Доклад на тему: Архитектура и организация глобальных сетей

Кижваткина Анна Юрьевна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Целью данного доклада является ознакомление архитектурой и организацией глобальных сетей. Нужно выявить ключевые тенденции в технологиях, определяющих развитие глобальных сетей, и оценить влияние этих сетей на современное общество.

2 Теоретическое введение

В эпоху цифровой трансформации глобальные сети, в первую очередь Интернет, стали фундаментальным элементом современной цивилизации. Они обеспечивают связь, обмен информацией и доступ к ресурсам в глобальном масштабе, формируя основу для экономики, социальной сферы, образования и культуры. Понимание архитектуры и организации этих сложных систем является ключом к обеспечению их эффективной, безопасной и устойчивой работы.

В теоретическом плане, архитектура глобальных сетей представляет собой многоуровневую структуру, определяющую взаимодействие различных компонентов и протоколов. Организация же включает в себя широкий спектр участников, от международных организаций и провайдеров до конечных пользователей, а также механизмы управления и координации. Изучение этих аспектов требует глубокого анализа сетевых моделей, принципов маршрутизации, технологий доступа и организационных структур, а также понимания тенденций развития и возникающих угроз. Данное теоретическое введение закладывает основу для дальнейшего рассмотрения этих ключевых аспектов в рамках доклада.

Некоторые особенности глобальных сетей:

• Неограниченный территориальный охват. Сеть объединяет ЭВМ разных классов (от персональных до суперЭВМ), локальные и территориальные сети разных технологий.

• Использование специального оборудования для объединения различных сетей и передачи данных на большие расстояния. Это аппаратура передачи данных (модемы, приёмопередатчики и т. п.) и активное сетевое оборудование (маршру-

тизаторы, коммутаторы, шлюзы).

• Возможность доступа к ресурсам сети практически из любой точки земного шара.

• Передача по сети любых видов данных, в том числе таких специфических, как аудио и видео.

3 Основная часть

Многоуровневая архитектура и протоколы

Модель OSI (Open Systems Interconnection):

Уровни архитектуры глобальных сетей могут быть описаны в рамках сетевой модели OSI. Всего в ней 7 уровней, каждый уровень выполняет определенную функцию и взаимодействует с соседними уровнями все они обеспечивают модульность и упрощают разработку и понимание сетевых технологий:

- Физический. Включает в себя все физические устройства и соединения, которые обеспечивают передачу данных. Это оптоволоконные кабели, медные провода, маршрутизаторы и коммутаторы.
- Канальный. Отвечает за установление и поддержание соединений между устройствами на физическом уровне. Этот уровень включает в себя протоколы, которые определяют, как данные передаются по сети.
- Сетевой. Отвечает за маршрутизацию данных между устройствами. Основным протоколом этого уровня является IP (Internet Protocol), который определяет, как данные упаковываются в пакеты и передаются по сети.
- Транспортный. Обеспечивает надёжную передачу данных между устройствами и включает протоколы, которые контролируют, как данные разбиваются на сегменты и собираются обратно.
- Сеансовый. Управляет установлением, управлением и завершением сеансов связи между устройствами.

- Представительский. Отвечает за преобразование информации в форму, понимаемую получателем, и обеспечивает шифрование и сжатие.
- Прикладной. Включает в себя протоколы и приложения, которые используют интернет для передачи данных. Это уровень, с которым взаимодействуют пользователи.

Модель TCP/IP

Протоколы TCP (Transmission Control Protocol) и IP (Internet Protocol) ключевые и являются основой сети Интернет. В отличие от OSI имеет упрощенную модель (4 или 5 уровней):

- Канальный (Link). Определены правила взаимодействия сетевого оборудования между собой. На этом уровне определены физические свойства среды обмена информацией: максимальное расстояние, на которое передаются пакеты, частота сигнала, время задержки ответа.
- Межсетевой (Internet). Мировая паутина состоит из множества локальных подсетей, которые объединяются между собой посредством протокола TCP/IP. Для организации взаимодействия между ними и корректного предоставления информации необходимо обеспечить возможность соединяться с другими локальными сетями.
- Транспортный (Transport). Берёт на себя функцию контроля доставки пакетов. На этом уровне работают протоколы TCP и UDP.
- Прикладной (Application). На этом уровне происходит поддержание сеанса связи между хостами, преобразование передаваемых данных, работа с конечным пользователем и сетью.

