

Лабораторная работа №1

Основы компьютерных сетей. Физический и канальный уровень модели OSI/ISO. Знакомство с Cisco Packet Tracer

Цель работы: изучить задачи физического и канального уровня модели OSI/ISO, ознакомиться с видами топологий, средами передачи данных в компьютерных сетях и другими сетевыми моделями, научиться пользоваться основными командами в CiscoIOS.

1. Введение

Компьютерные сети – совокупность устройств и систем, которые подключены друг к другу и общающихся между собой. К устройствам и системам можно отнести: сервера, компьютеры, телефоны, коммутаторы, маршрутизаторы и т.д. Компоненты сети можно разделить на следующие группы:

- **Оконечные узлы.** Устройства, которые передают и/или принимают какие-либо данные. Это могут быть компьютеры, телефоны, сервера, какие-то терминалы или тонкие клиенты, телевизоры.
- **Промежуточные устройства.** Это устройства, которые соединяют оконечные узлы между собой. Сюда можно отнести коммутаторы, концентраторы, маршрутизаторы, точки доступа Wi-Fi.
- **Сетевые среды.** Это те среды, в которых происходит непосредственная передача данных. Сюда относятся кабели, сетевые карты, различного рода коннекторы, беспроводная среда передачи данных.

1.1 Модель OSI/ISO. Стек протоколов TCP/IP

Для того, чтобы понимать, как данные передаются с одного места на другое, рассмотрим данный процесс на модели OSI/ISO. Модель OSI/ISO была создана в 80-ые годы и является одним из первых стандартов для описания передачи информации между сетевыми устройствами, каналами связи и конечными пользователями.



Рисунок 1. Модель OSI/ISO

Состоит она из 7 уровней и каждый уровень выполняет определенную ему роль и задачи. Разберем, что делает каждый уровень снизу вверх:

1) Физический уровень (Physical Layer) определяет метод передачи данных, какая среда используется (передача электрических сигналов, световых импульсов или радиоэфир), уровень напряжения, метод кодирования двоичных сигналов.

2) Канальный уровень (Data Link Layer) берет на себя задачу адресации в пределах локальной сети, обнаруживает ошибки, проверяет целостность данных.

3) Сетевой уровень (Network Layer) берет на себя объединения участков сети и выбор оптимального пути (т.е. маршрутизация). Каждое сетевое устройство должно иметь уникальный сетевой адрес в сети.

4) Транспортный уровень (Transport Layer) берет на себя функцию транспорта. К примеру, когда вы скачиваете файл с Интернета, файл в виде сегментов отправляется на Ваш компьютер. На данном уровне вводятся понятия портов, которые нужны для указания назначения к конкретной службе. На этом уровне работают протоколы TCP (с установлением соединения) и UDP (без установления соединения).

5) Сеансовый уровень (Session Layer) – уровень в установлении, управлении и разрыве соединения между двумя хостами. К примеру, когда открываете страницу на веб-сервере, то Вы не единственный посетитель на нем. И вот для того, чтобы поддерживать сеансы со всеми пользователями, нужен сеансовый уровень.

6) Уровень представления (Presentation Layer): Он структурирует информацию в читабельный вид для прикладного уровня. Например, многие компьютеры используют таблицу кодировки ASCII для вывода текстовой информации или формат jpeg для вывода графического изображения.

7) Прикладной уровень (Application Layer) самый понятный для всех уровень. Как раз на этом уровне работают привычные для нас приложения — e-mail, браузеры по протоколу HTTP, FTP и остальное.

Данные проходят каждый уровень, начиная с Прикладного уровня, заканчивая физическим, не пропуская не один. Данный процесс называется инкапсуляция.

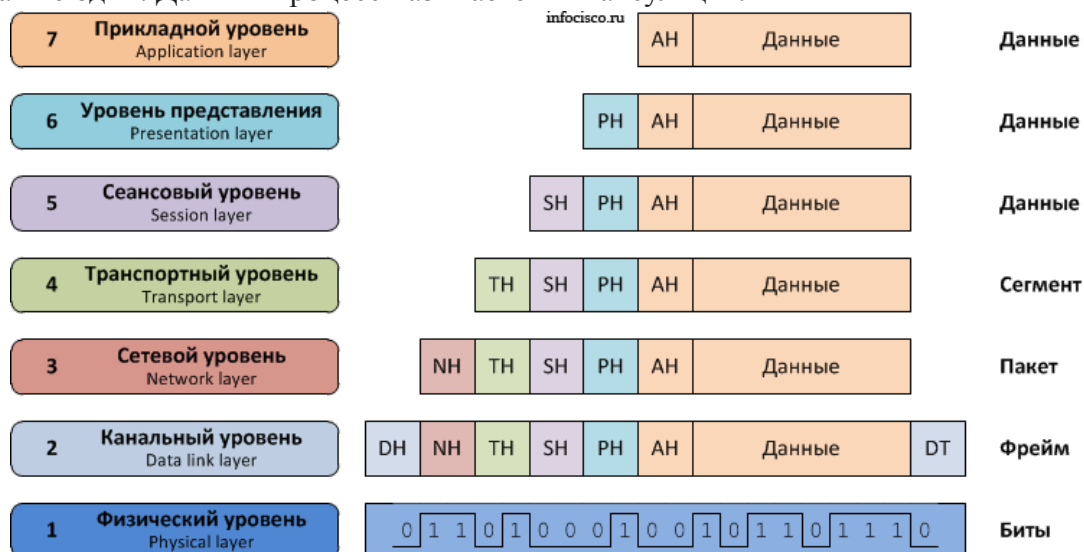


Рисунок 2. – Инкапсуляция данных

В настоящее время в сетях используется стек протоколов TCP/IP (модель DoD)

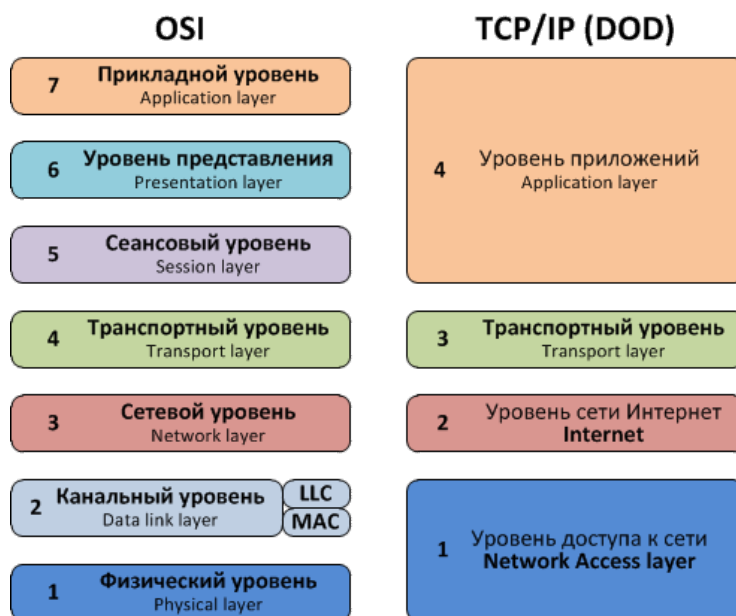


Рисунок 3. – Модель OSI/ISO и стек протоколов TCP/IP (Модель DoD)

Как видно из рисунка 3, он отличается от OSI и даже сменил название некоторых уровней. По сути, принцип у него тот же, что и у OSI. Но только три верхних уровня OSI: прикладной, представления и сеансовый объединены у TCP/IP в один, под названием прикладной. Сетевой уровень сменил название и называется — уровень сети Интернет. Транспортный остался таким же и с тем же названием. А два нижних уровня OSI: канальный и физический объединены у TCP/IP в один с названием — уровень доступа к сети. Стек TCP/IP в некоторых источниках обозначают еще как модель DoD (Department of Defence).

1.2 Физический уровень модели OSI/ISO

Физический уровень (Physical layer) имеет дело с передачей битов по физическим каналам связи, таким, например, как коаксиальный кабель, витая пара, оптоволоконный кабель или радиоканал. К этому уровню имеют отношение характеристики физических сред передачи данных, такие как полоса пропускания, помехозащищенность, волновое сопротивление и другие.

На этом же уровне определяются характеристики электрических сигналов, передающих дискретную информацию, например, крутизна фронтов импульсов, уровни напряжения или тока передаваемого сигнала, тип кодирования, скорость передачи сигналов. Кроме этого, здесь стандартизируются типы разъемов и назначение каждого контакта.

Функции физического уровня реализуются во всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом. Сетевой адаптер работает на физическом и канальном уровнях. К физическому уровню относится та часть функций сетевого адаптера, которая связана с приемом и передачей сигналов по линии связи, а получение доступа к разделяемой среде передачи, распознавание MAC-адреса компьютера – это уже функция канального уровня.

Осуществляют передачу электрических или оптических сигналов в кабель или в радиоканал и, соответственно, их приём и преобразование в биты данных в соответствии с методами кодирования цифровых сигналов.

На этом уровне также работают концентраторы, повторители сигнала и медиаконвертеры.

К физическому уровню относятся физические, электрические и механические интерфейсы между двумя системами. Физический уровень определяет такие виды сред передачи данных как оптоволокно, витая пара, коаксиальный кабель, спутниковый канал передачи данных и т.п. Стандартными типами сетевых интерфейсов, относящимися к физическому уровню, являются: V.35, RS-232, RS-485, RJ-11, RJ-45, разъемы AUI и BNC.

Для построения простейшей односегментной сети достаточно иметь сетевые адаптеры и кабель подходящего типа. Но даже в этом простом случае часто используются дополнительные устройства – повторители сигналов, позволяющие преодолеть ограничения на максимальную длину кабельного сегмента.

При организации сети по каналу 100 Мбит/сек используются 2 пары витой пары и используются жилы 1, 2, 3 и 6. При организации гигабитной сети используются 4 пары, т.е. все 8 жил витой пары.

