DNS

DNS (Domain Name System) - это распределенная система, которая переводит доменные имена (например, example.com) в соответствующие им IP-адреса компьютеров и устройств, а также выполняет обратное преобразование (перевод IP-адресов в доменные имена). DNS является фундаментальным протоколом в Интернете, используемым для разрешения имен в сети.



DNS использует два основных протокола и порты для своей работы:

1. Протокол DNS (Domain Name System): DNS использует собственный протокол DNS для обмена информацией между клиентскими устройствами и серверами DNS. Протокол DNS работает на прикладном уровне OSI (уровень 7).
2. Протоколы транспортного уровня:
   - TCP (Transmission Control Protocol): TCP используется для передачи данных DNS в случае больших объемов или сложных запросов, которые не могут быть переданы через одиночный пакет UDP.
   - UDP (User Datagram Protocol): UDP используется для основной передачи данных DNS. Он предоставляет ненадежный и безсоединительный транспорт данных, что делает его быстрее и более эффективным для большинства DNS-запросов.

Порты, используемые протоколами DNS:

- Порт 53: Это стандартный порт для DNS-серверов. Он используется как для TCP, так и для UDP протоколов. Клиентские устройства отправляют запросы DNS на порт 53 сервера DNS, а серверы DNS отправляют ответы на этот же порт клиентского устройства.

DNS находится на прикладном уровне OSI (уровень 7). Он предоставляет службу разрешения имен, которая облегчает использование доменных имен вместо IP-адресов. DNS работает

поверх протоколов транспортного уровня (TCP и UDP) и использует протокол DNS для обмена информацией. На прикладном уровне, DNS запросы и ответы передаются через приложения (браузеры, почтовые клиенты и т.д.), чтобы перевести доменные имена в соответствующие IP-адреса и наоборот.

DNS находится на прикладном уровне OSI, потому что его функциональность относится к обработке запросов и предоставлению служб разрешения имен, в то время как протоколы транспортного уровня обеспечивают надежную и эффективную передачу данных между клиентом и сервером DNS.

Это база:

- Распределенная структура: DNS работает на основе распределенной базы данных, называемой DNS-кэшами или серверами имен. Они разделены по всему миру и содержат информацию о доменных именах и соответствующих IP-адресах.
- Резолверы DNS: Клиентские устройства, такие как компьютеры или мобильные устройства, используют резолверы DNS для запроса соответствующего IP-адреса доменного имени. Резолверы могут быть настроены вручную или автоматически получать информацию от DNS-серверов, предоставляемых интернет-провайдерами.
- DNS-записи: DNS-записи содержат информацию о доменных именах и их ассоциированных IP-адресах. Некоторые распространенные типы DNS-записей включают записи типа A (преобразование доменного имени в IPv4-адрес), AAAA (преобразование доменного имени в IPv6-адрес), CNAME (псевдонимы для других доменных имен), MX (записи почтовых серверов) и NS (серверы имен для домена).
- Процесс разрешения DNS: Когда пользователь вводит доменное имя в веб-браузере или приложении, резолвер DNS инициирует процесс разрешения DNS. Резолвер отправляет запрос DNS на ближайший DNS-сервер, который затем перенаправляет запрос по иерархии DNS-серверов до тех пор, пока не будет найден соответствующий IP-адрес. Затем IP-адрес возвращается обратно резолверу, который затем использует его для установления соединения с запрашиваемым сервером.
- DNS-кэширование: Для улучшения производительности и снижения нагрузки на DNS-серверы, резолверы DNS могут временно сохранять полученные записи в своем кэше. При следующем запросе на тот же домен или на другой домен, резолвер DNS сначала проверяет свой локальный кэш на наличие соответствующей записи. Если запись найдена, резолвер использует сохраненный IP-адрес без необходимости отправлять новый запрос DNS. Это позволяет ускорить процесс разрешения и снизить нагрузку на DNS-серверы.
- Однако, если записи не найдены в локальном кэше резолвера или если записи в кэше устарели, резолвер отправляет запрос на DNS-серверы, начиная с корневых серверов. Запросы передаются по иерархии DNS-серверов, начиная с корневых серверов, затем серверов верхнего уровня, серверов авторитетных зон и наконец, до серверов, которые содержат требуемую запись. Когда найден соответствующий IP-адрес, он возвращается резолверу, который затем сохраняет запись в свой кэш и использует ее для будущих запросов.

- DNS также играет роль в других функциях, таких как обратное преобразование IP-адресов в доменные имена (резолюция обратных записей), маршрутизация почты с помощью записей MX, обнаружение служб с помощью записей SRV и другие.

  DNS является неотъемлемой частью функционирования Интернета, обеспечивая преобразование доменных имен в IP-адреса и позволяя пользователям получать доступ к веб-сайтам, отправлять электронную почту и выполнять другие сетевые операции с использованием удобных доменных имен вместо запоминания числовых IP-адресов

Запросы:

DNS-запросы могут быть классифицированы как рекурсивные и итеративные (нерекурсивные).

