Linux Network Administration

Domain Name System
COMP1071 - Fall 2020

Concept

- Naming hosts made it much easier to identify them in commands, people work better with names

- Once the networks grew beyond a small number of hosts, managing those names and their addresses by passing around host file information became impractical

- A way of spreading the management of names and addresses transparently and with a minimum of overhead became very important

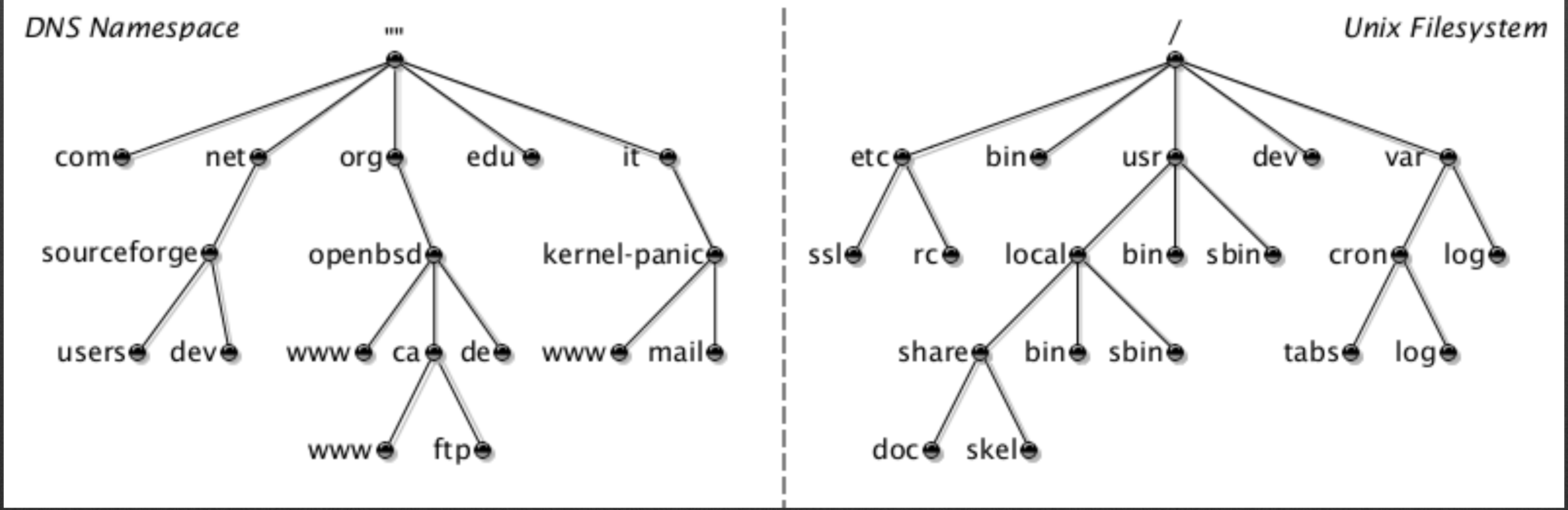
Software

ISC Internet Systems Consortium

- BIND is the current reference implementation of software that allows domain-based management of names and address on the internet
- It is open source, very low overhead, and is actively maintained
- Implements the DNS namespace by defining a protocol for sending DNS resource record queries and responses using UDP on port 53, or TCP using port 53 (multicast DNS uses port 5353 tcp/udp)

