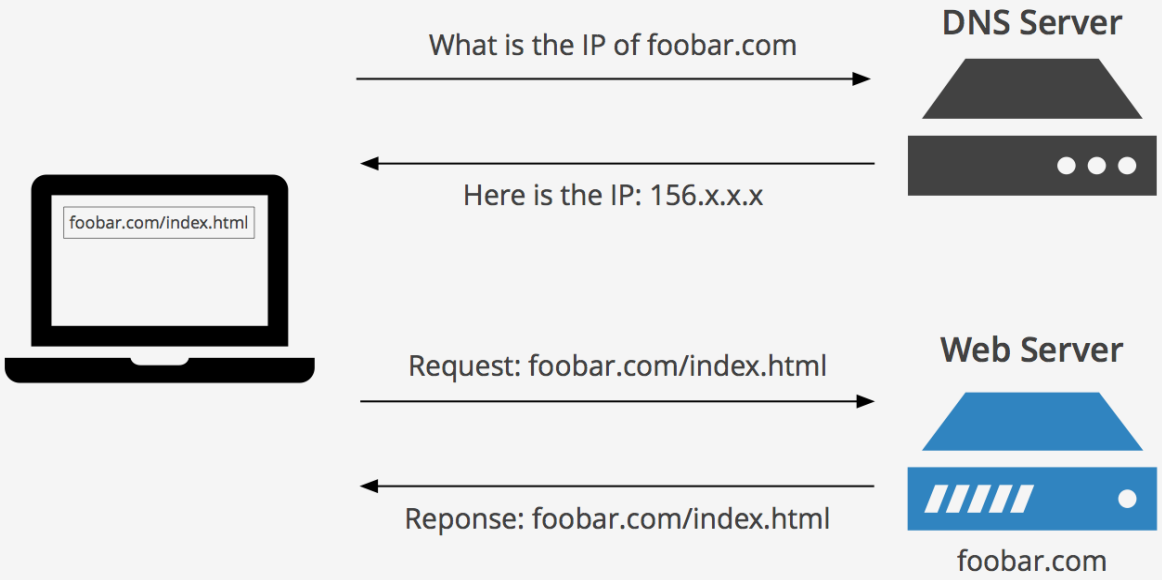
Conceitos sobre DNS



Quando você digita uma URL no navegador, como o seu computador encontra um endereço de IP para se conectar a um servidor?

O DNS é dividido em níveis de domínios, cada domínio representa um “pedaço” distinto e é gerenciado por uma única entidade administrativa, delegando, assim, sua responsabilidade.

Por isso dizemos que o DNS é similar a uma árvore, uma “árvore de Domínios”.

o domínio é o nome único usado para localizar o endereço/apontamento de destino.

Este é o nome do host. É o nome de um servidor específico NO Domínio.

Esta parte aqui é o nome do domínio.

Isto é o que chamamos de nome de domínio totalmente qualificado (FQDN) porque todas as partes estão presentes. Este sim é o real nome do site!

www.hfhealthclub.com

Este final é o que chamamos de nome de domínio de nível alto. Há diferentes domínios para diferentes propósitos: .com, .org, .gov e também para países diferentes: .ar, .uk, .jp

Os chamados TLDs (Top level domains). são bastante conhecidos, sendo os principais:

com: Organizações comerciais

gov: Organizações governamentais

edu: Instituições educacionais

org: Organizações não comerciais

net: Serviços de rede e comunicação

biz: Área administrativa, e negócios “bussiness”

Acima dos domínios de primeiro nível temos os códigos dos países chamados de **CcTLDs**

(country code Top Level Domains)

Dividem os domínios em países, como por exemplo **“.br”** para hosts de origem no Brasil **“.ar”** para Argentina, **“.ch”** etc...

Controladores

- ARIN: American Registry Internet Numbers.
- LACNIC: Latin American and Caribbean Network Information Center.
- AFRINIC: African Network Information Center
- APNIC: Asian and Pacific Network Information Center
- RIPE: Réseaux IP Européens (RIPE NCC – Réseaux IP Européens Network Coordination Centre)

Controladores

Esses controladores são responsáveis pela designação dos Nomes de Domínio para seus respectivos registros, subdivididos por região.