1. Рекурсивный DNS-запрос: В рекурсивном запросе резолвер полностью обрабатывает запрос от начала до конца. Резолвер отправляет запрос на DNS-сервер и ожидает полного ответа. Если DNS-сервер не имеет информации о запрашиваемом домене в своем кэше, он может перенаправить запрос на другой сервер и продолжать делать это, пока не будет найден и вернутся полные данные о домене. Затем резолвер возвращает полный ответ клиенту, который инициировал запрос. Рекурсивные запросы обычно используются клиентскими устройствами, чтобы получить полные данные о домене и упростить процесс для конечного пользователя.
2. Итеративный (нерекурсивный) DNS-запрос: В итеративном запросе резолвер отправляет запрос на DNS-сервер и ожидает ответа с максимально доступной информацией о запрашиваемом домене. Если DNS-сервер не имеет информации о домене, он возвращает резолверу наиболее близкий результат или информацию о сервере, который может предоставить дальнейшую информацию. Затем резолвер должен отправить дополнительные запросы на другие серверы для получения полного ответа. Итеративные запросы требуют более активного участия резолвера в процессе разрешения и могут быть использованы, например, серверами DNS для получения информации о других серверах, необходимых для обработки запросов.
3. Запросы типа Forward (Прямой запрос): Это обычные DNS-запросы, в которых клиентская машина или резолвер обращается к DNS-серверу для получения информации о домене или ресурсе.
4. Запросы типа Reverse (Обратный запрос): В обратных DNS-запросах клиентская машина или резолвер отправляет запрос на DNS-сервер, чтобы получить доменное имя, соответствующее определенному IP-адресу. Обратные запросы часто используются для идентификации домена, связанного с IP-адресом, например, при отображении имени хоста при сканировании сети или анализе журналов.

Путь DNS запроса:

Полная цепочка DNS-запроса может выглядеть следующим образом:

1. Браузер отправляет запрос на DNS-резолвер. Если запись о доменном имени не найдена в локальном DNS-кэше браузера, то он проверяет кэш операционной системы, файл hosts и кэш роутера, если они есть.
2. Если запись не найдена в локальных кэшах и файлах, то резолвер отправляет запрос на первый DNS-сервер в списке, настроенном в операционной системе или роутере.
3. Первый DNS-сервер, получив запрос, проверяет свой кэш. Если запись найдена, то сервер возвращает IP-адрес в DNS-резолвер, который передает его браузеру.
4. Если запись не найдена в кэше первого DNS-сервера, то он перенаправляет запрос на следующий DNS-сервер в цепочке. Обычно это будет DNS-сервер на более высоком уровне иерархии DNS.
5. Процесс перенаправления продолжается, пока DNS-сервер не найдет запись в своем кэше или не получит ее от другого DNS-сервера выше в иерархии.
6. Когда DNS-сервер находит запись о доменном имени, он возвращает ее IP-адрес в DNS-резолвер, который передает его браузеру.
7. Браузер использует полученный IP-адрес для установки соединения с веб-сервером, который хостит веб-страницу, соответствующую доменному имени.
8. Если в процессе запроса DNS-записи была найдена новая запись, она может быть кэширована в локальном DNS-кэше браузера, операционной системы, файле hosts, кэше роутера и на других DNS-серверах на пути запроса, для более быстрого доступа в будущем.

DNS записи:

В системе DNS существует несколько типов записей, которые используются для хранения информации о доменных именах и их связи с IP-адресами и другими данными. Вот некоторые из основных типов записей DNS:

1. Запись A (Address): Используется для связи доменного имени с IPv4-адресом.
2. Запись AAAA (IPv6 Address): Аналогично записи A, но используется для связи доменного имени с IPv6-адресом.
3. Запись CNAME (Canonical Name): Устанавливает псевдоним для указанного доменного имени, позволяя одному домену быть псевдонимом для другого.
4. Запись MX (Mail Exchange): Указывает почтовый сервер, отвечающий за доставку электронной почты для домена.
5. Запись NS (Name Server): Определяет DNS-серверы, которые являются авторитетными для домена и отвечают за предоставление информации о домене.
6. Запись PTR (Pointer): Используется для обратного преобразования IP-адреса в доменное имя.
7. Запись TXT (Text): Позволяет хранить произвольные текстовые данные для доменного имени, часто используется для добавления дополнительной информации, например, SPF-записей для авторизации отправителей электронной почты.
8. Запись SRV (Service): Используется для обнаружения служб, предоставляемых на указанном домене или порту, и содержит информацию о доменном имени, порте, протоколе и приоритете.

9. Запись SOA (Start of Authority): Содержит информацию об авторитетном сервере для домена, включая контактные данные, периоды обновления и другие настройки.
10. Запись SPF (Sender Policy Framework): Определяет список IP-адресов или доменных имен, которые авторизованы для отправки электронной почты от имени домена.

Revision #3
Created 10 May 2023 12:33:22 by Maru
Updated 11 May 2023 13:11:00 by Maru