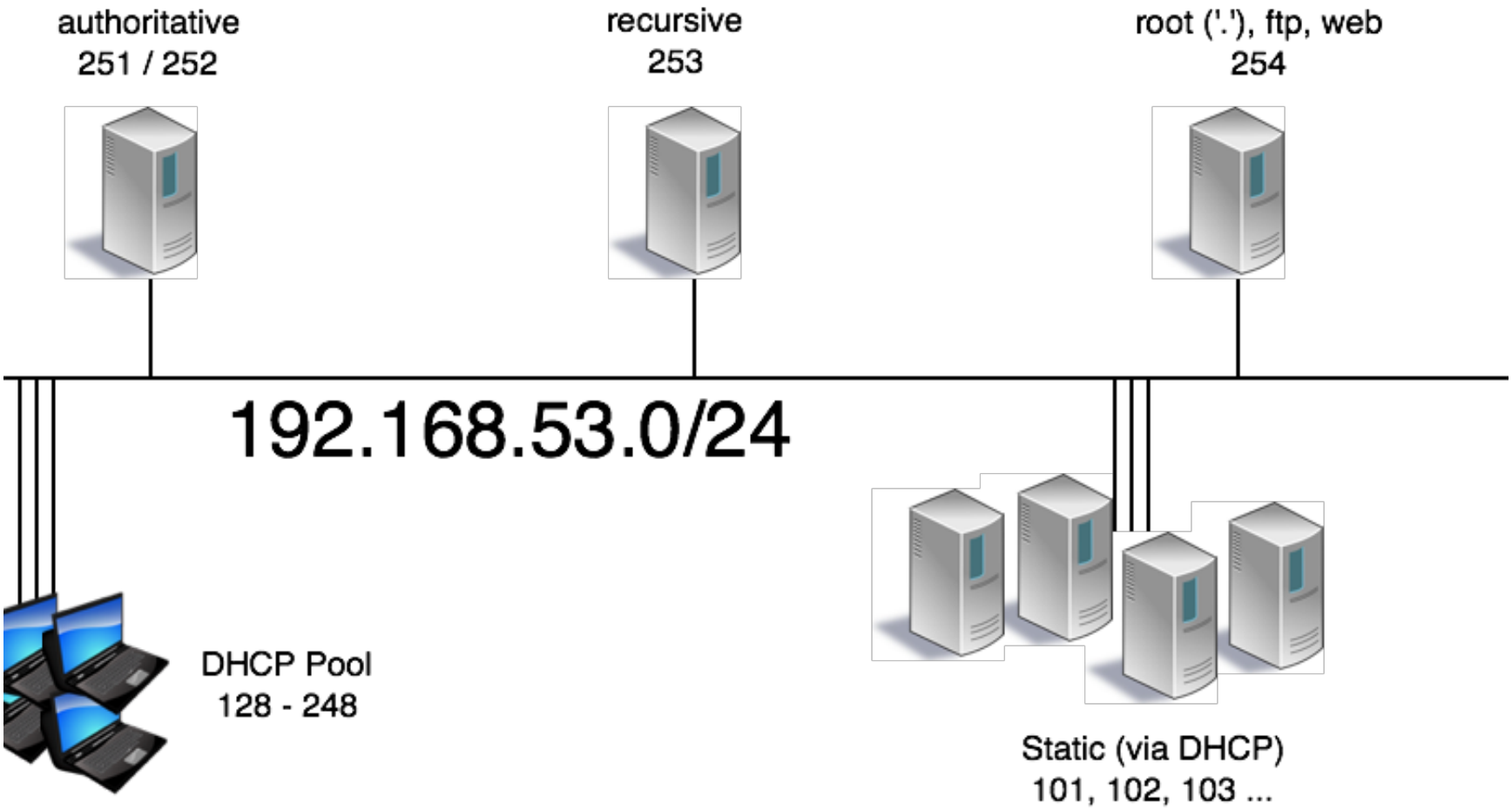
- What would you do if dropped into an existing organization to run their DNS?

First action, Recon!

- Actually, first action is freak out!
- 2nd action is caffeine, then deep breath and recon:

Any network or infrastructure diagrams available?

diagrams



Pick a nameserver, login!