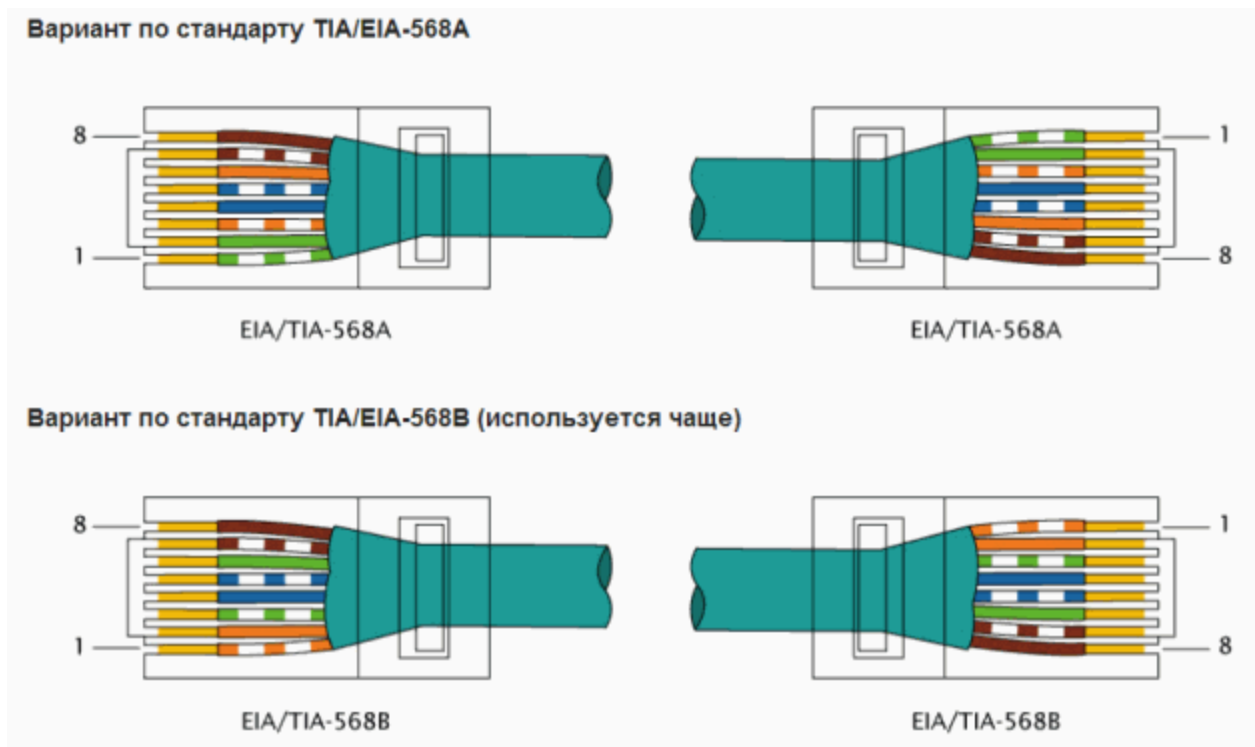
Для прокладки новых сетей лучше всего использовать кабель CAT 5e. И хотя CAT 5 и CAT 5e оба пропускают частоту 100 МГц, кабель CAT5e производится с учетом дополнительных параметров, важных для лучшей передачи высокочастотных сигналов.

Гигабитный Ethernet может работать на существующей кабельной структуре 5 категории. Согласитесь, подобная возможность очень удобна. Как правило, все современные сети используют кабель пятой категории, если только ваша сеть не была установлена в 1996 году или

раньше (стандарт был утвержден в 1995 году). Однако здесь существует несколько подводных камней:

В сети Ethernet существует два типа разводки кабелей. Первый тип используется для прямых соединений (коммутатор-коммутатор, компьютер-коммутатор) и кроссовер, который используется в локальных компьютерных сетях для прямого соединения двух компьютеров, однако в последнее время производства сетевого оборудования вышло далеко вперед, поэтому каждое сетевое устройство понимает как им работать и с чем они соединены, поэтому кроссоверный тип провода уже практически не используется.

Расшифка кабеля в RJ-45:



Основная функция *повторителя* (repeater), как это следует из его названия – повторение сигналов, поступающих на один из его портов, на всех остальных портах (Ethernet). Повторитель улучшает электрические характеристики сигналов и их синхронность, и за счет этого появляется возможность увеличивать общую длину кабеля между самыми удаленными в сети станциями.

Концентратор работает на физическом уровне сетевой модели OSI, ретранслируя входящий сигнал с одного из портов в сигнал на все остальные (подключённые) порты, реализуя, таким образом, свойственную Ethernet топологию общая шина, с разделением пропускной способности сети между всеми устройствами и работой в режиме полудуплекса. Коллизии (то есть попытка двух и более устройств начать передачу одновременно) обрабатываются аналогично сети Ethernet на других носителях — устройства самостоятельно прекращают передачу и возобновляют попытку через случайный промежуток времени, говоря современным языком, концентратор объединяет устройства в одном домене коллизий.

Концентраторы образуют из отдельных физических отрезков кабеля общую среду передачи данных – *логический сегмент*. Логический сегмент также называют доменом коллизий, поскольку при попытке одновременной передачи данных любых двух компьютеров этого сегмента, хотя бы и принадлежащих разным физическим сегментам, возникает блокировка передающей среды. Следует особо подчеркнуть, что какую бы сложную структуру не образовывали концентраторы, например, путем иерархического соединения, все компьютеры, подключенные к ним, образуют единый логический сегмент, в котором любая пара взаимодействующих компьютеров полностью блокирует возможность обмена данными для других компьютеров.

1.2 Топология сети

Топология сети — это способ описания конфигурации сети, схема расположения и соединения сетевых устройств. Топология сети позволяет увидеть всю ее структуру, сетевые устройства, входящие в сеть, и их связь между собой.

Выделяют несколько видов топологий: физическую (как соединены сетевые устройства), логическую (как передается информация между сетевыми устройствами), информационную (как направлены потоки информации) и топологию управления обменом (принцип передачи права на пользование сети).

Выделяют несколько основных видов топологий сетей:

1. **Шинная топология сети** — топология, при которой все компьютеры сети подключаются к одному кабелю, который используется совместно всеми рабочими станциями. При такой топологии выход из строя одной машины не влияет на работу всей сети в целом. Недостаток же заключается в том, что при выходе из строя или обрыве шины нарушается работа всей сети.

2. **Топология сети «Звезда»** — топология, при которой все рабочие станции имеют непосредственное подключение к серверу, являющемуся центром "звезды". При такой схеме подключения, запрос от любого сетевого устройства направляется прямым путем к серверу, где он обрабатывается с различной скоростью, зависящей от аппаратных возможностей центральной машины. Выход из строя центральной машины приводит к остановке всей сети. Выход же из строя любой другой машины на работу сети не влияет.

3. **Кольцевая топология сети** — схема, при которой все узлы соединены каналами связи в неразрывное кольцо (необязательно окружность), по которому передаются данные. Выход одного ПК соединяется с входом другого. Начав движение из одной точки, данные, в конечном счете, попадают на его начало. Данные в кольце всегда движутся в одном и том же направлении. Такая топология сети не требует установки дополнительного оборудования (сервера или хаба), но при выходе из строя одного компьютера останавливается и работа всей сети.

4. **Ячеистая топология сети** — топология, при которой каждая рабочая станция соединяется со всеми другими рабочими станциями этой же сети. Каждый компьютер имеет множество возможных путей соединения с другими компьютерами. Поэтому обрыв кабеля не

приведет к потере соединения между двумя компьютерами. Эта топология сети допускает соединение большого количества компьютеров и характерна, как правило, для крупных сетей.

5. При **смешанной топологии** применяются сразу несколько видов соединения компьютеров между собой. Встречается она достаточно редко в особо крупных компаниях и организациях.

1.3 Канальный уровень модели OSI/ISO

Канальный уровень (англ. data link layer) предназначен для обеспечения взаимодействия сетей по физическому уровню и контролем над ошибками, которые могут возникнуть. Полученные с физического уровня данные, представленные в битах, он упаковывает в кадры, проверяет их на целостность и, если нужно, исправляет ошибки (формирует повторный запрос поврежденного кадра) и отправляет на сетевой уровень. Канальный уровень может взаимодействовать с одним или несколькими физическими уровнями, контролируя и управляя этим взаимодействием.

Спецификация IEEE 802 разделяет этот уровень на два подуровня: MAC (англ. media access control) регулирует доступ к разделяемой физической среде, LLC (англ. logical link control) обеспечивает обслуживание сетевого уровня.

На этом уровне работают коммутаторы, мосты и другие устройства. Эти устройства используют адресацию второго уровня (по номеру уровня в модели OSI).

1.3.1 Подуровни LLC и MAC

На сегодняшний день Ethernet является наиболее широко используемой технологией локальных сетей. Однако существуют и другие технологии такие как TokenRing или FDDI. Поэтому **Ethernet** – это семейство технологий пакетной передачи данных, работающая по логической топологии шина.

Ethernet функционирует на канальном и физическом уровнях. Это семейство сетевых технологий, которые регламентируются стандартами IEEE 802.2 и 802.3. Технология Ethernet поддерживает передачу данных на скоростях:

Как показано на рисунке ниже, стандарты Ethernet регламентируют как протоколы уровня 2, так и технологии уровня 1. Для протоколов второго уровня, как и в случае со всеми стандартами группы IEEE 802, технология Ethernet полагается на работу этих двух отдельных подуровней канального уровня, а также на подуровни управления логическим каналом (LLC) и MAC.

Подуровень LLC

Подуровень LLC технологии Ethernet обеспечивает связь между верхними и нижними уровнями. Как правило, это происходит между сетевым программным обеспечением и аппаратным обеспечением устройства. Подуровень LLC использует данные сетевых протоколов, которые обычно представлены в виде пакета IPv4, и добавляет управляющую информацию,

чтобы помочь доставить пакет к узлу назначения. LLC используется для связи с верхними уровнями приложений и перемещает пакет для доставки на нижние уровни.

