

Лабораторная работа № 1.

Знакомство с Cisco Packet Tracer

Козлов Всеволод Павлович

Содержание

Цель работы	1
Задание	2
Выполнение лабораторной работы.....	2
Ответы на контрольные вопросы	13
Выводы	14
Список литературы.....	14

Список иллюстраций

Установка Cisco Packet Tracer	2
Создание проекта	3
Создание ip-адреса	3
Отправка пакета данных	4
Ответ на вопросы	4
Структура пакета ICMP	5
Коллизия при отправке пакетов данных	6
Коммутатор и 4 оконечных устройства	6
Отправка пакета данных	7
Структура пакета ICMP	8
Отсутствие коллизии при использовании коммутатора.....	9
Соединение между концентратором и коммутатором	10
Структура STP	11
Добавление маршрутизатора	12
Отправка пакета данных от PC3 к маршрутизатору	12
Структура пакета CDP	13

Список таблиц

Элементы списка иллюстраций не найдены.

Цель работы

Установка инструмента моделирования конфигурации сети Cisco Packet Tracer, знакомство с его интерфейсом.

Задание

1. Установить на домашнем устройстве Cisco Packet Tracer.
2. Постройте простейшую сеть в Cisco Packet Tracer, проведите простейшую настройку оборудования.

Выполнение лабораторной работы

Установил Cisco Packet Tracer, изменил настройки в брандмаузере Windows (рис. 1).

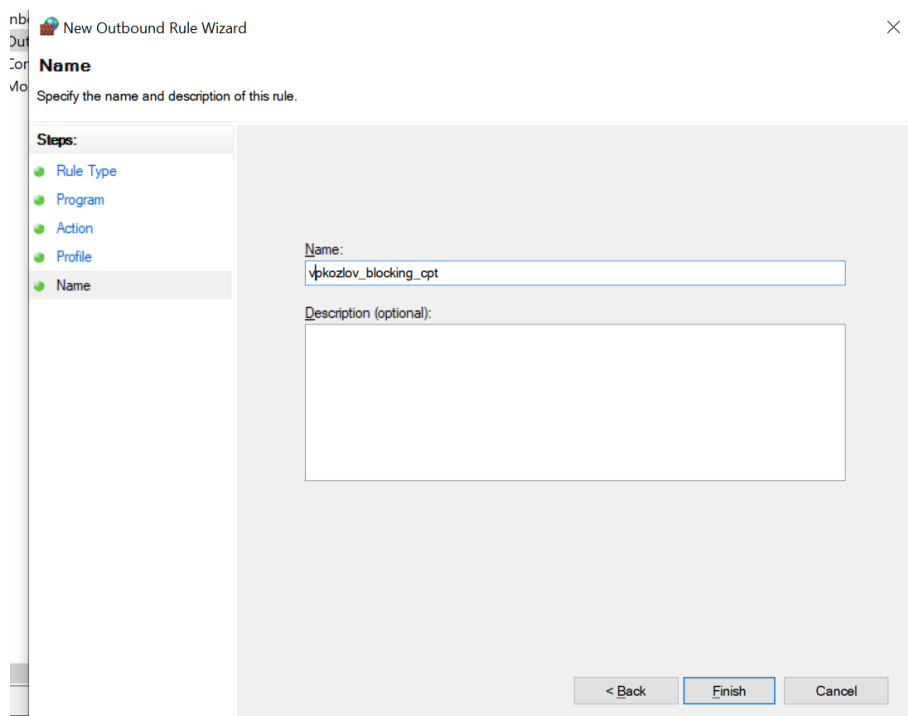


Рис. 1. Установка Cisco Packet Tracer

Создал новый проект lab_PT-01.pkt (рис. 2).

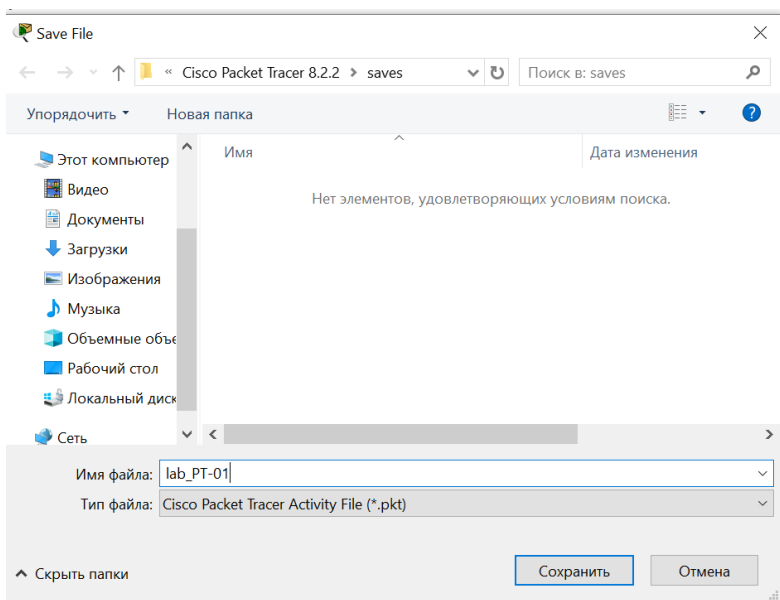


Рис. 2. Создание проекта

Задал ip-address для PC0. Произвел аналогичные изменения для PC1, PC2, PC3 (рис. 3).

