**Введение**

Сетевые приложения и сервисы на одном оконечном устройстве могут взаимодействовать с приложениями и сервисами, запущенными на другом аналогичном устройстве. Каким образом обеспечивается максимальная эффективность передачи этих данных по сети?

Протоколы сетевого уровня модели OSI определяют адресацию и процессы, которые позволяют упаковывать и передавать данные транспортного уровня. Инкапсуляция сетевого уровня обеспечивает прохождение данных по сети к адресату (или другой сети) с минимальной нагрузкой.

В этой главе основное внимание уделено роли сетевого уровня. В ней анализируется процесс разделения сетей на группы узлов для управления потоком пакетов данных в пределах одной сети. Кроме того, в ней описываются способы упрощения обмена данными между сетями. Такой межсетевой обмен данными называется маршрутизацией.

**Сетевой уровень**

Сетевой уровень, или уровень 3 OSI, предоставляет сервисы, позволяющие оконечным устройствам обмениваться данными по сети. Для выполнения такой сквозной передачи в сетевом уровне используются четыре основных процесса.

* **Адресация оконечных устройств**: подобно тому, как телефону присваивается индивидуальный номер, оконечным устройствам необходимо назначить уникальный IP-адрес для возможности идентификации в сети. Оконечное устройство с настроенным IP-адресом называется узлом.
* **Инкапсуляция**: сетевой уровень получает блок данных протокола (PDU) от транспортного уровня. Во время выполнения процесса, который называется инкапсуляцией, сетевой уровень добавляет информацию заголовка IP, например IP-адрес узла источника (отправляющего) и узла назначения (получающего). После добавления в блок PDU информации заголовка такой блок будет называться пакетом.
* **Маршрутизация**: сетевой уровень предоставляет сервисы, с помощью которых пакеты направляются к узлу назначения в другой сети. Для перемещения к другим сетям пакет должен быть обработан маршрутизатором. Роль маршрутизатора заключается в том, чтобы выбрать пути для пакетов и направить их к узлу назначения. Такой процесс называется маршрутизацией. До того, как достигнуть узла назначения, пакет может пройти через несколько промежуточных устройств. Каждый маршрут на пути пакета к узлу назначения называется переходом.
* **Деинкапсуляция**: по прибытии пакета на сетевой уровень узла назначения этот узел проверяет IP-заголовок пакета. Если IP-адрес назначения в заголовке совпадает с его собственным IP-адресом, заголовок IP удаляется из пакета. Процесс удаления заголовков из нижних уровней называется деинкапсуляцией. После деинкапсуляции пакета, выполняемой сетевым узлом, полученный блок PDU уровня 4 пересылается соответствующей службе на транспортном уровне.

В отличие от транспортного уровня (уровень 4 OSI), который управляет передачей данных между процессами, запущенными на каждом узле, протоколы сетевого уровня указывают структуру пакета и тип обработки, которые используются для перемещения данных от одного узла к другому. Функционирование без учета данных, передаваемых в каждом пакете, позволяет сетевому уровню передавать пакеты для нескольких типов коммуникации между несколькими узлами.

Анимация на рисунке демонстрирует процесс обмена данными.

**Протоколы сетевого уровня**

Существует несколько протоколов сетевого уровня, но, как правило, используются только следующие два (см. рисунок).

* Протокол IP версии 4 (IPv4)
* Протокол IP версии 6 (IPv6)

Среди других устаревших протоколов сетевого уровня, которые не нашли широкого применения, можно выделить следующие.

* Межсетевой обмен пакетами компании Novell (протокол IPX)
* AppleTalk
* Сетевое обслуживание без установления соединения (CLNS/DECNet)

Эти устаревшие протоколы будут упомянуты только поверхностно.

**Характеристики IP**

IP — это сервис сетевого уровня, который реализовывается набором протоколов TCP/IP.

IP был разработан как протокол с низкой нагрузкой. Он обеспечивает только те функции, которые необходимы для доставки пакета от узла источника к узлу назначения по взаимосвязанной системе сетей. Этот протокол не предназначен для мониторинга и управления потоком пакетов. При необходимости эти функции выполняют другие протоколы на других уровнях.

К основным характеристикам IP относятся следующие.

* **Без установления соединения**: перед отправкой пакетов данных соединение с узлом назначения не устанавливается.
* **Доставка с максимальными усилиями (ненадёжная)**: доставка пакетов не гарантируется.
* **Независимость от среды**: функционирует независимо от среды, в которой передаются данные.