- Running a current version of dns software?
- OS?
- How is dns service started on this box? Does this match the version currently running?
- Is there a nanny script in use?

named -V

```
% named -V
BIND 9.8.4-P2 built with '--prefix=/usr' '--infodir=/usr/
share/info' '--mandir=/usr/share/man' '--enable-threads'
'--enable-getifaddrs' '--disable-linux-caps' '--with-
openssl=/usr' '--with-randomdev=/dev/random' '--without-
idn' '--without-libxml2'
using OpenSSL version: OpenSSL 0.9.8zd-freebsd 8 Jan
2015
```

On to configuration

- Do the global options make sense?

- Basic security check:
  - TSIG secured zone transfers?
  - allow-transfer?
  - allow-query (is this an open resolver?)

Global options

```
options {
        directory "/etc/namedb/";
        dnssec-enable yes;
        dnssec-validation yes;
        allow-recursion { none; };
        allow-query { any; };
        allow-transfer { none; };
        notify no;
        key-directory "/etc/namedb/keys";
        max-journal-size 32k;
        zone-statistics yes;
        listen-on { 192.168.53.251; };
        listen-on-v6 { 2001:db8:100::251; };
        notify-source 192.168.53.251;
        notify-source-v6 2001:db8:100::251;
};
```

zone stanzas

```
zone "example.com" IN {
  file "example.com-zone";
  type slave;
  masters { 192.168.53.4; 192.168.53.8; };
  notify no;
};
```

logging

- Is the logging stanza sane and actually occurring?
- Check the config as well as the actual logs.
- Have a look at the system logs

logging stanza

```
logging {
        channel query_log {
                file "logs/query.log" versions 5 size 1M;
                severity info;
                print-time yes;
        };
        category queries { query_log; };
};
```

checkconf is your friend

$ named-checkconf –z

zone ./IN: loaded serial 121 (DNSSEC signed)
zone test.dnslab.org/IN: loaded serial 50 (DNSSEC signed)

rndc

- Is rndc configured?
- If not, ‘rndc-confgen –a’

- rndc status

- rndc notify zone
- rndc retransfer zone

Recon Repeat

- Repeat the prior Recon for all known nameservers!
- If diagrams were available, check to see if configs match stated functionality.

SOME FUN THINGS YOU OUGHT TO KNOW…

DNS personality disorders

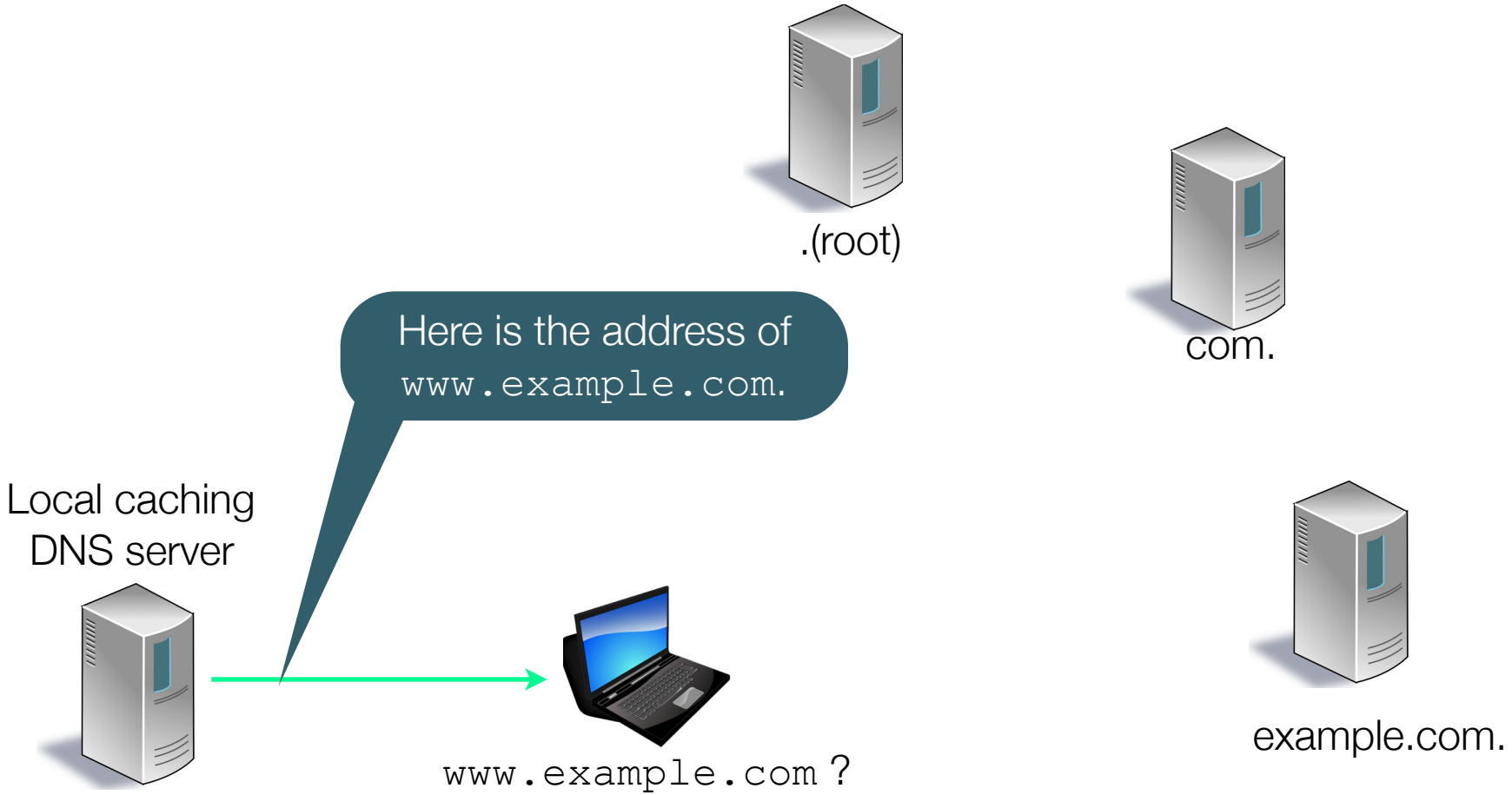
- Clients are often happy even when servers aren't configured well.
- A bit passive-aggressive… things are acceptable until they're not.
- OCD, clients and resolvers are content to retry and retry and retry…