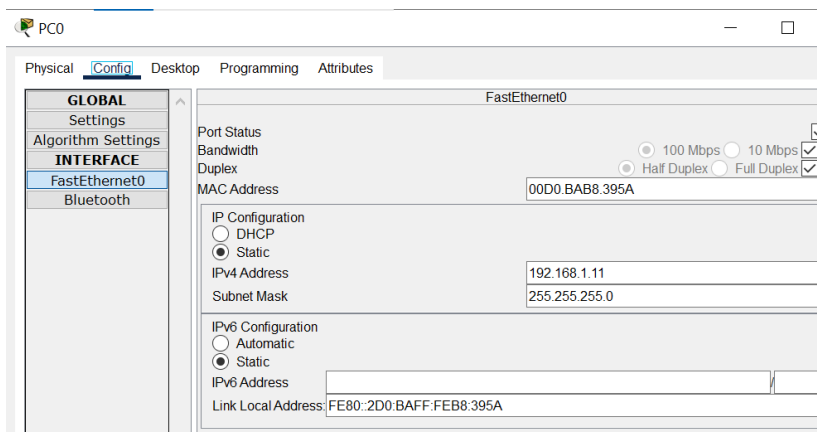


Рис. 3. Создание ip-адреса

Отправил пакет данных от PC0 к PC2 (рис. 4).

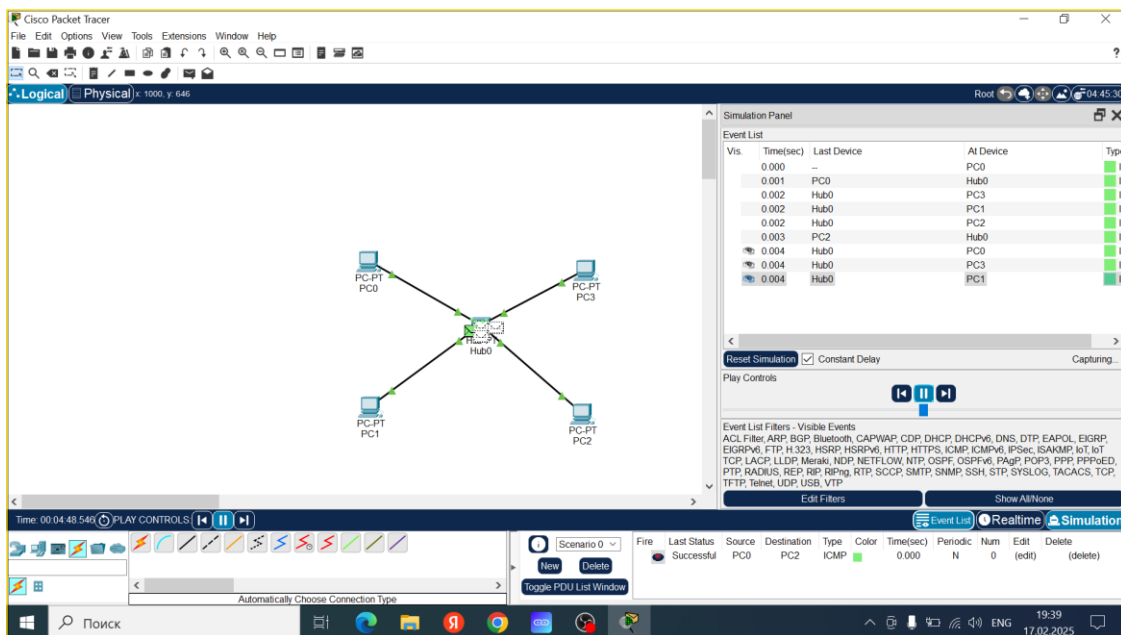


Рис. 4. Отправка пакета данных

Отвечил на вопросы, нажав на кнопку “Challenge me” (рис. 5).

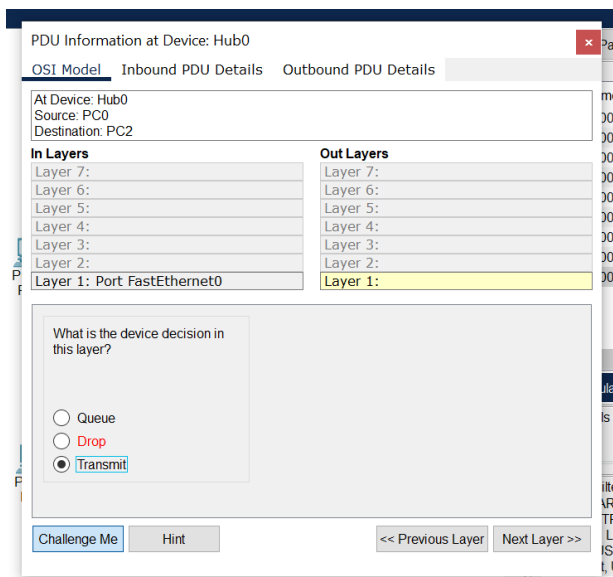


Рис. 5. Ответ на вопросы

Открыл вкладку с информацией о PDU. Исследовал структуру пакета ICMP (рис. 6).

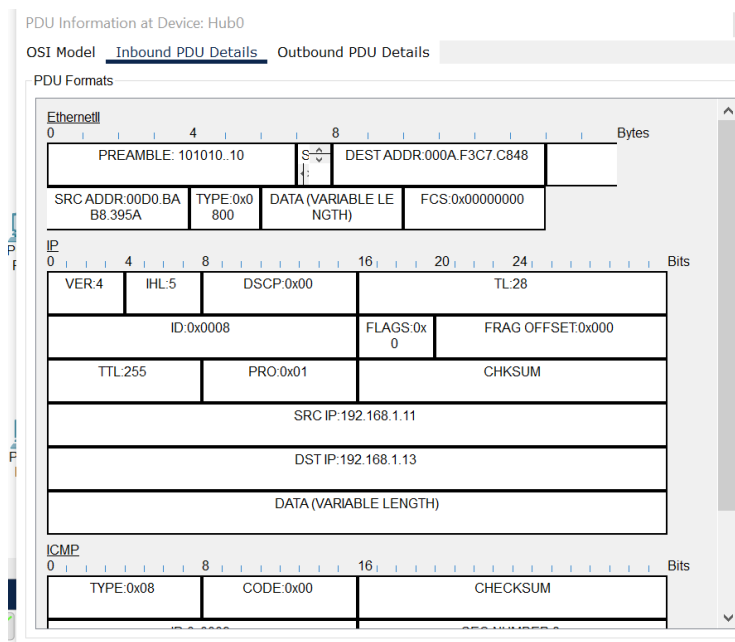


Рис. 6. Структура пакета ICMP

Когда простой PDU (такой как ICMP-пакет) отправляется с PC0 на PC2 в данном сценарии, он будет инкапсулирован в кадр Ethernet перед отправкой по сети. Фрейм Ethernet будет иметь следующую структуру:

- Преамбула: 7-байтовый (56-битный) шаблон (10101010), используемый для синхронизации часов приемника с входящими данными.
- Разделитель начального кадра (SFD): Однобайтовый (8-разрядный) шаблон (10101011), используемый для обозначения начала кадра.
- MAC-адрес назначения: 0003 E446 6514
- MAC-адрес источника: 00D0 BCA4 3403
- EtherType: двухбайтовое (16-разрядное) поле, которое идентифицирует тип протокола, передаваемого в полезной нагрузке фрейма. Для ICMP-пакетов значение EtherType обычно равно 0x0800.
- Полезная нагрузка: фактические передаваемые данные (в данном случае ICMP-пакет).
- Последовательность проверки кадра (FCS): Четырехбайтовое (32-разрядное) поле, содержащее значение контрольной суммы, используемое для обнаружения ошибок в кадре.

Когда фрейм Ethernet перемещается с одного устройства на другое, единственными изменениями, которые происходят в фрейме Ethernet, являются изменения MAC-адресов источника и назначения. MAC-адрес источника будет изменен на MAC-адрес устройства, отправляющего кадр, в то время как MAC-адрес назначения будет изменен на MAC-адрес устройства назначения. Этот процесс известен как изучение MAC-адреса и выполняется концентратором. Типом фрейма Ethernet, используемого в этом сценарии, является стандартный фрейм Ethernet, который также известен как фрейм Ethernet II.

Очистил список событий. Отправил пакет данных от PC0 к PC2 и от PC2 к PC0 (рис. 7).

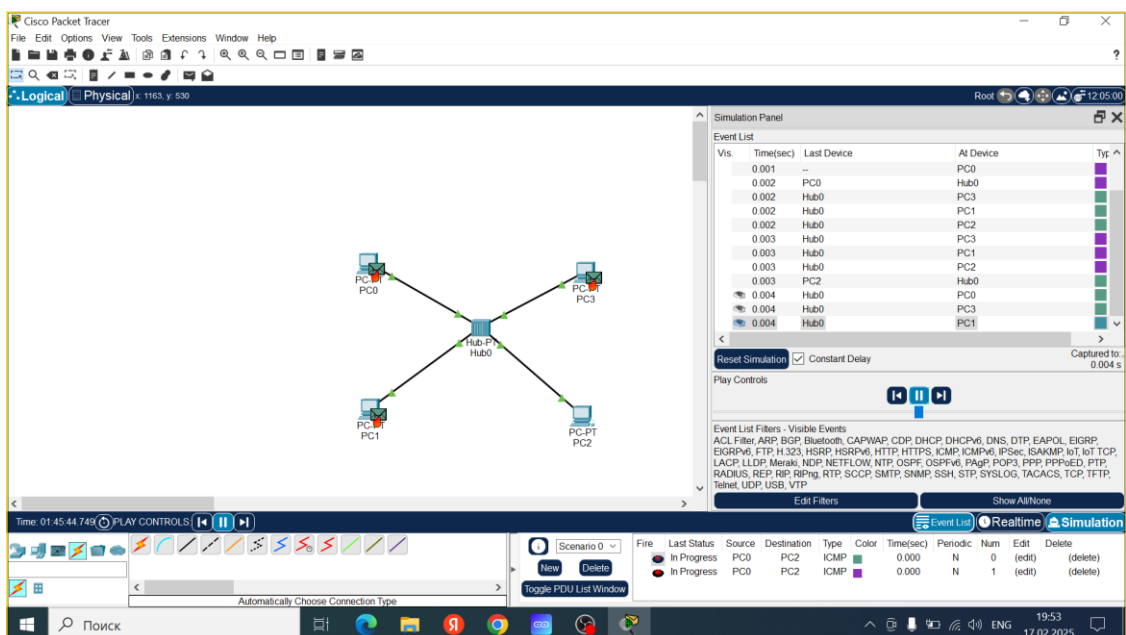


Рис. 7. Коллизия при отправке пакетов данных

Когда несколько устройств подключены к концентратору в сети, они совместно используют один и тот же сегмент сети, и концентратор пересылает все входящие данные всем устройствам в этом сегменте. Это означает, что когда два или более устройства пытаются передать данные одновременно, может произойти коллизия. Коллизия – это ситуация, при которой два или более устройства пытаются передать данные в одном и том же сегменте сети одновременно, в результате чего данные становятся поврежденными и нечитаемыми принимающими устройствами.

В рабочем пространстве разместил коммутатор и 4 оконечных устройства. Произвел настройку ip-адресов (рис. 8).

