Overview of Services

siriuskoan

Outline

- DNS
- Mail
- LDAP

DNS

siriuskoan & shenchris

DNS - Background Knowledge

- **IP Address** - A numerical label to every device connect to the Internet
- **Domain Name** - A name that maps to a numeric IP address
- **DNS** - Like phone book, it maps domain name to IP address

DNS - Background Knowledge

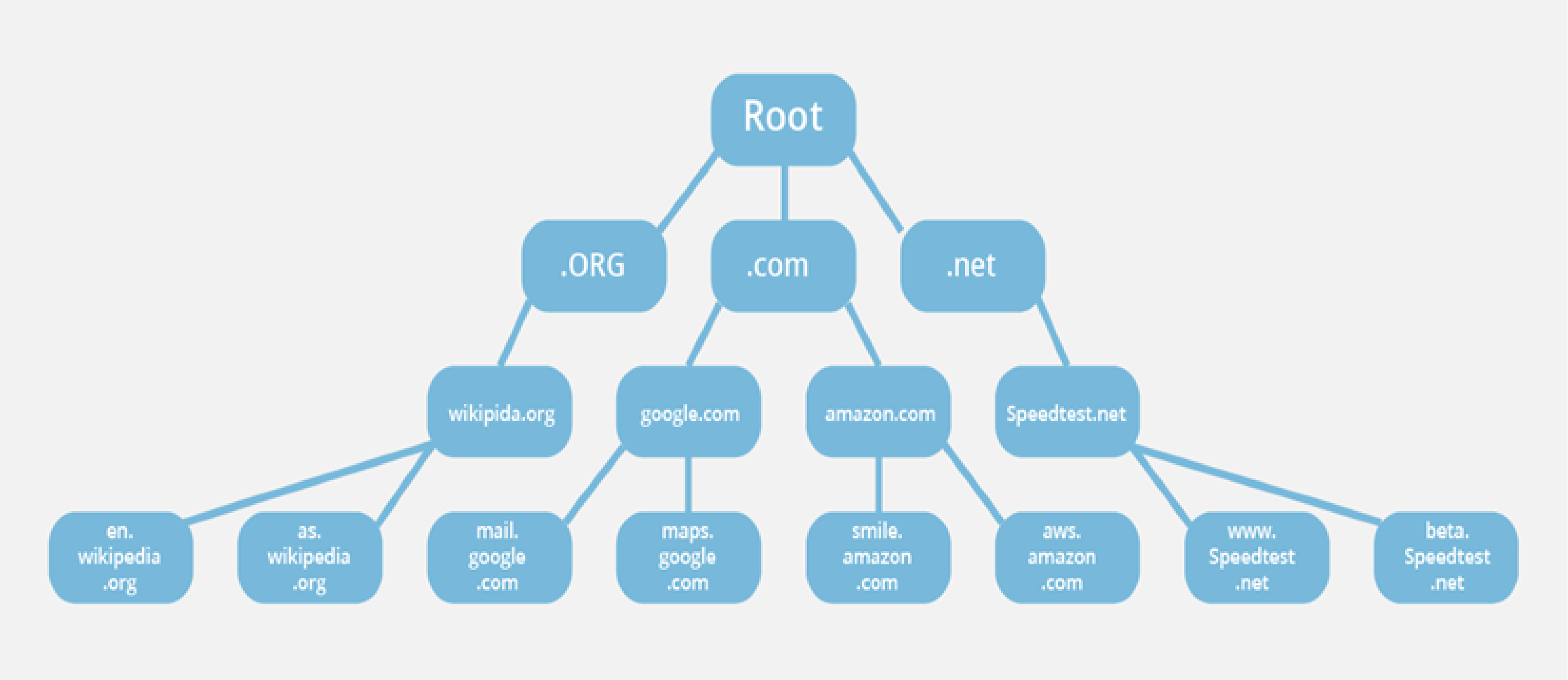
For example

- `www.hs.ntnu.edu.tw` -> `203.68.92.132`
- 師大附中 -> 台北市大安區信義路三段143號

`nslookup` and `dig` are useful tools that can check DNS records.

DNS - How It Works

DNS is hierarchical and decentralized (prevent single point failure).