Протоколы

TCP (Transmission Control Protocol): протокол управления передачей, ориентированный на подключение. Обеспечивает надёжную доставку потока с использо-

ванием последовательного подтверждения. Устанавливает соединение между приложениями перед отправкой каких-либо данных.

- UDP (User Datagram Protocol): протокол без установления соединения, который предоставляет базовую, но ненадёжную службу обмена сообщениями. Работает в случаях, когда надёжность не требуется. Используется для более быстрой передачи, для многоадресной передачи и широковещательных соединений.
- HTTP (Hypertext Transfer Protocol): протокол передачи гипертекста между двумя или более системами. Работает по модели клиент-сервер, большая часть обмена данными через Интернет осуществляется с помощью HTTP.
- SMTP (Simple Mail Transfer Protocol): протокол передачи электронной почты. Отвечает за отправку писем.
- DNS (Domain Name System): протокол, который преобразует доменные имена в IP-адреса. Позволяет пользователям использовать удобные для чтения имена вместо числовых IP-адресов. Играет ключевую роль в работе интернета, обеспечивая быстрый и надёжный доступ к веб-ресурсам и другим сетевым сервисам.
- BGP (Border Gateway Protocol): протокол маршрутизации, который управляет тем, как пакеты проходят через маршрутизатор в независимой системе, одной или нескольких сетях, управляемых одной организацией, и подключаются к разным сетям. Соединяет конечные точки локальной сети с другими локальными сетями, а также соединяет конечные точки в разных локальных сетях друг с другом.

Адресация и маршрутизация

IP-адресация (IPv4 и IPv6)

IPv4: 32-битные адреса, ограниченное адресное пространство, проблемы с масштабируемостью. (Internet Protocol version 4) — устаревшая версия протокола

интернет-адресов, разработанная в 1980 году. Каждый IP-адрес в IPv4 состоит из четырёх чисел (от 0 до 255), разделённых точками, например, 192.168.0.1. Максимальное количество таких адресов — около 4,3 миллиарда.

IPv6: 128-битные адреса, значительно расширенное адресное пространство, упрощенная маршрутизация. (Internet Protocol version 6) — более новая версия протокола, разработанная для того, чтобы решить проблему исчерпания IP-адресов. Вместо 32 бит в IPv4, IPv6 использует 128 бит, что позволяет создавать не миллиарды, а 340 ундециллионов уникальных адресов. IPv6-адреса выглядят значительно сложнее: вместо четырёх чисел, разделённых точками, используются восемь групп шестнадцатеричных чисел, разделённых двоеточиями, например: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

Некоторые отличия между IPv4 и IPv6:

- Объём адресов: IPv4 — около 4,3 миллиарда адресов, IPv6 — 340 ундециллионов.
- Простота работы с сетями: IPv6 упрощает работу с сетями благодаря функции автоконфигурации, что значит, что устройства могут автоматически получать IP-адрес без необходимости вручную настраивать DHCP-серверы или вводить данные вручную. В IPv4 это обычно требует больше ручных настроек.
- Безопасность: IPv6 был разработан с учётом новых стандартов безопасности. Встроенная поддержка шифрования и аутентификации с использованием IPsec делает IPv6 более защищённым по умолчанию, в то время как в IPv4 эти функции необходимо настраивать отдельно.
- Скорость работы: на практике разница в скорости между IPv4 и IPv6 минимальна или вовсе отсутствует. В некоторых случаях IPv6 может работать быстрее, так как его маршрутизация и обработка более оптимизированы для современных сетей.

Маршрутизация

Маршрутизация — это процесс выбора пути для передачи данных от источника к назначению в компьютерных сетях. Она помогает пакетам данных точно и эффективно добираться до их конечного пункта назначения. Основная задача маршрутизации — выбор оптимального пути для передачи пакетов через сеть. Этот процесс включает использование различных протоколов и алгоритмов, обеспечивающих эффективную транспортировку данных

- Статическая. Маршруты устанавливаются вручную администратором сети. Применяется в небольших сетях, где нет необходимости в сложной динамической маршрутизации, а маршруты редко изменяются.
- Динамическая. Используется для автоматического выбора наилучшего пути при изменении сетевой топологии. Основана на специальных протоколах маршрутизации, которые непрерывно обмениваются информацией об изменениях в сети.
- Гибридная. Сочетает в себе элементы как статического, так и динамического подхода. Администратор может задать основные маршруты вручную, а динамические протоколы управляют остальными.