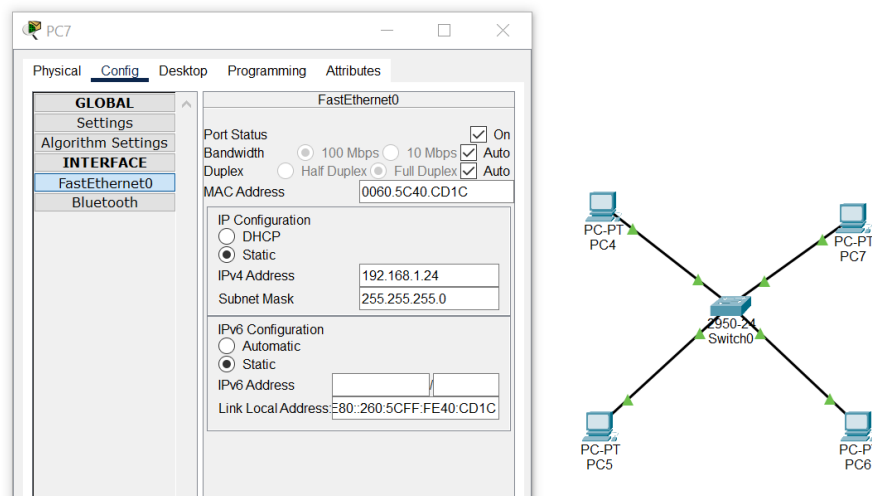


Рис. 8. Коммутатор и 4 оконечных устройства

Отправил пакет данных от PC4 к PC6 (рис. 9).

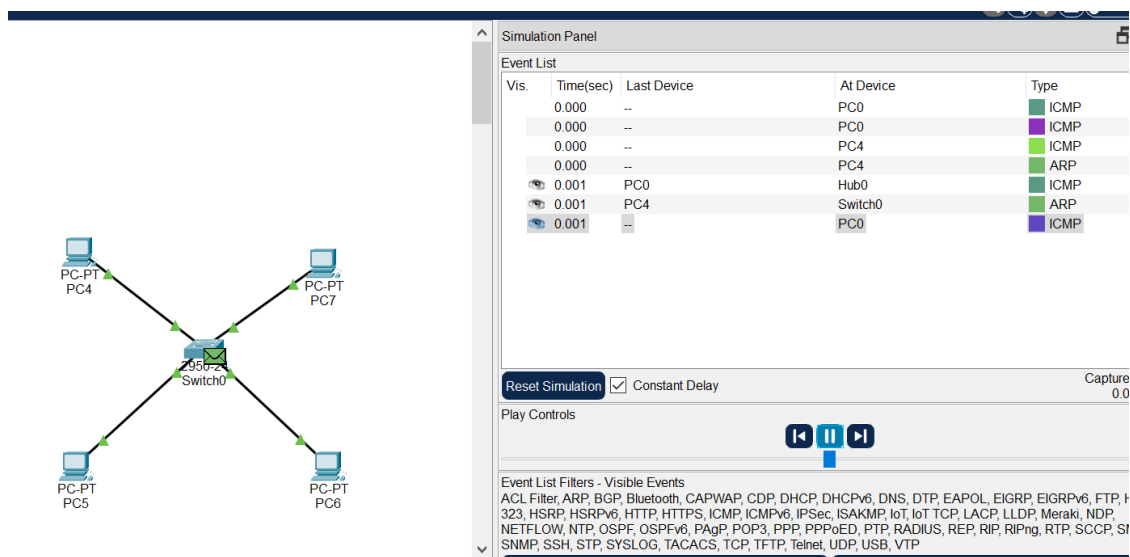


Рис. 9. Отправка пакета данных

- В сценарии, когда PC0, PC1, PC2 и PC3 подключены к концентратору и PDU отправляется с PC0 на PC2, протокол ARP будет генерировать пакеты запроса ARP и ответа для обнаружения и сопоставления MAC-адреса PC2. Пакет запроса ARP будет транслироваться на все устройства в сети, включая PC2. PC2 получит запрос ARP и ответит ответным пакетом ARP, который включает его MAC-адрес. Ответный пакет ARP будет передан на все устройства в сети, включая PC0, а MAC-адрес PC2 будет добавлен в ARP-кэш PC0.
- В сценарии, когда PC4, PC5, PC6 и PC7 подключены к коммутатору и PDU отправляется с PC4 на PC6, протокол ARP также будет генерировать пакеты запроса ARP и ответа для обнаружения и сопоставления MAC-адреса PC6. Однако, поскольку коммутатор перенаправляет PDU непосредственно на PC6, пакеты запроса ARP и ответа будут отправляться только между PC4 и PC6, а не транслироваться на все устройства в сети.
- Следовательно, основное различие в событиях протокола ARP между сценариями концентратора и коммутатора заключается в том, что в сценарии концентратора пакеты запроса ARP и ответа будут транслироваться на все устройства в сети, в то время как в сценарии коммутатора пакеты запроса ARP и ответа будут отправляться только между исходным и целевым устройствами.

Исследуйте структуру пакета ICMP (рис. 10).

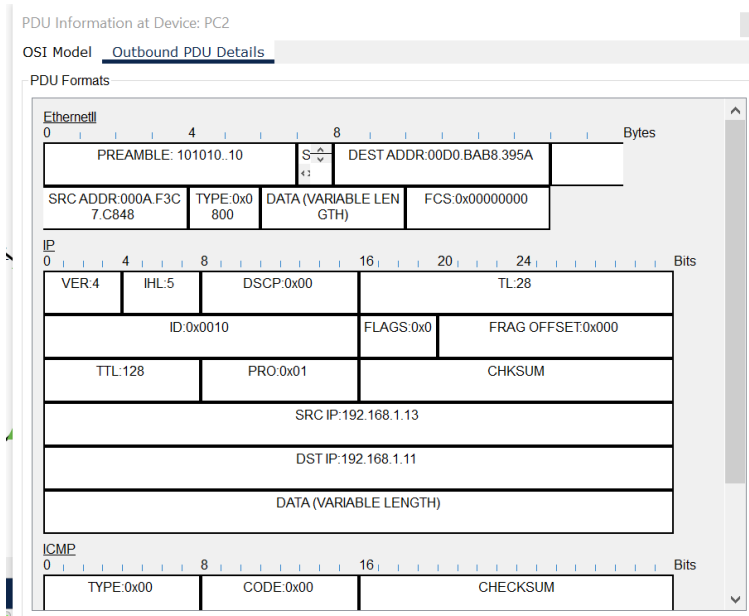


Рис. 10. Структура пакета ICMP

Тип фрейма Ethernet, используемого в этом сценарии Ethernet II. Фрейм Ethernet будет иметь следующую структуру:

- Преамбула: 7 байтовый шаблон (10101010), используемый для синхронизации часов приемника с входящими данными.
- Разделитель начального кадра (SFD): Однобайтовый шаблон (10101011), используемый для указания начала кадра.
- MAC-адрес назначения ADDR 0009 7CD0 1DBB: 6-байтовое поле, содержащее MAC-адрес устройства назначения (в данном случае MAC-адрес PC6).
- MAC-адрес источника ADDR 00D0 5848 DCE0: 6-байтовое поле, содержащее MAC-адрес исходного устройства (в данном случае MAC-адрес PC4).
- EtherType: Двухбайтовое поле, которое идентифицирует тип протокола, передаваемого в полезной нагрузке фрейма. Для ICMP-пакетов значение EtherType обычно равно 0x0800.
- Полезная нагрузка (DATA): фактически передаваемые данные (в данном случае ICMP-пакет).
- Последовательность проверки кадра (FCS): Четырехбайтовое поле, содержащее значение контрольной суммы, используемое для обнаружения ошибок в кадре. Когда кадр Ethernet перемещается с PC4 на коммутатор, коммутатор считывает MAC-адрес назначения и пересылает кадр из соответствующего порта, подключенного к PC6. Исходный MAC-адрес фрейма Ethernet останется прежним, но MAC-адрес назначения будет изменен на MAC-адрес порта, подключенного к PC6 на коммутаторе. Этот процесс известен как изучение MAC-адреса и выполняется коммутатором.

Структура пакета ICMP будет содержать следующие поля:

- Тип: Однобайтовое поле, которое определяет тип ICMP-сообщения. Например, эхо-запрос ICMP имеет тип 8.
- Код: Однобайтовое поле, которое предоставляет дополнительную информацию о сообщении ICMP.
- Контрольная сумма: двухбайтовое поле, содержащее значение контрольной суммы, используемое для обнаружения ошибок в сообщении ICMP.
- Идентификатор: Двухбайтовое поле, используемое для идентификации ICMP-сообщения. Это поле используется в сочетании с полем порядкового номера для уникальной идентификации каждого ICMP-сообщения.
- Порядковый номер: Двухбайтовое поле, используемое для идентификации ICMP-сообщения. Это поле используется в

сочетании с полем идентификатора для уникальной идентификации каждого ICMP-сообщения.

Очистил список событий. Отправил пакет данных от PC4 к PC6 и от PC6 к PC4 (рис. 11).

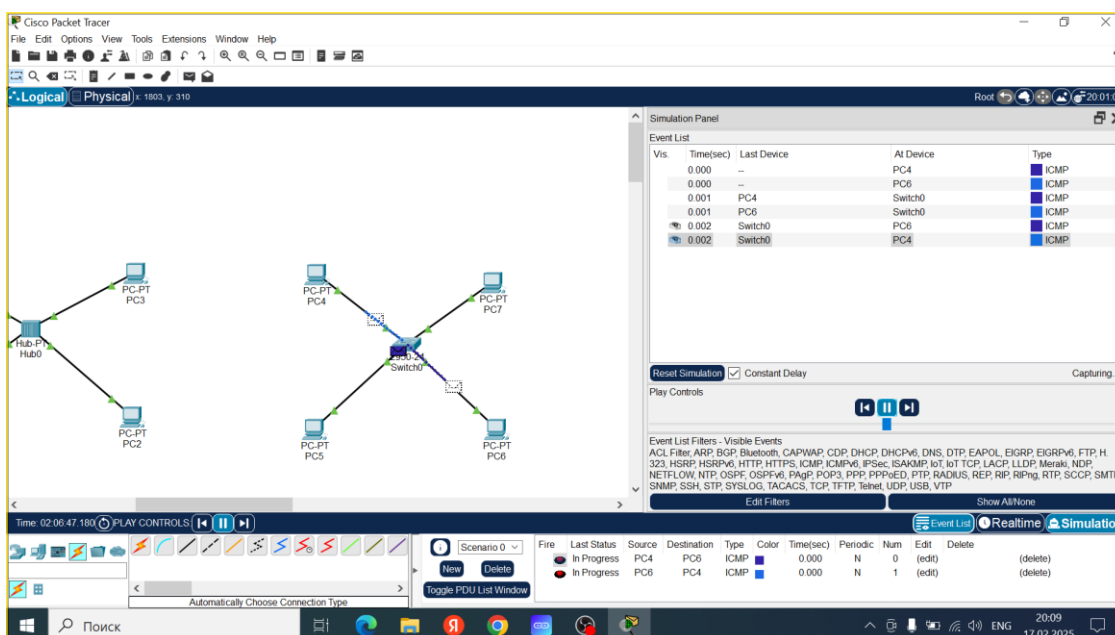


Рис. 11. Отсутствие коллизии при использовании коммутатора

- В сети с коммутатором устройства подключены к разным портам коммутатора, и каждый порт находится в отдельном домене столкновения. Это означает, что когда два устройства взаимодействуют друг с другом, передача данных происходит непосредственно между двумя устройствами.
- Когда коммутатор получает данные от устройства, он проверяет MAC-адрес назначения данных и использует свою таблицу MAC-адресов, чтобы определить, на какой порт коммутатора пересылать данные. Коммутатор пересылает данные только из порта, подключенного к устройству назначения, и все остальные порты коммутатора на коммутаторе остаются незатронутыми.