Namespace

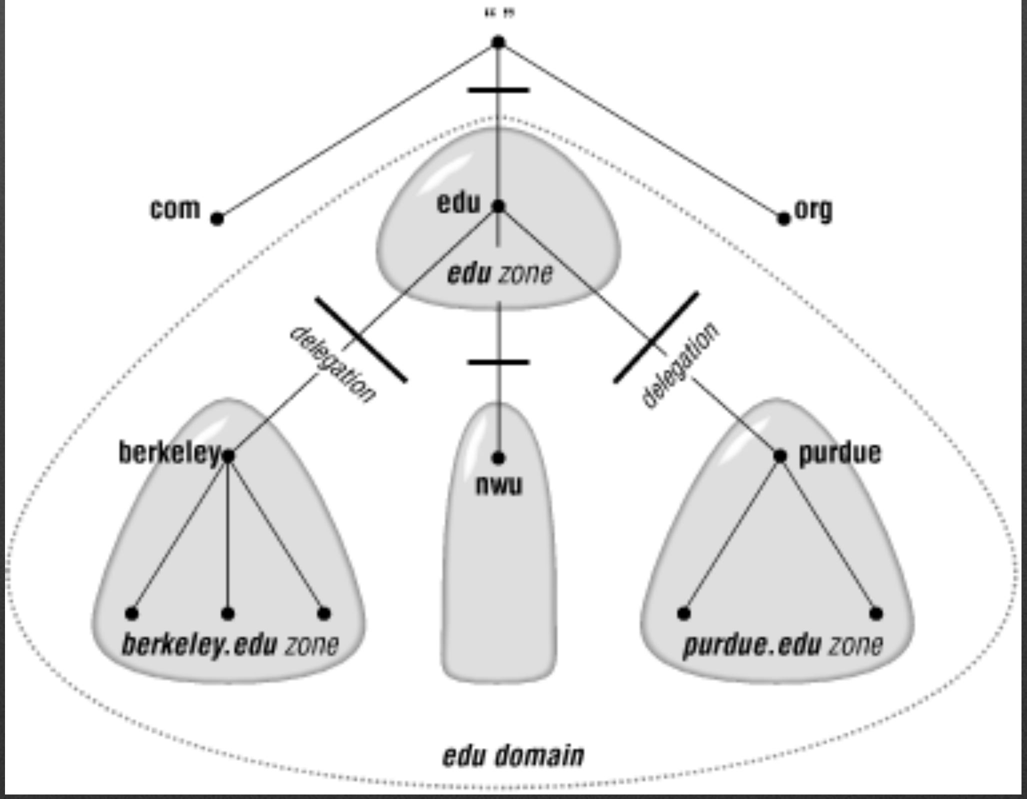
- A hierarchical organization of names, similar to file system organization
- There is a root, represented by a period (.) and the domains attached to the root level are called top level domains (e.g. com, net, org, edu, etc.)
- The complete name of a host including all components up to the root is called the Fully Qualified Domain Name (FQDN)



Delegation

- Root servers only contain information about the top level domains, top level domain (TLD) servers only know about second level domains belonging to their own TLD, and so on

- A domain exists if a domain server has NS records for the domain name specifying one or more name servers, known as delegation