O controlador responsável pelo ".br" é o LACNIC e parte de seus servidores estão localizados em São Paulo, especificamente na FAPESP trabalhando em parceria com o NIC.br um dos órgãos de gestão da internet no Brasil.

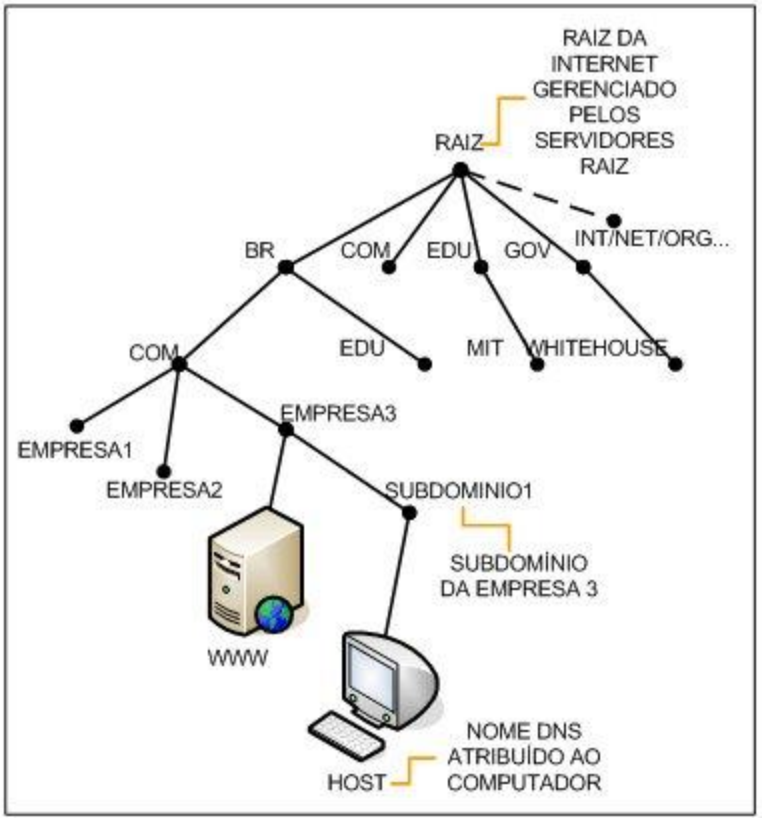
Núcleo de Informação e Coordenação do Ponto BR

Registro de Domínios

Registro de Domínios

Pense em um DNS como uma árvore de cabeça para baixo.

A tradução entre nomes de domínios e endereços de IP é possível graças a hierarquia de servidores de nome.



Hierarquia de Domínios

1. **Começamos com os servidores raiz:** Eles possuem os nomes de domínios de alto nível **(Cctld ou tld)** aqui será verificado qual deles utilizar na busca do endereço **fiap.com.br** para identificar o país em que estamos, neste caso **.br**

