Использование TCP\IP: IPv4, IPv6. Протоколы маршрутизации.

Введение

Компьютер в сети TCP/IP может иметь адреса трех уровней (но не менее двух):

• Локальный адрес компьютера. Для узлов, входящих в локальные сети - это MAC-адрес сетевого адаптера. Эти адреса назначаются производителями оборудования и являются уникальными адресами.

• IP-адрес, состоящий из 4 байт, например, 109.26.17.100. Этот адрес используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов.

• Символьный идентификатор-имя (DNS), например, www.seti.ucoz.ru.

Сетевые протоколы

Сетевой протокол — набор правил, позволяющий осуществлять обмен данными между составляющими сеть устройствами, например, между двумя сетевыми картами (рис. 1).

Рис. 1. Иллюстрация к понятию Сетевой протокол

TCP/IP

Стэк- это набор разноуровневых протоколов, объединенных в группу.

Стек протоколов TCP/IP — это два протокола, являющиеся основой связи в сети Интернет. Протокол TCP разбивает передаваемую информацию на порции (пакеты) и нумерует их. С помощью протокола IP все пакеты передаются получателю. Далее с помощью протокола TCP проверяется, все ли пакеты получены. При получении всех порций TCP располагает их в нужном порядке и собирает в единое целое. В сети Интернет используются две версии этого протокола:

• Маршрутизируемый сетевой протокол IPv4. В протоколе этой версии каждому узлу сети ставится в соответствие IP-адрес длиной 32 бита (т.е. 4 октета или 4 байта).

• IPv6 позволяет адресовать значительно большее количество узлов, чем IPv4. Протокол Интернета версии 6 использует 128-разрядные адреса, и может определить значительно больше адресов.

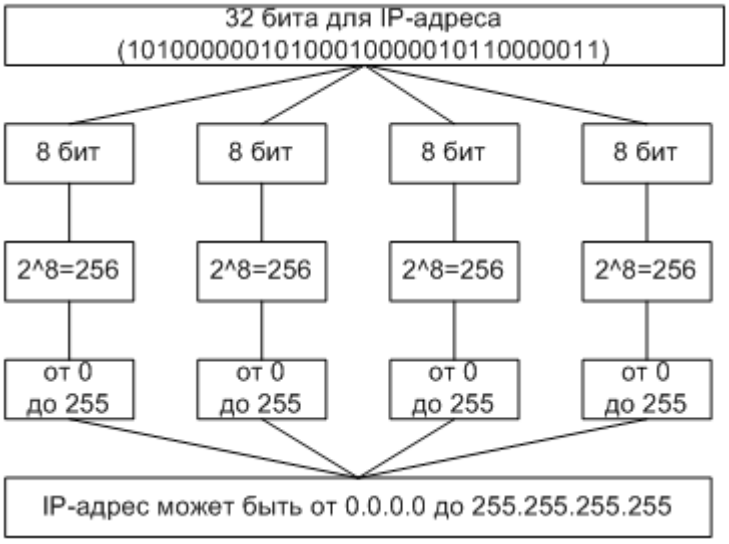
IP-адреса версии v6 записываются в следующем виде:X:X:X:X:X:X:X:X, где X является шестнадцатеричным числом, состоящим из 4-х знаков(16 бит), а каждое число имеет размер 4 бит. Каждое число располагается в диапазоне от 0 до F. Вот пример IP-адреса шестой версии: 1080:0:0:0:7:800:300C:427A. В подобной записи незначащие нули можно опускать, поэтому фрагмент адреса: 0800: записывается, как 800:.

IP-адреса принято записывать разбивкой всего адреса по октетам (8), каждый октет записывается в виде десятичного числа, числа разделяются точками. Например, адрес

10100000010100010000010110000011

записывается как

10100000.01010001.00000101.10000011 = 160.81.5.131



Перевод адреса из двоичной системы в десятичную

IP-адрес хоста состоит из номера IP-сети, который занимает старшую область адреса, и номера хоста в этой сети, который занимает младшую часть.

