Министерство образования Республики Беларусь

Учреждение образования

«Белорусский государственный университет

информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к курсовой работе

на тему

ПОДСИСТЕМА МАРШРУТИЗАТОРА

БГУИР КР 1-40 02 01 043 ПЗ

Студент А. С. Басько

Руководитель В. А. Марцинкевич

МИНСК 2021

**СОДЕРЖАНИЕ**

[**ВВЕДЕНИЕ** 3](#_Toc88664520)

[**1 ОБЗОР ЛИТЕРАТУРЫ** 4](#_Toc88664521)

[**1.1 IPv6** 4](#_Toc88664522)

[**1.2 Статическая конфигурация GUA на маршрутизаторе** 5](#_Toc88664523)

[**1.3 Динамическая адресация для IPv6 GUA** 6](#_Toc88664524)

[**1.4 Динамическая адресация для LLA IPv6** 7](#_Toc88664525)

[**1.4.1 Сообщения ICMPv4 и ICMPv6** 7](#_Toc88664526)

[**1.5 Возможности TCP** 8](#_Toc88664527)

[**1.6 Возможности UDP** 9](#_Toc88664528)

[**1.7 Надежность и контроль потока** 10](#_Toc88664529)

[**ЗАКЛЮЧЕНИЕ** 13](#_Toc88664530)

## **ВВЕДЕНИЕ**

Компьютерные сети являются одной из важнейших частей всех любой современной сферы деятельности. Они нужны практически везде, например, заводы, учебные заведения, исследовательские лаборатории, банковские системы, офисы, кафе и рестораны и многое другое. Благодаря компьютерным сетям работа во всех сферах деятельности становиться намного быстрей и надежней нежели без них.

Основной задачей компьютерных сетей является совместный и одновременный доступ к данным. В наше время данных очень много, так как быстрое развитие информационных технологий повлияло на развитие автоматизации и внедрение компьютерных технологий во всех видах деятельности человека, что повлекло за собой необходимость быстрого доступа к большим объемам данных. Именно компьютерные сети и помогают решить эту проблему. Например, ученому нужны данные исследований, которые сохраняются на исследовательском оборудовании, работнику офиса необходимо распечатать документы, команда программистов нуждается в общем доступе к коду, над которым они работают. Другими словами, связь между множеством компьютеров и устройствами позволяет ускорить и упростить работу любого предприятия. Так же они позволяют обеспечить резервное копирование данных на сервере и облачных хранилищах, что обеспечивает восстановление важных данных в случае их утери.

Неисправность компьютерных сетей, может заморозить все производство, в следствие чего компания понесет большие убытки. Для предотвращения подобных ситуаций по всему миру разрабатываются методы их предотвращения и минимизации.

В наше время использование компьютерных сетей необходимы любому современному производству, для того чтобы оставаться выгодным и конкурентоспособным.

В качестве курсовой работы была избирательно выбрана и описана изученная, при ознакомлении с курсом CCNA: Introduction to Networks (Сертификация циско: введение в сети), информация.

Этот вводный курс о работе сетей помог начать подготовку к карьере в сфере сетевых технологий. Первый курс из серии CCNA, включающей три курса, содержит вводные сведения об архитектурах, моделях, протоколах и элементах сетей. В рамках этого курса мы научились создавать простые локальные сети, получили практические знания о схемах IP-адресации, базовых понятиях сетевой безопасности, а также научились выполнять настройку основных параметров маршрутизаторов и коммутаторов.

Лабораторные работы выполнялись в программах Cisco Packet Tracer, а также GNS3.

Вся, приведенная ниже информация была предоставлена на официальном ресурсе компании Cisco: netacad.com.

## **1 ОБЗОР ЛИТЕРАТУРЫ**

# **1.1 IPv6**

IPv6 разработан, чтобы стать преемником IPv4. IPv6 имеет большее 128-битное адресное пространство, обеспечивая 340 ундециллионов (т. е. 340, за которыми следуют 36 нулей) возможных адресов. Однако IPv6 — это больше, чем просто адреса большего размера.