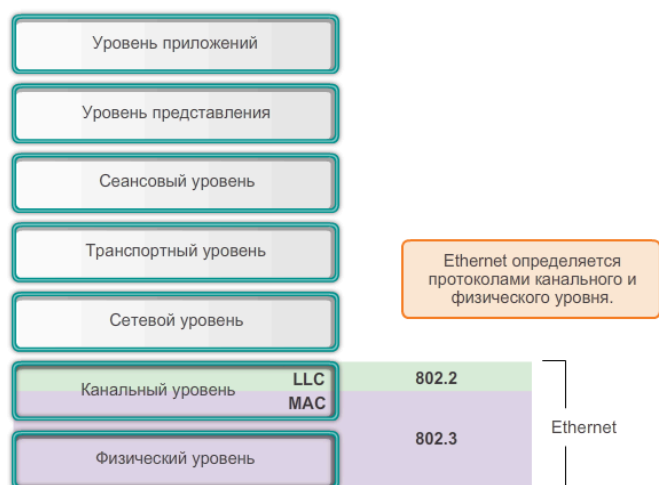


Рисунок 1 – Ethernet

LLC реализован в программном обеспечении, и его применение не зависит от оборудования. LLC для компьютера можно рассматривать как программное обеспечение драйвера сетевой платы (NIC). Драйвер сетевой платы — это программа, которая непосредственно взаимодействует с аппаратными средствами компьютера на сетевой интерфейсной плате для передачи данных между подуровнем MAC и физической средой.

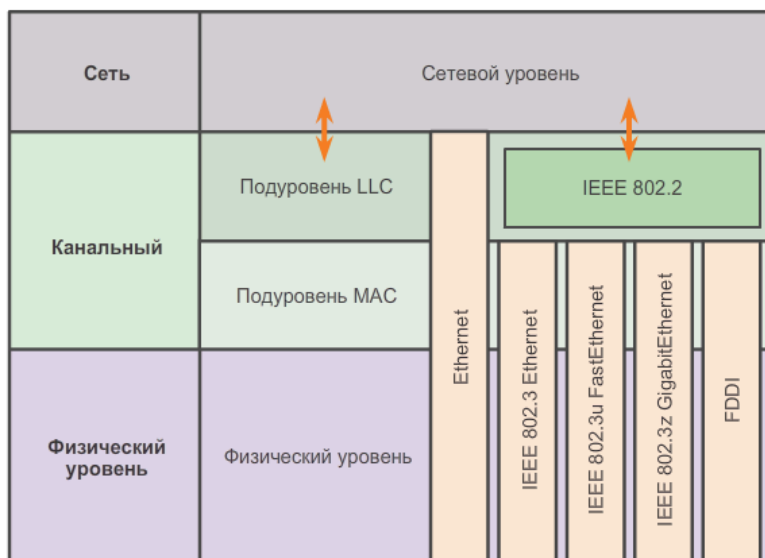


Рисунок 2 – Список общих стандартов IEEE Ethernet

Подуровень MAC

MAC представляет собой более низкий подуровень канального уровня. MAC реализуется аппаратно — обычно в сетевой интерфейсной плате компьютера. Спецификации содержатся в стандартах IEEE 802.3. Рисунок 2 показывает список общих стандартов IEEE Ethernet.

Как показано на рисунке ниже (Рисунок 3), подуровень MAC Ethernet выполняет две основные задачи:

- Инкапсуляция данных
- Управление доступом к среде передачи данных, в нее входят:

Канальный уровень	Подуровень управления логическим каналом								
	Управление доступом к среде передачи данных группы 802.3								
Физический уровень	Физический подуровень передачи сигналов	10BASE-5 (500m) 50 Ohm Коакс. N-Style	10BASE-5 (185m) 50 Ohm Коакс. BNC	10BASE-T (100m) 100 Ohm UTP RJ-45	100BASE-TX (100m) 100 Ohm UTP RJ-45	1000BASE-CX (25m) 150 Ohm STP mini-DB-9	1000BASE-T (100m) 100 Ohm UTP RJ-45	1000BASE-ST (220-550m) Волокно MM SC	1000BASE-LX (550-5000m) Волокно MM или SM SC
	Физическая среда передачи данных								

Рисунок 3 - подуровень MAC Ethernet

Инкапсуляция данных

Процесс инкапсуляции данных включает в себя сборку кадра перед его отправкой и разборку кадра после его получения. При формировании кадра на уровне MAC к PDU сетевого уровня добавляются заголовок и концевик.

Инкапсуляция данных обеспечивает три основных функции:

- Разделение кадра. Процесс формирования кадров предоставляет важные разделители, которые используются для определения группы битов, составляющих кадр. Этот процесс обеспечивает синхронизацию между передающими и получающими узлами.
- Адресация. Процесс инкапсуляции также обеспечивает адресацию канального уровня. Каждый заголовок Ethernet, добавляемый в кадр, содержит физический адрес (MAC-адрес), посредством которого кадр доставляется к узлу назначения.
- Обнаружение ошибок. Каждый кадр Ethernet содержит концевик с циклическим контролем по избыточности (CRC) содержимого кадра. После приёма кадра получающий узел

создаёт CRC для сравнения с аналогичным параметром в кадре. Если эти два расчета CRC совпадают, кадр может считаться полученным без ошибок.

Использование кадров помогает при передаче битов, так как они помещаются в среду передачи данных, а также при группировании битов на принимающем узле.

Управление доступом к среде передачи данных

Второй функцией подуровня MAC является управление доступом к среде передачи данных. Управление доступом к среде передачи данных отвечает за размещение кадров в этой среде и удаление из нее кадров. Этот подуровень напрямую взаимодействует с физическим уровнем.

Основная логическая топология Ethernet — это шина с множественным доступом; следовательно, среда передачи данных используется всеми узлами (устройствами) в одном сегменте сети. Ethernet — это способ ассоциативного доступа организации сети. При этом если несколько устройств в одной среде начнут вместе передавать информацию, то возникнет конфликт при передаче данных, который приведёт к их повреждению и невозможности дальнейшего использования. Чтобы не допустить подобной ситуации, Ethernet задействует метод множественного доступа с контролем несущей (CSMA) для управления общим доступом узлов.

Процесс CSMA используется для того, чтобы сначала определить, передаётся ли сигнал в среде. Если в среде обнаружен сигнал несущей частоты, исходящий от другого узла, это значит, что в данный момент другое устройство осуществляет передачу данных. Если среда занята, когда устройство пытается передать данные, оно подождёт и повторит попытку позже. Если сигнал несущей частоты не обнаружен, данное устройство начнёт передачу данных. Существует вероятность возникновения сбоя процесса CSMA, в результате чего два устройства будут передавать данные одновременно. Это называется коллизией данных. В этом случае данные, отправленные обоими устройствами, будут повреждены, из-за чего потребуются их повторная отправка.

Как показано на рисунке (Рисунок 4), CSMA обычно используется совместно с одним из методов разрешения конфликтов в среде. К двум наиболее широко распространённым методам относятся следующие.

Обнаружение коллизий/CSMA

При обнаружении коллизий/CSMA (CSMA/CD) устройство проверяет среду на наличие в ней сигнала данных. Если этот сигнал отсутствует, указывая на то, что среда передачи не загружена, устройство передаёт данные. Если позже обнаруживаются сигналы о том, что в то же время передачу данных осуществляло другое устройство, передача данных на всех устройствах прерывается и переносится на другое время. Для использования этого метода были разработаны традиционные формы Ethernet.

В современных сетях широкое применение технологий коммутации позволило практически полностью исключить первоначальную потребность в CSMA/CD для локальных сетей. Почти все проводные соединения между устройствами в современных локальных сетях являются полнодуплексными, т. е. способность устройства одновременно отправлять и принимать данные. Это означает, что несмотря на то, что сети Ethernet разрабатывались с учетом использования технологии CSMA/CD, современные промежуточные устройства позволяют устранить коллизии, и процессы, обеспечиваемые CSMA/CD, в действительности уже не требуются.

Тем не менее, для беспроводных соединений в среде локальной сети возможность возникновения таких коллизий всё еще необходимо учитывать. Устройства в беспроводной локальной сети используют метод доступа к среде передачи данных с контролем несущей и предотвращением коллизий (CSMA/CA).

Контроль несущей и предотвращение коллизий (CSMA/CA)

При использовании CSMA/CA устройство проверяет среду передачи данных на наличие в ней сигнала данных. Если среда не загружена, данное устройство отправляет по среде уведомление о намерении использовать её для передачи данных. Затем устройство отправляет данные. Этот способ используется беспроводными сетевыми технологиями стандарта 802.11.

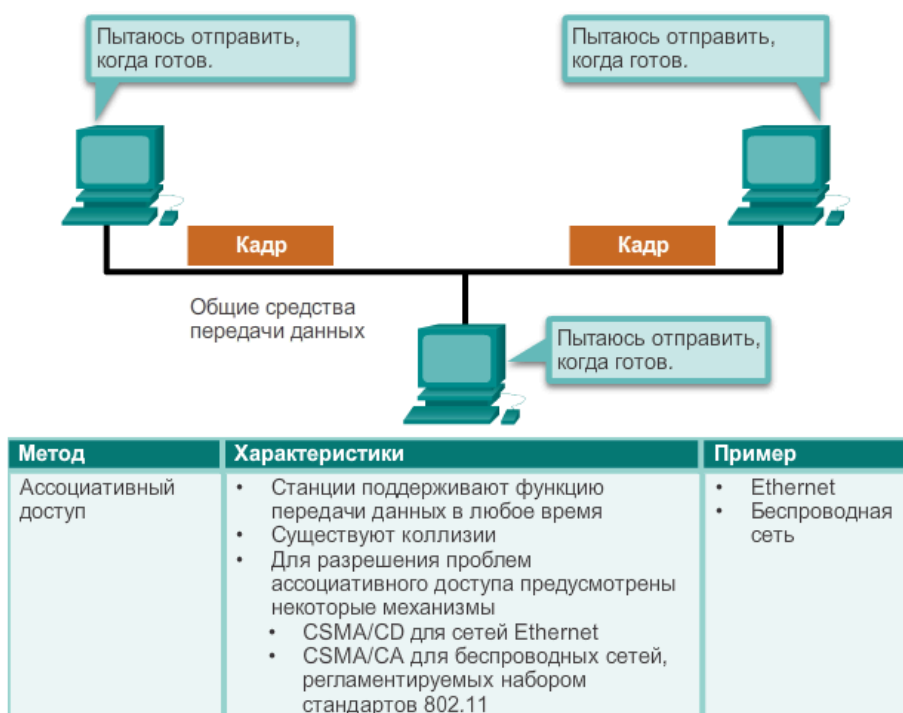


Рисунок 4 – Ассоциативный доступ

1.3.2 MAC-адрес: идентификация Ethernet

Для предотвращения чрезмерных нагрузок, возникающих при обработке каждого кадра, был создан уникальный идентификатор — MAC-адрес, который используется для определения фактических узлов источника и назначения в пределах сети Ethernet. Независимо от типа используемой сети Ethernet MAC-адресация обеспечила метод идентификации устройств на более низком уровне модели OSI. MAC-адрес Ethernet — это 48-битное двоичное значение, выраженное в виде 12 шестнадцатеричных чисел (4 бита для каждой шестнадцатеричной цифры).