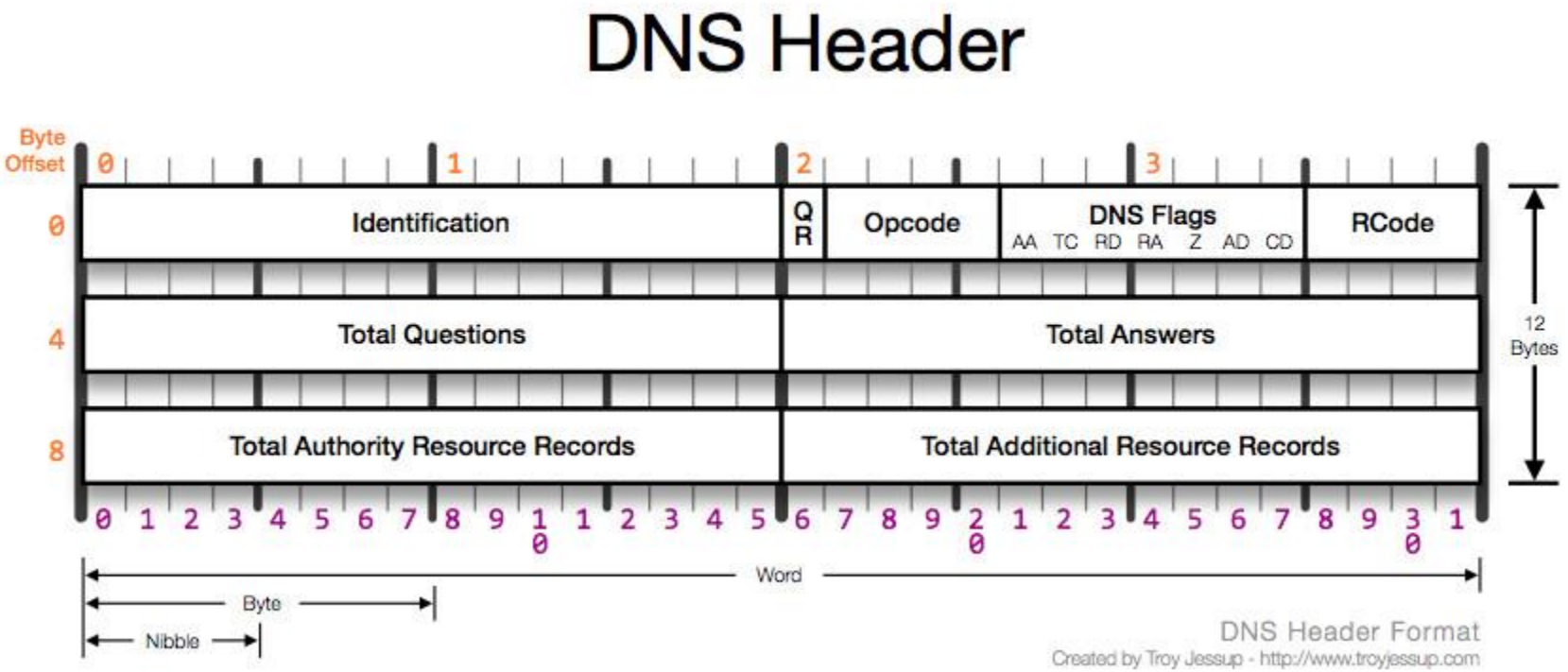
2. **A seguir vem o tld .com:** Os servidor de alto nível .com saberá tudo sobre os domínios .com, ele percebe que o que queremos na verdade é **fiap.com.br** então ele envia essa informação.

3. O servidor destino será o NS da fiap que conhece todos os seus hosts e subdomínios;

4. **E aqui estamos:** Ao receber os apontamentos responsáveis pelo site o resto é função do servidor de conteúdo;

Cabeçalho de uma requisição de DNS

O protocolo em si é relativamente leve, trafegando em UDP temos 512 bytes em uma consulta padrão, consultas maiores como transferência de zona são executadas em **TCP,** verifique a referência no final da aula para mais detalhes;



Tipos de registros

O processo de resolução de nomes é baseado em tipos de registros com finalidades específicas, alguns deles são extremamente relevantes para arquitetura de sistemas;

Type	Value (decimal)	Defining RFC	Description	Function
A	1	RFC 1035 [1]	Address record	Returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host, but also used for DNSBLs, storing subnet masks in RFC 1101, etc.
AAAA	28	RFC 3596 [2]	IPv6 address record	Returns a 128-bit IPv6 address, most commonly used to map hostnames to an IP address of the host.
CNAME	5	RFC 1035 [1]	Canonical name record	Alias of one name to another: the DNS lookup will continue by retrying the lookup with the new name.

Tipos de registros

FIAP

IPSECKEY	45	RFC 4025	IPsec Key	Key record that can be used with IPsec
MX	15	RFC 1035[1]	Mail exchange record	Maps a domain name to a list of message transfer agents for that domain
NS	2	RFC 1035[1]	Name server record	Delegates a DNS zone to use the given authoritative name servers
PTR	12	RFC 1035[1]	Pointer record	Pointer to a canonical name. Unlike a CNAME, DNS processing does *NOT* proceed, just the name is returned. The most common use is for implementing reverse DNS lookups, but other uses include such things as DNS-SD.
SOA	6	RFC 1035[1] and RFC 2308[9]	Start of [a zone of] authority record	Specifies *authoritative* information about a DNS zone, including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone.
SPF	99	RFC 4408	Sender Policy Framework	Specified as part of the SPF protocol as an alternative to storing SPF data in TXT records, using the same format. It was later found[10] that the majority of SPF deployments lack proper support for this record type, and support for it was discontinued.[11]
SRV	33	RFC 2782	Service locator	Generalized service location record, used for newer protocols instead of creating protocol-specific records such as MX.
TXT	16	RFC 1035[1]	Text record	Originally for arbitrary human-readable *text* in a DNS record. Since the early 1990s, however, this record more often carries machine-readable data, such as specified by RFC 1464, opportunistic encryption, Sender Policy Framework, DKIM, DMARC, DNS-SD, etc.

