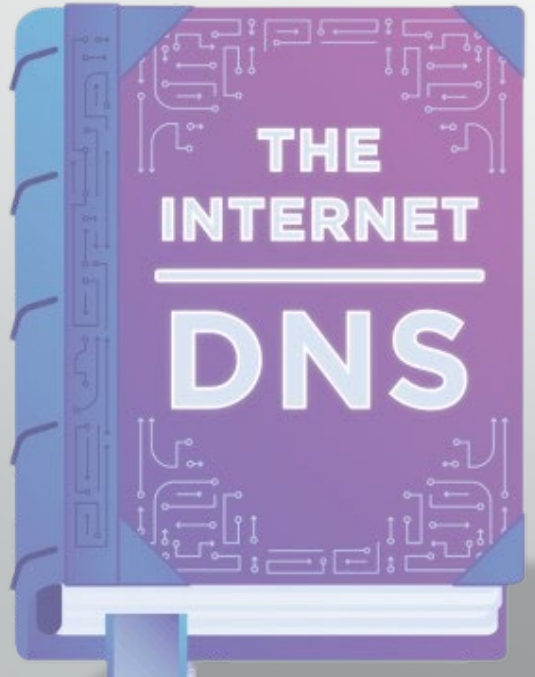
Domain Name System(DNS)

ارائه دهنده: مهدی صفری و شروین ایران عقیده
استاد:کاظم کنی
نیم سال اول ۱۴۰۱-۱۴۰۲

DNS، مخفف Domain Name System، یکی از پایه‌های اینترنت است و بیشتر ما در طول روز بدون آن‌که بدانیم از DNSاستفاده می‌کنیم. در این ارائه سعی کردیم به بررسی مفهوم و کارایی DNSبپردازیم و برخی از مزایای و معایب آن را نیز بیان کنیم. ما در بسیاری از کارهای روزمره خود مانند کار با تلفن همراه، چک کردن ایمیل و گشت‌وگذار در اینترنت، از DNSاستفاده می‌کنیم.

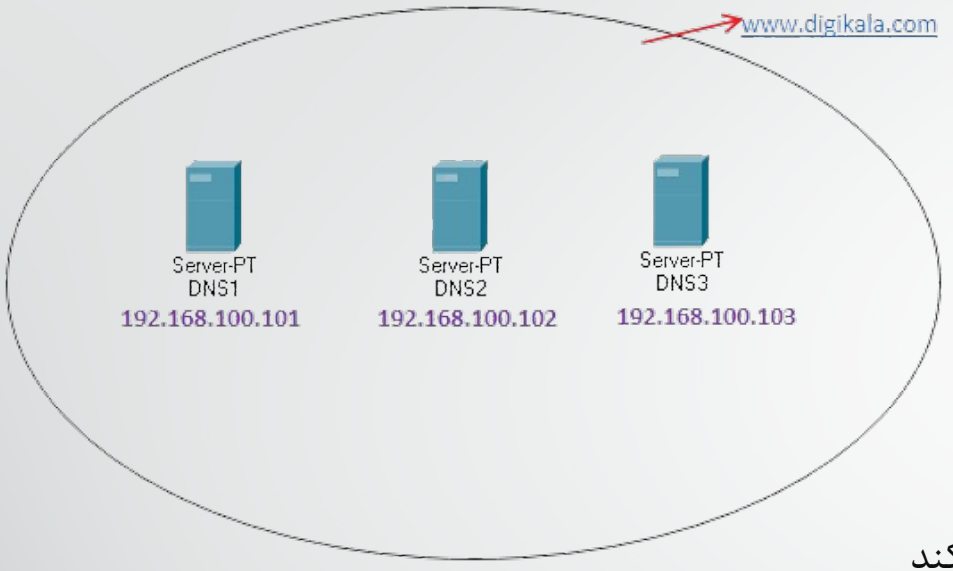
DNSچیست؟

DNSمانند یک دفترچه تلفن برای اینترنت است. همانطور که شما برای تماس با دیگران به جای بخاطر سپردن شماره‌ی آن‌ها، از دفترچه تلفن استفاده می‌کنید، DNSنیز مانند یک دفترچه تلفن عمل می‌کند و نیازی به حفظ کردن آدرس IPها نیست. همانطور که می‌دانید، کامپیوترها برای اتصال به یکدیگر از اعداد یا همان IP آدرس‌ها استفاده می‌کنند.



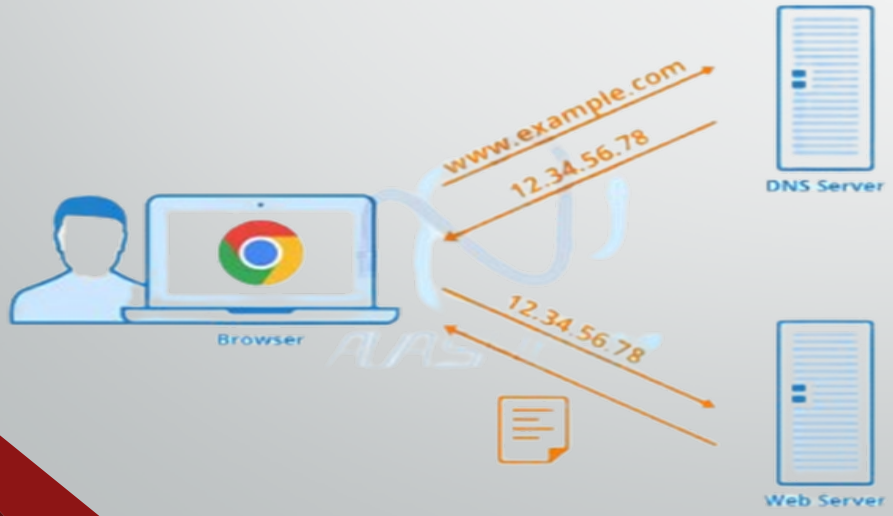
چرا از DNS استفاده کنیم ؟

جواب را با یک سوال میدهیم،آیا حفظ کردن یک اسم مثلا google.com بهتر است یا 216.239.38.120 ؟
قطعا که حفظ کردن اسم راحت تراست.