Рисунок 5 – Структура MAC-адресов Ethernet

Структура MAC-адресов

MAC-адреса должны быть уникальными в глобальном масштабе. Значение MAC-адреса — это непосредственный результат применения правил, которые разработаны институтом IEEE для поставщиков, чтобы обеспечить глобальные уникальные адреса для каждого устройства Ethernet. В соответствии с этими правилами каждый поставщик, который занимается реализацией Ethernet-устройств, должен быть зарегистрирован в IEEE. IEEE присваивает поставщику 3-байтный (24-битный) код, который называется уникальным идентификатором организации (OUI).

Институт IEEE требует от поставщиков соблюдения двух простых правил, как показано на рисунке (Рисунок 5):

- Все MAC-адреса, назначаемые сетевой интерфейсной плате или другому устройству Ethernet, должны в обязательном порядке использовать этот идентификатор OUI поставщика в виде первых 3 байтов.

- Всем MAC-адресам с одним и тем же идентификатором OUI должно быть присвоено уникальное значение (код производителя или серийный номер), которое указывается в виде последних 3 байтов.

1.3.3 Обработка кадров

MAC-адрес часто называется аппаратным адресом (BIA), поскольку исторически сложилось так, что он записывается в ПЗУ (постоянное запоминающее устройство) на сетевой интерфейсной плате. Это означает, что адрес вносится в чип ПЗУ на аппаратном уровне, и его изменение с помощью программного обеспечения невозможно.

MAC-адреса присваиваются рабочим станциям, серверам, принтерам, коммутаторам и маршрутизаторам — любому устройству, которое должно отправлять или получать данные в сети. Все устройства, подключённые к локальной сети Ethernet, имеют интерфейсы с использованием MAC-адресов. Различные производители оборудования и программного обеспечения могут представлять MAC-адрес в разных шестнадцатеричных форматах. Форматы адресов могут иметь примерно следующий вид:

- 00-05-9A-3C-78-00
- 00:05:9A:3C:78:00
- 0005.9A3C.7800

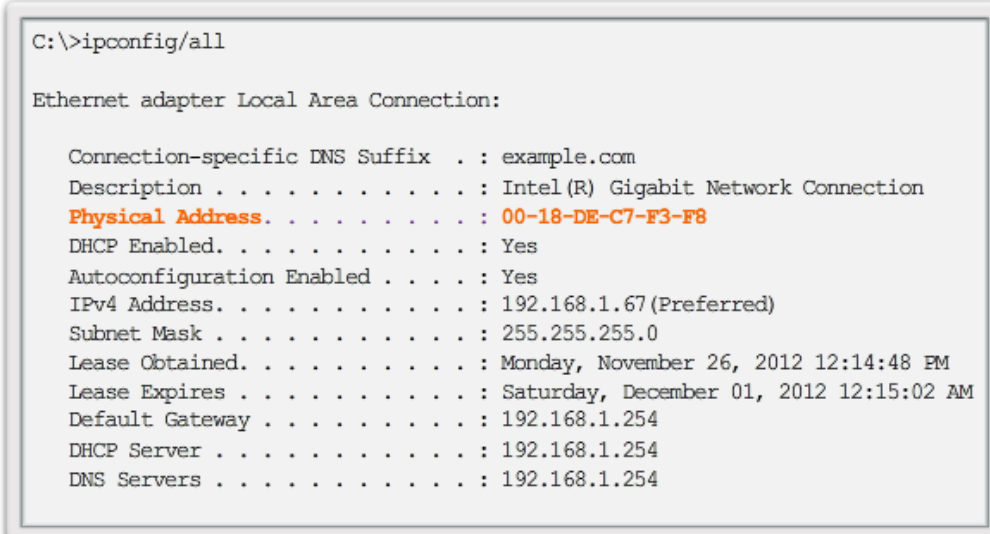
Каждая сетевая плата в сети просматривает информацию (на подуровне MAC), чтобы узнать, соответствует ли MAC-адрес назначения в кадре MAC-адресу физического устройства в ОЗУ. Если не удаётся обнаружить совпадения, устройство отклоняет кадр. Когда кадр достигает назначения, в котором MAC-адрес сетевой платы соответствует MAC-адресу получателя кадра, сетевая плата передаёт кадр на верхние уровни OSI, где происходит процесс деинкапсуляции.

1.3.4. MAC Ethernet

На узле Windows MAC-адрес адаптера Ethernet можно определить с помощью команды `ipconfig /all`. Обратите внимание (Рисунок 6) — на дисплее отображается, что физический адрес (MAC-адрес) компьютера имеет вид 00-18-DE-C7-F3-FB. Если у вас есть соответствующие права доступа, вы можете выполнить эту операцию на своем компьютере.

В зависимости от устройства и операционной системы вы увидите различные представления MAC-адресов, как показано на рисунке (Рисунок 7). Маршрутизаторы и

коммутаторы Cisco используют форму XXXX.XXXX.XXXX, где X — это шестнадцатеричный символ.



```
C:\>ipconfig/all

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : example.com
    Description . . . . . : Intel(R) Gigabit Network Connection
    Physical Address. . . . . : 00-18-DE-C7-F3-F8
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IPv4 Address. . . . . : 192.168.1.67 (Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Monday, November 26, 2012 12:14:48 PM
    Lease Expires . . . . . : Saturday, December 01, 2012 12:15:02 AM
    Default Gateway . . . . . : 192.168.1.254
    DHCP Server . . . . . : 192.168.1.254
    DNS Servers . . . . . : 192.168.1.254
```

Рисунок 6 – Физический (MAC) адрес узла

1.3.4.1 MAC-адрес одноадресной рассылки

В сети Ethernet разные MAC-адреса используются для одноадресной, многоадресной и широковещательной рассылки уровня 2.

MAC-адрес одноадресной рассылки — это уникальный адрес, который используется при отправке кадра от одного передающего устройства к одному устройству назначения.

В примере, приведённом на рисунке (Рисунок 8), узел с IP-адресом 192.168.1.5 (источник) запрашивает веб-страницу с сервера с IP-адресом 192.168.1.200. Для отправки и приёма одноадресного пакета в заголовке IP-пакета должен указываться IP-адрес назначения. Кроме того, в заголовке кадра Ethernet должен присутствовать MAC-адрес назначения. IP-адрес и MAC-адрес — это данные для доставки пакета одному узлу.

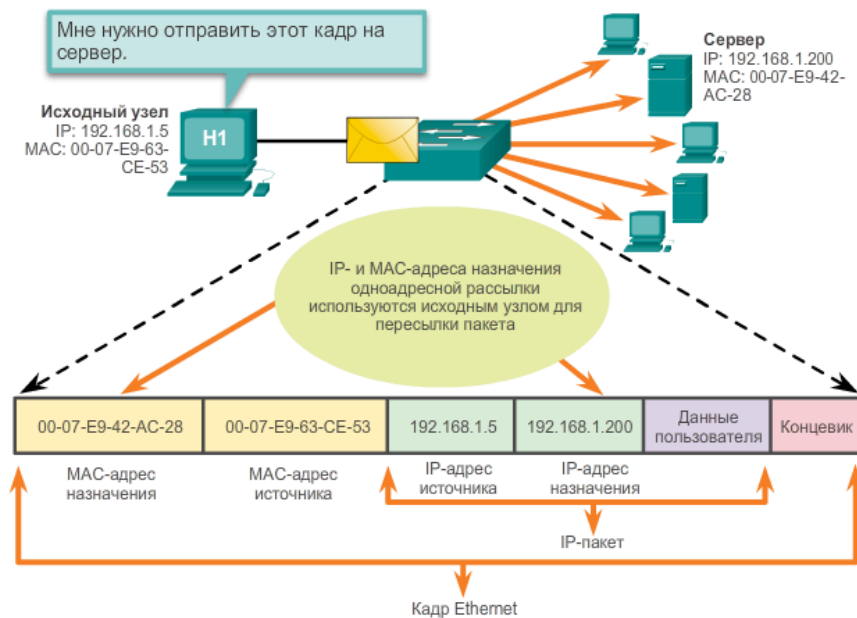


Рисунок 8 – Одноадресная рассылка

1.3.4.2 MAC-адрес широковещательной рассылки

В пакете широковещательной рассылки содержится IP-адрес назначения, в узловой части которого присутствуют только единицы (1). Эта нумерация в адресе означает, что все узлы в локальной сети (домене широковещательной рассылки) получают и обрабатывают пакет. Многие сетевые протоколы, в частности, DHCP и протокол разрешения адресов (ARP), используют широковещательные рассылки. Использование широковещательных рассылок протоколом ARP для сопоставления адресов уровня 2 с уровнем 3 будет рассмотрено в этой главе немного позже.

Как показано на рисунке (Рисунок 9), IP-адресу широковещательной рассылки требуется соответствующий MAC-адрес широковещательной рассылки в кадре Ethernet. В сетях Ethernet используется MAC-адрес широковещательной рассылки из 48 единиц, который в шестнадцатеричном формате выглядит как FF-FF-FF-FF-FF-FF.