DNS - How It Works

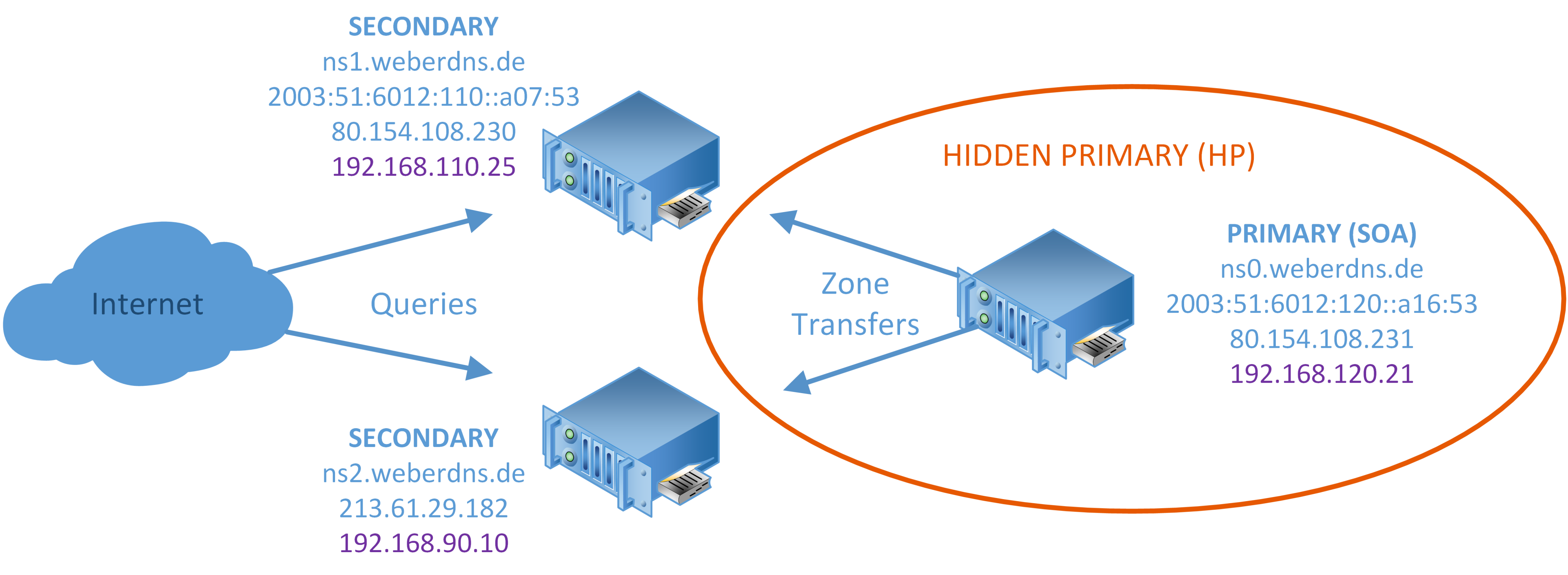
- **Root Nameserver** - First stop. It directs the query to a TLD nameserver
- **TLD (Top Level Domain)** - There are many TLD (`.com`). It maintains information under a common domain extension.
- **Authoritative Nameserver** - Last stop in the query. It returns the IP address or alias for the requested domain name back to the DNS resolver.
- **Resolver** - Agent between a client and a DNS nameserver.

DNS - How It Works

Two types of servers

- Master - Main server, the real one to do name resolution and get data from disk.
- Slave - It gets data from master server periodically.

DNS - How It Works



DNS - Record Types

- `A` - domain name -> IPv4 address
- `AAAA` - domain name -> IPv6 address
- `NS` - zone name -> domain name of NS server
- `MX` - domain name -> domain name of mail server and precedence
- `CNAME` - alias domain -> real domain
- `SOA` - domain name -> domain information