DNSچگونه کار می‌کند؟

برای مثال اگر client بزند www.google.com اول حافظه cache را چک میکند اگر جواب اونجا نبود از طریق کارت شبکه به دنبال **DNS** میگردد اگر جواب را پیدا نکرد ERROR می دهد اگر جواب را گرفت که IP اون سایت هست از سایت مورد نظر بازدید می کند

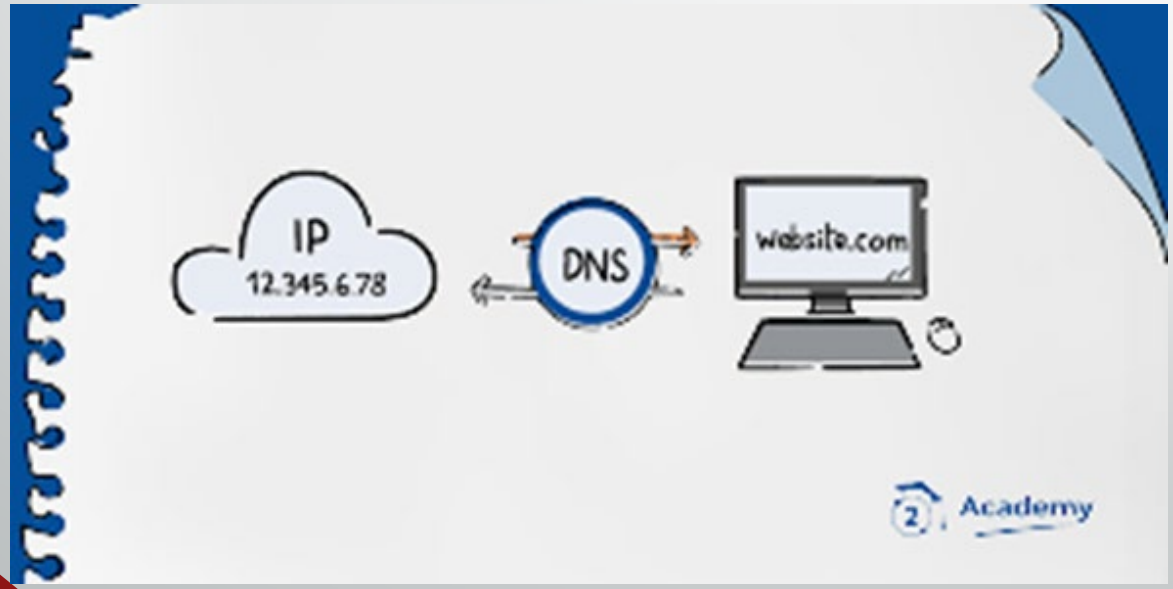


مزایای DNS چیست؟

به دلایل مختلفی ممکن است IP سرور ها عوض شود، بنابراین اگر میخواهیم به یک وبسایت دسترسی داشته باشیم نه تنها باید IP آن را بدانیم بلکه اطلاعات ما باید بروز باشد. سیستم **DNS** وظیفه دارد تا آدرس‌های IP را به روشی بسیار سریع و ثابت، به روز کند و دسترسی ما به وبسایت‌ها را آسان کند. چون در **DNS** دیگر ما با اسم ها سر و کار داریم.

معایب DNS چیست؟

یکی از اصلی‌ترین معایب آن **DNS Attacks** است که در آن مهاجم آدرس واقعی را با یک آدرس جعلی به منظور کلاه‌برداری جایگزین می‌کند و با فریب کاربران آن‌ها را بدون اطلاع به آدرس‌های مخرب هدایت می‌کند. معمولاً هدف از این کار گرفتن اطلاعات بانکی یا سایر داده‌های مهم و حساس کاربران است.

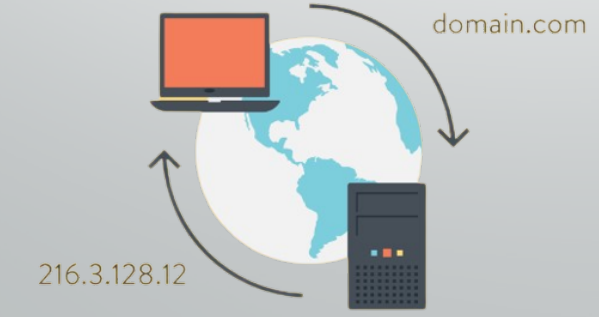


تاریخچه DNS چیست؟

در زمان‌های ابتدایی پیدایش اینترنت، تمام سایت‌ها با آدرس‌های IP شناخته می‌شدند و چون تعداد آن‌ها کم بود به راحتی قابل شناسایی بودند.
بعد از گسترش اینترنت و زیاد شدن وب سایت‌ها روش‌هایی برای ذخیره نام و IP وب سایت ها ارائه شد. اولین بار فردی به نام Elizabeth J. Feinler فایلی به نام **host.txt** که حاوی نام وب سایت ها و آدرس آی پی آن‌ها بود را ایجاد کرد.
بعد از آن Paul Mockapetris سیستمی برای این منظور ایجاد کرد که اساس کارDNS امروزی را تشکیل می‌دهد.

۴ سرور DNS در بارگذاری یک صفحه وب دخیل هستند:

- **Recursive Resolver** : می‌توان به‌عنوان کتابداری در نظر گرفت که از او خواسته می‌شود تا کتاب خاصی را در جایی در کتابخانه پیدا کند.
- **Root Server : Root nameserver** اولین گام در ترجمه (حل) نام هاست قابل خواندن انسان به آدرس های IP است.
- **TLD nameserver** : سرور دامنه سطح بالا **(TLD)** را می توان به عنوان یک قفسه خاص از کتاب در یک کتابخانه در نظر گرفت.
- **Authoritative nameserver** : این سرور را می توان به عنوان یک فرهنگ لغت در یک قفسه کتاب در نظر گرفت که در آن نام خاصی را می توان به تعریف آن ترجمه کرد.