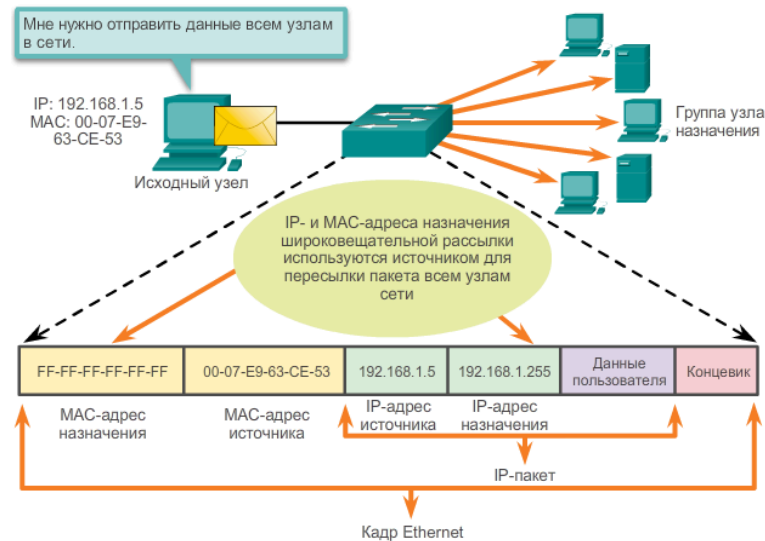


Рисунок 9 – Широковещательная рассылка

1.3.4.3 MAC-адрес многоадресной рассылки

Адреса многоадресных рассылок позволяют исходному устройству рассылать пакет группе устройств. Устройства, относящиеся к многоадресной группе, получают ее IP-адрес. Диапазон адресов многоадресных рассылок IPv4 — от 224.0.0.0 до 239.255.255.255. Поскольку адреса многоадресных рассылок соответствуют группам адресов (которые иногда называются группами узлов), они используются только как адресаты пакета. У источника всегда одноадресный адрес.

Адреса многоадресных рассылок используются, например, в играх с удалённым подключением, в которых участвуют несколько человек из разных мест. Кроме того, такие адреса используются при дистанционном обучении в режиме видеоконференции, когда несколько учащихся подключены к одному и тому же курсу.

Как и в случае с адресами для одноадресной и широковещательной рассылки, IP-адресу для многоадресной рассылки требуется соответствующий MAC-адрес, чтобы фактически передавать кадры по локальной сети. MAC-адрес многоадресной рассылки — это особое значение, которое в шестнадцатеричном формате начинается с 01-00-5E. Остальная часть MAC-адреса многоадресной рассылки создаётся путем преобразования нижних 23 бит IP-адреса группы многоадресной рассылки в 6 шестнадцатеричных символов.

Как показано на рисунке (Рисунок), в качестве примера используется шестнадцатеричный адрес многоадресной рассылки 01-00-5E-00-00-C8.

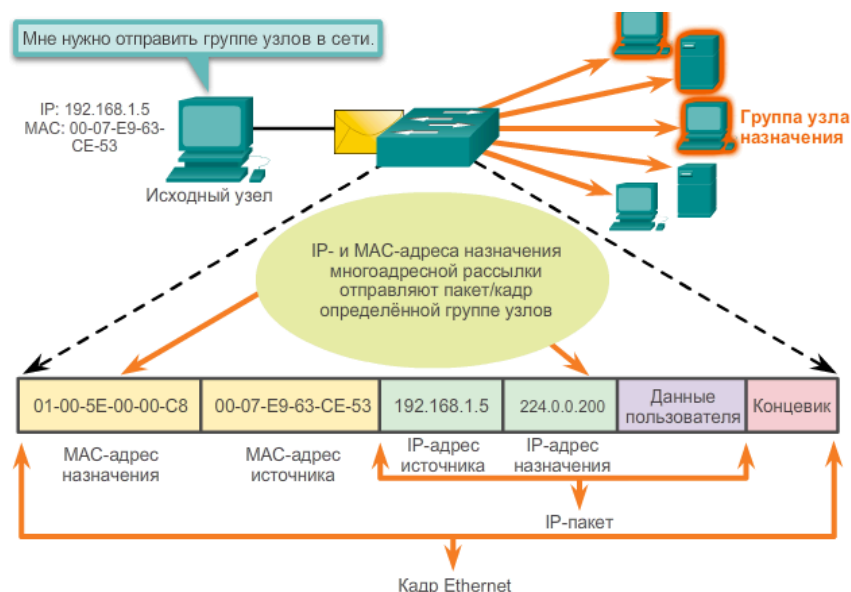


Рисунок 10 – Многоадресная рассылка

1.3.5 Сетевой коммутатор

Сетевой коммутатор (англ. switch — переключатель) — устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. Коммутатор работает на канальном (втором) уровне модели OSI. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты. Для соединения нескольких сетей на основе сетевого уровня служат маршрутизаторы (3 уровень OSI).

В отличие от концентратора (1 уровень OSI), который распространяет трафик от одного подключённого устройства ко всем остальным, коммутатор передаёт данные только непосредственно получателю (исключение составляет широковещательный трафик всем узлам сети и трафик для устройств, для которых неизвестен исходящий порт коммутатора). Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

1.3.5.1 Принцип работы коммутатора

Коммутатор хранит в памяти (т.н. ассоциативной памяти) таблицу коммутации, в которой указывается соответствие MAC-адреса узла порту коммутатора. При включении коммутатора эта таблица пуста, и он работает в режиме обучения. В этом режиме поступающие на какой-либо порт данные передаются на все остальные порты коммутатора. При этом коммутатор анализирует фреймы (кадры) и, определив MAC-адрес хоста-отправителя, заносит его в таблицу на некоторое время. Впоследствии, если на один из портов коммутатора поступит кадр, предназначенный для хоста, MAC-адрес которого уже есть в таблице, то этот кадр будет передан

только через порт, указанный в таблице. Если МАС-адрес хоста-получателя не ассоциирован с каким-либо портом коммутатора, то кадр будет отправлен на все порты, за исключением того порта, с которого он был получен. Со временем коммутатор строит таблицу для всех активных МАС-адресов, в результате трафик локализуется. Стоит отметить малую латентность (задержку) и высокую скорость пересылки на каждом порту интерфейса.

1.3.5.2 Режимы коммутации

Существует три способа коммутации. Каждый из них — это комбинация таких параметров, как время ожидания и надёжность передачи.

- С промежуточным хранением (Store and Forward). Коммутатор читает всю информацию в кадре, проверяет его на отсутствие ошибок, выбирает порт коммутации и после этого посылает в него кадр.

- Сквозной (cut-through). Коммутатор считывает в кадре только адрес назначения и после выполняет коммутацию. Этот режим уменьшает задержки при передаче, но в нём нет метода обнаружения ошибок.

- Бесфрагментный (fragment-free) или гибридный. Этот режим является модификацией сквозного режима. Передача осуществляется после фильтрации фрагментов коллизий (первые 64 байта кадра анализируются на наличие ошибки и при её отсутствии кадр обрабатывается в сквозном режиме).

Задержка, связанная с «принятием коммутатором решения», добавляется к времени, которое требуется кадру для входа на порт коммутатора и выхода с него, и вместе с ним определяет общую задержку коммутатора.

1.3.5.3 Симметричная и асимметричная коммутация

Свойство симметрии при коммутации позволяет дать характеристику коммутатора с точки зрения ширины полосы пропускания для каждого его порта. Симметричный коммутатор обеспечивает коммутируемые соединения между портами с одинаковой шириной полосы пропускания, например, когда все порты имеют ширину пропускания 10 Мб/с или 100 Мб/с.

Асимметричный коммутатор обеспечивает коммутируемые соединения между портами с различной шириной полосы пропускания, например, в случаях комбинации портов с шириной полосы пропускания 10 Мб/с или 100 Мб/с и 1000 Мб/с.

Асимметричная коммутация используется в случае наличия больших сетевых потоков типа клиент-сервер, когда многочисленные пользователи обмениваются информацией с сервером одновременно, что требует большей ширины пропускания для того порта коммутатора, к которому подсоединён сервер, с целью предотвращения переполнения на этом порте. Для того чтобы направить поток данных с порта 100 Мб/с на порт 10 Мб/с без опасности переполнения на последнем, асимметричный коммутатор должен иметь буфер памяти.

Асимметричный коммутатор также необходим для обеспечения большей ширины полосы пропускания каналов между коммутаторами, осуществляемых через вертикальные кросс-соединения, или каналов между сегментами магистрали.

2. Cisco IOS

Сетевые операционные системы во многом похожи на ОС для ПК. Существует ряд сетевых операционных систем для каждой марки сетевого оборудования. Однако, стоит заметить, по синтаксису и названиям команд они очень схожи. В данной лабораторной работе и последующих мы будем рассматривать операционную систему для сетевого оборудования компании Cisco – Cisco IOS. Функциональные возможности IOS отличаются на разных сетевых устройствах в зависимости от устройства и поддерживаемых функций.

2.1. Местоположение операционной системы Cisco IOS

Размер самого файла IOS составляет несколько мегабайт и хранится в полупостоянной памяти, которая называется флеш памятью. Флеш память обеспечивает энергонезависимое хранение данных. Несмотря на то, что содержимое флеш памяти не теряется во время потери питания, при необходимости их можно изменить или перезаписать. Благодаря этому IOS можно обновлять до более новой версии или добавлять новые функциональные возможности без замены оборудования. Кроме того, флеш память можно использовать для одновременного хранения нескольких версий ПО IOS.

Во многих устройствах Cisco при подключении к сети IOS копируется из флеш памяти в оперативное запоминающее устройство (ОЗУ). Затем, при работе устройства, IOS запускается из ОЗУ. ОЗУ обладает множеством функций, включая хранение данных, которые используются устройством для поддержки работы сети. Запуск IOS из ОЗУ повышает производительность устройства, при этом ОЗУ считается энергозависимой памятью, поскольку данные теряются во время отключения питания. Количество необходимой флеш памяти и оперативной памяти зависит от версии IOS. Для технического обслуживания сети и планирования крайне важно определить требования флеш памяти и ОЗУ для каждого устройства, включая максимальные конфигурации флеш памяти и ОЗУ. Возможно, новейшие версии IOS могут запросить больше ОЗУ и флеш памяти, чем возможно установить на некоторых устройствах.

2.2 Доступ к устройству Cisco IOS

Существует несколько способов доступа к среде интерфейса командной строки (CLI). Ниже приведены наиболее распространённые методы.