160.81.5.131 - IP-адрес

160.81.5. - номер сети

131 - номер хоста

Базовые протоколы (IP, TCP, UDP)

Стек протоколов TCP/IP

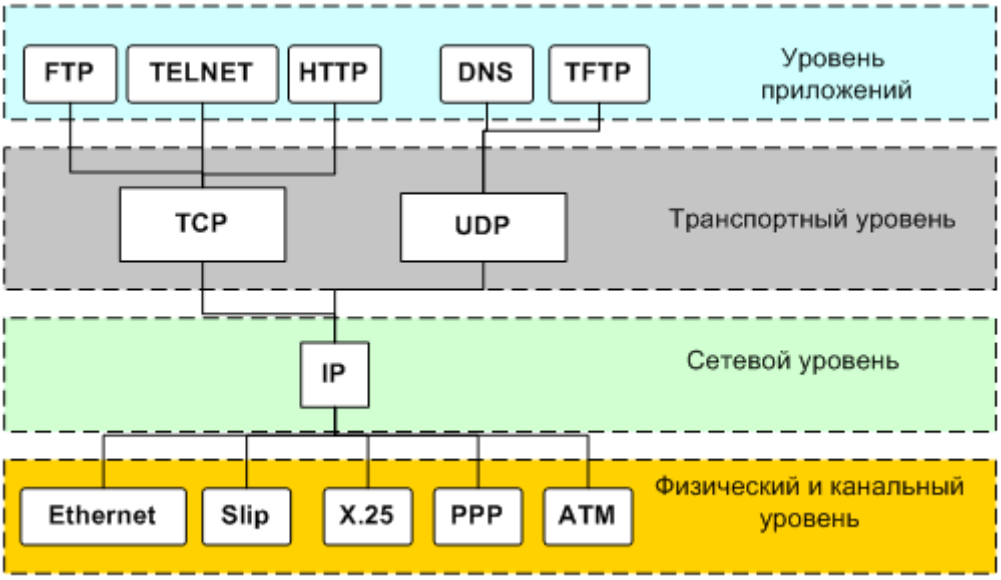
TCP/IP - собирательное название для набора (стека) сетевых протоколов разных уровней, используемых в Интернет. Особенности TCP/IP:

• Открытые стандарты протоколов, разрабатываемые независимо от программного и аппаратного обеспечения;

• Независимость от физической среды передачи;

• Система уникальной адресации;

• Стандартизованные протоколы высокого уровня для распространенных пользовательских сервисов.



Стек протоколов TCP/IP

Стек протоколов TCP/IP делится на 4 уровня:

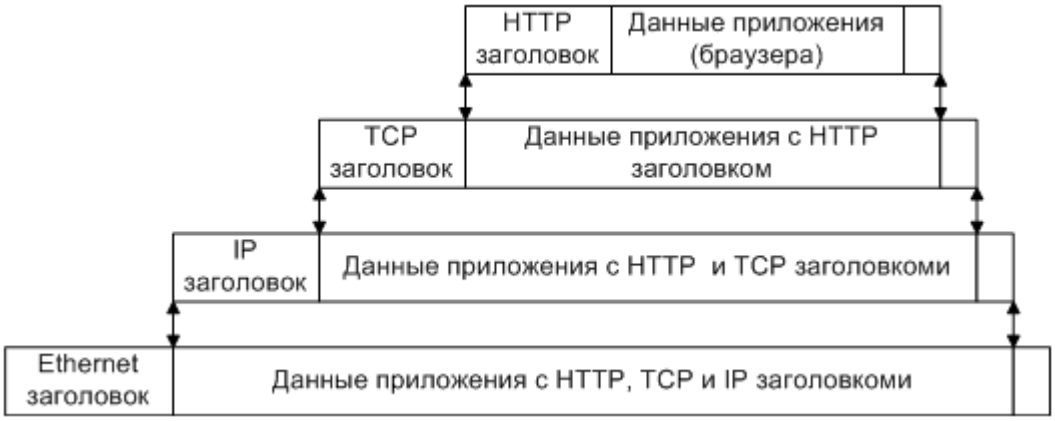
• Прикладной,

• Транспортный,

• Межсетевой,

• Физический и канальный.

Данные передаются в пакетах. Пакеты имеют заголовок и окончание, которые содержат служебную информацию. Данные, более верхних уровней вставляются, в пакеты нижних уровней.