Когда IETF приступила к разработке преемника IPv4, она использовала эту возможность, чтобы исправить ограничения IPv4 и включить улучшения. Одним из примеров является протокол управляющих сообщений Интернета версии 6 (ICMPv6), который включает разрешение адресов и автоконфигурацию адресов, которых нет в ICMP для IPv4 (ICMPv4).

Истощение адресного пространства IPv4 было мотивирующим фактором для перехода на IPv6. По мере того, как Африка, Азия и другие регионы мира становятся все более подключенными к Интернету, для удовлетворения этого роста не хватает адресов IPv4. Как показано на рисунке, у четырех из пяти RIR закончились адреса IPv4.

IPv4 имеет теоретический максимум 4,3 миллиарда адресов. Частные адреса в сочетании с преобразованием сетевых адресов (NAT) сыграли важную роль в замедлении истощения адресного пространства IPv4. Однако NAT проблематичен для многих приложений, создает задержки и имеет ограничения, которые серьезно затрудняют одноранговую связь.

С постоянно растущим числом мобильных устройств операторы мобильной связи лидируют в переходе на IPv6. Два ведущих оператора мобильной связи в США сообщают, что более 90% их трафика проходит через IPv6.

Большинство ведущих интернет-провайдеров и контент-провайдеров, таких как YouTube, Facebook и NetFlix, также осуществили переход. Многие компании, такие как Microsoft, Facebook и LinkedIn, переходят на IPv6 только внутри страны. В 2018 году широкополосный интернет-провайдер Comcast сообщил о развертывании более 65%, а British Sky Broadcasting - более 86%.

Как и в случае с IPv4, существуют разные типы адресов IPv6. Фактически, существует три широких категории адресов IPv6:

* Одноадресная рассылка - IPv6-адрес одноадресной рассылки однозначно определяет интерфейс на устройстве с поддержкой IPv6.
* Многоадресная рассылка - многоадресный адрес IPv6 используется для отправки одного пакета IPv6 нескольким получателям.
* Anycast - Anycast-адрес IPv6 - это любой одноадресный IPv6-адрес, который может быть назначен нескольким устройствам. Пакет, отправленный на произвольный адрес, направляется на ближайшее устройство, имеющее этот адрес. Адреса Anycast выходят за рамки этого курса.

В отличие от IPv4, IPv6 не имеет широковещательного адреса. Однако существует многоадресный IPv6-адрес для всех узлов, который по существу дает тот же результат.

Префикс или сетевая часть IPv4-адреса может быть идентифицирована по десятичной маске подсети с точками или длине префикса (обозначение косой черты). Например, IPv4-адрес 192.168.1.10 с десятичной маской подсети с точками 255.255.255.0 эквивалентен 192.168.1.10/24.

В IPv6 это называется только длиной префикса. IPv6 не использует десятичную маску подсети с разделительными точками. Как и в случае с IPv4, длина префикса представлена в виде косой черты и используется для обозначения сетевой части адреса IPv6.

Длина префикса может находиться в диапазоне от 0 до 128. Рекомендуемая длина префикса IPv6 для локальных сетей и большинства других типов сетей составляет / 64

# **1.2 Статическая конфигурация GUA на маршрутизаторе**

GUA IPv6 — это то же самое, что и общедоступные адреса IPv4. Они глобально уникальны и маршрутизируются в Интернете IPv6. LLA IPv6 позволяет двум устройствам с поддержкой IPv6 взаимодействовать друг с другом по одному каналу (подсети). На маршрутизаторах легко статически настроить GUA и LLA IPv6, чтобы помочь вам создать сеть IPv6.

Большинство команд настройки и проверки IPv6 в Cisco IOS аналогичны своим аналогам для IPv4. Во многих случаях единственная разница заключается в использовании ipv6 вместо ip в командах.

Например, команда Cisco IOS для настройки IPv4-адреса на интерфейсе — это [IP-адрес IP-адрес маска подсети]. Напротив, команда для настройки GUA IPv6 на интерфейсе — это ipv6-адрес ipv6- адрес / длина префикса.