1) **Консоль:** использует низкоскоростные последовательные или USB-подключения для обеспечения прямого подключения и внеполосного административного доступа к устройству Cisco.

2) **Telnet или SSH:** два способа удалённого доступа к сеансу использования интерфейса командной строки (CLI) через активный сетевой интерфейс. Telnet – незащищенное подключение к сетевому оборудованию, а SSH – защищенное.

3) **Порт AUX:** используется для удалённого управления маршрутизатором с помощью телефонной линии коммутируемого доступа и модема.

Далее будет рассмотрена базовая конфигурация маршрутизатора на основе CLI IOS (режимы конфигурации коммутатора практически идентичны).

После включения маршрутизатора в первый раз он осуществляет тест самопроверки POST, который запускает диагностические утилиты с целью проверки внутренних цепей маршрутизатора. Если тест завершён успешно, начинается поиск и загрузка Cisco IOS из флеш-памяти при условии её наличия. Затем IOS загружает конфигурацию, которая находится в NVRAM (файл startup-config). Это позволяет загрузить настройки конфигурации Cisco IOS, и интерфейс пользователя Cisco становится доступным.

2.2.1. Программы эмуляции терминала

Существует множество программ эмуляции терминала, доступных для подключения к сетевому устройству или последовательного подключения через консольный порт или соединение Telnet/SSH. К некоторым из этих программ относятся:

- PuTTY
- Tera Term
- SecureCRT
- HyperTerminal
- Terminal OS X

Эти программы позволяют максимально повысить продуктивность работы за счёт регулировки размеров окна, изменения размера шрифта и изменения комбинации цветов.

2.3. Навигация по операционной системе IOS

Интерфейс пользователя Cisco IOS разделён на несколько различных режимов, а команды, доступные в каждом из режимов, определяют его. Когда начинается сеанс связи с маршрутизатором, он начинается с режима USER EXEC, который зачастую называется просто режимом EXEC. Список команд, доступных в режиме EXEC, весьма ограничен. Для того чтобы иметь доступ ко всем командам, необходимо войти в режим привилегированного EXEC с помощью команды **enable**. Из режима привилегированного EXEC можно ввести любую из команд EXEC, или войти в режим глобальной конфигурации, которая предлагает ещё более широкий выбор команд и опций. Вход в глобальный режим из привилегированного осуществляется с использованием команды **configure terminal**. Из режима глобальной конфигурации можно выйти в режим конфигурации любого из интерфейсов, для того чтобы сконфигурировать этот интерфейс (порт или подинтерфейс).

Основные командные состояния маршрутизатора или коммутатора, его режимы, приведены в таблице 1.2.

Таблица 1.2 – Отображение команд в режимах конфигурации в IOS

<u>1 - USER EXEC</u> Switch> Router>	<u>3 - Global Configuration Mode</u> Switch(config)# Router(config)#
<u>2 - Privileged EXEC</u> Switch# Router#	<u>4 - Specialized Configuration Mode</u> Switch(config-mode)# Router(config-mode)#

Основными режимами являются пользовательский и привилегированный. Осуществляя функции защиты, ПО CISCO IOS разделяет сессии режимов на два уровня доступа. Привилегированный режим обладает более высоким уровнем прав в возможностях использования устройства.

2.3.1 Пользовательский режим (USER EXEC)

Функциональные возможности пользовательского режима ограничены, при этом он эффективно выполняет некоторые базовые операции. Пользовательский режим находится на базовом уровне иерархической структуры режимов. Это первый режим, в котором пользователь начинает работу при входе в интерфейс командной строки (CLI) устройства IOS.

Пользовательский режим позволяет выполнять ограниченное количество базовых команд. Этот режим часто называют «режимом для просмотра». В пользовательском режиме запрещается выполнять команды, которые могут изменить параметры устройства.

По умолчанию для входа в пользовательский режим из консоли аутентификация не требуется. Однако во время начальной конфигурации рекомендуется настроить процедуру аутентификации.

Пользовательский режим определяется с помощью команды интерфейса командной строки, оканчивающейся символом «>». Следующий пример демонстрирует символ «>» в командной строке маршрутизатора:

```
Router>
```

2.3.2 Привилегированный режим (Privileged EXEC)

Для выполнения команд конфигурации и управления сетевой администратор должен использовать привилегированный режим или более специализированный режим в иерархии. Это означает, что сначала пользователю нужно войти в пользовательский режим, а из него – в привилегированный режим. Это можно осуществить с помощью команды **enable**.

Привилегированный режим можно определить по командной строке, оканчивающейся символом «#».

```
Router#
```

Привилегированный режим открывает доступ к режиму глобальной конфигурации и ко всем другим более конкретным режимам настройки.

2.3.3 Режим глобальной конфигурации (Global Configuration Mode)

Основной режим конфигурации называется глобальным режимом конфигурации. В режиме глобальной конфигурации выполняются изменения конфигурации интерфейса командной строки (CLI), влияющие на работу устройства в целом. Перед доступом к специализированным режимам конфигурации нужно войти в режим глобальной конфигурации.

Чтобы перевести устройство из привилегированного режима в режим глобальной конфигурации и выполнить ввод команд конфигурации из терминала, используется следующая команда интерфейса командной строки:

Router#configure terminal

После ввода команды командная строка изменяется таким образом, чтобы показать, что он находится в режиме глобальной конфигурации.

Router(config)#

2.3.4 Специальные режимы конфигурации (Specialized Configuration Modes)

Из режима глобальной конфигурации пользователь может перейти в различные режимы конфигурации для подкоманд. Каждый из этих режимов позволяет выполнить настройку параметров конкретной области или функции устройства с операционной системой IOS. Ниже приведены некоторые из них:

- режим конфигурации интерфейса предназначен для настройки одного из сетевых интерфейсов (например, Fa0/0, G0/1 или S0/1/0);
- режим конфигурации линии предназначен для настройки одной из физических или виртуальных линий (консоль, AUX, VTY).

Чтобы вернуться в режим глобальной конфигурации из конкретного режима, введите **exit** в командной строке. Чтобы окончательно выйти из режима конфигурации и вернуться в привилегированный режим, введите **end** или воспользуйтесь комбинацией клавиш **Ctrl + Z**.

2.3.5 Командные строки

При использовании интерфейса командной строки (CLI) режим определяется по командной строке, которая является уникальной для каждого режима. По умолчанию каждая командная строка начинается с имени устройства. После имени следует остаток командной строки, который определяет режим. Например, запрос по умолчанию для режима глобальной конфигурации на маршрутизаторе выглядит так:

Router(config)#

Отдельное внимание следует уделить различным вариантам базовой команды для проверки – **show**.

Типичная команда **show** предоставляет сведения о конфигурации, эксплуатации и состоянии компонентов коммутатора или маршрутизатора Cisco.

Довольно распространена команда группы **show** – **show interfaces**. Эта команда служит для отображения статистических сведений по всем интерфейсам устройства. Для отображения статистики по определённому интерфейсу введите команду **show interfaces** с указанием типа интерфейса и номера порта (слота). Например:

Router# **show interfaces gigabitEthernet 0/1**

К дополнительным командам show относят:

- **show startup-config**, которая отображает сохранённую конфигурацию, расположенную в NVRAM;
- **show running-config**, которая отображает содержимое файла текущей конфигурации.

Команда **show version** позволяет проверить некоторые основные средства программно-аппаратного обеспечения маршрутизатора (коммутатора), а также устранить связанные с ними неполадки. Эта команда отображает версию системы Cisco IOS, которая используется в настоящий момент на устройстве, а также версию программы начальной загрузки и информацию о конфигурации оборудования, включая количество системной памяти.

2.3.6. Навигация между режимами IOS

Навигация между пользовательским и привилегированным режимами

Команды **enable** и **disable** используются для переключения интерфейса командной строки (CLI) между пользовательским и привилегированным режимами соответственно.

Чтобы получить доступ к привилегированному режиму, используйте команду **enable**. Иногда привилегированный режим называют режимом включения (enable).

Синтаксис для ввода **enable** выглядит так:

Switch> **enable**

Выполнение этой команды не требует какого-либо параметра или ключевого слова. После нажатия клавиши Enter командная строка изменится так:

Switch#

Символ «#» в конце командной строки означает, что коммутатор переключён в привилегированный режим.

Команды для доступа к привилегированному режиму и для возврата в пользовательский режим на маршрутизаторе Cisco идентичны тем же командам на коммутаторе Cisco.

2.3.7. Справка

В операционной системе IOS предусмотрены несколько доступных видов справки:

- Контекстная справка
- Проверка синтаксиса команды
- Горячие клавиши и клавиши быстрого вызова

Контекстная справка

Контекстная справка предоставляет список команд и параметров, связанных с этими командами в контексте текущего режима. Для доступа к контекстной справке введите вопросительный знак (?) в любой командной строке. Последует немедленный ответ даже без нажатия клавиши Enter.

Контекстная справка полезна для получения списка доступных команд. Этот вид справки можно использовать в тех случаях, когда вы не знаете имени команды или хотите узнать, поддерживает ли IOS ту или иную команду в определённом режиме.

Например, для получения списка доступных команд в пользовательском режиме введите вопросительный знак (?) в командной строке Switch>.

Кроме того, контекстную справку можно использовать для отображения списка команд или ключевых слов, которые начинаются с определённого символа или символов. Если указать вопросительный знак без пробела сразу после ввода последовательности символов, IOS отобразит список команд или ключевых слов для этого контекста, которые начинаются с указанных символов.

Например, введите **sh?** для получения списка команд, которые начинаются с сочетания символов **sh**.

Последний вид контекстной справки используется для определения параметров, ключевых слов или параметров, соотносящихся с определённой командой. При вводе команды введите пробел перед вопросительным знаком ?, чтобы определить, что можно или нужно ввести далее.

Как показано на рисунке (Рисунок 5), после команды **clock set 19:50:00** можно ввести символ ?, чтобы определить дополнительные параметры или ключевые слова, доступные для этой команды.