DNS - DNSSEC

DNS query will NOT verify the response

DNSSEC signs the response to detect fake response

Mail

siriuskoan

Mail - Protocols

There are three important protocols

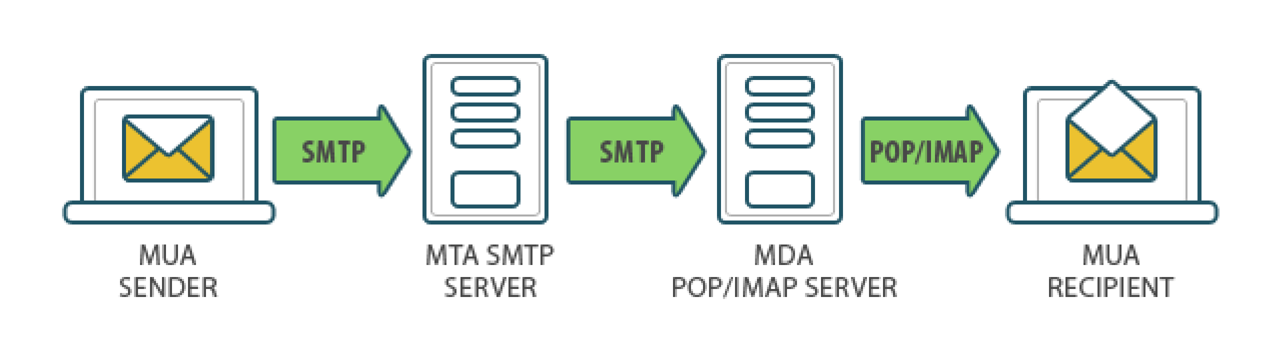
- `SMTP` - It is used to send and receives mails through mail servers
- `IMAP` - It is used to allow users get their mails from anywhere
- `POP3` - It is used to allow users get their mails from anywhere

They can all be encrypted and become `SMTPS`, `IMAPS` and `POP3S`

Mail - MUA / MTA / MDA / MRA

- `MUA` - Mail User Agent. It is a software between users and mail server
- `MTA` - Mail Transfer Agent. It is so-called "mail server". It receives and sends (relays) emails from or to other mail servers
- `MDA` - Mail Delivery Agent. It decides what to do to emails
- `MRA` - Mail Retrieval Agent. It gets email from remote server and allows users to access their mailboxes

Mail - MUA / MTA / MDA / MRA



Mail - Open Relay

A mail server can sends (relays) mails to other mail servers when it finds that it cannot handle them.

However, if a mail server relays all mails to other mail servers, it is considered to be an open relay server and will be **banned**.

Mail - Greylisting

Do temporarily rejection

Mail - Security

An email is just a text file

Spoofing mail is easy to make, we have to prevent this

Mail - SPF (Sender Policy Framework)

The mechanism makes all domain has one DNS record that records which IP addresses its mail servers have

However, if the mail is intercepted and the content is changed by a bad guy, SPF is useless

Mail - SRS (Sender Rewriting Scheme)

If the mail server want to forward the mail, SPF test will fail

SRS can rewrite the sender and make it pass SPF test. After passing SPF test, the destination server can convert it back to original sender and show it to receivers

Mail - DKIM (DomainKeys Identified Mail)

The mechanism encrypts some of the headers and content and add its hash to header

In this way, if the mail is modified by others, DKIM can detect it

However, the sender shown on MUA is `header.from`, and SPF and DKIM check `smtp.MailFrom`, so this can still be spoofed