Пример инкапсуляции пакетов в стеке TCP/IP

Физический и канальный уровень.

Стек TCP/IP не подразумевает использования каких-либо определенных протоколов уровня доступа к среде передачи и физических сред передачи данных. От уровня доступа к среде передачи требуется наличие интерфейса с модулем IP, обеспечивающего передачу IP-пакетов. Также требуется обеспечить преобразование IP-адреса узла сети, на который передается IP-пакет, в MAC-адрес. Часто в качестве уровня доступа к среде передачи могут выступать целые протокольные стеки, тогда говорят об IP поверх ATM, IP поверх IPX, IP поверх X.25 и т.п.

Межсетевой уровень и протокол IP.

Основу этого уровня составляет IP-протокол.

Ip (Internet Protocol) – интернет протокол.

Первый стандарт IPv4 определен в RFC-760 (DoD standard Internet Protocol J. Postel Jan-01-1980)

Последняя версия IPv4 - RFC-791 (Internet Protocol J. Postel Sep-01-1981).

Первый стандарт IPv6 определен в RFC-1883 (Internet Protocol, Version 6 (IPv6) Specification S. Deering, R. Hinden December 1995)

Последняя версия IPv6 - RFC-2460 (Internet Protocol, Version 6 (IPv6) Specification S. Deering, R. Hinden December 1998).

Основные задачи:

• Адресация

• Маршрутизация

• Фрагментация датаграмм

• Передача данных

Протокол IP доставляет блоки данных от одного IP-адреса к другому.

Программа, реализующая функции того или иного протокола, часто называется модулем, например, "IP-модуль", "модуль TCP".

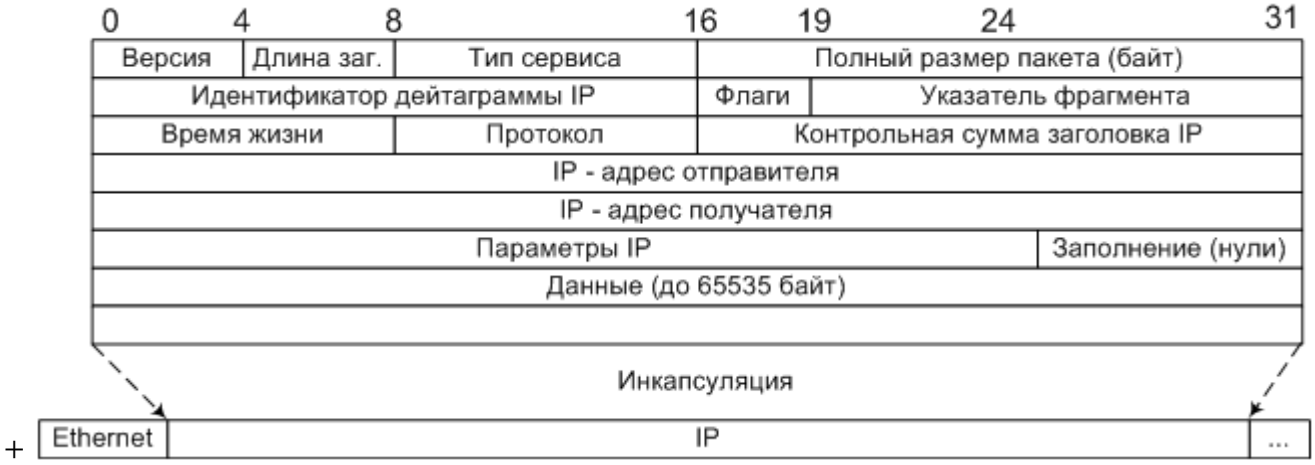
Когда модуль IP получает IP-пакет с нижнего уровня, он проверяет IP-адрес назначения.

• Если IP-пакет адресован данному компьютеру, то данные из него передаются на обработку модулю вышестоящего уровня (какому конкретно - указано в заголовке IP-пакета).

• Если же адрес назначения IP-пакета - чужой, то модуль IP может принять два решения: первое - уничтожить IP-пакет, второе - отправить его дальше к месту назначения, определив маршрут следования - так поступают маршрутизаторы.

Также может потребоваться, на границе сетей с различными характеристиками, разбить IP-пакет на фрагменты (фрагментация), а потом собрать в единое целое на компьютере-получателе.