В примере конфигурации используется топология, показанная на рисунке, и следующие подсети IPv6:

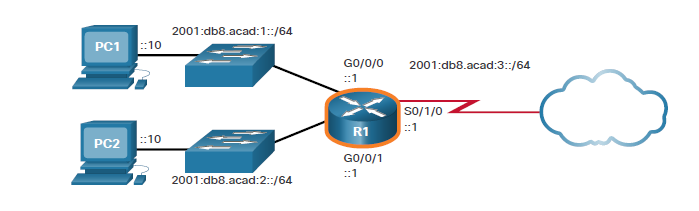
1. 2001: db8: acad: 1: / 64
2. 2001: db8: acad: 2: / 64
3. 2001: db8: acad: 3: / 64

Рисунок 1.1 – Пример топологии для конфигурации

Конфигурация IPv6 GUA на маршрутизаторе R1

R1(config)# interface gigabitethernet 0/0/0

R1(config-if)# ipv6 address 2001:db8:acad:1::1/64

R1(config-if)# no shutdown R1(config-if)# exit

R1(config)# interface gigabitethernet 0/0/1

R1(config-if)# ipv6 address 2001:db8:acad:2::1/64

R1(config-if)# no shutdown R1(config-if)# exit

R1(config)# interface serial 0/1/0

R1(config-if)# ipv6 address 2001:db8:acad:3::1/64

R1(config-if)# no shutdown

# **1.3 Динамическая адресация для IPv6 GUA**

Сообщения RS и RA

Если вы не хотите статически настраивать GUA IPv6, не о чем беспокоиться. Большинство устройств получают свои GUA IPv6 динамически.

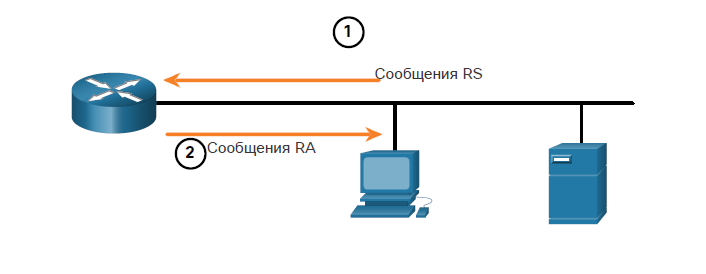
Для GUA устройство динамически получает адрес через сообщения протокола управляющих сообщений Интернета версии 6 (ICMPv6). Маршрутизаторы IPv6 периодически отправляют сообщения ICMPv6 RA . Каждые 200 секунд всем устройствам с поддержкой IPv6 в сети. Сообщение RA также будет отправлено в ответ на отправку хостом сообщения ICMPv6 RS, которое является запросом сообщения RA. Оба сообщения показаны на рисунке.

Рисунок 1.2 – Пример отправки сообщений

1. Сообщения RS отправляются на все маршрутизаторы IPv6 хостами, запрашивающими информацию об адресации.

2. Сообщения RA отправляются на все узлы IPv6. Если используется метод 1 (только SLAAC), RA включает в себя сетевой префикс, длину префикса и информацию о шлюзе по умолчанию.

Сообщения RA находятся на интерфейсах Ethernet маршрутизатора IPv6. На маршрутизаторе должна быть включена маршрутизация IPv6, которая по умолчанию отключена. Чтобы включить маршрутизатор в качестве маршрутизатора IPv6, необходимо использовать команду глобальной конфигурации ipv6 unicast-routing .

Сообщение ICMPv6 RA — это предложение устройству о том, как получить IPv6 GUA. Окончательное решение остается за операционной системой устройства. Сообщение ICMPv6 RA включает следующее:

Сетевой префикс и длина префикса - сообщает устройству, к какой сети оно принадлежит.

Адрес шлюза по умолчанию — это IPv6 LLA, исходный IPv6-адрес сообщения RA.

Адреса DNS и доменное имя — это адреса DNS-серверов и доменное имя.

Есть три метода для сообщений RA:

Метод 1: SLAAC - «У меня есть все, что вам нужно, включая префикс, длину префикса и адрес шлюза по умолчанию».