Соединил крестовым кабелем концентратор и коммутатор. Отправил пакет данных от PC0 к PC4 и от PC4 к PC0 (рис. 12).

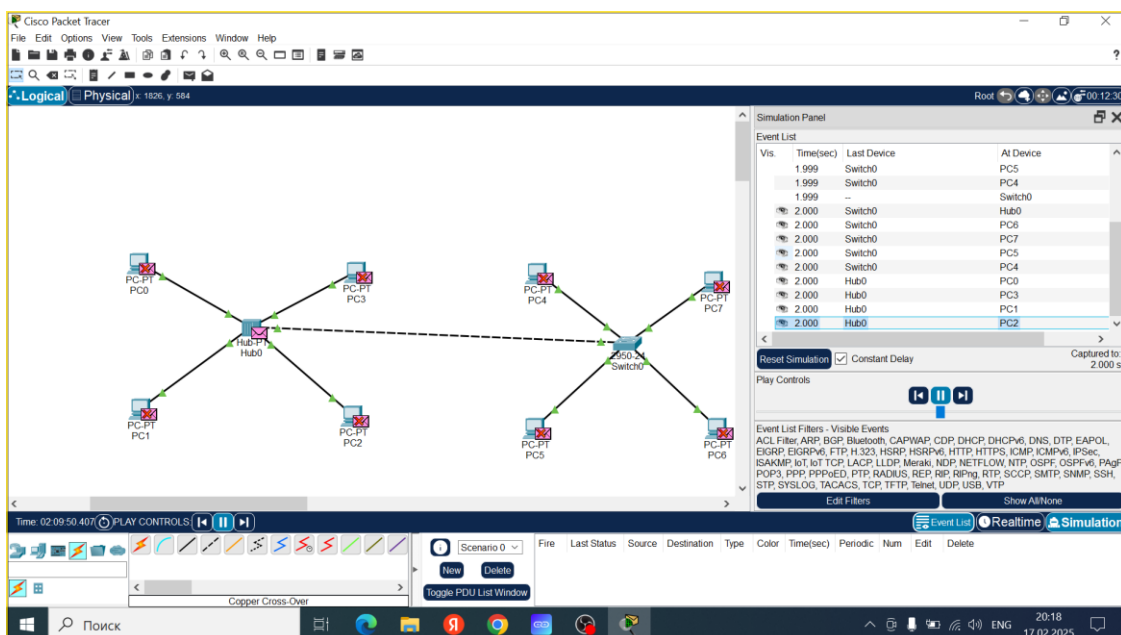


Рис. 12. Соединение между концентратором и коммутатором

- Это происходит потому, что концентратор является общим сетевым устройством, которое пересылает все входящие данные на все устройства в сетевом сегменте, включая коммутатор. Когда PC0 отправляет сообщение на PC4, концентратор пересылает сообщение всем устройствам в сетевом сегменте, включая коммутатор. В то же время PC4 также может передавать данные на другое устройство, и эти данные могут конфликтовать с данными, передаваемыми PC0.
- Аналогично, когда PC4 пытается отправить сообщение обратно на PC 0, концентратор пересылает сообщение всем устройствам в сетевом сегменте, включая PC0. В то же время PC0 также может передавать данные на другое устройство, и эти данные могут конфликтовать с данными, передаваемыми PC4.

Исследовал структуру STP (рис. 13).

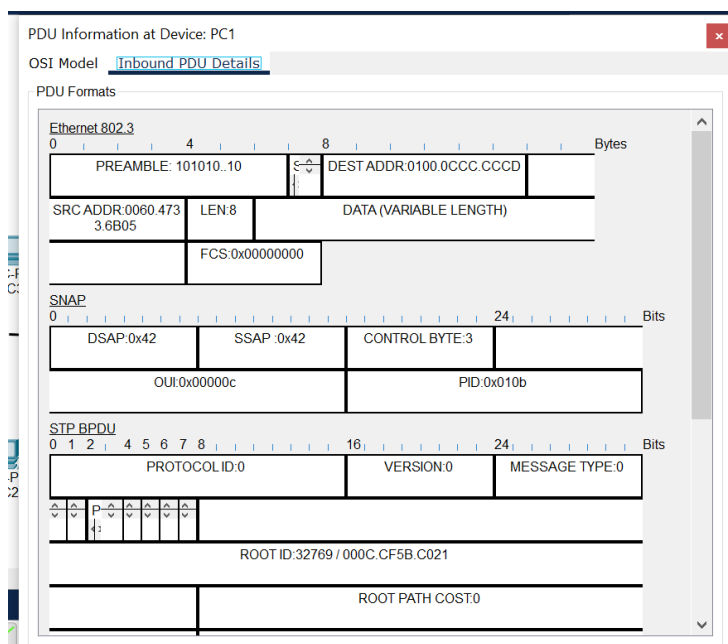


Рис. 13. Структура STP

- Protocol ID: 2 байта, установлено значение 0x0000
- Protocol Version: 1 байт, установлено значение 0x00
- Тип BPDU: 1 байт, определяет тип BPDU
- Flags: 1 байт, содержит флаги, используемые в протоколе STP
- Root ID: 8 байт, идентифицирует корневой мост.
- Root Path Cost: 4 байта, указывает стоимость пути к корневому мосту
- Bridge ID: 8 байт, идентифицирует отправителя BPDU
- Part ID: 2 байта, идентифицирует порт отправителя BPDU
- Message Age: 2 байта, указывает возраст BPDU
- Max Age: 2 байта, указывает максимальный возраст BPDU
- Hello Time: 2 байта, указывает интервал между передачами BPDU
- Forward Delay: 2 байта, указывает на задержку перед пересылкой BPDU
- Ethernet в STP-пакете имеет следующую структуру:
 - Преамбула: 7 байт, устанавливается в чередующиеся 0 и 1 с
 - Разделитель начального фрейма: 1 байт, установлен в 0x55
 - MAC-адрес назначения: 6 байт, устанавливается на адрес многоадресной рассылки STP (01:80:C2:00:00:00)
 - MAC-адрес источника: 6 байт, устанавливается в качестве MAC-адреса коммутатора, отправляющего BPDU
 - Ethertype: 2 байта, установлено значение 0x0000 для STP
 - STP-пакет: переменной длины, как описано выше
 - FCS: 4 байта, контрольная сумма CRC, используемая для проверки целостности фрейма