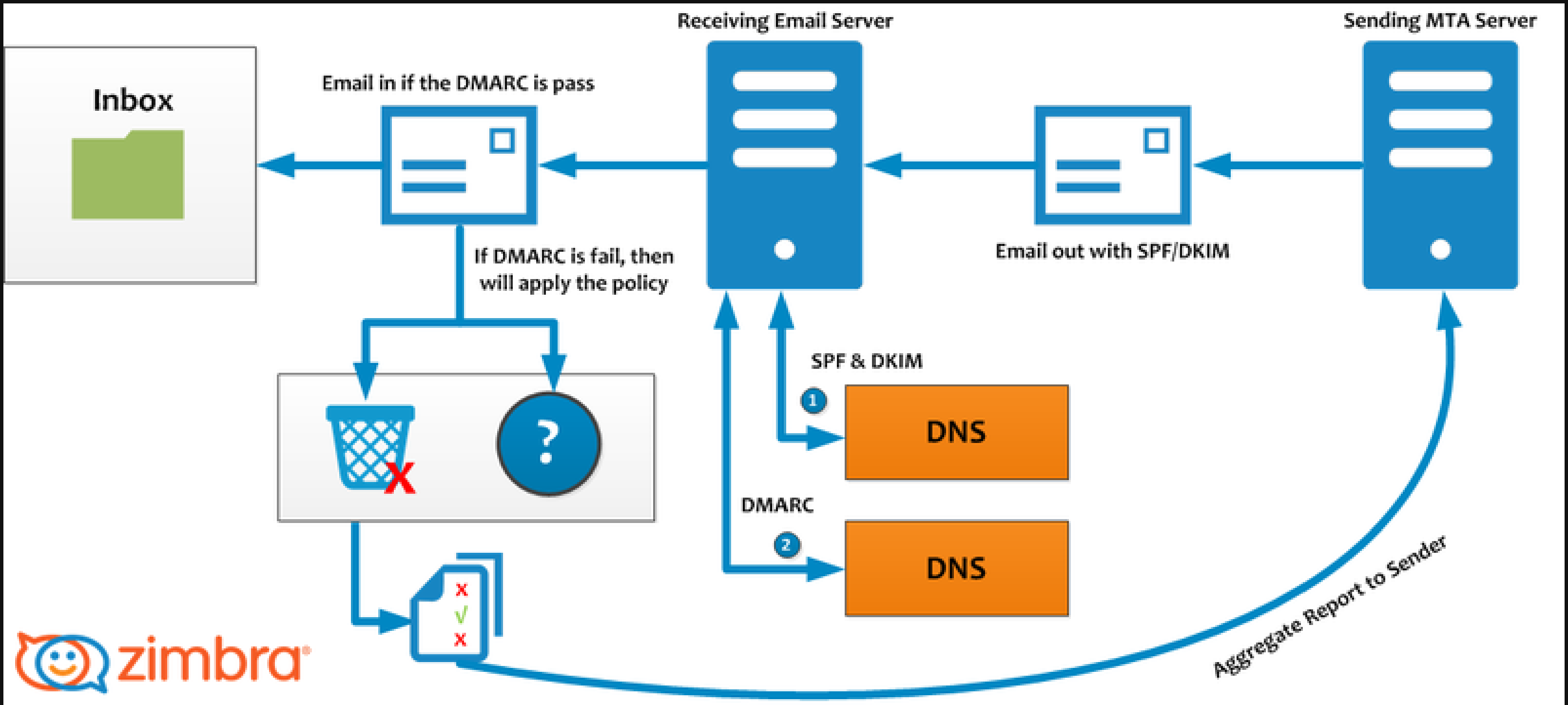
Mail - DMARC

DMARC stands for Domain-based Message Authentication, Reporting and Conformance

It will check
whether `header.from` and `smtp.MailFrom` are the same, and the process is called **alignment**

It will also check whether SPF and DKIM are passed

Mail - Security



LDAP

siriuskoan

LDAP

Suppose that your team are system admins, and the system you are responsible for is large

Your team should be able to login to the server, so all of them have accounts on all these servers

LDAP

LDAP, standing for Lightweight Directory Access Protocol, is a good system to solve this problem

LDAP stores all user data in one server, and other servers can get users data from it to do authentication or get users' home directories