Метод 2: SLAAC с сервером DHCPv6 без сохранения состояния - «Вот моя информация, но вам необходимо получить другую информацию, например адреса DNS, от сервера DHCPv6 без отслеживания состояния».

Метод 3: DHCPv6 с отслеживанием состояния (без SLAAC) - «Я могу дать вам адрес шлюза по умолчанию. Вам нужно запросить у DHCPv6-сервера с отслеживанием все остальную информацию».

# **1.4 Динамическая адресация для LLA IPv6**

Все устройства IPv6 должны иметь LLA IPv6. Как и GUA IPv6, вы также можете создавать LLA динамически. Независимо от того, как вы создаете свои LLA (и GUA), важно проверять всю конфигурацию адресов IPv6.

# **1.4.1 Сообщения ICMPv4 и ICMPv6**

Хотя IP — это только протокол максимальной эффективности, пакет TCP / IP действительно обеспечивает сообщения об ошибках и информационные сообщения при обмене данными с другим IP-устройством. Эти сообщения отправляются с использованием служб ICMP. Эти сообщения предназначены для предоставления обратной связи по вопросам, связанным с обработкой IP-пакетов при определенных условиях, а не для обеспечения надежности IP. Сообщения ICMP не требуются и часто не разрешаются в сети по соображениям безопасности.

ICMP доступен как для IPv4, так и для IPv6. ICMPv4 — это протокол обмена сообщениями для IPv4. ICMPv6 предоставляет те же услуги для IPv6, но включает дополнительные функции. В этом курсе термин ICMP будет использоваться для обозначения как ICMPv4, так и ICMPv6.

Типы сообщений ICMP и причины их отправки обширны. Сообщения ICMP, общие для ICMPv4 и ICMPv6 и обсуждаемые в этом модуле, включают:

1. Доступность хоста
2. Пункт назначения или служба недоступны
3. Время истекло

Доступность хоста

Эхо-сообщение ICMP может использоваться для проверки доступности хоста в IP-сети. Локальный хост отправляет хосту эхо-запрос ICMP. Если хост доступен, целевой хост отвечает эхо-ответом. Такое использование сообщений ICMP Echo лежит в основе утилиты ping .

Чтобы проверить возможность подключения к другому узлу в сети, на адрес узла отправляется эхо- запрос с помощью команды ping . Если хост по указанному адресу получает эхо-запрос, он отвечает эхо-ответом. Когда получен каждый эхо-ответ, ping предоставляет обратную связь о времени между отправкой запроса и получением ответа. Это может быть мерой производительности сети.

Ping имеет значение тайм-аута для ответа. Если ответ не получен в течение тайм-аута, ping выдает сообщение, указывающее, что ответ не был получен. Это может указывать на наличие проблемы, но также может указывать на то, что в сети включены функции безопасности, блокирующие сообщения ping. Обычно первый эхо-запрос до истечения времени ожидания, если разрешение адреса (ARP или ND) необходимо выполнить перед отправкой эхо-запроса ICMP.

После того, как все запросы отправлены, утилита ping предоставляет сводку, которая включает процент успешных попыток и среднее время возврата к месту назначения.

Типы тестов подключения, выполняемых с помощью команды ping, включают следующее:

1. Проверка локальной петли
2. Проверка связи шлюза по умолчанию
3. Проверка связи с удаленным хостом

# **1.5 Возможности TCP**

Помимо поддержки основных функций сегментации и повторной сборки данных, TCP также предоставляет следующие услуги:

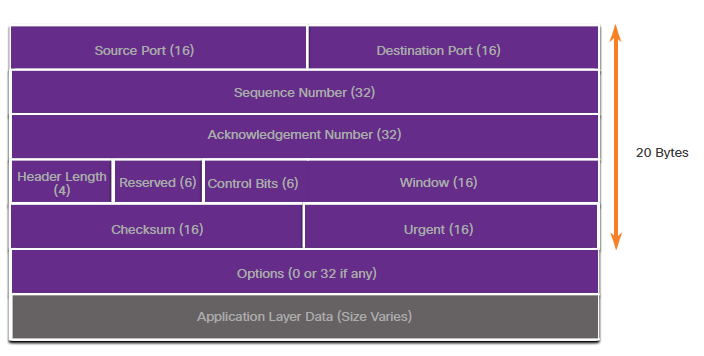
1. Устанавливает сеанс - TCP — это протокол с установлением соединения, который согласовывает и устанавливает постоянное соединение (или сеанс) между исходным и целевым устройствами до пересылки любого трафика. Посредством установления сеанса устройства согласовывают объем трафика, который может быть перенаправлен в данный момент времени, и данными связи между ними можно точно управлять.
2. Обеспечивает надежную доставку - по многим причинам сегмент может быть поврежден или полностью утерян, поскольку он передается по сети. TCP гарантирует, что каждый сегмент, отправленный источником, прибывает в пункт назначения.
3. Обеспечивает доставку в том же порядке - поскольку сети могут предоставлять несколько маршрутов с разной скоростью передачи, данные могут поступать в неправильном порядке. Путем нумерации и упорядочивания сегментов TCP обеспечивает повторную сборку сегментов в правильном порядке.
4. Поддерживает управление потоком - сетевые узлы имеют ограниченные ресурсы (например, память и вычислительную мощность). Когда TCP знает, что эти ресурсы перегружены, он может потребовать от отправляющего приложения снизить скорость потока данных. Это делается с помощью TCP, регулирующего объем данных, передаваемых источником. Управление потоком может предотвратить необходимость повторной передачи данных, когда ресурсы принимающего хоста перегружены.

Рисунок 1.3 – Поля в заголовке TCP

TCP - хороший пример того, как разные уровни набора протоколов TCP / IP выполняют определенные роли. TCP выполняет все задачи, связанные с разделением потока данных на сегменты, обеспечивая надежность, контролируя поток данных и переупорядочивая сегменты. TCP освобождает приложение от необходимости управлять любой из этих задач. Приложения, подобные тем, которые показаны на рисунке, могут просто отправлять поток данных на транспортный уровень и использовать службы TCP.

# **1.6 Возможности UDP**

UDP - настолько простой протокол, что его обычно описывают в терминах того, чего он не делает по сравнению с TCP.

Функции UDP включают следующее:

1. Данные восстанавливаются в порядке их получения.
2. Потерянные сегменты не отправляются повторно.
3. Нет установления сеанса.
4. Отправка не информируется о доступности ресурса.

UDP — это протокол без сохранения состояния, то есть ни клиент, ни сервер не отслеживают состояние сеанса связи. Если при использовании UDP в качестве транспортного протокола требуется надежность, это должно обрабатываться приложением.

Одним из наиболее важных требований для передачи видео и голоса в реальном времени по сети является то, чтобы данные продолжали быстро передаваться. Приложения для передачи видео и голоса в реальном времени могут допускать некоторую потерю данных с минимальным или отсутствующим заметным эффектом и идеально подходят для UDP.

Блоки связи в UDP называются дейтаграммами или сегментами. Эти дейтаграммы отправляются протоколом транспортного уровня с максимальной эффективностью.

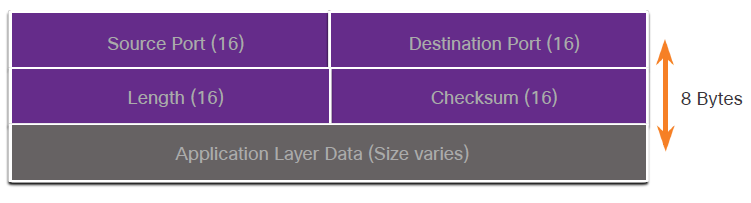
Заголовок UDP намного проще, чем заголовок TCP, потому что он имеет только четыре поля и требует 8 байтов (т. е. 64 бита).

Рисунок 1.4 – Поля в заголовке UDP

# **1.7 Надежность и контроль потока**

Причина, по которой TCP является лучшим протоколом для некоторых приложений, заключается в том, что, в отличие от UDP, он повторно отправляет отброшенные пакеты и нумерует пакеты, чтобы указать их правильный порядок перед доставкой. TCP также может помочь поддерживать поток пакетов, чтобы устройства не были перегружены.