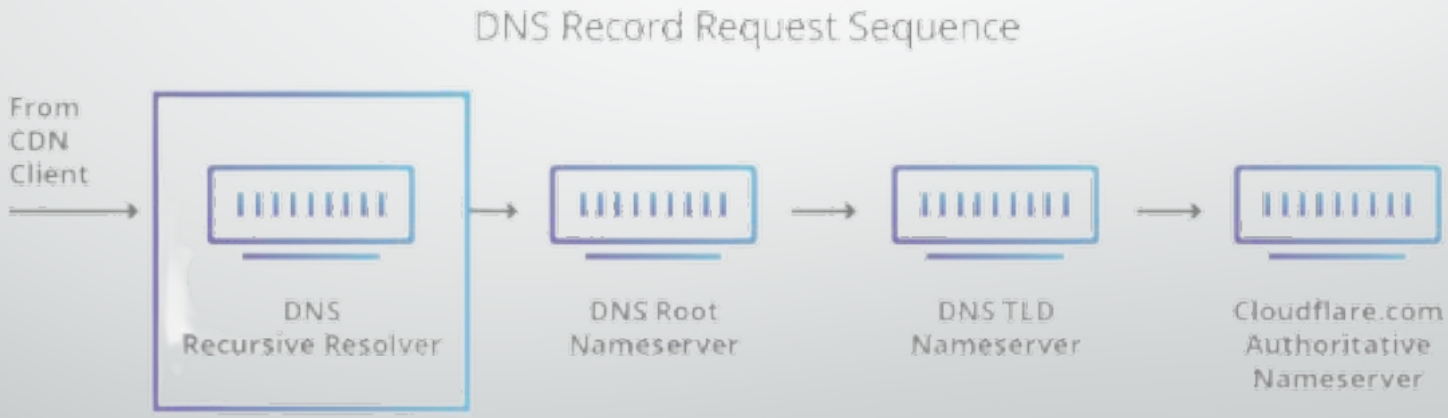


تفاوت بین Authoritative DNS server و Recursive DNS Resolver چیست؟

هر دو مفهوم به سرورهایی اشاره می‌کنند که یکپارچه از زیرساخت‌های DNSهستند، اما هر یک نقش متفاوتی را ایفا می‌کنند و در مکان‌های مختلفی در داخل pipeline of a DNS query زندگی می‌کنند. یکی از راه‌های فکر کردن به تفاوت این است کهRecursive Resolver در ابتدای Query DNSو Authoritative Nameserverدر انتهای آن قرار دارد.

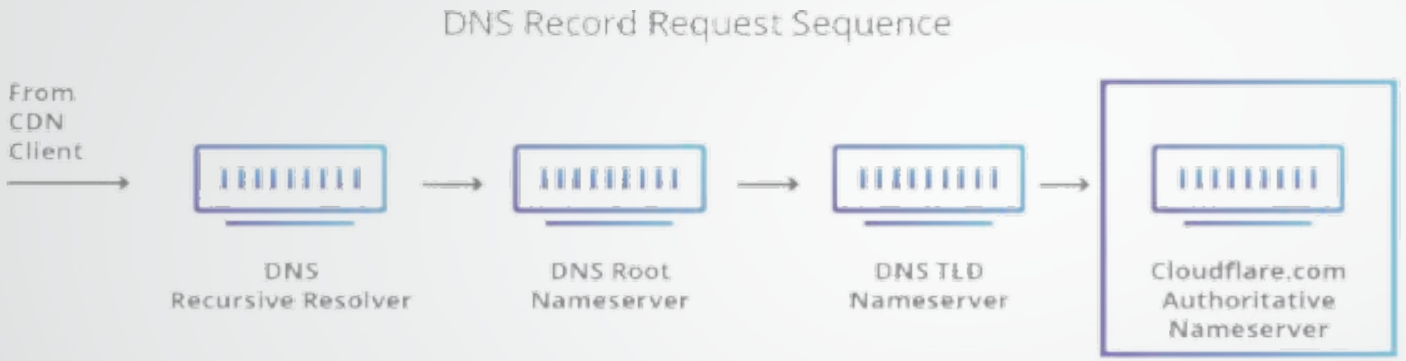
Recursive DNS Resolver

Recursive Resolver کامپیوتری است که به درخواست Recursive از client پاسخ می‌دهد و برای ردیابی DNS Record زمان می‌برد. این کار را با ایجاد یک سری درخواست انجام می دهد تا زمانی که به نام authoritative DNS nameserver برای رکورد درخواستی برسد (یا در صورت یافتن هیچ رکوردی، زمان را تمام کند یا خطا را برگرداند). خوشبختانه، Recursive DNS Resolvers برای ردیابی سوابق مورد نیاز برای پاسخگویی به client، همیشه نیازی به درخواست‌های متعدد ندارند. کش کردن یک فرآیند تداوم داده است که به اتصال کوتاه درخواست های ضروری با ارائه رکورد منبع درخواستی در جستجوی DNS کمک می کند.

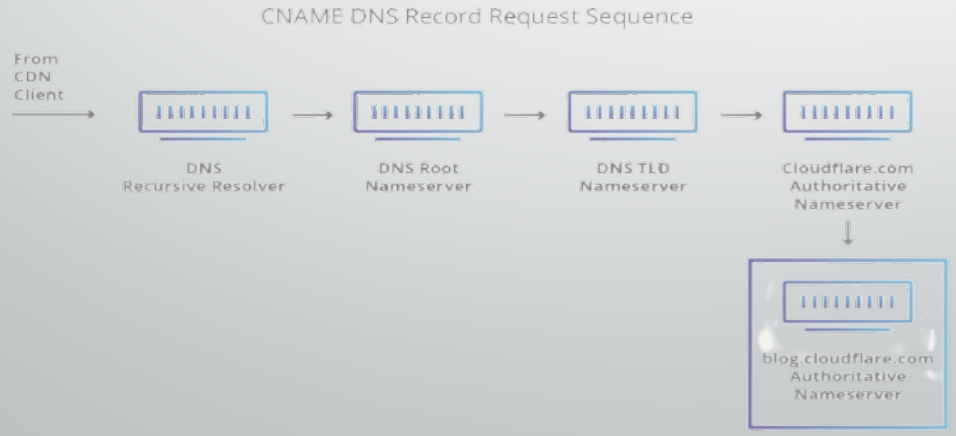


Authoritative DNS server

به بیان ساده، Authoritative DNS Server سروری است که در واقع سوابق منابع DNS را نگه می دارد و مسئول آن است. این سرور در پایین زنجیره جستجوی DNS است که با رکورد منبع درخواست شده پاسخ می دهد و در نهایت به مرورگر وب اجازه می دهد تا به آدرس IP مورد نیاز برای دسترسی به یک وب سایت یا سایر منابع وب برسد. یک NameServer می تواند query ها را از داده های خود بدون نیاز به query از منبع دیگری برآورده کند، زیرا منبع نهایی حقیقت برای برخی رکوردهای DNS است.



