DNS:
Backbone of the Internet

• Translates Domains into unique IP Addresses
  – i.e. “dns.google” = “8.8.8.8” & “8.8.4.4”

• Distributed Database of Host Information

• Works seamlessly “behind the scenes”
So what is a “Domain”?

• RFC 920: Domains are Administrative entities

• A unique name

• Can contain subdomain names
Basic Structure

Hierarchical, Tree-like structure

• Made up of individual Nodes
DNS: Series of Delegated Information

A Silly Example...

cHECKERS.BOARDGAMES.GAMES.FUN.COM
Domain Namespace:

Another Picture

This “tree” is also called a “domain namespace.”
Components of DNS

• Domain Name Space
• Name Servers (Authoritative Name Servers)
• Resolvers (Caching Name Servers)
DNS Zones

A portion of a Domain Namespace defined by Zone Files (which contain Zone Records)
• Portion of a Domain Namespace that has been administratively delegated
• … Therefore, this information comes from an authoritative source (Master Name Server)
• Can be loaded by Slave Name Servers (for backup and redundancy purposes)
Components of Zone Files

• TTL (Time to Live)
  – Tells caching nameservers how long they should cache information from an authoritative source

• The domain administrator’s contact information

• DNS Records
Common DNS Records (Resource Records)

• SOA Record (Start of Authority)
  • Indicates that the nameserver is the best source of info for data within a domain’s zone

• A Record (Address)
  • Directly maps a name to an IP address

• MX Record (Mail Exchanger)
  • Specifies which servers receive email for a domain (and in what order they should be tried)
Common DNS Records (Resource Records)

• NS Records (nameserver)
  – Required
  – Identify which servers are a particular zone’s nameservers
  – Does NOT have to be the same as the zone’s domain
Glue Records: What and Why?

• Solve a circular dependency problem:
  – The TLD delegates DNS requests for “example.com” to the particular authoritative name servers for example.com.
  – But this DNS information is contained within example.com’s nameservers.

• A record that’s served by a DNS server that’s not authoritative for the zone.
Glue Records: How?

• Add IP addresses to your nameservers in your Domain Registrar

• THEN... add NS records AND A records for your authoritative nameservers:

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IN</td>
<td>NS</td>
<td>ns1.example.com.</td>
<td></td>
</tr>
<tr>
<td>IN</td>
<td>NS</td>
<td>ns2.example.com.</td>
<td></td>
</tr>
<tr>
<td>ns1</td>
<td>IN</td>
<td>A</td>
<td>1.2.3.4</td>
</tr>
<tr>
<td>ns2</td>
<td>IN</td>
<td>A</td>
<td>2.3.4.5</td>
</tr>
</tbody>
</table>
Anti-Spam Mechanisms

• SPF Records
  • Identifies which IP addresses are allowed to send an email from a certain domain.

• DKIM Records
  • Uses encryption keys to determine if a sending mail server is who it says it is.

• DMARC
  • Specifies what should happen to email if a SPF and DKIM check fails.
Introduction to BIND

Berkeley Internet Name Domain
• Originally developed at University of California Berkeley
• Maintained and supported by ISC (Internet Systems Consortium)
  – https://www.isc.org/software/bind/
Intro to BIND (con’t)

• Most widely used Domain Name Server Software
• Ported to most flavors of UNIX (including Ubuntu, RHEL, and CentOS)
• Can also be run on Microsoft Windows
Configuring BIND (for CentOS)

First, install BIND with: “Yum install bind”

Main config file: /etc/named.conf

Zone file(s) for Master: /var/named/

Zone file(s) for Slave (Caching): /var/named/slaves
Options {
    listen-on port 53 { any; };
    allow-transfer { 2.3.4.5; };
    recursion no;
};
BIND’s named.conf for Authoritative Name Server

zone “example.com” IN {
    type master;
    file “path-to-zone-file-location”;
};
BIND’s named.conf for Recursive Name Server

Options {
    recursion: yes;
};
A Couple Security Considerations

An Open Resolver is a BAD IDEA

DNS Security Extensions (DNSSEC)
- Digitally signs DNS data so that you are assured its valid. It’s a digital signature,
- No encryption or decryption takes place
- Must be deployed at each step of the lookup process
Recommended Resources

BIND Homepage
• https://www.isc.org/software/bind

O’Reilly’s DNS and BIND
•
• RFCs 920, 1034, 1035, 2308
• & their updates - http://tools.ietf.org/html/

Recommended Resources (con’t)

Website (Intro to DNS): “How does DNS work?”
• [http://cr yp.to/djbdns/intro-dns.html](http://cr.yp.to/djbdns/intro-dns.html)

• Pingdom’s DNS Check Tool: [http://dnscheck.pingdom.com/](http://dnscheck.pingdom.com/)

MX Toolbox (for testing MX and DNS configuration):
Recommended Resources (con’t)

**DNSSEC – What Is It and Why Is It Important?**

This presentation was prepared and presented by David White, Founder of Barred Owl Web.