протоколы

- IP (Internet Protocol) – основной сетевой протокол, который используется для передачи данных в интернет-сети. Он отвечает за маршрутизацию пакетов от отправителя к получателю.
- TCP (Transmission Control Protocol) – обеспечивает надежную передачу данных по сети, гарантируя, что все пакеты достигнут получателя в правильном порядке и без потерь.
- UDP (User Datagram Protocol) – протокол, который передает данные без установления соединения и без гарантии доставки. Используется в приложе-

ниях, требующих высокой скорости, таких как видеостриминг или онлайн-игры.

- BGP (Border Gateway Protocol) – протокол динамической маршрутизации, который используется для обмена маршрутизаторами информацией о доступных сетевых путях в больших сетях, включая глобальный интернет.

Автономные системы (AS) и Интернет

Автономные системы (AS):

Автономная система (AS, autonomous system) в интернете — система IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации с Интернетом. Каждой автономной системе присваивается уникальный номер (ASN), необходимый для обмена информацией о маршрутах с другими AS по протоколу междоменной маршрутизации Border Gateway Protocol.

Некоторые типы автономных систем:

- Многоинтерфейсная (multihomed) AS. Имеет соединения с более чем одним интернет-провайдером. Это позволяет системе оставаться подключённой к интернету в случае выхода из строя соединения с одним из провайдеров.
- Ограниченная (stub) AS. Имеет единственное подключение к одной внешней автономной системе.
- Транзитная (transit) AS. Пропускает через себя транзитный трафик сетей, подключённых к ней.

BGP (Border Gateway Protocol)

Border Gateway Protocol (BGP) — это протокол маршрутизации, разработанный для управления трафиком между автономными системами (AS) в глобальной сети интернет. BGP относится к категории протоколов маршрутизации по вектору пути и определяет маршруты на основе информации о пути, полученной от других

маршрутизаторов. Это делает его подходящим для маршрутизации на больших расстояниях, где требуется гибкость и надежность при выборе оптимальных маршрутов.

Некоторые особенности BGP:

- Определение маршрутов на основе информации о пути, полученной от других маршрутизаторов. Это делает его подходящим для маршрутизации на больших расстояниях, где требуется гибкость и надёжность при выборе оптимальных маршрутов.
- Использование атрибутов маршрутов для контроля и настройки маршрутов сетевыми администраторами. Некоторые ключевые атрибуты: AS-Path, Next-Hop, Local Preference и Multi-Exit Discriminator (MED).

Два основных режима работы: eBGP (External BGP) для связи между разными автономными системами и iBGP (Internal BGP) для работы внутри одной автономной системы. Поддержка маршрутизации на основе политики позволяет операторам настраивать и оптимизировать маршруты по собственным требованиям. Обновления маршрутов происходят только при изменении состояния маршрута, что снижает нагрузку на сеть.

Оптимизация производительности и контент-доставка

CDN (Content Delivery Networks):

CDN (Content Delivery Network, «сеть доставки контента») — это группа связанных между собой серверов в разных географических точках, которые помогают быстрее загружать контент веб-сайтов и приложений. Основная функция CDN — распределение информации на множество серверов, расположенных по всему миру. Это сокращает физическое расстояние, которое проходят данные до пользователя, и, как следствие, уменьшается время загрузки. CDN ускоряет работу не только сайтов, но и мобильных приложений. Скорость загрузки здесь тоже зависит от географии пользователя.

Некоторые преимущества использования CDN:

- Сокращение времени загрузки контента. Кэширующие узлы быстро загружают страницы интернет-сайтов для пользователей из разных регионов, снижая вероятность потери клиентов.

- Уменьшение нагрузки на основной сервер. Поскольку большая часть статического контента раздаётся через CDN-провайдера, можно высвободить оперативную память и мощности процессора для других нагрузок.

- Стабильность работы при пиковых нагрузках. Благодаря перенаправлению трафика на кэширующие узлы CDN одновременно обрабатывает большие объёмы запросов, а интернет-сайт остаётся доступным даже в периоды пиковых нагрузок без использования дополнительных мощностей.

