

(1) از پروتکل DNS چه استفاده‌ای می‌شود؟

سیستم نام دامنه که صورت اختصاری DNS نامیده می‌شود، یک نوع پروتکل شناخته شده‌ی شبکه و اینترنت است که به ما اجازه می‌دهد نام‌های آشنا برای انسان را به آدرس‌های منحصر به فرد نگاشت کنیم.

DNS، یک "بانک اطلاعاتی توزیع شده" است که بر روی ماشین‌های متعددی مستقر می‌شود (مشابه ریشه‌های یک درخت که از ریشه اصلی انشعاب می‌شوند) امروزه اکثر شرکت‌ها و موسسات دارای یک سرویس دهنده DNS کوچک در سازمان خود می‌باشند تا این اطمینان ایجاد گردد که کامپیوترها بدون بروز هیچگونه مشکلی، یکدیگر را پیدا می‌نمایند.

از پروتکل DNS در مواردی که سیستم اقدام به ارسال یک درخواست مبتنی بر DNS برای یک سرویس دهنده‌ی نام به منظور یافتن آدرس Domain می‌نماید، استفاده می‌شود. مثلاً در صورتی که در مرورگر آدرس `www.google.com` وارد شود، یک درخواست مبتنی بر DNS از کامپیوتر مبدأ و به مقصد یک سرویس دهنده DNS صادر می‌شود. مأموریت درخواست ارسالی، یافتن آدرس IP وب سایت google است.

(2) رکوردهای مختلف DNS را نام ببرید و هر یک را در به صورت مختصر توضیح دهید.

- A: به آدرس IPv4 دستگاهی که وب سایت در آن میزبانی می‌شود اشاره می‌کند.
- AAAA: به آدرس IPv6 دستگاهی که وب سایت در آن میزبانی می‌شود اشاره می‌کند.
- MX: به سرورهای ایمیل اشاره می‌کند.
- CNAME: رکورد نام متعارف برای نام مستعار نقاط میزبان به نام میزبان است.
- ANAME: نام مستعار را به صورت خودکار حل و فصل می‌کند، مانند CNAME کار می‌کند اما نام میزبان را به IP نام میزبان نشان می‌دهد.
- NS: رکورد سرورهای نام برای دامنه‌های فرعی است.
- PTR: از آدرس IP به نام میزبان اشاره می‌کند.
- SOA: حاوی اطلاعات اداری در مورد منطقه DNS است.
- SRV: سابقه‌ی سرویس را برای سایر سرویس‌ها مشخص می‌کند.
- TXT: سوابق متنی، که بیشتر برای تأیید SPF، DKIM، DMARC و موارد دیگر استفاده می‌شود، است.
- CAA: سابقه‌ی مرجع صدور گواهی‌نامه برای گواهی SSL / TLS است.

(3) DNS server چیست و آدرس سه مورد از معروفترین DNS server ها را نام

ببرید.

سرورهای DNS رایانه‌هایی هستند که به همراه یکدیگر سیستمی را تشکیل می‌دهند، که امکان استفاده از نام‌ها به جای آدرس را می‌دهند و می‌توانند کارکردهای مختلفی را ارائه دهند، که هر یک می‌توانند بر توانایی دسترسی به سرورها از طریق نام تأثیر بگذارند.

- [Cisco OpenDNS](#): 208.67.222.222 and 208.67.220.220
- [Cloudflare 1.1.1.1](#): 1.1.1.1 and 1.0.0.1
- [Google Public DNS](#): 8.8.8.8 and 8.8.4.4

(4) پورت پیشفرض مورد استفاده در پروتکل DNS چیست؟

Port 53

(5) ساختار بسته‌های DNS به چه شکل می‌باشد؟

Identification	Flags	12 bytes
Number of questions	Number of answer RRs	
Number of authority RRs	Number of additional RRs	
Questions (variable number of questions)		Name, type fields for a query
Answers (variable number of resource records)		RRs in response to query
Authority (variable number of resource records)		Records for authoritative servers
Additional information (variable number of resource records)		Additional "helpful" info that may be used

ساختار بسته‌های DNS

به شکل مقابل، شامل بخش‌های زیر می‌باشد:

- سربرگ (Header)
- سوالات (Questions)
- پاسخ‌ها (Answers)
- قدرت (Authority)
- اطلاعات اضافه (Additional information)

(6) دلیل توصیه RFC برای استفاده از پروتکل UDP در Query ها نسبت به TCP چیست؟

پروتکل DNS معمولاً از پروتکل UDP به منظور حمل داده استفاده می نماید. پروتکل UDP نسبت به TCP دارای overhead کمتری می باشد. هر اندازه overhead یک پروتکل کمتر باشد، سرعت آن بیشتر خواهد بود. در مواردی که حمل داده با استفاده از پروتکل UDP با مشکل و یا بهتر بگوییم خطاء مواجه گردد، پروتکل DNS از پروتکل TCP به منظور حمل داده استفاده نموده تا این اطمینان ایجاد گردد که داده به درستی و بدون بروز خطاء به مقصد خواهد رسید.

فرآیند ارسال یک درخواست DNS و دریافت پاسخ آن، متناسب با نوع سیستم عامل نصب شده بر روی یک کامپیوتر است. برخی از سیستم های عامل اجازه ی استفاده از پروتکل TCP برای DNS را نداده و صرفاً می بایست از پروتکل UDP به منظور حمل داده استفاده شود. بدیهی است در چنین مواردی همواره این احتمال وجود خواهد داشت که با خطاهائی مواجه شده و عملاً امکان ترجمه نام یک کامپیوتر و یا Domain به آدرس IP وجود نداشته باشد.

(7) سوکت چیست؟

سوکت ترکیبی از IP آدرس و پورت است، که درگاهی جهت ارسال و دریافت داده در شبکه ایجاد می کند. بسته ها از طریق این درگاه در اینترنت جا به جا می شوند. این سیستم کلی و ترکیبی توسط IP/TCP سازماندهی و مرتب می شود و در پشت صحنه کار می کند.

به تعبیر ساده تر، کار سوکت ایجاد این کانال است. از طریق کانال ارتباطی ایجاد شده توسط سوکت، داده هایی در طول شبکه ارسال و دریافت می شوند.

انواع سوکت:

- سوکت های منطقی استریم: که بر پایه ی پروتکل TCP اند و به Connection Oriented شهرت دارند.
- سوکت های دیتاگرام (Datagram): بر پایه ی پروتکل UDP اند و به Connectionless معروف اند.
- سوکت های خام
- سوکت های بسته متوالی

منابع:

Kurose, Ross. (2017). *Computer Networking A Top-Down Approach: DNS—The Internet's Directory Service*. US: Pearson
<https://blog.faradars.org/dns-terminology-components-and-concepts/>
<http://www.srco.ir/Articles/TipsView.asp?ID=327>
<https://www.geeksforgeeks.org/working-of-domain-name-system-dns-server/>
<https://www2.cs.duke.edu/courses/fall16/compsci356/DNS/DNS-primer.pdf>
<https://www.hpe.com/us/en/insights/articles/get-faster-internet-with-better-dns-1909.html>
<https://ruternet.com/blog/%D8%B3%D9%88%DA%A9%D8%AA-%DA%86%DB%8C%D8%B3%D8%AA%D8%9F/>