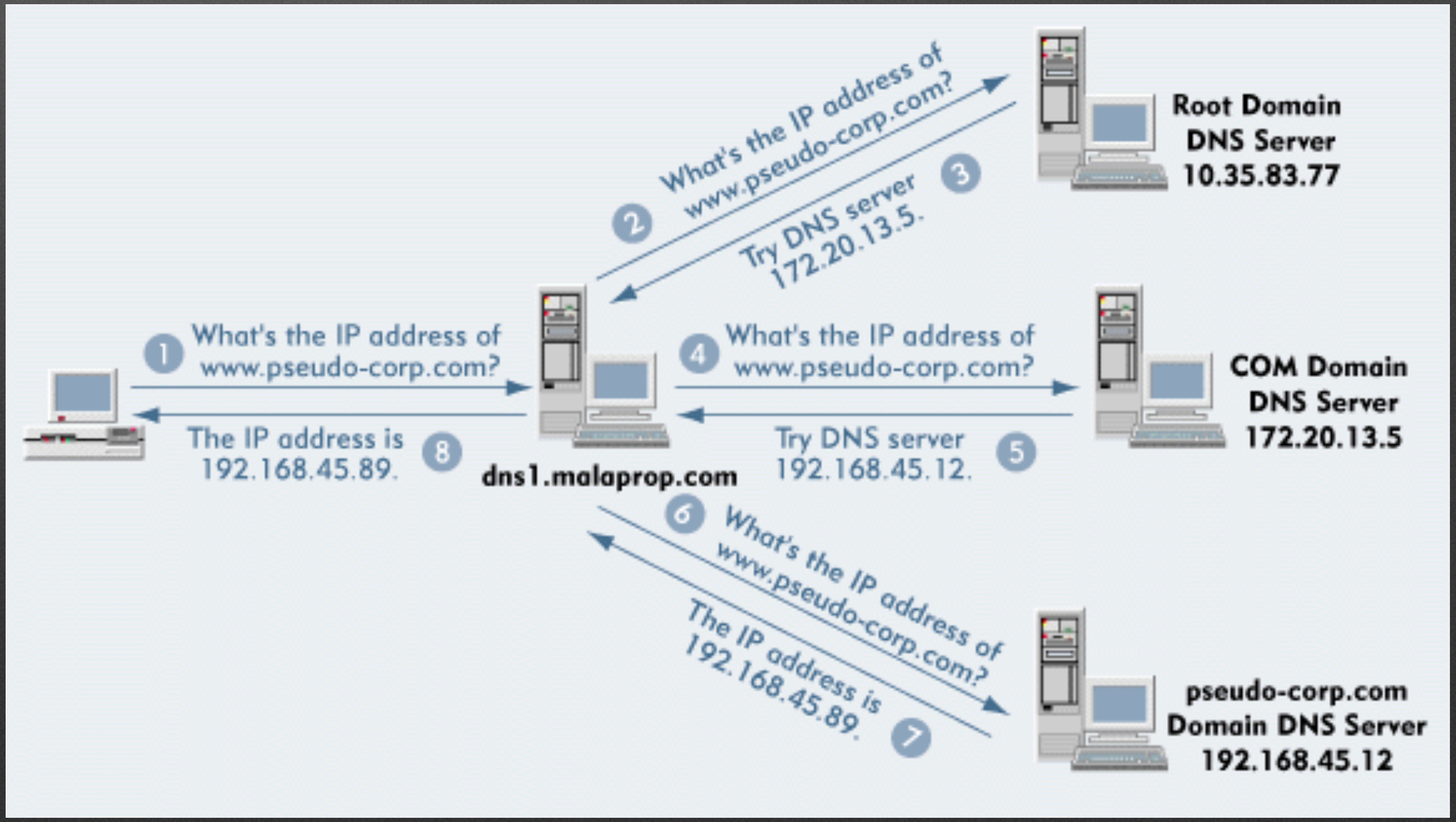
Resolver

- Client software providing transparent, automatic name resolution

- /etc/nsswitch.conf defines the system data sources for various naming services including host naming

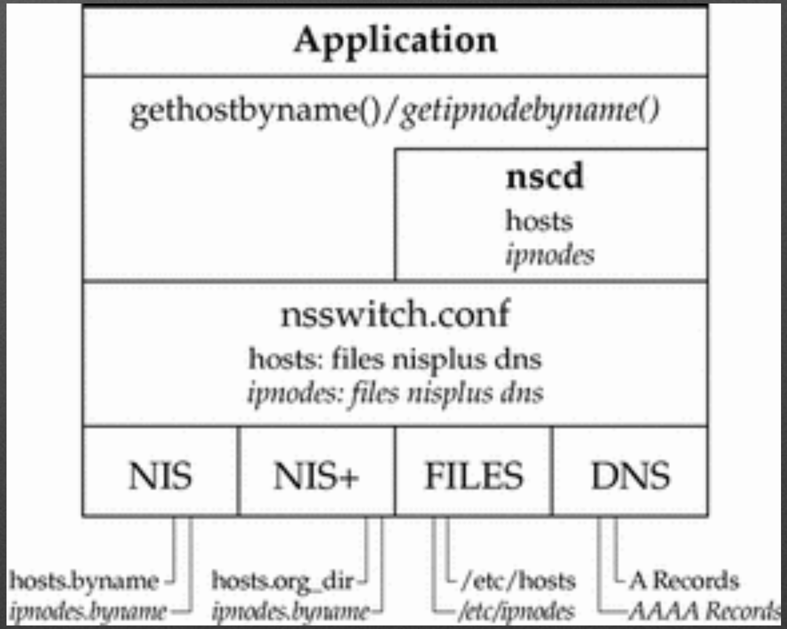
- DNS services and parameters may be in /etc/resolv.conf