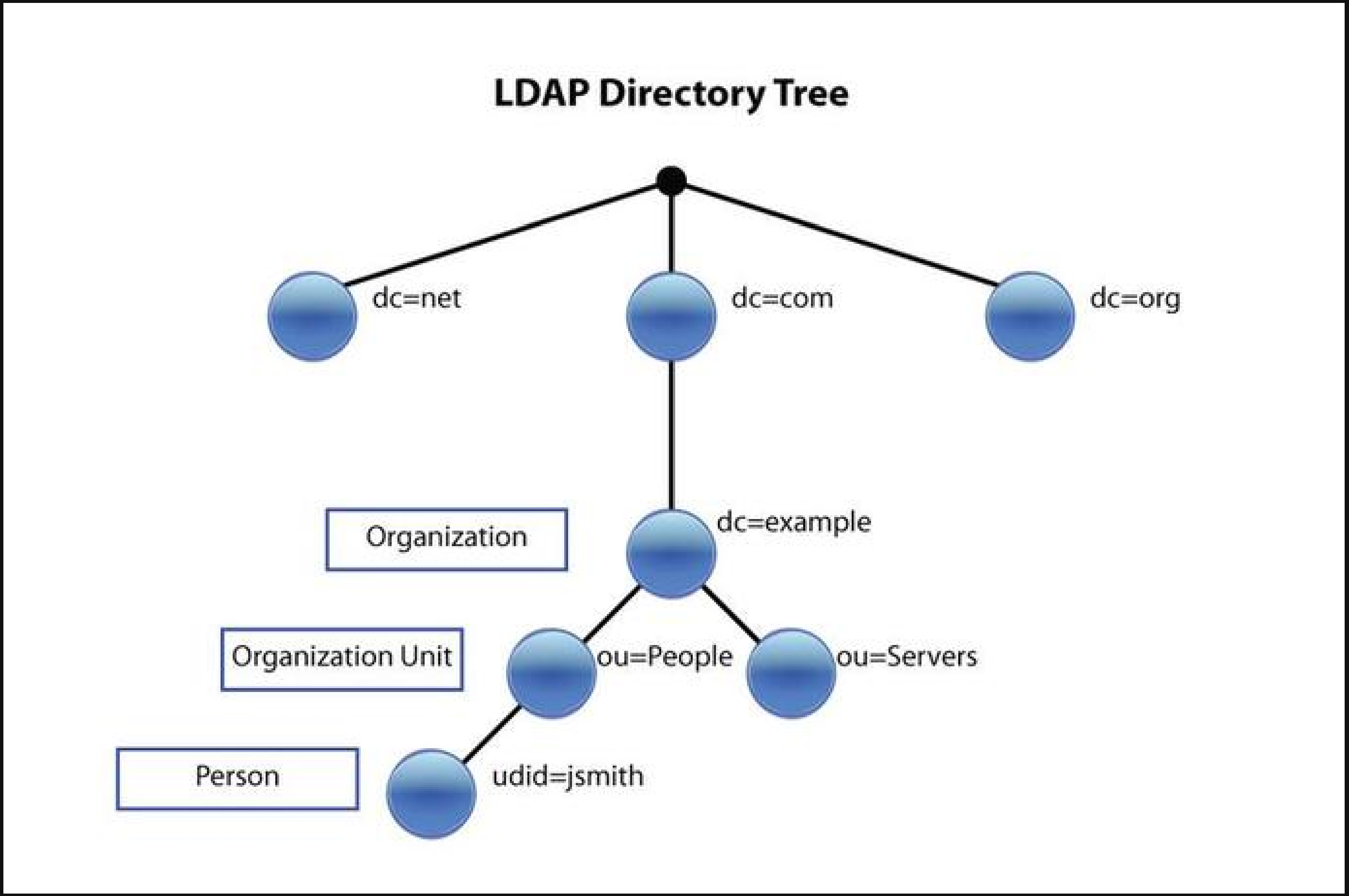
LDAP - How It Works

LDAP is hierarchical as well.

It has DIT (Directory Information Tree), and it contains `dc`, `ou`, `cn`, `o`, `c`, etc.

- `dc` - Domain Component (`edu`, `tw`, `com`, ...)
- `ou` - Organization Unit (`People`, `Group`, ...)
- `cn` - Common Name (Username)
- `o` - Organization name
- `c` - Country name

LDAP - How It Works



LDAP - How It Works

For example, my DN (Distinguish Name) in CNMC may

`siriuskoan,ou=People,dc=siriuskoan,dc=cnmc,`

A node stores many things, like real name, phone number, email, home directory, `objectClass`, etc.

LDAP - How It Works

`objectClass` is an entry template, just like database schema

It defines what an entry should contain.

For example, `Person` defines an entry must contain `sn` (surname) and `cn` (common name), and it can contain password, phone number, etc.

LDAP - How It Works

LDIF stands for LDAP Interchange Format

It is the standard text file format for storing LDAP config information and directory content

LDAP - How It Works

For example, we have two LDAP entries

```
# siriuskoan, People, cnmc.tw
dn: cn=siriuskoan,ou=People,dc=cnmc,dc=tw
objectClass: person
sn: koan

# shenchris, People, cnmc.tw
dn: cn=shenchris,ou=Person,dc=cnmc,dc=tw
objectClass: person
sn: shen
```