RFCs

https://www.isc.org/community/rfcs/dns/

RFC	Type	Status	Title	Bgnd	Prot	Names	Ops	RR	Proxy	Stub	Auth	Res	Xfr	DDNS	DNSSEC
882		Obsolete	Domain Names – Concepts and Facilities	x		x	x				x				
883		Obsolete	Domain Names – Implementation and Specification		x		x	x			x	x			
920			Domain Requirements				x								
973		Obsolete	Domain System Changes and Observations			x		x			x	x			
1032			Domain Administrators Guide				x								
1033			Domain Administrators Operations Guide				x								
1034	Standard		Domain Names – Concepts and Facilities	x		x	x			x	x	x			
1035	Standard		Domain Names – Implementation and Specification		x	x		x			x	x	x		
1101			DNS Encoding of Network Names and Other Types			x									
1123	Standard		Requirements for Internet Hosts – Application and Support	x							x	x			
1178	Informational		Choosing a Name for Your Computer				x								
1183	Experimental		New DNS RR Definitions					x							
1348	Experimental	Obsolete	DNS NSAP RRs					x							
1401	Informational		Correspondence between the IAB and DISA on the use of DNS throughout the Internet	x											
1535	Informational		A Security Problem and Proposed Correction With Widely Deployed DNS Software									x			
1536	Informational		Common DNS Implementation Errors and Suggested Fixes							x		x			
1537	Informational	Obsolete	Common DNS Data File Configuration Errors				x								
1591	Informational		Domain Name System Structure and Delegation				x								
1611	Historic	Historic	DNS Server MIB Extensions				x								
1612	Historic	Historic	DNS Resolver MIB Extensions				x								

DNS Resolution



BACK TO YOUR NEW PREDICAMENT…

Authoritative specific

- Use external tools to check service:
  - DNSViz
  - dnscheck.iis.se
  - ednscomp.isc.org (firewall check)

Recursive specific

- Perform queries against these servers via dig

  dig @192.168.53.53 www.example.com.

- Are they answering appropriately?

- Are they refusing appropriately?

Actions for Day 2 and beyond

- Meet with the following teams:
  - Provisioning: how fast for new servers?
  - Operations: how's life?
  - Security: about those firewalls…
  - Monitoring: alerting on?, peak traffic?
  - Architecture: future plans?
  - Management: support?

Interconnectedness

- Get your boss to send you to DNS-OARC meeting(s)

- Join some lists:
  - dns-operations (DNS OARC)
  - nanog
  - etc

Questions

?

Thank You!

www.isc.org

info@isc.org