**IP: без установления соединения**

Основная роль сетевого протокола — пересылка пакетов между узлами при наименьшей нагрузке на сеть. Сетевой уровень не имеет отношения (и даже не обладает какой-либо информацией) к типу обмена данными, который содержится внутри пакета. IP является протоколом без установления соединения, а это означает, что перед отправкой данных выделенное сквозное соединение не устанавливается. По своей сути обмен данными без установления соединения аналогичен отправке письма без предварительного уведомления получателя.

Как показано на рис. 1, почтовая служба использует информацию, указанную на конверте, чтобы доставить письмо получателю. Адрес на конверте не содержит информации о том, будет ли получатель присутствовать в момент доставки письма или о том, сможет ли он его прочитать. По сути, почтовой службе неизвестно содержание доставляемого пакета, и, следовательно, она не может задействовать какие-либо механизмы исправления ошибок.

При передаче данных без установления соединения используется аналогичный принцип.

Протокол IP не использует соединения и, следовательно, ему не требуется первоначального обмена контрольной информацией для установления сквозного подключения до начала пересылки пакетов. IP также не нуждается в дополнительных полях в заголовке блока данных протокола (PDU) для поддержки установленного соединения. Этот процесс значительно снижает нагрузку IP. Тем не менее, без предварительно установленного сквозного подключения отправителям неизвестно, имеются ли устройства-адресаты и способны ли они функционировать в момент отсылки пакетов, а также получит ли пакет узел назначения и смогут ли устройства-адресаты получить доступ к пакету и прочитать его. На рис. 2 показан пример обмена данными без установления соединения.

**IP: доставка с максимальными усилиями**

IP часто называют ненадёжным протоколом или протоколом доставки с максимальными усилиями. Это не означает, что в некоторых случаях протокол IP функционирует надлежащим образом, а все остальное время работает с ошибками, или то, что он плохо подходит для передачи данных. «Ненадёжный» протокол — тот, который не способен контролировать не доставленные или повреждённые пакеты и восстанавливаться в случае их появления. Это связано с тем, что хотя отправляемые пакеты IP и содержат сведения о месте доставки, в них отсутствует информация, которую можно обработать, чтобы сообщить отправителю об успешно выполненной доставке. Заголовок пакета не содержит данных синхронизации для отслеживания очерёдности доставки пакетов. Также не предусмотрены подтверждения доставки пакетов по IP и отсутствуют данные контроля ошибок, с помощью которых можно отследить, доставлены ли пакеты без повреждений. Пакеты могут прибыть на узел назначения повреждёнными или с нарушенным порядком, либо не прибыть совсем. В случае возникновения таких ошибок информация, которая содержится в заголовке IP, не позволяет выполнить повторную пересылку пакетов.

Если отсутствие пакетов или несоблюдение очерёдности создаёт проблемы для приложений, использующих данные, сервисы верхнего уровня, например TCP, должны устранить эти проблемы. Это обеспечивает высокую эффективность работы протокола IP. Если нагрузки надёжности были включены в IP, то процессы обмена данными, для которых не требуется подключения, или надёжность могут пострадать от уменьшения пропускной способности и задержек, вызванных такими нагрузками. В пакете протоколов TCP/IP транспортный уровень может использовать либо TCP, либо UDP, в зависимости от необходимости обеспечения надёжности передачи данных. Если решение об обеспечении надёжности принимается на транспортном уровне, это позволит IP быстрее адаптироваться к различным типам передачи данных.

На рисунке приводится пример передачи данных с использованием протокола IP. Протоколам с установлением соединения, таким как TCP, для установки соединения требуется обмен управляющими данными. Для предоставления информации о подключении протоколу TCP также необходимы дополнительные поля в заголовке PDU.

**IP: независимость от среды**

Сетевой уровень также не нагружается характеристиками данных среды, в которой передаются пакеты. Протокол IP действует независимо от среды, которая служит для передачи данных на нижних уровнях стека протоколов. Как показано на рисунке, любой отдельный пакет IP может передаваться по кабелю (с помощью электрических импульсов, например оптических сигналов по волоконному кабелю) или в виде радиосигналов в беспроводных сетях.

Канальный уровень OSI должен принять пакет IP и подготовить его для передачи в коммуникационной среде. Это означает, что пересылка пакетов IP не ограничивается какой-либо конкретной коммуникационной средой.

Тем не менее, существует одна важная характеристика среды передачи, которая учитывается на сетевом уровне: максимальный размер блока PDU, который способна переслать каждая среда. Эта характеристика называется максимальным размером передаваемого блока данных (MTU). Часть обмена контрольными данными между канальным уровнем и сетевым уровнем — это установление максимального размера пакета. Канальный уровень передаёт значение MTU к сетевому уровню. Затем сетевой уровень определяет размер пакетов.