Ferramentas de resolução de nomes

Apesar do uso tradicional o NSLookup não é mais a recomendação como solução para processos de consulta, A organização que mantém o código do nslookup, Internet Systems Consortium (ISC), declara isso, é possível encontrar essa nota nas versões recente do próprio nslookup:

```
Note: nslookup is deprecated and may be removed from future releases.
Consider using the 'dig' or 'host' programs instead. Run nslookup with
the '-sil[ent]' option to prevent this message from appearing.
```

O DIG é uma alternativa mais completa a consulta e resolução de nomes:

https://linux.die.net/man/1/dig

Recomendação: A página https://cheatography.com/tme520/cheat-sheets/dig-english/ possui um ótimo *cheat sheets* sobre o utilitário dig:

Ferramentas de resolução de nomes

FIAP

Syntax

dig [@server] [-b address] [-c class] [-f filename] [-k filename] [-m] [-p port#] [-q name] [-t type] [-x addr] [-y [hmac:]name:key] [-4] [-6] [name] [type] [class] [query-opt...]

Config

Tired of always typing the same options ? Create a Run Control file for dig.	`vi $HOME/.digrc`

```
$ cat $HOME/.digrc
+noall +answer
```

List specific types of RRs (Resource Records)

List address records	`dig -t A tme520.net`
List aliases	`dig -t CNAME tme520.net`
Find who manages a domain	`dig -t SOA tme520.net`
List mail servers	`dig tme520.net MX`
List name servers	`dig tme520.net NS`
List any type of Resource Record	`dig tme520.net ANY`

There are about 40 DNS Resources Records types, but you only have to know 5 of them:

- **A** : Address record (IPv4); AAAA for IPv6,
- **CNAME** : Canonical Name. Aliases to A or AAAA records,
- **SOA** : Start Of Authority: primary name server, email of the domain admin, domain serial number, and timers relating to refreshing the zone,
- **MX** : Mail eXchange. Points to a mail server,
- **NS** : Name Server (a DNS).

Output sections

HEADER	Displays the dig command version, the global options used, the type of operation (opcode), the status of the operation (NOERROR) and the message id (necessary to match responses to queries).
QUESTION	This is your input, the question that has been asked to the DNS.
ANSWER	The 2nd field is the time in seconds that the record may be cached (0 = don't cache), the 3rd field is the class (Internet (IN), Chaos (CH), Hesiod (HS)...), the 4th is the type (A, NS, CNAME, MX...) and the 5th, the IP.
AUTHORITY	This section contains the DNS name server that has the authority to answer your query (type: NS, Name Server).
ADDITIONAL	The additional section carries Resource Records related to the RRs from the other sections.
STATISTICS	Displays the time it took to get an answer, the IP of the DNS server used, the date and size of the message.

If you ever get confused about whether or not *dig* found any result for your query, check the ANSWER field from the header; if it's at 0, your query returned no proper answer.

Batch mode: multiple queries in one go

Using a list	`dig -f names.list`
Using several arguments	`dig centos.org MX +noall +answer suckless.org ANY +short`

Batch mode takes a filename as input; the file must be plain text and contain one domain per line:

```
$ cat names.list

redhat.com
ubuntu.com
perdu.com
```

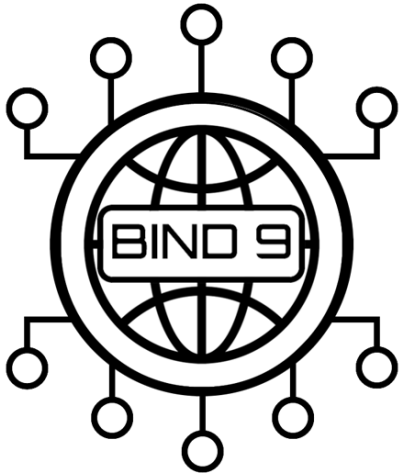
Make that DNS talk !