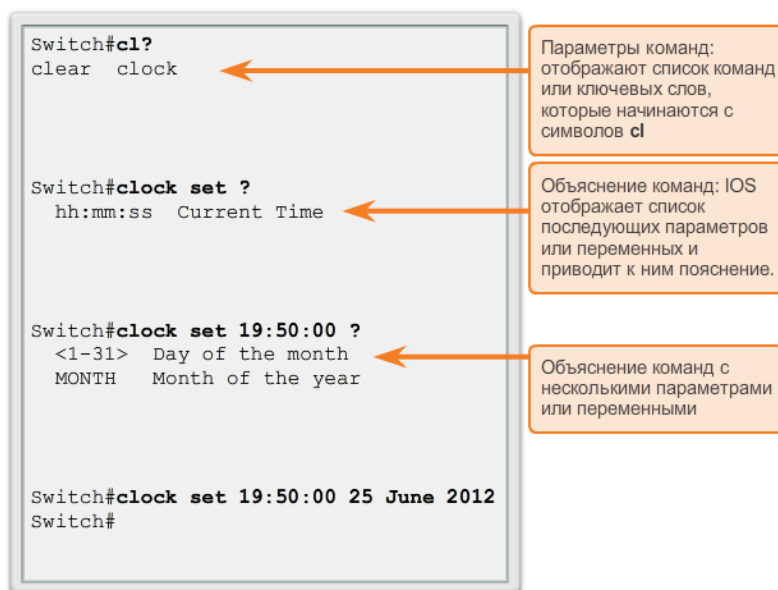


Рисунок 5 – Контекстная справка

2.3.8. Горячие клавиши и клавиши быстрого вызова

Интерфейс командной строки (CLI) IOS предусматривает горячие клавиши и клавиши быстрого вызова, которые упрощают процесс настройки, мониторинга, поиска и устранения неполадок.

Необходимо отметить следующие горячие клавиши:

- **Стрелка вниз** — позволяет пользователю пролистывать предыдущие команды вперед
- **Стрелка вверх** — позволяет пользователю пролистывать предыдущие команды назад
- **Tab** — завершает частично набранную команду или ключевое слово
- **Ctrl-A** — перемещает в начало строки
- **Ctrl-E** — перемещает в конец строки
- **Ctrl-R** — обновляет строку
- **Ctrl-Z** — выходит из режима конфигурации и возвращает в пользовательский режим
- **Ctrl-C** — выходит из режима конфигурации или прерывает текущую команду
- **Ctrl-Shift-6** — позволяет пользователю прервать процесс IOS, например, ping или traceroute

Сокращённые команды или ключевые слова

Команды и ключевые слова можно сократить до минимального количества символов, которые останутся уникальными. Например, команду **configure** можно сократить до **conf**, поскольку **configure** — это единственная команда, которая начинается с символов **conf**. Сокращение **con** не подходит, так как с символов **con** начинается несколько команд. Ключевые слова также можно сокращать. Например, **show interfaces** можно сократить следующим образом **sh int**

3. Задание к лабораторной работе

3.1 Знакомство с интерфейсом Packet Tracer

(выполнять в Cisco Packet Tracer 6.0.1 или старше)

1. Откройте файл «1.2.4.4 Packet Tracer - Representing the Network.pka» и выполните задания, представленные в файле. **Примечание:** Если в этом и последующих заданиях при двойном клике на файл открывается пустая рабочая область, воспользуйтесь функцией **File\Open** и выберите нужный файл.

3.2. Режимы работы и структура команд интерфейса командной строки CLI.

(выполнять в Cisco Packet Tracer 6.0.1 или старше)

1. Создайте новый файл.
2. Переключитесь на вкладку логического представления (Logical)
3. На рабочую область из нижней левой вкладки «конечные устройства» поместите ПК (**End Devices > PC-PT**). Кликнув на ПК, выберете вкладку «Desktop»\ «**IP Configuration**». Установите

в качестве IP адреса 192.168.10.5, в качестве маски подсети 255. 255. 255.0, в качестве шлюза по умолчанию 192.168.10.1

4. На рабочую область из нижней левой вкладки «Коммутаторы» поместите коммутатор 2950-24 (Switches > 2950-24).

5. Подключите ПК к коммутатору с помощью консольного кабеля

- Щёлкните значок **Connections (Соединения)** (в виде молнии) в левом нижнем углу окна Packet Tracer.

- Выберите светло-голубой консольный кабель, щёлкнув по нему. Указатель мыши примет вид разъёма со свисающим концом кабеля.

- Щёлкните на ПК. В окне будет показан вариант для подключения RS-232.

- Перетащите другой конец консольного подключения к коммутатору и щёлкните коммутатор, чтобы открыть список подключений.

- Выберите консольный порт, чтобы завершить подключение.

6. Установите сеанс терминальной связи с коммутатором S1

- Щёлкните на ПК и откройте вкладку **Desktop (Рабочий стол)**.

- Щёлкните значок приложения **Terminal**. Проверьте правильность параметров по умолчанию, установленных для порта. Каково значение параметра в битах в секунду?

- Нажмите кнопку ОК.

- В появившемся окне может быть показано несколько сообщений. В какой-либо части окна должно

- появиться сообщение Press RETURN to get started! (Нажмите клавишу ВВОД, чтобы начать работу). Нажмите клавишу ВВОД. Какое приглашение показано на экране?

7. Изучение справки по IOS.

- В IOS доступна справка по командам в зависимости от уровня работы. В данный момент отображается приглашение, называемое Пользовательским режимом, и устройство ожидает ввода команд. Самый простой способ вызова справки — ввести вопросительный знак (?) в приглашении, чтобы получить список команд.

S1> ?

- Какая команда начинается с буквы «с»?

- В командной строке введите **t** с вопросительным знаком в конце (?).

S1> t?

- Какие отображаются команды?

- В командной строке введите **te** с вопросительным знаком в конце (?).

S1> te?

- Какие отображаются команды?

- Такой тип справки называется контекстной; в ней предоставляются дополнительные сведения при расширении команд.

8. Войдите в привилегированный режим.

a. В командной строке введите вопросительный знак (?).

S1> ?

Какие из показанных данных описывают команду **enable**?

b. Введите **en** и нажмите клавишу TAB.

S1> en<Tab>

Что отображается после нажатия клавиши TAB?

Это называется завершением команды или завершением клавишей TAB. После ввода части команды с помощью клавиши TAB можно завершить ввод этой команды. Если введённых

символов достаточно для уникального определения команды (например, как в случае с командой **enable**), оставшаяся часть будет введена автоматически. Что произойдёт, если ввести **te<Tab>** в командной строке?

- с. Введите команду **enable** и нажмите клавишу ВВОД. Как изменилась строка приглашения?
- d. Введите в строке вопросительный знак (?).

S1# ?

Ранее уже использовалась одна команда, которая началась с буквы «с» в пользовательском режиме. Сколько команд показано теперь, когда включён привилегированный режим? (Подсказка. Можно было ввести «с?» для вывода только команд, начинающихся с «с».)

9. Переход в режим глобальной конфигурации.

а. Одной из команд, доступных в привилегированном режиме и начинающихся с буквы «с», является **configure**. Введите команду полностью или только её часть, достаточную для завершения, клавишей TAB, а затем нажмите клавишу ВВОД.

S1# configure

Какое отобразилось сообщение?

б. Нажмите клавишу ВВОД, чтобы принять параметр по умолчанию, заключённый в квадратные скобки [**terminal**].

Как изменилась строка приглашения?

с. Такой режим называется режимом глобальной конфигурации. А теперь вернитесь в привилегированный режим, введя команду **exit** или **end**, либо нажав сочетание клавиш Ctrl-Z.

10. Настройка часов

а. Используйте команду **clock**, чтобы подробнее изучить справку и синтаксис команды. Введите **show clock** в привилегированном режиме.

S1# show clock

Какая информация отображается? Какой год отображается?

б. Используйте контекстную справку и команду **clock**, чтобы установить текущее время на коммутаторе. Введите команду **clock** и нажмите клавишу ВВОД.

S1# clock<ENTER>

с. IOS выдала сообщение **% Incomplete command**, которое означает, что для команды **clock** требуются дополнительные параметры. В справке можно получить дополнительные сведения о времени, если ввести после команды пробел и вопросительный знак (?).

S1# clock ?

Какая информация отображается?

д. Настройте время с помощью команды **clock**. Продолжайте изучение команды, выполняя по одному действию за один раз.

S1# clock set ?

Какая запрашивается информация?

Какие отобразятся сведения, если ввести только команду **clock**, не выполняя запрос справки с помощью вопросительного знака?

е. На основе данных, запрошенных с помощью команды **clock set ?**, введите время 15:00, используя 24-часовой формат. Проверьте, нужны ли дополнительные параметры.

S1# clock set 15:00:00 ?

Выходные данные содержат запрос на получение дополнительных сведений:

<1-31> Day of the month

MONTH Month of the year

f. Попробуйте установить сегодняшнюю дату и время

11. Изучение дополнительных сообщений команд.

a. IOS выводит различные данные для неправильных или неполных команд, в чём можно было убедиться в предыдущих разделах. Продолжайте работать с командой `clock`, чтобы изучить дополнительные сообщения, которые могут появиться в ходе обучения работы с IOS.

b. Введите следующую команду и запишите сообщение:

S1# cl

Какие возвращены данные?

S1# clock

Какие возвращены данные?

S1# clock set 25:00:00

Какие возвращены данные?

S1# clock set 15:00:00 32

Какие возвращены данные?

3.3. Установка первоначальных настроек безопасности в интерфейсе командной строки CLI

Откройте файл «2.2.3.3 Packet Tracer - Configuring Initial Switch Settings.pka» и выполните задания, представленные в файле.

3.4 Реализация базовой схемы подключения

Откройте файл " 2.3.2.5 Packet Tracer - Implementing Basic Connectivity.pka " и выполните указанные задания

3.5 Просмотр ARP с помощью интерфейса командной строки Windows и Wireshark

Команда **arp** позволяет пользователю просматривать и изменять ARP-кэш в ОС Windows. Команда вводится в командную строку Windows.

Шаг 1: Отобразите ARP-кэш.

1) Откройте окно командной строки на ПК-А и введите **arp**.

C:\Users\User1> **arp**

2) Изучите выходные данные.

Какая команда позволяет отобразить все записи в ARP-кэше?