Бывают случаи, когда сегменты TCP не достигают места назначения. В других случаях сегменты TCP могут поступать не по порядку. Чтобы исходное сообщение было воспринято получателем, все данные должны быть получены, и данные в этих сегментах должны быть повторно собраны в исходном порядке. Для достижения этой цели порядковые номера назначаются в заголовке каждого пакета. Порядковый номер представляет собой первый байт данных сегмента TCP.

Во время настройки сеанса устанавливается начальный порядковый номер (ISN). Этот ISN представляет собой начальное значение байтов, которые передаются принимающему приложению. Поскольку данные передаются во время сеанса, порядковый номер увеличивается на количество переданных байтов. Это отслеживание байтов данных позволяет однозначно идентифицировать и подтверждать каждый сегмент. Затем можно определить недостающие сегменты.

ISN не начинается с единицы, а фактически представляет собой случайное число. Это сделано для предотвращения определенных типов злонамеренных атак. Для простоты мы будем использовать ISN 1 для примеров в этой главе.

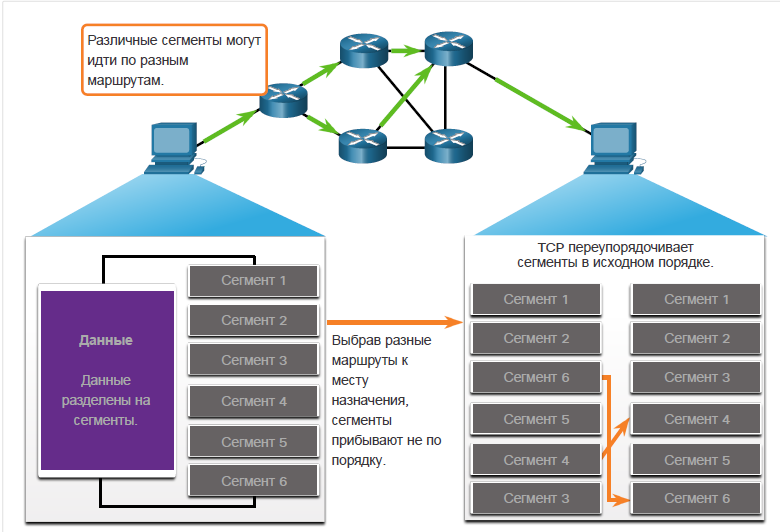
Порядковые номера сегментов указывают, как заново собрать и изменить порядок полученных сегментов, как показано на рисунке.

Рисунок 1.5 – Сегменты TCP переупорядочены в месте назначения

Принимающий процесс TCP помещает данные из сегмента в принимающий буфер. Затем сегменты размещаются в правильном порядке и передаются на уровень приложения при повторной сборке. Любые сегменты, поступающие с неупорядоченными порядковыми номерами, задерживаются для последующей обработки. Затем, когда прибывают сегменты с недостающими байтами, эти сегменты обрабатываются по порядку.

Как и сегменты с TCP, когда дейтаграммы UDP отправляются адресату, они часто идут разными путями и прибывают в неправильном порядке. UDP не отслеживает порядковые номера, как это делает TCP. UDP не имеет возможности переупорядочить датаграммы в порядке их передачи, как показано на рисунке.

Следовательно, UDP просто повторно собирает данные в том порядке, в котором они были получены, и пересылает их приложению. Если последовательность данных важна для приложения, приложение должно определить правильную последовательность и определить, как данные должны обрабатываться.

## **ЗАКЛЮЧЕНИЕ**

Изучение курса показало, насколько важна технология компьютерных сетей в наше время, в независимости от отрасли, в которой работает предприятие. Сейчас они необходимы практически везде, поскольку они упрощают и ускоряют работу организаций.

При написании данной курсовой работы были описаны 3 модуля курса CCNA:

1. Адресация IPv6
2. ICMP
3. Транспортный уровень

Также была описана конфигурация IPv6 GUA на маршрутизаторе Cisco, приведены изображения с примером отправления сообщений RS и RA. Были продемонстрированы поля в заголовках TCP и UDP.