- Доступность онлайн-ресурса даже при сбоях. Если случится крупная поломка на сервере онлайн-площадки — пользователи всё равно смогут загрузить контент из кэша, чтобы приобрести товары или заказать услуги.

-Оптимизация расходов на хостинг. Поскольку хостинг-провайдеры взимают плату за превышение лимитов трафика с подключённых к ним сайтов, можно снизить затраты с помощью сжатия контента и его переноса на ближайшие к пользователям узлы.

Кэширование

Кэширование — это стратегия оптимизации, которая заключается во временном хранении часто запрашиваемых данных в специальном буфере, называемом кэшем. Оно позволяет ускорить доступ к информации, поскольку её не нужно каждый раз извлекать из постоянного хранилища, например из базы данных, с диска или удалённого сервера.

Некоторые виды кэширования:

- Клиентское (браузерное). Браузер кэширует статические ресурсы, такие как HTML, CSS, JavaScript и изображения, из предыдущих посещений сайта, что уменьшает количество запросов к серверу и ускоряет загрузку страниц.

- Серверное. Серверное ПО, например Varnish, Nginx, Memcached, кэширует результаты обработки запросов. Применяется для часто запрашиваемых, но редко изменяющихся данных.
- На стороне приложения. Программное кэширование данных в оперативной памяти приложения. Используется в фреймворках, таких как Rails и Django, а также в CMS, библиотеках данных.
- Распределённое (кэширование CDN — сетей доставки контента). Копирование контента на распределённые кэш-серверы, близкие к клиентам. Ускоряет загрузку статических файлов из ближайших кэш-узлов.

Преимущества кэширования:

- повышение скорости загрузки страниц;
- уменьшение нагрузки на сервер;
- улучшение отказоустойчивости;
- экономия трафика;
- ускорение рендеринга для повторных посетителей;
- улучшение пользовательского опыта;
- SEO-преимущества;
- снижение затрат на базы данных.

Безопасность глобальных сетей

Брандмауэры (Firewalls): Брандмауэр (файрвол, межсетевой экран) — это программное или аппаратное средство, которое защищает компьютерные сети и устройства от несанкционированного доступа. Название происходит от немецкого «Brandmauer» («противопожарная стена»). Основная задача брандмауэра — фильтрация входящего и исходящего сетевого трафика. Он устанавливает правила для управления этим трафиком, блокируя подозрительные соединения и разрешая безопасные.

Некоторые функции брандмауэра:

- Защита от внешних угроз. Брандмауэр блокирует попытки взлома со стороны злоумышленников, которые пытаются проникнуть в сеть.
- Контроль трафика. Фильтрует входящий и исходящий трафик, разрешая только надёжные соединения.
- Обеспечение конфиденциальности. Помогает защитить личные данные от утечки.
- Защита устройств. Снижает уязвимость устройств для атак.
- Защита бизнеса. Для компаний потеря данных может обернуться репутационными и финансовыми потерями, брандмауэр минимизирует такие риски.
- Фильтрация контента. Некоторые брандмауэры позволяют блокировать нежелательный контент, что особенно полезно в образовательных учреждениях и корпоративной среде.
- Обнаружение угроз. Современные системы способны выявлять и предотвращать сложные угрозы.

Некоторые типы брандмауэров:

- Аппаратные. Это физические устройства, которые устанавливаются между локальной сетью и интернетом.
- Программные. Это приложения, которые устанавливаются на компьютеры или серверы.
- Сетевые. Работают на уровне сети и фильтруют трафик между различными сегментами сети.
- Межсетевые экраны следующего поколения (NGFW). Предлагают расширенные функции, такие как инспекция SSL, обнаружение угроз и интеграция с другими системами безопасности.

- Облачные. Используются для защиты облачных инфраструктур и приложений. Брандмауэры для мобильных устройств. Специализированные решения для защиты смартфонов и планшетов, которые часто используются для доступа к корпоративным сетям.