В некоторых случаях промежуточное устройство (как правило, это маршрутизатор) должно разделить пакет во время его пересылки из одной среды обработки данных в среду с меньшим максимальным размером пакета. Этот процесс называется разделением пакета или фрагментацией.

**Ограничения IPv4**

На протяжении многих лет протокол IPv4 периодически обновлялся для решения новых задач. Тем не менее, даже в результате изменений IPv4 по-прежнему имеет три основных недостатка.

* **Нехватка IP-адресов**. IPv4 может предложить лишь ограниченное количество уникальных общедоступных IP-адресов. Несмотря на то, что существует примерно 4 миллиарда IPv4-адресов, возросшее число новых устройств, в которых используется протокол IP, а также потенциальный рост менее развитых регионов привели к необходимости дополнительно увеличить количество адресов.
* **Расширение таблицы интернет-маршрутизации**. Таблица маршрутизации используется маршрутизаторами для определения оптимальных путей пересылки данных. По мере увеличения количества серверов (узлов), подключённых к Интернету, также растет число сетевых маршрутов. Эти маршруты IPv4 потребляют значительное количество памяти и ресурсов процессоров интернет-маршрутизаторов.
* **Нехватка сквозных соединений**. Преобразование сетевых адресов (NAT) представляет собой технологию, которая обычно применяется в сетях IPv4. NAT позволяет различным устройствам совместно использовать один публичный IP-адрес. При этом, поскольку публичный IP-адрес используется совместно, IP-адрес узла внутренней сети скрыт. Это может представлять проблему при использовании технологий, для которых необходимы сквозные подключения.

В начале 90-х годов специалисты инженерной группы по развитию Интернета (IETF) подняли вопрос о недостатках протокола IPv4 и начали поиски альтернативных решений. Результатом поисков стала разработка протокола IP версии 6 (IPv6). IPv6 помогает преодолеть ограничения протокола IPv4 и значительно расширяет доступные возможности, предлагая функции, которые оптимально соответствуют текущим и прогнозируемым сетевым требованиям.

К улучшениям, которые предлагает протокол IPv6, относятся следующие.

* **Расширенное адресное пространство**: IPv6-адреса используют 128-битную иерархическую адресацию, в отличие от протокола IPv4, использующего 32 бита. Это существенно увеличивает количество доступных IP-адресов.
* **Улучшенная обработка пакетов**: структура заголовка IPv6 была упрощена благодаря уменьшению количества полей. Это повышает обработку пакетов промежуточными маршрутизаторами, а также предоставляет поддержку расширений и дополнительных параметров, обеспечивая повышенную масштабируемость и долговечность.
* **Отсутствие необходимости в использовании NAT**: благодаря большому количеству общедоступных IPv6-адресов трансляция сетевых адресов (NAT) не требуется. Клиентские узлы, от самых крупных предприятий до жилых домов, могут получить общедоступный сетевой IPv6-адрес. Это позволяет устранить некоторые проблемы, связанные с преобразованием сетевых адресов, которые возникают при работе приложений, требующих наличия сквозного подключения.
* **Интегрированная безопасность**: протокол IPv6 изначально обладает средствами для аутентификации и обеспечения конфиденциальности. При использовании протокола IPv4 для этого требовалось реализовать дополнительные функции.

32-битное пространство адресов IPv4 предусматривает примерно 4 294 967 296 уникальных адресов. Из этого количества могут быть назначены только 3,7 миллиарда, поскольку система адресации IPv4 подразделяет адреса на классы, резервируя адреса для многоадресных рассылок, тестирования и других особых целей.

Как показано на рисунке, адресное пространство протокола IP версии 6 поддерживает 340 282 366 920 938 463 463 374 607 431 768 211 456 или 340 ундециллионов адресов, что примерно равно количеству песчинок на Земле.

**Решение о перенаправлении узла**

Другим предназначением сетевого узла является пересылка пакетов между узлами. Узел может отправить пакет на следующие адреса.

* **Самому себе**: специальный IP-адрес, который представлен как 127.0.0.1 и называется интерфейсом loopback. Этот loopback-адрес автоматически назначается узлу при запуске TCP/IP. Возможность узла отправлять пакет самому себе, используя сетевые функции, полезна для тестирования. Любой IP-адрес в пределах сети 127.0.0.0/8 относится к локальному узлу.
* **Локальный узел**: узел в той же сети, в которой также находится отправляющий узел. Узлы используют один и тот же сетевой адрес.
* **Удалённый узел**: узел в удалённой сети. Узлы не используют один и тот же сетевой адрес.