Display only the ANSWER section	`dig opensuse.org +noall +answer`
Activate the short output	`dig perdu.com +short`
Reverse DNS (get name from IP)	`dig -x 208.97.177.124`
Use a specific DNS server	`dig @8.8.4.4 redhat.com`
Display the name resolution path	`dig google.com +trace`
Request a zone transfer	`dig microsoft.com AXFR`

A zone transfer is a mechanism allowing an administrator to replicate DNS databases across a set of DNS servers. There are two methods: full (aka AXFR) and incremental (aka IXFR). Zone transfers were often used by people wanting to retrieve a list of all the Resource Records of a DNS server. Nowadays, most servers will refuse your request, mostly for security reasons.

Serviços de DNS (Linux Like)

Naturalmente existem várias implantações de serviços de resolução de nomes com base em arquiteturas open source, a mais tradicional delas é provavelmente o Bind da ISC: https://www.isc.org/bind/



Serviços de DNS (Linux Like)

Existem outras alternativas com finalidades específicas como o roteamento simples de consultas para “NS” distintos, ou serviços avançados como os serviços de **Service Discovery**

Solução de DNS baseada em containers voltado para integração com micro serviços;

dnsmasq

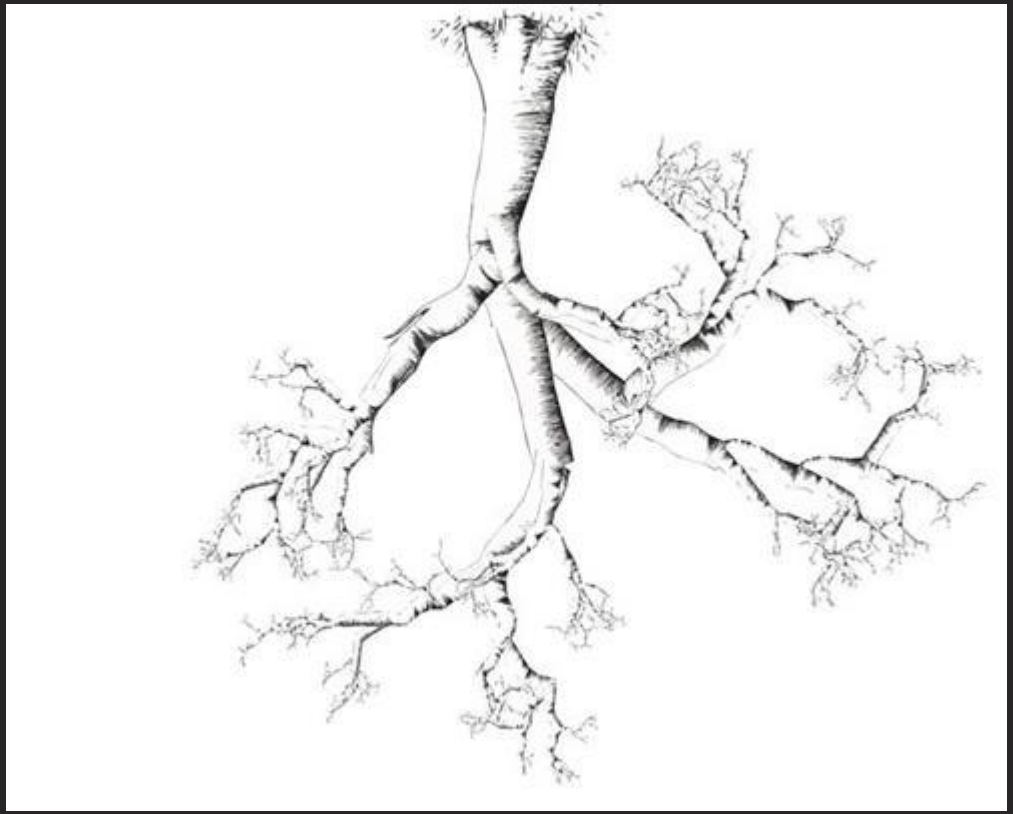
Solução simples que permite encaminhar o processo de resolução de nomes de acordo com o domínio utilizado;