Системы обнаружения вторжений (IDS) и предотвращения вторжений (IPS)

Системы обнаружения и предотвращения вторжений (IDS/IPS) — это комплекс программных или аппаратных средств, которые выявляют факты и предотвращают попытки несанкционированного доступа в корпоративную систему. Система обнаружения вторжений (IDS) (англ. название — Intrusion Detection System) предназначена для мониторинга и анализа сетевого трафика на предмет подозрительной активности и потенциальных угроз. IDS не предпринимает мер для их предотвращения. Основная задача — найти известную угрозу или выявить новую аномалию, оценить её критичность и передать сообщение администратору либо сигнал в IPS. Система предотвращения вторжений (IPS) (англ. название — Intrusion Prevention System) автоматически предотвращает атаки на информационные ресурсы. Для этого IPS запускает подходящий сценарий реагирования, например, разрывает соединение или блокирует вредоносный трафик, изменяет маршрутизацию трафика.

Некоторые задачи, которые решают IDS/IPS:

- Помогают выявлять потенциально опасную или аномальную активность в сети на ранних стадиях;
- Могут выявлять не только внешние, но и внутренние угрозы, например, предотвращать утечки конфиденциальных данных;
- Предоставляют подробные отчёты о сетевой активности и инцидентах безопасности;
- Дополняют другие средства безопасности, такие как межсетевые экраны и антивирусное ПО, создавая эшелонированную защиту и повышая общий уровень защищённости сети.

Основное различие IDS и IPS заключается в том, как оба решения реагируют на инциденты. IDS — это инструмент мониторинга, который распознаёт потенциально опасную активность и предупреждает о ней. IPS способен не только выявить проблему, но и предпринять действия, направленные на борьбу с угрозой — разорвать соединение или заблокировать IP-адрес, с которого ведутся подозрительные действия.

VPN (Virtual Private Network)

VPN (англ. virtual private network — «виртуальная частная сеть») — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх чьей-либо другой сети. При подключении к интернету через VPN программное обеспечение создаёт безопасное соединение между устройством и удалённым VPN-сервером, шифруя данные просмотра веб-страниц и скрывая IP-адрес. В зависимости от применяемых протоколов и назначения VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть.

Некоторые задачи VPN:

- Защита личных данных. VPN скрывает IP-адрес и шифрует весь трафик, что предотвращает утечку личной информации.
- Безопасность в общественных сетях. VPN защищает онлайн-активность и предотвращает доступ к данным в открытых Wi-Fi сетях.
- Доступ к контенту. С помощью VPN можно получить доступ к ресурсам, открытым только для определённых сетей, например, работа в корпоративной сети офиса на удалёнке.

Шифрование (SSL/TLS)

SSL (Secure Sockets Layer) и TLS (Transport Layer Security) — это криптографические протоколы, которые используются для защиты данных при их передаче через интернет. Они обеспечивают безопасность связи между двумя компьютерами, гарантируя, что информация не будет перехвачена или подделана.

Некоторые функции протокола SSL:

- Шифрование данных. Защищает сведения, передаваемые от клиента на сервер и обратно, что делает невозможным их прочтение третьими лицами.
- Аутентификация сервера. Применяет сертификаты, проверяющие подлинность сервера, чтобы клиент подключался к законному сайту, а не к фишинговому или вредоносному.
- Аутентификация клиента (необязательно). Может использоваться для подтверждения личности клиента с помощью цифровых сертификатов.
- Целостность данных. Защищает передаваемый трафик от изменений, предотвращая подделку или вмешательство.
- Предотвращение атак типа «злоумышленник в середине». Протокол защищает от атак, где злоумышленник перехватывает и манипулирует трафиком между двумя сторонами.

Основные задачи TLS:

- Шифрование данных — защита от перехвата и чтения третьими лицами.
- Аутентификация — подтверждение подлинности сервера и, опционально, клиента.
- Целостность данных — гарантия того, что данные не были изменены при передаче.

4 Выводы

Изучение архитектуры и организации глобальных сетей позволяет нам понять, как функционирует этот сложный и жизненно важный для современного общества механизм. В ходе доклада были рассмотрены ключевые компоненты и принципы построения глобальных сетей, проанализированы различные технологии доступа и организационная структура, а также выявлены основные тенденции развития. Оценка влияния глобальных сетей на различные сферы жизни общества показала их огромную роль в формировании современного мира. Несмотря на очевидные преимущества, важно помнить о потенциальных рисках и проблемах, связанных с зависимостью от глобальных сетей, и стремиться к обеспечению их стабильной, безопасной и справедливой работы. В будущем глобальные сети будут продолжать развиваться, открывая новые возможности и ставя перед нами новые вызовы, требующие постоянного изучения и адаптации.