В рабочем пространстве добавил маршрутизатор, соединил с коммутатором. Произвел настройку ip-адреса (рис. 14).

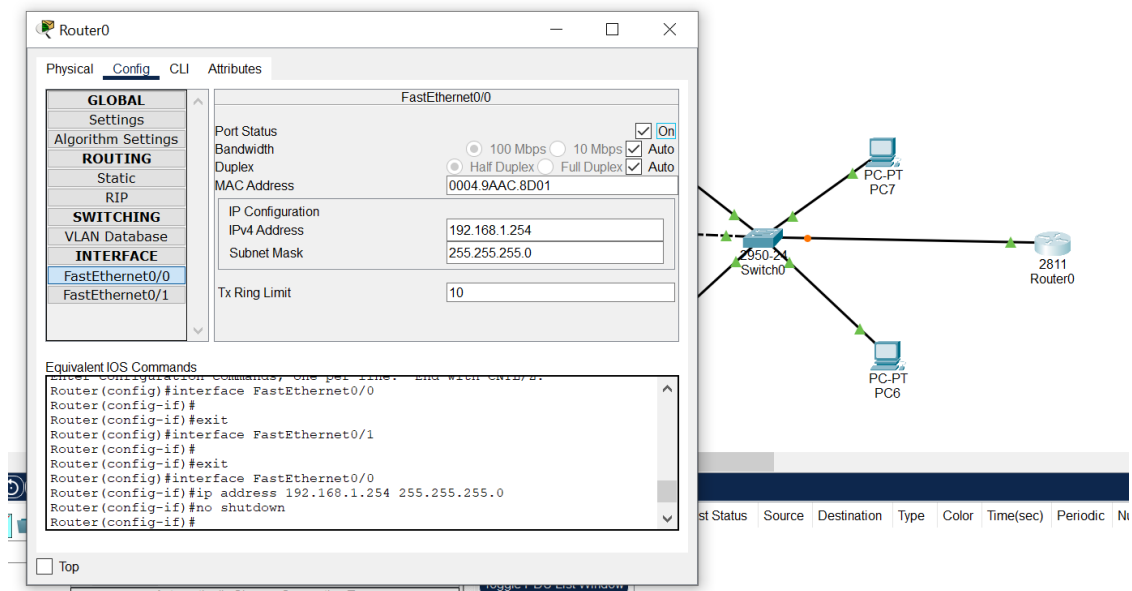


Рис. 14. Добавление маршрутизатора

Очистил список событий. Отправил пакет данных от PC3 к маршрутизатору. Проследил за движением пакетов ARP, ICMP, STP и CDP (рис. 15).

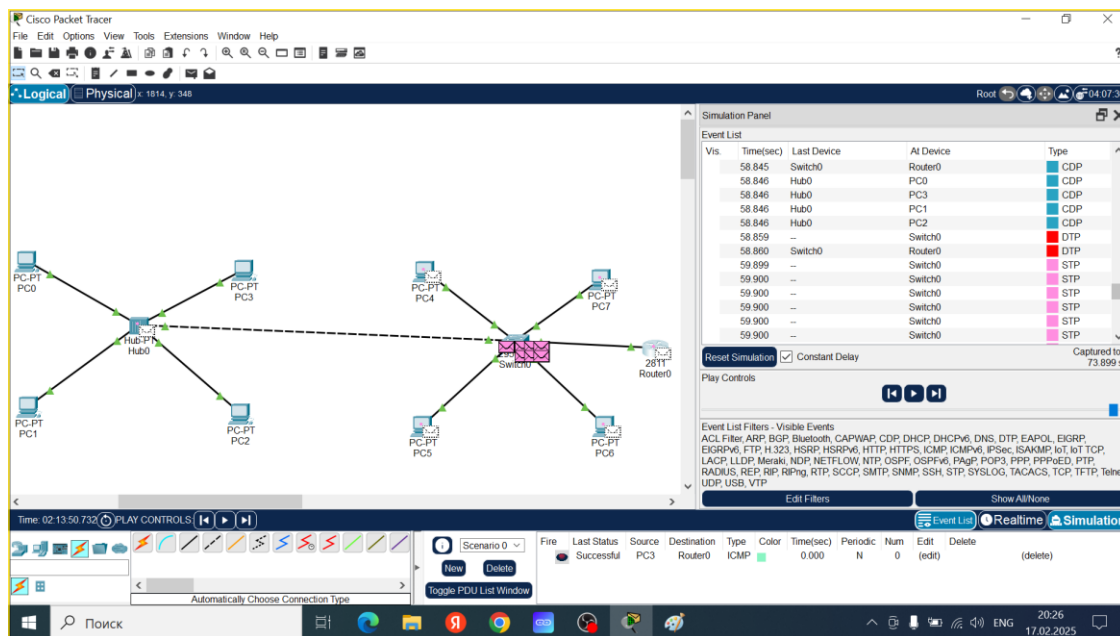


Рис. 15. Отправка пакета данных от PC3 к маршрутизатору

Исследуйте структуру пакета CDP (рис. 16).