شایان ذکر است که در مواردی که query برای یک زیر دامنه مانند foo.example.com یا blog.cloudflare.com است، یک nameserverاضافی بعد ازAuthoritative nameserver به دنباله اضافه می شود که وظیفه ذخیره CNAME Record زیر دامنه را بر عهده دارد.

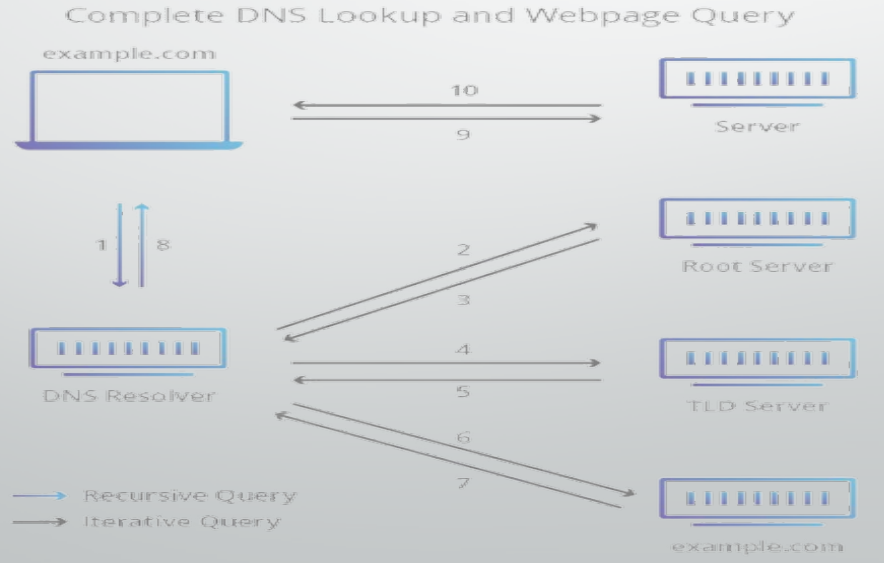


انواع DNS QUERY را نام ببرید؟

- **Recursive query** : در یکrecursive query ، یک سرویس گیرنده DNS نیاز دارد که یک سرور DNS (معمولاً یک حل کننده بازگشتی DNS) به client با رکورد منبع درخواستی یا یک پیام خطا در صورتی که resolverنتواند رکورد را پیدا کند به client پاسخ دهد.

- **Iterative query** : در این شرایط سرویس گیرنده DNS به سرور DNS اجازه می دهد تا بهترین پاسخی را که می تواند ارائه دهد.اگر سرور DNSمورد بررسی برای query name مطابقت نداشته باشد، یک ارجاع به DNS server authoritativeبرای سطح پایین‌تری از فضای نام دامنه را برمی‌گرداند. سپس DNS clientیک query به آدرس ارجاع می دهد. این فرآیند با سرورهای DNSاضافی در زنجیره queryادامه می یابد تا زمانی که یک خطا یا timeoutرخ دهد.

- **Non-Recursive query** : معمولاً این اتفاق زمانی رخ می‌دهد که کوئری های یک DNS resolver clientاز سرور DNS برای رکوردی که به آن دسترسی دارد یا به دلیل معتبر بودن رکورد یا وجود رکورد در حافظه پنهان آن به آن دسترسی دارد، سؤال می‌کند. به طور معمول، یک سرور DNS برای جلوگیری از مصرف پهنای باند اضافی و بارگذاری در سرورهای بالادست، سوابق DNS را کش می کند.



بخش دوم

چه فرایندی برای Name Resolution اتفاق میفته؟

اول فرایندی که سمت DNS client میفته رو بررسی میکنیم، برای مثال میخوایم ببینیم IP ، www.varzesh3.com چی هست؟

1) اسمی که از DNS Server میخواهد بپرسد را با اسم خودش مقایسه میکند، پیش خودش فکر میکنه شاید با خودش کار دارد

2) بررسی DNS Client Cache

cmd → ipconfig /displaydns

```
C:\Users\mahdi>ipconfig /displaydns

Windows IP Configuration
```

```
www.varzesh3.com
----------------------------------------
Record Name . . . . . : www.varzesh3.com
Record Type . . . . . : 1
Time To Live  . . . . : 3272
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 94.182.113.149

Record Name . . . . . : www.varzesh3.com
Record Type . . . . . : 1
Time To Live  . . . . : 3272
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 94.182.113.150
```

3) بهره برداری از فایل Host که در قسمت C:\Windows\System32\drivers\etc


host.txt

4) سوال کردن از خود DNS Server.

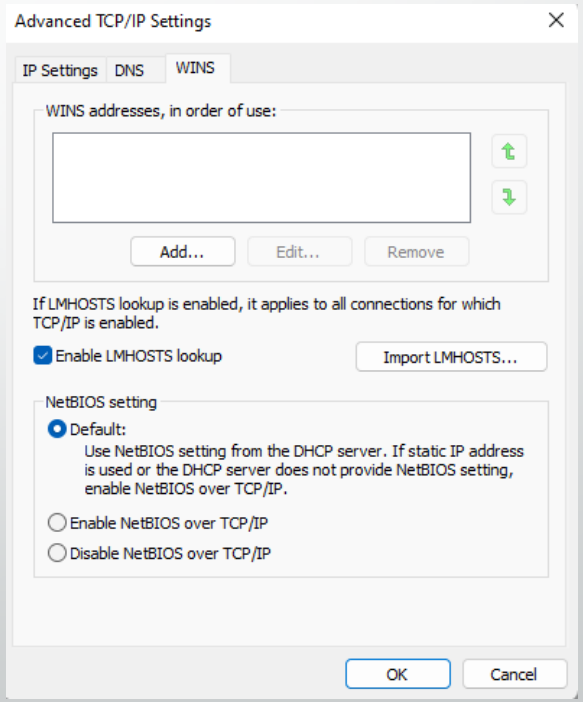
اگر جوابی هم از DNS Server نگرفت یعنی جواب timeout شد.