Если модуль IP по какой-либо причине не может доставить IP-пакет, он уничтожается. При этом модуль IP может отправить компьютеру-источнику этого IP-пакета уведомление об ошибке; такие уведомления отправляются с помощью протокола ICMP, являющегося неотъемлемой частью модуля IP. Более никаких средств контроля корректности данных, подтверждения их доставки, обеспечения правильного порядка следования IP-пакетов, предварительного установления соединения между компьютерами протокол IP не имеет. Эта задача возложена на транспортный уровень.



Структура дейтограммы ip. Слова по 32 бита.

Версия - версия протокола IP (например, 4 или 6)

Длина заг. - длина заголовка IP-пакета.

+Тип сервиса (TOS - type of service) - Тип сервиса ().

TOS играет важную роль в маршрутизации пакетов. Интернет не гарантирует запрашиваемый TOS, но многие маршрутизаторы учитывают эти запросы при выборе маршрута (протоколы OSPF и IGRP).

Идентификатор дейтаграммы, флаги (3 бита) и указатель фрагмента - используются для распознавания пакетов, образовавшихся путем фрагментации исходного пакета.

Время жизни (TTL - time to live) - каждый маршрутизатор уменьшает его на 1, что бы пакеты не блуждали вечно.

Протокол - Идентификатор протокола верхнего уровня указывает, какому протоколу верхнего уровня принадлежит пакет (например: TCP, UDP).

Маршрутизация.

Протокол IP является маршрутизируемый, для его маршрутизации нужна маршрутная информация.

Маршрутная информация, может быть:

• Статической (маршрутные таблицы прописываются вручную)

• Динамической (маршрутную информацию распространяют специальные протоколы)

Протоколы динамической маршрутизации:

• RIP (Routing Information Protocol) - протокол передачи маршрутной информации, маршрутизаторы динамически создают маршрутные таблицы.

• OSPF (Open Shortest Path First) - протокол "Открой кротчайший путь первым", является внутренним протоколом маршрутизации.

• IGP (Interior Gateway Protocols) - внутренние протоколы маршрутизации, распространяет маршрутную информацию внутри одной автономной системе.

• EGP (Exterior Gateway Protocols) - внешние протоколы маршрутизации, распространяет маршрутную информацию между автономными системами.

• BGP (Border Gateway Protocol) - протокол граничных маршрутизаторов.

Протокол icmp

ICMP (Internet Control Message Protocol) - расширение протокола IP, позволяет передавать сообщения об ошибке или проверочные сообщения.

Другие служебные IP-протоколы

IGMP (Internet Group Management Protocol) - позволяет организовать многоадресную рассылку средствами IP.

RSVP (Resource Reservation Protocol) - протокол резервирования ресурсов.

ARP (Address Resolution Protocol) - протокол преобразования IP-адреса и адреса канального уровня.

Транспортный уровень

Протоколы транспортного уровня обеспечивают прозрачную доставку данных между двумя прикладными процессами. Процесс, получающий или отправляющий данные с помощью транспортного уровня, идентифицируется на этом уровне номером, который называется номером порта. Таким образом, роль адреса отправителя и получателя на транспортном уровне выполняет номер порта (или проще - порт).

Анализируя заголовок своего пакета, полученного от межсетевого уровня, транспортный модуль определяет по номеру порта получателя, какому из прикладных процессов направлены данные, и передает эти данные соответствующему прикладному процессу. Номера портов получателя и отправителя записываются в заголовок транспортным модулем, отправляющим данные; заголовок транспортного уровня содержит также и другую служебную информацию; формат заголовка зависит от используемого транспортного протокола.

На транспортном уровне работают два основных протокола: UDP и TCP.

Протокол надежной доставки сообщений TCP

TCP (Transfer Control Protocol) – протокол контроля передачи, протокол TCP применяется в тех случаях, когда требуется гарантированная доставка сообщений.

Первая и последняя версия TCP - RFC-793 (Transmission Control Protocol J. Postel Sep-01-1981).