Какому узлу адресован пакет — локальному или удалённому — определяется комбинацией IP-адреса и маски подсети устройства источника (или отправляющего устройства), которые сравниваются с IP-адресом и маской подсети устройства назначения.

В домашней или корпоративной сети могут находиться несколько проводных и беспроводных устройств, соединённых друг с другом с помощью промежуточного устройства, такого как коммутатор локальной сети или точка беспроводного доступа (WAP). Это промежуточное устройство обеспечивает соединение между локальными узлами в локальной сети. Локальные узлы могут получать доступ друг к другу и обмениваться информацией без использования каких-либо дополнительных устройств. Если узел отправляет пакет устройству, которое настроено в этой же IP-сети в качестве главного устройства, пакет просто пересылается из интерфейса узла через промежуточное устройство прямо на устройство назначения.

Разумеется, в большинстве случаев нам требуется, чтобы наши устройства могли устанавливать соединения за пределами сегмента локальной сети: подключаться к другим домам, офисам и Интернету. Устройства, которые не входят в сегмент локальной сети, называются удалёнными узлами. Если исходное устройство отправляет пакет к удалённому устройству назначения, то в этом случае требуется помощь маршрутизаторов и выполнение маршрутизации. Маршрутизация — это процесс определения наилучшего пути к узлу назначения. Маршрутизатор, подключённый к сегменту локальной сети, называется **шлюзом по умолчанию**.

**Шлюз по умолчанию**

Шлюз по умолчанию — это устройство, которое направляет трафик из локальной сети к устройствам в удалённых сетях. В домашних условиях или на малых предприятиях шлюз по умолчанию часто используется для подключения локальной сети к Интернету.

Если узел отправляет пакет устройству в другой IP-сети, то в этом случае он должен пересылать пакет через промежуточное устройство к шлюзу по умолчанию. Это связано с тем, что главное устройство не сохраняет информацию о маршрутизации за пределами локальной сети, чтобы достичь удалённых адресатов. Шлюз по умолчанию, напротив, сохраняет такую информацию. Шлюз по умолчанию, в роли которого чаще всего выступает маршрутизатор, сохраняет таблицу маршрутизации. Таблица маршрутизации — это файл данных в ОЗУ, который используется для хранения информации о маршрутах для напрямую подключённых сетей, а также записей удалённых сетей, о которых стало известно устройству. Маршрутизатор использует информацию в таблице маршрутизации, чтобы определить наилучший путь к узлам назначения.

Итак, каким образом узел отслеживает необходимость пересылки пакетов на шлюз по умолчанию? На узлах должна храниться их собственная локальная таблица маршрутизации, чтобы пакеты сетевого уровня гарантированно направлялись к нужной сети назначения. Как правило, локальная таблица узла содержит следующую информацию.

* **Прямое подключение** — маршрут к интерфейсу loopback (127.0.0.1).
* **Маршрут локальной сети** — информация о сети, к которой подключён узел, автоматически добавляется в таблицу маршрутизации узла.
* **Локальный маршрут по умолчанию** — это маршрут, который должны пройти пакеты, чтобы достичь всех удалённых сетевых адресов. Маршрут по умолчанию создаётся в том случае, когда на узле имеется адрес шлюза по умолчанию. Адрес шлюза по умолчанию — это IP-адрес сетевого интерфейса маршрутизатора, подключённого к локальной сети. Адрес шлюза по умолчанию можно настроить на узле вручную, либо его можно получить динамически.

Важно отметить, что маршрут по умолчанию, а, следовательно, и шлюз по умолчанию используется только в том случае, если узлу необходимо пересылать пакеты к удалённой сети. Он не требуется (и его можно даже не настраивать), если выполняется только отправка пакетов устройствам в локальной сети.

В качестве примера представьте себе сетевой принтер или сканер. Если на сетевом принтере настроены IP-адрес и маска подсети, то узлы могут отправлять на принтер документы для печати. Кроме того, принтер может переслать отсканированные документы на любой локальный узел. До тех пор, пока принтер используется только локально, адрес шлюза по умолчанию не требуется. В действительности, не настроив на принтере адрес шлюза по умолчанию, вы фактически отклоняете доступ к Интернету, что может являться разумным решением с точки зрения безопасности. Отсутствие интернет-подключения означает и отсутствие внешних угроз безопасности. Поскольку устройства, например принтеры, могут автоматически обновляться через Интернет, обычно проще и безопаснее устанавливать такие обновления с помощью локальной загрузки с безопасного локального узла, например, с компьютера.