5) به ترتیب این موارد بررسی میشود

1) Broadcast

2) از WINS سوال میکند

3) از فایل lmhost استفاده میکند



اولویت چک کردن این سه موارد بر اساس nodetype هست

اگر این 5 گزینه انجام شد و جواب نگرفت DNS Client فرایند Name Resolution تمام میشه.

نکته : cache DNS client برای هر رکورد یک time to live (TTL) دارد.

DNS Server وقتی میخواهد به سوالی جواب دهد مراحلی را طی میکند :

- ✓ ایا نسبت به سوال Authority دارد یعنی صلاحیت این را دارد که به سوال جواب دهد ، برای مثال اگر یک سیستم DNS Server ، google.com باشد پس قطعا نسبت به سوال های google.com ، Authority دارد.

یک سوال از DNS Server میپرسیم که www.contoso.com کی هست ؟
اگر DNS Server ما نسبت به سوال Authority داشت که جواب می دهد اگر نداشت سوال رو به DNS Server میفرستد تا جواب را بدهد
اصطلاحا سوال مارو Forward کرده است.

این DNS Server اگر Authority داشت نسبت به سوال باید یک Datebase برای contoso.com داشته باشه که بتونه جواب بده این Database رو در DNS Server بهش میگن **ZONE**

وقتی ما ZONE داریم به ازاش یک Datafile داریم که یک فایل هست به اسم ZONE با پسوند DNS .

ZONE → contoso.com
→ datafile
→ contoso.com.dns

✓ DNS Server که هیچ Zone ندارد برای جواب سوال ها چه کاری میکند؟

سوال ها را Forward میکنه و جواب را میاورد و Cache میکند این نوع DNS ها Datafile ندارند ولی یک Cache بزرگ دارند این نوع DNS را **CACHING ONLY SERVER** می نامند. DNS Server هایی هستند که توی ISP ها را اندازی میشوند

نکته : اطلاعات DNS در system32 هست که همان فایلی هست که با پسوند DNS است .

در DNS Server دو نوع Zone داریم :

- Zone
  - Forward Lookup Zone → IP
  - Reverse Lookup Zone → FQDN

چرا 2 نوع Zone داریم؟

وقتی ما یک سوالی از DNS میپرسیم یا یک QUERY میفرستیم از Resource Record استفاده میکند تا جواب سوال ما را بدهد.

- Resource Reord
  - Host Record
    - A Record ------IPV4
    - AAAA Record-----IPV6
  - CNAME Record

چرا از CNAME باید استفاده کنیم؟ چون ممکن است از یک سرور با یک IP بخواهیم سرویس های متفاوتی بدهیم برای مثال قراره روی یک سرور سرویس Exchange, web server,FTP بدیم با یک اسم این کار میسر نیست پس میام از CNAME استفاده میکنیم .

Ex.contoso.local,www.contoso.local,FTP.contoso.local

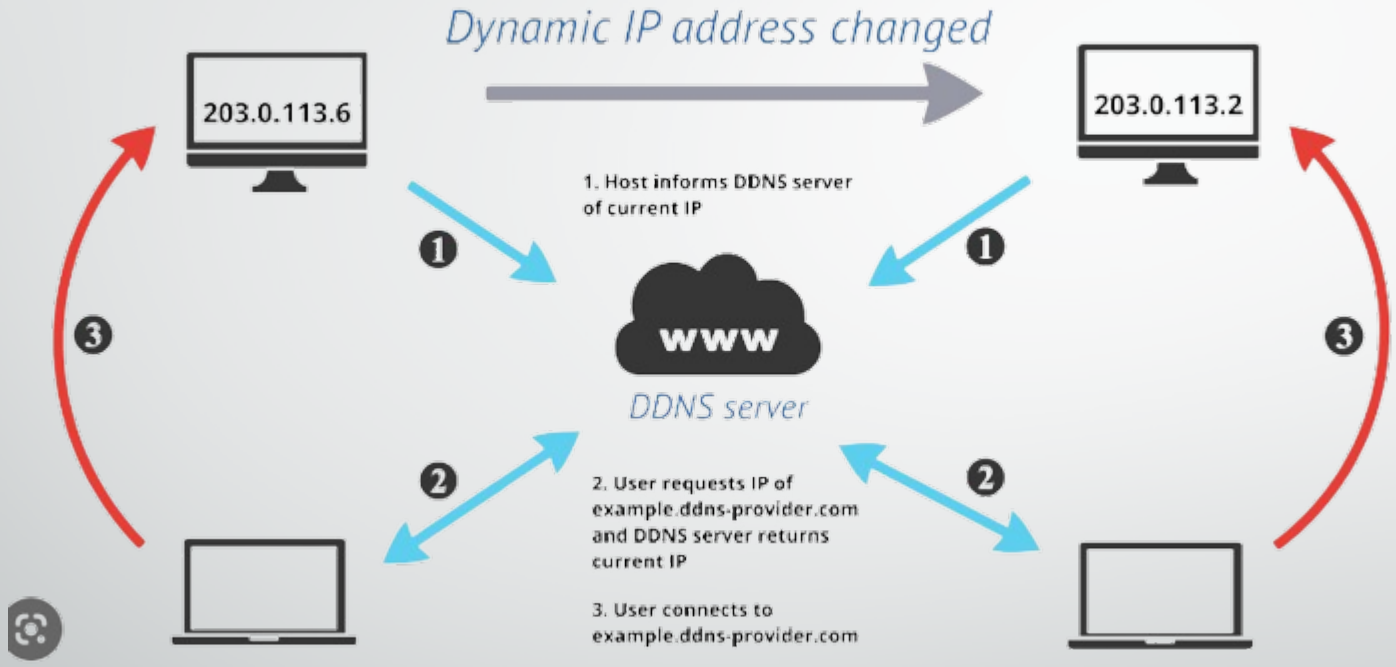
خب حالا ممکنه بگید بیایم بابت تمام این سرویس ها یک A Record بسازیم اگر روزی اتفاق افتاد که IP سرور ما عوض شد باید بیایم تک تک این A Record هارا درست کنیم یعنی IP رکورد هارا تغییر دهیم پس بهتر از CNAME استفاده کنیم .