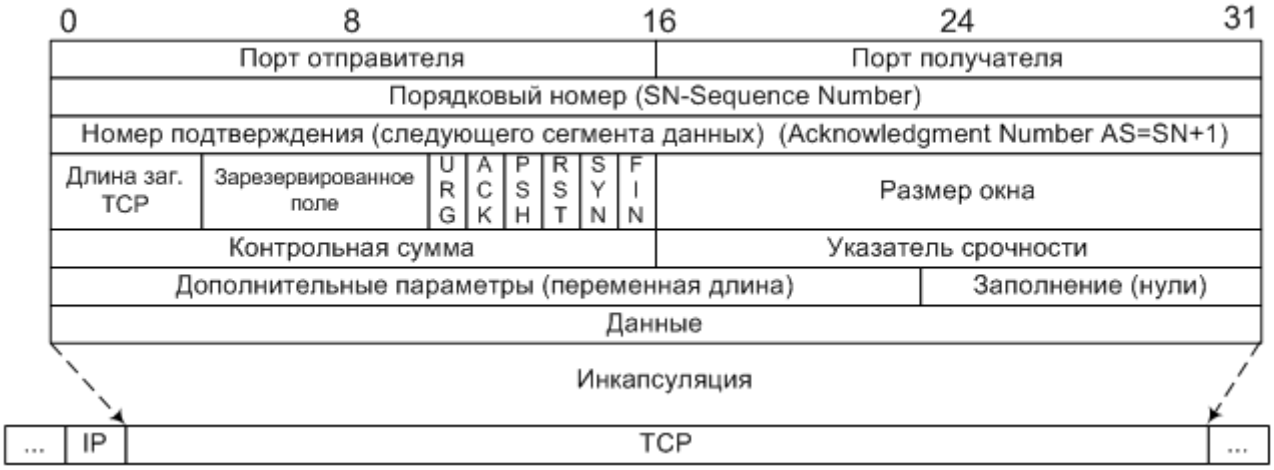
Основные особенности:

• Устанавливается соединение.

• Данные передаются сегментами. Модуль TCP нарезает большие сообщения (файлы) на пакеты, каждый из которых передается отдельно, на приемнике наоборот файлы собираются. Для этого нужен порядковый номер (Sequence Number - SN) пакета.

• Посылает запрос на следующий пакет, указывая его номер в поле "Номер подтверждения" (AS). Тем самым, подтверждая получение предыдущего пакета.

• Делает проверку целостности данных, если пакет битый посылает повторный запрос.



Структура дейтограммы tcp. Слова по 32 бита.

Длина заголовка - задается словами по 32бита.

Размер окна - количество байт, которые готов принять получатель без подтверждения.

Контрольная сумма - включает псевдо заголовок, заголовок и данные.

Указатель срочности - указывает последний байт срочных данных, на которые надо немедленно реагировать.

URG - флаг срочности, включает поле "Указатель срочности", если =0 то поле игнорируется.

ACK - флаг подтверждение, включает поле "Номер подтверждения, если =0 то поле игнорируется.

PSH - флаг требует выполнения операции push, модуль TCP должен срочно передать пакет программе.

RST - флаг прерывания соединения, используется для отказа в соединении

SYN - флаг синхронизация порядковых номеров, используется при установлении соединения.

FIN - флаг окончание передачи со стороны отправителя

Протокол udp

UDP (Universal Datagram Protocol) - универсальный протокол передачи данных, более облегченный транспортный протокол, чем TCP.

Первая и последняя версия UDP - RFC-768 (User Datagram Protocol J. Postel Aug-28-1980).

Основные отличия от TCP:

• Отсутствует соединение между модулями UDP.

• Не разбивает сообщение для передачи

• При потере пакета запрос для повторной передачи не посылается

UDP используется если не требуется гарантированная доставка пакетов , например, для потокового видео и аудио, DNS (т.к. данные небольших размеров). Если проверка контрольной суммы выявила ошибку или если процесса, подключенного к требуемому порту, не существует, пакет игнорируется (уничтожается). Если пакеты поступают быстрее, чем модуль UDP успевает их обрабатывать, то поступающие пакеты также игнорируются.

Структура дейтограммы udp. Слова по 32 бита.

Не все поля UDP-пакета обязательно должны быть заполнены. Если посылаемая дейтаграмма не предполагает ответа, то на месте адреса отправителя могут поме-щаться нули.