Какая команда позволяет удалить все записи в ARP-кэше (очистить ARP-кэш)?

Какая команда позволяет удалить все записи в ARP-кэше для 192.168.1.11?

3) Введите **arp -a**, чтобы отобразить таблицу ARP.

C:\Users\User1> **arp -a**

4) Отправьте эхо-запрос с помощью команды `ping` с вашего ПК на ПК другого учащегося для динамического добавления записей в ARP-кэш.

C:\Documents and Settings\User1> **ping IP-адрес устройства коллеги**

Назовите физический адрес узла с IP-адресом

Шаг 2. Настройте записи в ARP-кэш вручную.

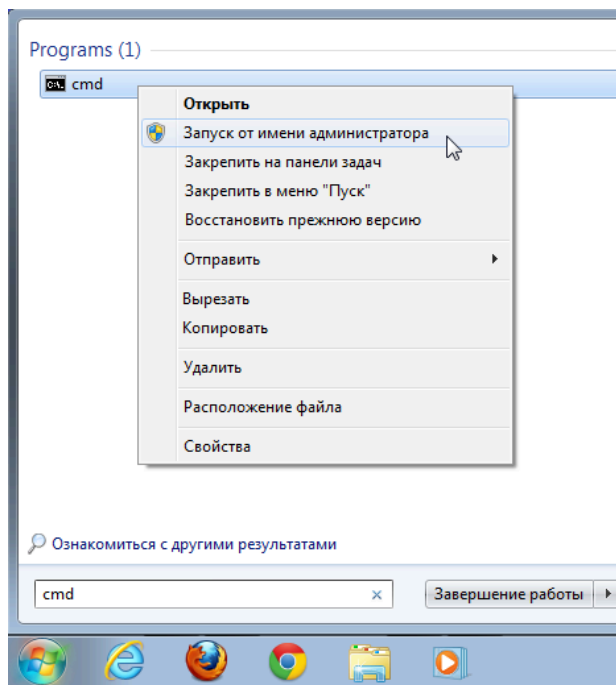
Чтобы удалить записи из ARP-кэша, выполните команду **arp -d {inet- addr | *}**. Можно удалить адреса по отдельности, указав соответствующие IP-адреса, либо стереть сразу все записи с помощью подстановочного символа *****.

1) С вашего ПК отправьте эхо-запросы с помощью команды **ping** на все адрес другого учащегося и на адрес шлюза по умолчанию.

2) Убедитесь в том, что все адреса добавлены в ARP-кэш. Если адрес в ARP-кэше отсутствует, отправьте эхо-запрос с помощью команды **ping** на адрес назначения и проверьте, добавлен ли адрес в ARP-кэш.

C:\Users\User1> **arp -a**

3) Откройте командную строку от имени администратора. Нажмите кнопку **Пуск** и в поле *Найти программы и файлы* введите команду **cmd**. Когда появится значок **cmd**, нажмите на него правой кнопкой мыши и выберите параметр **Запуск от имени администратора**. Нажмите кнопку **Да**, чтобы разрешить этой программе вносить изменения.



4) В окне командной строки администратора введите **arp -d ***. Эта команда удалит все записи из ARP-кэша. Убедитесь в том, что все записи из ARP-кэша удалены. Для этого в командной строке введите **arp -a**.

C:\windows\system32> **arp -d ***

C:\windows\system32> **arp -a**

5) Подождите несколько минут. Протокол обнаружения соседей снова начинает заполнять ARP-кэш.

C:\Users\User1> **arp -a**

Часть 2. Анализ обмена сообщениями ARP с помощью программы Wireshark

В части 2 вам предстоит изучить обмен сообщениями ARP, используя программу Wireshark для их захвата и оценки. Кроме того, вы проанализируете задержки сети, вызванные обменом сообщениями ARP между устройствами.

Шаг 1: Настройте программу Wireshark для захвата пакетов.

- 1) Запустите программу Wireshark.
- 2) Выберите сетевой интерфейс, который будете использовать для захвата сообщений ARP.

Шаг 2: Захватите и оцените сообщения ARP.

1) Начните захват пакетов в программе Wireshark. С помощью фильтра отобразите только пакеты ARP.

- Очистите ARP-кэш, набрав в командной строке команду **arp -d ***.
- Убедитесь в том, что ARP-кэш очищен.
- Отправьте эхо-запрос с помощью команды **ping** на шлюз по умолчанию с помощью команды **ping IP-адрес шлюза по умолчанию**.
- После отправки эхо-запроса на шлюз по умолчанию остановите захват данных программой Wireshark.
- В захваченных данных найдите сообщения ARP в панели сведений о пакетах.

Какой пакет ARP был первым? _____ ARP-запрос

Filter: **arp** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
6	1.795609000	De1l_19:55:92	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.3
7	1.796075000	Cisco_45:73:a1	De1l_19:55:92	ARP	60	192.168.1.1 is at c4:71:fe:45:73:a1

Frame 6: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

Ethernet II, Src: De1l_19:55:92 (5c:26:0a:19:55:92), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

- Hardware type: Ethernet (1)
- Protocol type: IP (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)
- Sender MAC address: De1l_19:55:92 (5c:26:0a:19:55:92)
- Sender IP address: 192.168.1.3 (192.168.1.3)
- Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
- Target IP address: 192.168.1.1 (192.168.1.1)

```

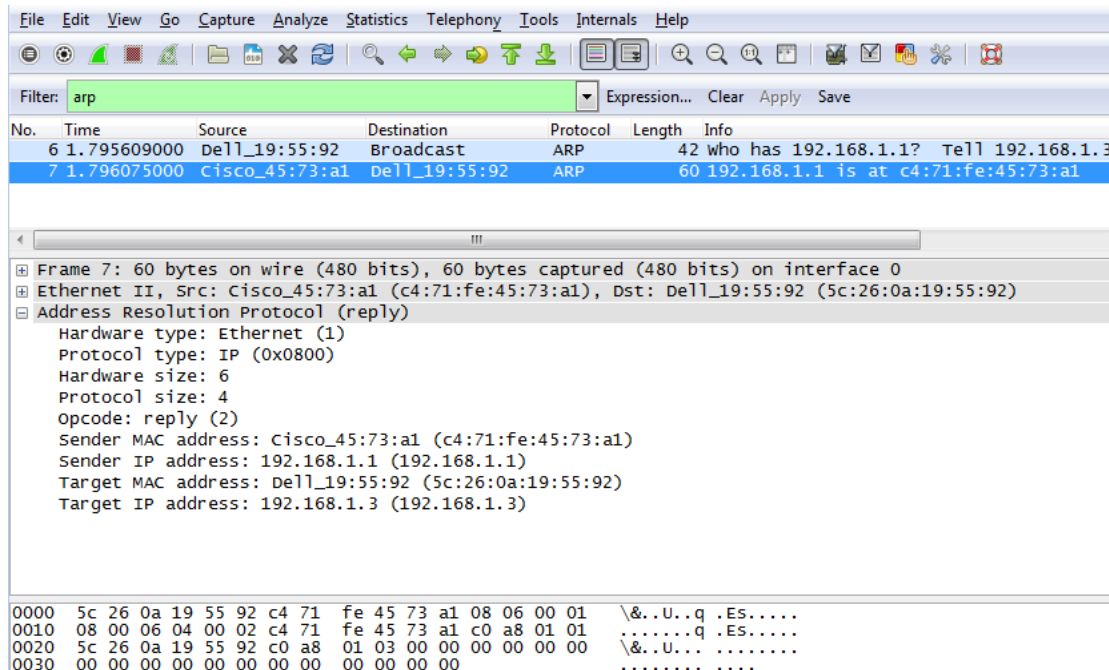
0000  ff ff ff ff ff ff 5c 26 0a 19 55 92 08 06 00 01  .....& ..U....
0010  08 00 06 04 00 01 5c 26 0a 19 55 92 c0 a8 01 03  .....& ..U....
0020  00 00 00 00 00 00 c0 a8 01 01  .....

```

Заполните приведённую ниже таблицу данными первого захваченного пакета ARP.

Поле	Значение
MAC-адрес отправителя	
IP-адрес отправителя	
MAC-адрес назначения	
IP-адрес назначения	

Какой пакет ARP был вторым? _____



Заполните приведённую ниже таблицу данными второго захваченного пакета ARP.

Поле	Значение
MAC-адрес отправителя	
IP-адрес отправителя	
MAC-адрес назначения	
IP-адрес назначения	

Шаг 3: Проанализируйте задержки сети, вызванные ARP.

1) Очистите записи ARP на своем ПК

- Начните захват данных программой Wireshark.
- Отправьте эхо-запрос с помощью команды ping на шлюз по умолчанию и на ПК другого учащегося.

C:\Users\User1> **ping IP-адрес другого устройства**

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 3ms, Average = 2ms

- После отправления эхо-запросов с помощью команды ping остановите захват данных программой Wireshark. С помощью фильтра отобразите только данные ARP и ICMP. В поле **Filter:** (Фильтр) программы Wireshark введите **arp** или **icmp**.

- Изучите захваченные данные. Как показано в захвате данных Wireshark, ARP — это яркий пример компромисса производительности. При отсутствии кэша протокол ARP должен непрерывно запрашивать трансляцию адресов каждый раз при помещении кадра в сеть. В этом случае для установления связи прибавляется время ожидания, что может вызвать перегрузку локальной сети.

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Вопросы на закрепление

1. Как и когда удаляются статические записи ARP?
2. Зачем добавить статические записи ARP в кэш?
3. Если ARP-запросы способны вызывать задержки сети, почему не рекомендуется снимать ограничения на время ожидания отклика для записей ARP?

4. Контрольные вопросы

1. Перечислите 7 уровней модели OSI/ISO
2. Назначение каждого уровня модели OSI/ISO
3. Чем отличается две сетевые модели: OSI/ISO и стек протоколов TCP/IP
4. Логическая и физическая топология. В чем отличие?
5. Типы каналов связи
6. На какие подуровни делиться канальный уровень и за что они отвечают
7. Режимы конфигураций в Cisco IOS

P.S. Преподаватель при сдаче лабораторной работы может задавать вопросы по всей методичке. Данный перечень вопросов является примерным.