- Resolver can look up names in DNS


Root Domain DNS Server 10.35.83.77
2 What's the IP address of www.pseudo-corp.com?
3 Try DNS server 172.20.13.5.
1 What's the IP address of www.pseudo-corp.com?
8 The IP address is 192.168.45.89.
dns1.malaprop.com
4 What's the IP address of www.pseudo-corp.com?
5 Try DNS server 192.168.45.12.
COM Domain DNS Server 172.20.13.5
6 What's the IP address of www.pseudo-corp.com?
7 The IP address is 192.168.45.89.
pseudo-corp.com Domain DNS Server 192.168.45.12

nsswitch

- /etc/nsswitch.conf defines data sources for information required by various programs
- Several data types are defined
- The hosts line controls where we look up host names and ip addresses



/etc/resolv.conf

- Used by resolvconf to find DNS data in many Linux distros
- nameserver directive specifies where to send DNS queries
- search line specifies domain names to try appending to names that fail to look up on their own
- Automatically updated by ifup, dhclient, resolvconf, netplan, etc. - systemd-resolved monster keeps the filename but it is a link to systemd-resolved's own version of the file
- Can be built from multiple interface configuration definitions (interfaces file(s)), applied according to /etc/resolvconf/interface-order

systemd-resolved

- Systemd monster has consumed the straightforward resolver configurations of the past

- systemd-resolved service has its own config files and rules, and includes windows-style magic names

- When using systemd-resolved, names hard-coded into the daemon will override your configuration and you have a multitude of name lookup services mixed in with your resolver - name service switch no longer provides sure control of name service

- systemd-resolved works fine for typical business desktops

- System administrators may choose to just turn it off and statically define name service for reliability and maintainability, or compatibility with services such as VPNs

Querying DNS

- nslookup is tool to retrieve DNS records, defaults to looking for hostnames (A records) or IP addresses (PTR records)
- dig is an alternate tool providing more information and options but isn’t always available
- nslookup [-querytype=RecordType] key [server]
- nslookup provides details about the lookup activity
- The host command allows for simplified output showing just the results of the lookup and works with multiple data sources
- getent hosts also allows name lookups regardless of what data source is being used

BIND

- bind9 is current version and package name, install with apt-get

- Installs some tools and the /etc/bind default configuration files

- Typically the dnsutils package is also installed to provide nslookup, dig, and nsupdate (bind9-host provides the host command)

- Supports primary, secondary, forwarding and caching servers

Primary Server

- Created by specifying type master in named.conf.local file
- Has source zone file for a domain where the data is maintained, specified with file directive in named.conf.local
- May provide zone data to secondary servers as well as other clients using allow-transfer keyword in named.conf.local
- Provides authoritative data for the domain

Secondary Server

- Created by specifying type slave in named.conf.local file
- Holds copy of zone file for a domain, specified with file keyword in named.conf.local
- Gets zone data using transfer from primary using master keyword in named.conf.local
- Secondaries poll the primary to check for updated serial number, and can also get notifications of change from the primary
- Provides authoritative data for a domain as long as it can stay up to date