Протокол реального времени RTP

RTP (Real Time Protocol) - транспортный протокол для приложений реального времени.

RTCP (Real Time Control Protocol) - транспортный протокол обратной связи для приложения RTP.

IPv4

Четвёртая версия интернет-протокола IP работает с 1982 года, с момента развертывания в спутниковой сети SATNET, сформировавшей основу для сети Интернет. До сих пор IPv4 — основной протокол в Интернете.

IPv4 обеспечивает возможность адресации примерно 4,3 млрд адресов. Каждое устройство в публичных и частных сетях, использующих протокол TCP / IP, должно иметь IP-адрес для идентификации устройства и определения его местоположения. После быстрого роста интернет-трафика в 1990-х годах стало очевидно, что для подключения всех пользователей потребуется гораздо больше адресов, чем было доступно в адресном запасе IPv4.

Он работает на сетевом уровене моделей OSI. Будучи протоколом, не требующим установления соединения, он отправляет пакеты к месту назначения по различным маршрутам.

Deep Packet Inspection

Четвертая версия протокола поддерживает 32-битные адреса. Такой адрес состоит из 4 частей, каждая из которых разделена точкой. Например: 100.101.102.103. Диапазон каждой части — 0-255. Адреса IPv4 были разделены на различные классы в зависимости от диапазона IP-адресов.

IPv6

Протокол IPv6 был представлен в декабре 1995 года. Он был разработан Инженерным советом интернета (IETF) и является самой последней версией интернет-протокола. IPv6 более продвинутый, чем IPv4, и предоставляет лучшую функциональность.

Как было обозначено выше, каждому устройству в интернете назначается определенный уникальный IP-адрес. Новый протокол может предоставить практически бесконечное количество адресов для устройств и заменяет прошлую версию для обслуживания растущего числа трафика по всему миру и решения проблемы нехватки IP-адресов.

Количество адресов в IPv6 составляет 5 x 10 ^ 28 (около 79 228 162 514 264 337 593 543 950 336 октиллионов). Это означает, что протокол обеспечит возможность использования более 300 млн IP-адресов на каждого жителя Земли.

В отличие от IPv4, типичный адрес IPv6 состоит из 128 бит. Он состоит из восьми групп, каждая из которых включает четыре шестнадцатеричных цифр, разделенных «:». Вот пример: 3005: 0db6: 82a5: 0000: 0000: 7a1e: 1460: 5334.

В 2012 году доля IPv6 в интернет-трафике составляла около 5 %. На 2020 год, согласно данным Google, эта доля составляет около 30 %.

Разница между двумя версиями

Основное внешнее отличие четвертой и шестой версии протокола — структура IP-адреса. IPv4 использует четыре однобайтовых десятичных числа, разделенных точкой (172.268.0.1). IPv6 — шестнадцатеричные числа, разделенные двоеточиями (fe70 :: d5a9: 4521: d1d7: d8f4b11). Что еще:

- В IPv4 применяются числовые методы адресации, а в и IPv6 — буквенно-числовые.
- Длина адреса IPv4 составляет 32 бита, у IPv6 — 128 бит.
- IPv4 и IPv6 предлагают поля с 12 и 8 заголовками соответственно.
- Широковещательные каналы поддерживаются только в IPv4. IPv6 поддерживает многоадресные группы.
- Поле контрольной суммы присутствует в IPv4, но не в IPv6.
- Концепция сетевых масок переменной длины применима только к IPv4.
- Для определения MAC-адресов четвертая версия использует ARP, а IPv6 использует NDP.
- IPv4 поддерживает ручную настройку и настройку адреса DHCP, в IPv6 поддерживается автоматическая настройка адреса и настройка адреса с перенумерацией.
- IPv4 может генерировать до 4,29 млрд адресного массива, тогда как IPv6 — до 79 228 162 514 264 337 593 543 950 336 октиллионов.
- В IPv4 используются уникальные публичные и «частные» адреса для трафика, в IPv6 — глобально уникальные юникаст-адреса и локальные адреса (FD00::/8).