Projeto que implementa o conceito de Service Discovery e Service Register no processo de resolução de nomes (Leia a referência da próxima página);

Recomendação de Leitura

*Boa parte das referências foram extraídas do ótimo artigo **"A DNS Primer"** publicado por Daniel Miessler em sua página de conteúdo:*

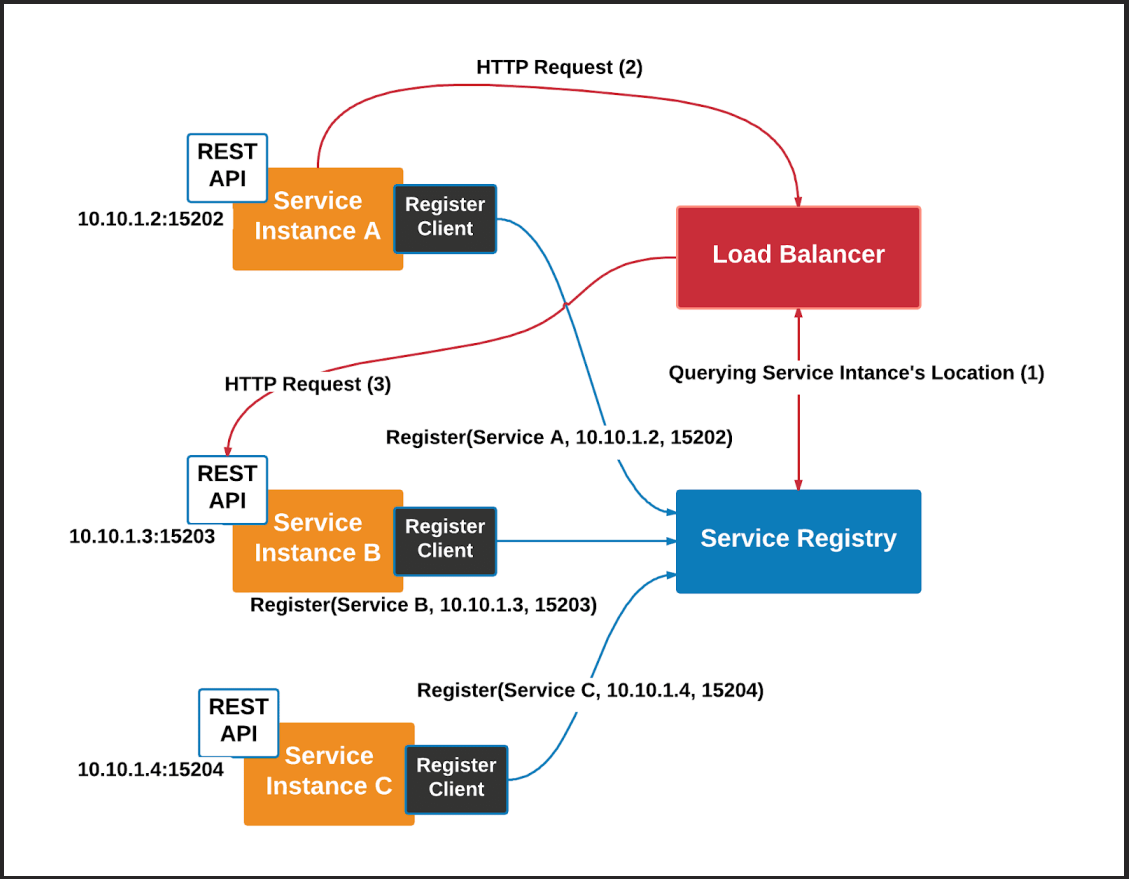
https://danielmiessler.com/study/dns/



Link do artigo para leitura:
https://danielmiessler.com/study/dns/

Recomendação de Leitura

O artigo publicado por https://medium.com/@jamesemyn no medium explica o conceito de Service Discovery e como isso se aplica em arquiteturas modernas de serviços como no exemplo ao lado



Link do artigo para leitura:

https://medium.com/@jamesemyn/service-discovery-in-microsrvice-cbd54afb94f3