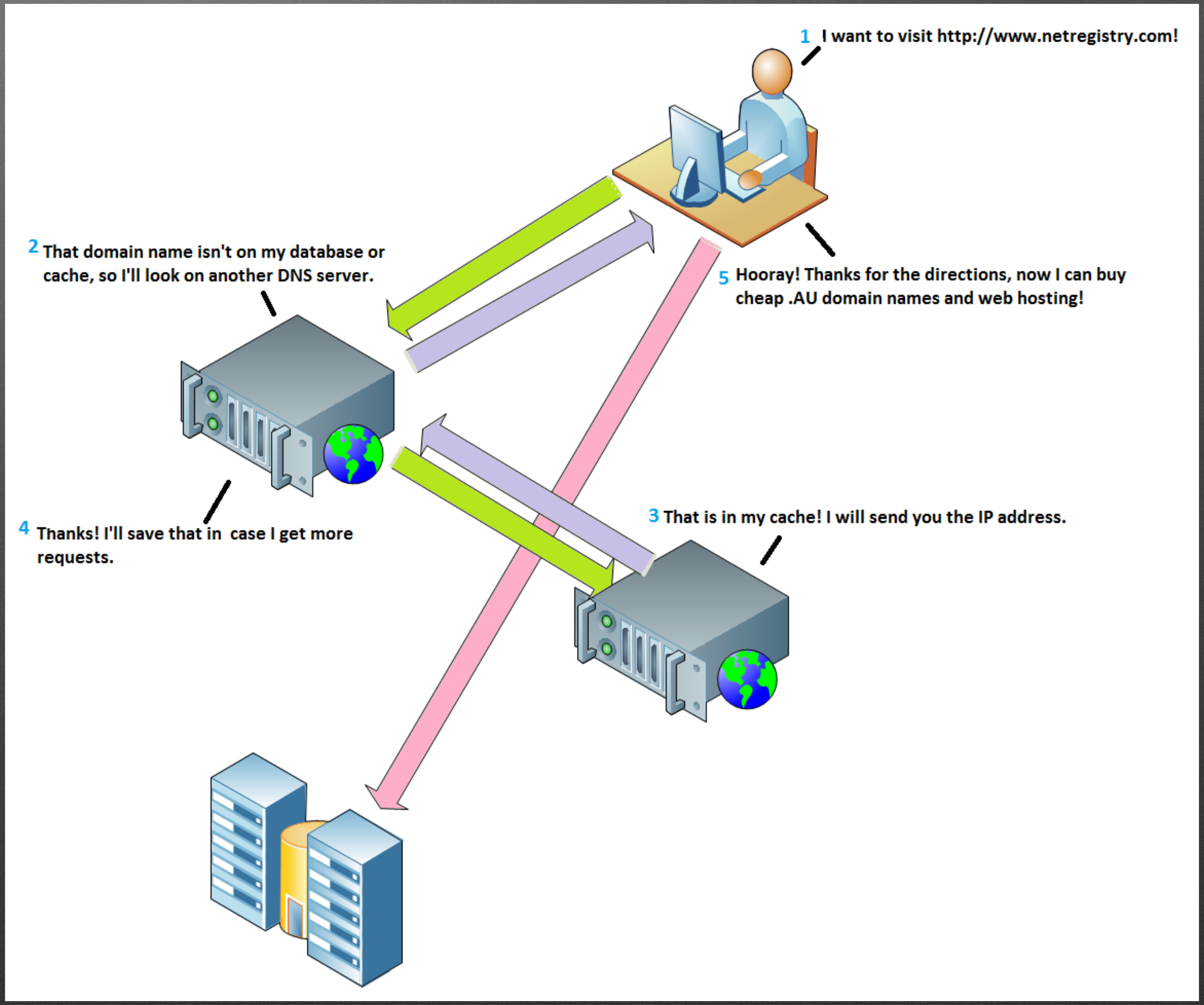
Forwarding Server

- Sends all DNS requests to another server
- Caches results
- Will not do recursive searches
- Used to control DNS traffic within an organization
- Provides non-authoritative data for domains

Caching Server

- Any server that saves responses and does recursive searches

- Small networks do caching on their primary and secondary servers and do not use forwarding servers



1 I want to visit http://www.netregistry.com!

2 That domain name isn't on my database or cache, so I'll look on another DNS server.

3 That is in my cache! I will send you the IP address.

4 Thanks! I'll save that in case I get more requests.

5 Hooray! Thanks for the directions, now I can buy cheap .AU domain names and web hosting!

BIND Configuration Directory

- BIND keeps its configuration files in /etc/bind and it contains 3 types of files we are interested in

- named.conf files configure the bind daemon and specify the domain names and which zone files provide records for those domains

- Key files used for DNS validation, maintained by apt upgrades

- Zone files hold DNS records

BIND Configuration Files

- named.conf includes other conf files
- named.conf.options sets daemon options
- named.conf.default-zones provides zone data for RFC-defined zones
- db.root provides DNS root server records
- localhost provides DNS data for localhost

Configuring Domains Served

- The named.conf.local file defines local stored zones (ones we are the primary or secondary for)

- For each domain, there is a zone stanza which specifies domain name, server type, and zone data file

- May also specify who can transfer zone data (if this is the primary), or who the zone data primary is (if this is a secondary)