Улучшения в IPv6

- IPv6 обеспечивает более эффективную маршрутизацию, поскольку значительно уменьшает размер таблицы маршрутизации.
- У нового протокола формат заголовка проще, чем у IPv4.
- Обработка пакетов более эффективна, поскольку заголовки пакетов оптимизированы.
- В протокол встроена технология Quality of Service (QoS), которая определяет чувствительные к задержке пакеты.
- Более упрощенные задачи маршрутизаторов по сравнению с IPv4.
- IPv6 обеспечивает большую полезную нагрузку, чем IPv4.
- В IPv6 встроены аутентификация и частная поддержка по сравнению с IPv4.

Зачем переходить на IPv6

В интернете заканчиваются адреса IPv4. Это было неизбежно, учитывая, насколько широко распространились сети и сетевые устройства. Даже в локальной сети пользователям приходится использовать подсети просто потому, что устройства, например, в корпоративной сети, могли занять все адреса 192.68.1.#. Для этого был разработан IPv6, который предлагает больший пул адресов для использования.

Однако появляется другая проблема: перейти на IPv6 и оптимизировать работу с новым протоколом не так просто. У пользователя могут быть сотни устройств и множество локаций. Вдобавок всегда есть DNS, который необходимо обновить (что может быть равносильно простою). В конце концов, 192.168.1.1 запомнить намного проще, чем 0: 0: 0: 0: 0: ffff: c0a8: 101.

На обновление всех серверов и устройств, которые до этого работали только с IPv4, может уйти много денег и времени. Этого можно избежать, с помощью некоторых инструментов.

Как организовать плавную миграцию

IPv6 не имеет обратной совместимости с IPv4. Из-за этого многие администраторы избегают нового протокола. Что делать?

Во-первых, нужно переместить устройства в гибридную среду, в которой сосуществуют IPv4 и IPv6. Для многих переход на IPv6 начался много лет назад. Большинство аналитиков предсказывали, что на это уйдут годы, но гибридные модели дают даже больше времени, поскольку пользователи будут запускать свои сети с использованием обоих типов адресов.

Поскольку структуры адресов сильно отличаются друг от друга, а IPv6 использует другую архитектуру пакетов данных, устройства IPv4 и устройства IPv6 не могут взаимодействовать без использования шлюза.

Наиболее популярные гибридные стратегии совместного использования включают туннелирование, при котором трафик IPv6 инкапсулируется в заголовок IPv4. Хотя это приводит к дополнительным накладным расходам, двойному стеку, который осложняет работу сети и требует дополнительных ресурсов..

Предположим, у компании есть настольные компьютеры, которые используют IPv6, но серверы используют IPv4. Между ПК и серверами будет шлюз, который сделает возможным преобразование IPv6-адресов в IPv4-адреса.

Многие производители маршрутизаторов и коммутаторов разрабатывают устройства , которые помогают с переходом на IPv6. Поэтому когда больше не нужно подключаться к службам, которые все еще используют IPv4, можно перейти от гибридной среды к сети, полностью оборудованной для IPv6.

В комфортном переходе на IPv6 может помочь механизм NAT (Network Address Translation — трансляция сетевых адресов и портов), который применяется в IP-протоколах и позволяет заменять локальный (серый) IP-адрес на публичный (белый). Исчерпание IPv4 увеличивает затраты поставщика услуг, тогда как инвестиции в NAT снизят затраты.

Например, технология Carrier-grade NAT позволяет нескольким абонентам совместно использовать один публичный IPv4-адрес, что продлевает использование ограниченного адресного пространства IPv4 и делает миграцию с IPv6-адресацией проще.

Мы рекомендуем инструмент CG-NAT в рамках стратегии плавной миграции на IPv6 и поддержки DualStack IPv4/IPv6, которая обеспечивает одновременную работу NAT v4 и v6. Сохранение IPv4 с помощью технологий миграции CG-NAT и IPv6, доступных в виде аппаратных или виртуальных решений, позволит удовлетворить растущие потребности абонентов и обеспечит расширение сети для возможности новых подключений.

Вопросы для повторения

1. Что такое набор (стек) протоколов?

2. Какие наборы протоколов вы знаете? Чем они различаются?

3. Какой стек протоколов сегодня наиболее популярен? Почему?

4. Какие уровни модели OSI поддерживаются в стеке протоколов TCP/IP ?

5. В чем сходство и различие между протоколами TCP и UDP?