DDNS

DDNS سرویسی است که به طور خودکار و دوره‌ای رکوردهای A (IPv4) یا AAAA (IPv6) DNS شما را هنگام تغییر آدرس IP به روزرسانی می‌کند. یعنی client ها خودشون به صورت اتوماتیک اسم (FQDN) و IP را در اختیار DNS Server بگذارند و DNS این اطلاعات را ذخیره کند

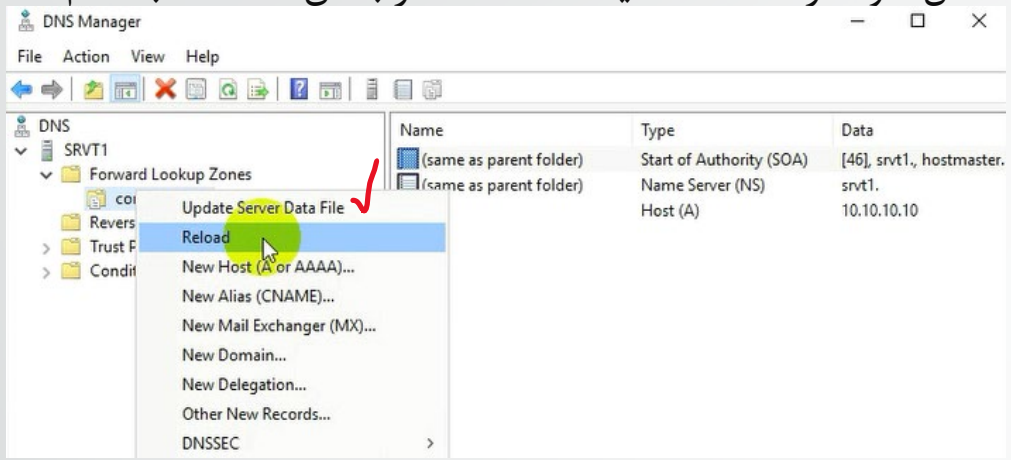
مزایای DDNS چیست؟

- ✓ دسترسی پذیری
- ✓ کار آمد بودن
- ✓ مقرون به صرفه بودن



بهترین ابزار برای سوال های DNS دستور **NSLOOKUP** هست.

اطلاعات ZONE ها که به صورت RECORD اضافه میکنیم در RAM ذخیره میشه بعد از یه مدتی روی هارد ذخیره میشه که همون فایل contoso.com.dns هست . اگر میخواهیم اطلاعات همون لحظه به هارد منتقل شود در قسمت تنظیمات DNS در بخش ZONE به اسم Update Server Datafile که این گزینه را باید بزنیم .

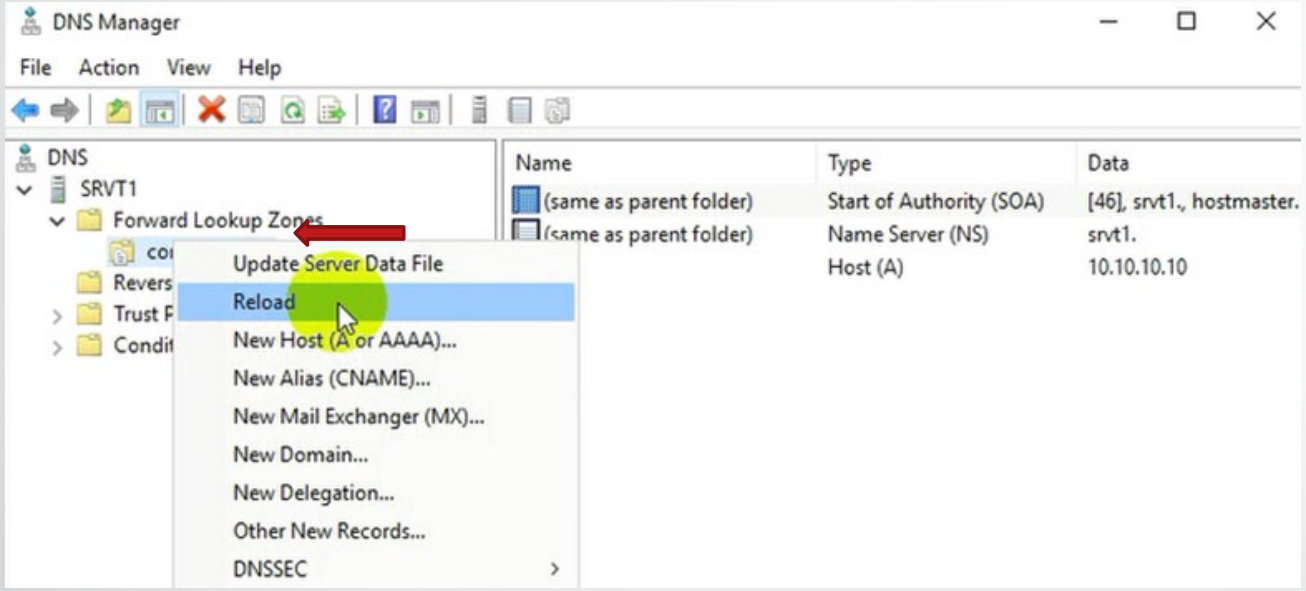


این اطلاعات خود Zone ها که در رم هست باید جایی ذخیره باشه که DNS استارت میشود اطلاعات رو بالا بیارد و خود DNS بداند چه Zone هایی دارد این اطلاعات در REGISTERY هست.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

حالا اگر ما بخوایم اطلاعات از توی Datafile اضافه کنیم همون فایل contoso.com.dns به چه شکل اطلاعات را همان لحظه به رم انتقال دهیم ؟

اولین راه اینه که خود DNS Server را restart کنیم خب با اینکار کل Zone ها Restart شدند ما مثلا میخوایم فقط Zone contoso.com اطلاعاتش بروز بشود بهترین کار اینه که خود Zone را با گزینه Reload اطلاعاتش آپدیت شود.