Zone Data File

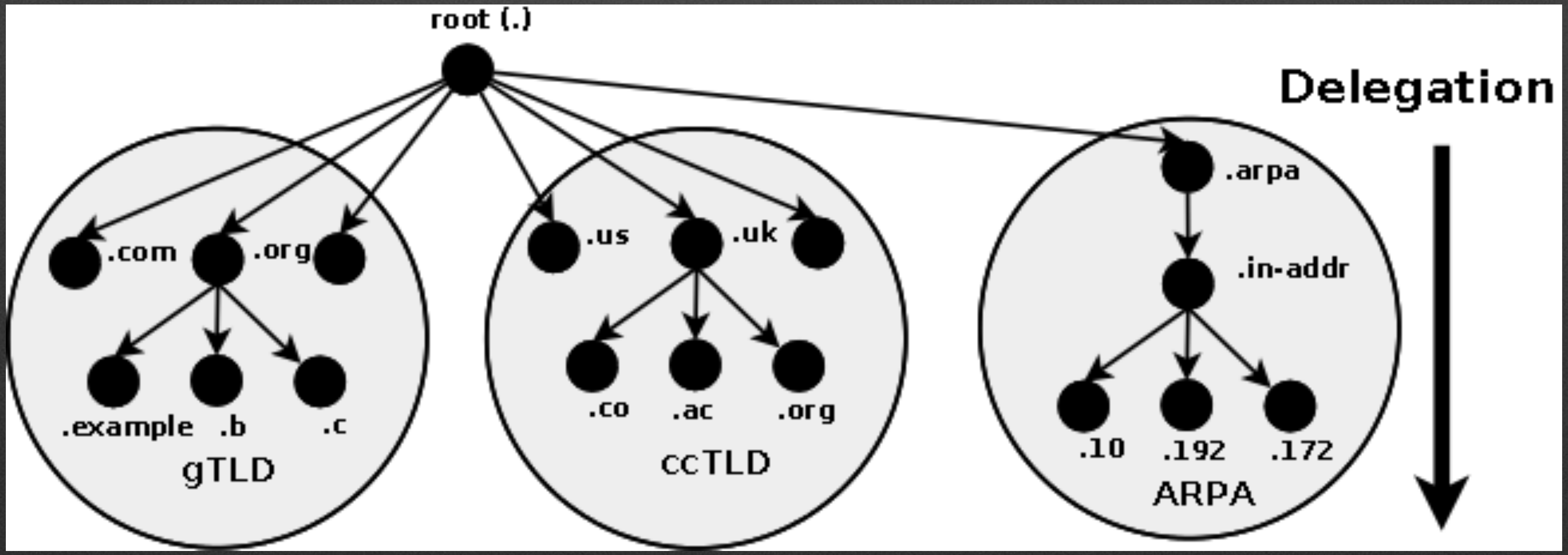
- Holds records for a zone, must have a Start Of Authority (SOA) record and at least one Name Server (NS) record
- Each record has a name, class, type, and data separated by the tab character
- The class we always use is IN, which means internet class record
- The name is also called the key and is the thing we are looking up when we request a record, along with having to specify a record type
- The data is what we get back and is record type specific

Record Types

- Start Of Authority (SOA) specifies global parameters for the zone
- Name Server (NS) specifies the names of the servers which are authoritative for the zone
- Address (A for IPV4 or AAAA for IPV6) specifies an address for a name
- Canonical Name (CNAME) specifies the target name for an alias
- Mail Exchanger (MX) specifies a host that handles email for a name
- Pointer (PTR) specifies a name for an address
- Location (LOC) specifies a latitude and longitude for a name

Reverse Lookups

- Allows looking up an address and getting the name for it
- Uses the address as the key and looks in the reserved domain name in-addr.arpa.
- Subdomains are created using the network number of the address block being served
- Names in the zone file are the host numbers on that network, with the FQDN being the data for those names



Syntax Checking

- named-checkzone can check the syntax for a zone file (e.g. named-checkzone zone zonefile)

- named-checkconf can check a conf file for syntax errors (e.g. named-checkconf conffilename)

- Neither can identify logic errors or missing information

- If both of these declare you have no errors, and things still don’t load, check your log files for more error information

Service Management

- Like most Linux services, the bind service can be managed with the service command (e.g. service bind9 start|stop|restart|reload)

- rndc is a command included with BIND that can send messages to the running service (e.g. rndc reload|stats|flush|status)

- rndc is recommended as it is less disruptive to a running server than using the service command

Log Files

- BIND logs errors and startup information to the syslog daemon by default

- In Ubuntu, the default place syslog sends messages from daemons like BIND is the /var/log/syslog file

- Like most files in /var/log, this file is automatically aged