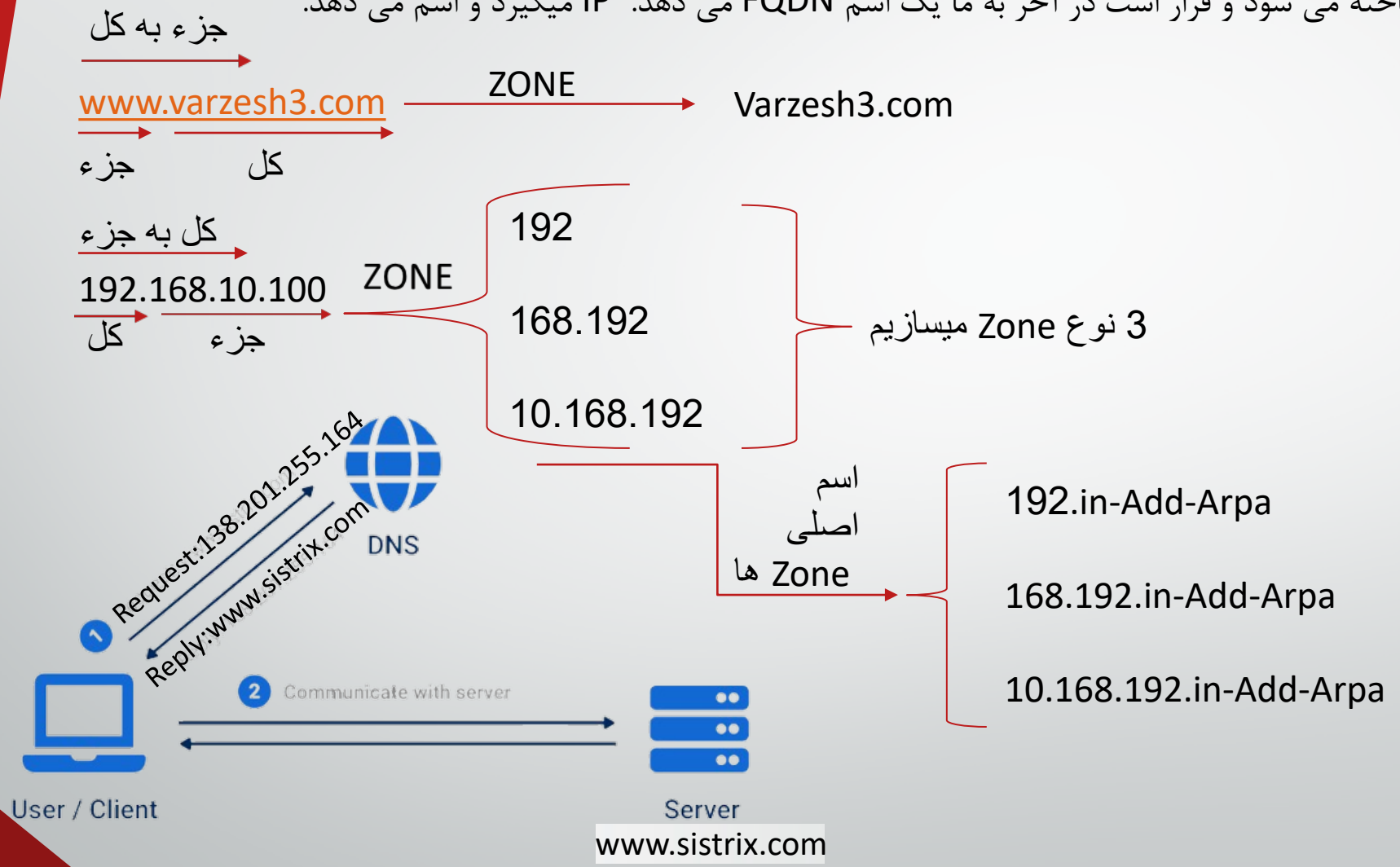
MX Record

وقتی ما یک سوالی داریم و میپرسیم Mail Server ، contoso.com چه کسی هست؟

با استفاده از این Record میتونیم به این سوال جواب بدهیم

PTR Record

توی Reverse Lookup Zone ساخته می شود و قرار است در آخر به ما یک اسم FQDN می دهد. IP میگیرد و اسم می دهد.



زمانی که ما یک DNS Server داریم در این جا single point of failer (SPOF) داریم یعنی اگر DNS دچار مشکل شد دیگر نمیتوانیم سرویس DNS بدهیم پس باید یک DNS Server دیگه داشته باشیم که **DNS SECONDRY** به DNS Serer دوم می گویند.

در این شرایط که 2 تا DNS Server داریم باید بین DNS اول و دوم اطلاعات SYNC بشه یعنی بین Zone ها اطلاعات جا بجا بشه که هر اطلاعاتی که در DNS اول هست در DNS دوم هم باشه به این همگام سازی اطلاعات بین Database ها **ZONE TRANSFER** می گویند.

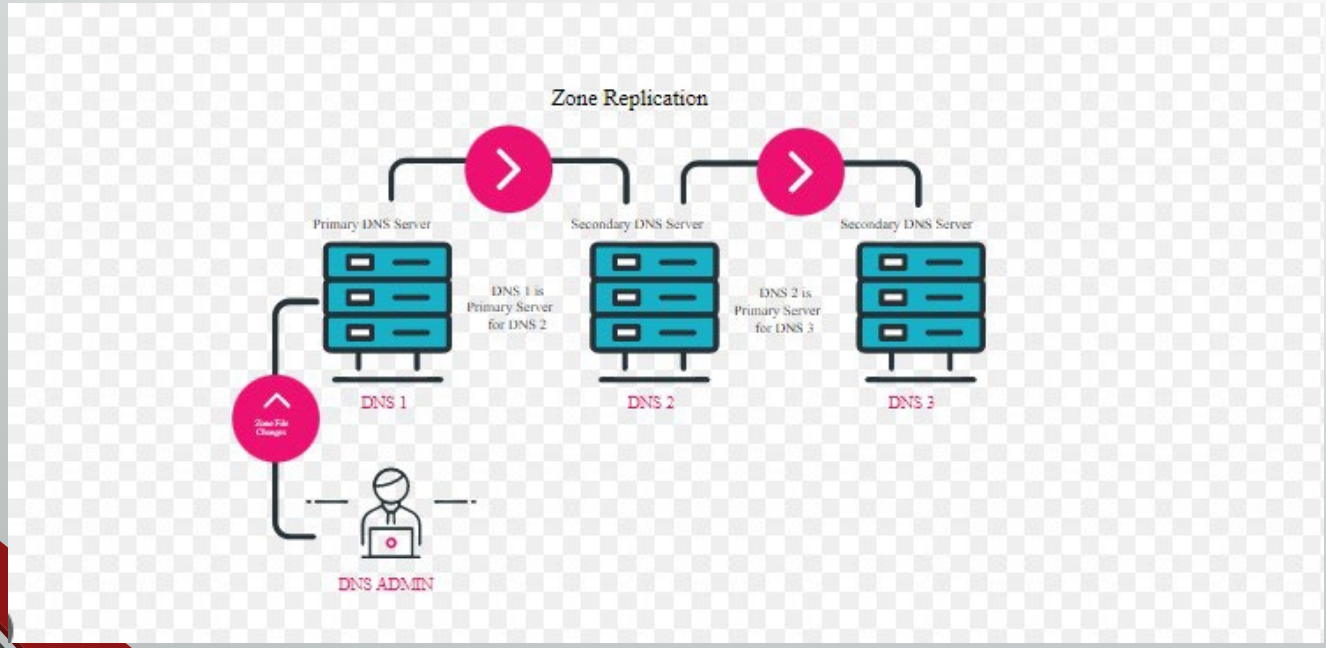
- ZONE TRANSFER
  - PULL
    - By notification
    - Time Interval
    - Force
  - PUSH

ZONE TRANSFER

نکته: DNS دوم به صورت READ ONLY کار میکنه و فقط اطلاعات رو میگیره

یعنی به صورت PULL هست و این ZONE TRANSFER یکطرفه هست یعنی اگر تغییرات روی سرور اول اتفاق افتاد سرور دوم میاد ازش تغییرات رو میگیره اگر تغییرات روی سرور دوم انجام شد سرور اول تغییرات رو نمیاد بگیره

نکته: روی DNS Secondry نمیشه record ساخت



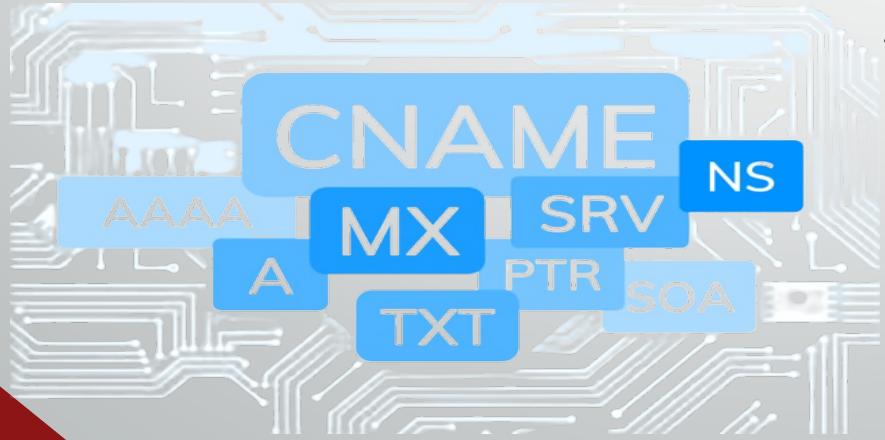
در عملیات ZONE TRANSFER فقط Record ها جابجا میشوند وقتی روی DNS Server در قسمت تنظیماتش تغییراتی ایجاد میکنیم به اصطلاح DNS Server را Reconfig کردیم این تنظیمات در هنگام ZONE TRANSFER انتقال پیدا نمی کنند در اینجا راهی که ارائه شد این بود که این تنظیمات در قالب یک Record جابجا میشوند که به آن **SOA Record** می گویند.

NS Record

از روی NS Record ، اسم DNS Server مشخص میشود برای اینکه این اسم تبدیل به IP شود نیاز به یک A Record هست به این A Record که از روی آن IP ، DNS server مشخص میشود **GLUE Record** می گویند.

SRV Record

SRV Record مشخص کننده ی هاست پشتیبانی کننده از یک سرویس خاص است. به بیان ساده اگر کاربری یا اپلیکیشنی درخواست دسترسی به یک سرویس خاص را برای سرور DNS ارسال کند، در پاسخ برای آن SRV Record حاوی نام دامنه و شماره پورتی که سرویس روی آن فعال است، ارسال می شود. ایجاد یک رکورد SRV به طور عجیبی می تواند بعداً باعث صرفه جویی در وقت شما شود، این رکورد مخفف Service یک رکورد کاربردی در ساختار DNS است که برای برقراری ارتباط نام دامنه با سرویس ها کاربرد دارد.



TXT Record

به Admin اجازه می دهد یادداشت های متنی را در رکورد ذخیره کند.

سوالات

- 2 نوع **ZONE** را نام برده و توضیح دهید و چرا بیشتر از 2 نوع ZONE نداریم ؟
- **SOA RECORD** را توضیح دهید و دلیل اصلی این نوع RECORD را بگویید؟
- 4 **DNS Server** که در بارگذاری یک صفحه وب دخیل هستند را نام ببرید و اختصارا توضیح دهید؟

باتشکر

ممنون از توجه شما