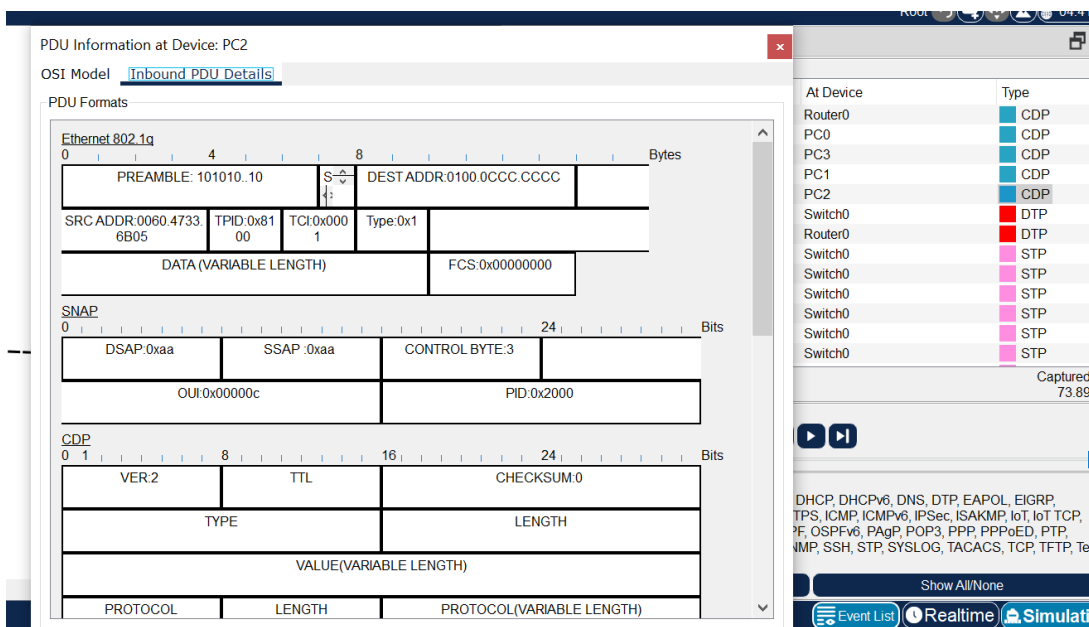


Рис. 16. Структура пакета CDP

Фрейм Ethernet 802.3, несущий пакет CDP, имеет следующую структуру: - MAC-адрес назначения: 01-00-0C-CC-CC-CC (MAC-адрес многоадресной рассылки CDP) - MAC-адрес источника 0001 968D E805: MAC-адрес устройства-отправителя - Тип эфира: 0x2000 (тип эфира протокола CDP) - FCS: 0x00000000 используется для обеспечения того, чтобы данные были переданы без ошибок, и они проверяются принимающим устройством для подтверждения того, что кадр не был поврежден во время передачи. Пакета CDP: • Версия: Это поле определяет версию используемого протокола CDP. • TTL: Это поле содержит значение времени ожидания, которое представляет собой максимальное количество сетевых переходов, которые проходит пакет CDP перед отбрасыванием. • Контрольная сумма: Это поле содержит значение контрольной суммы для всего пакета CDP.

Ответы на контрольные вопросы

1. Дайте определение следующим понятиям: концентратор, коммутатор, маршрутизатор, шлюз (gateway). В каких случаях следует использовать тот или иной тип сетевого оборудования? Концентратор (Hub): Это простое сетевое устройство, которое соединяет несколько Ethernet-устройств в одной локальной сети (LAN). Концентратор работает на физическом уровне модели OSI и передает данные, полученные от одного устройства, ко всем остальным, не различая адреса. Используется в небольших сетях, но в современных условиях практически не применяется из-за низкой эффективности и отсутствия управления трафиком.

Коммутатор (Switch): Это более сложное устройство, чем концентратор, которое работает на канальном уровне модели OSI. Коммутатор принимает данные от одного устройства и отправляет их только на тот порт, к которому подключено целевое устройство, что значительно уменьшает количество ненужного трафика в сети. Используется в большинстве современных локальных сетей для повышения производительности и управления трафиком.

Маршрутизатор (Router): Устройство, которое соединяет разные сети и направляет пакеты данных между ними. Маршрутизатор работает на сетевом уровне модели OSI и использует IP-адреса для определения наилучшего пути для передачи данных. Используется для подключения локальной сети к интернету или для соединения нескольких локальных сетей.

Шлюз (Gateway): Это устройство, которое служит “воротами” между двумя сетями, часто с различными протоколами. Шлюз может выполнять функции маршрутизатора, но также может преобразовывать данные между различными сетевыми протоколами. Используется, когда необходимо соединить сети с различными архитектурами или протоколами.

2. Дайте определение следующим понятиям: ip-адрес, сетевая маска, broadcastадрес. IP-адрес: Уникальный адрес, присваиваемый каждому устройству в сети, который позволяет идентифицировать его и обеспечивать маршрутизацию данных. IP-адрес может быть статическим (постоянным) или динамическим (изменяющимся).

Сетевая маска: Это 32-битное число, которое используется для определения сети и подсети, к которой принадлежит IP-адрес. Сетевая маска помогает разделить IP-адрес на две части: сеть и узел. Например, для IP-адреса 192.168.1.1 с маской 255.255.255.0, первые три октета (192.168.1) обозначают сеть, а последний октет (1) — узел.

Broadcast-адрес: Это специальный адрес, который используется для отправки данных всем устройствам в сети. В IPv4, broadcast-адрес формируется путем установки всех битов узловой части IP-адреса в единицы. Например, для сети с адресом 192.168.1.0 и маской 255.255.255.0, broadcast-адрес будет 192.168.1.255.

3. Как можно проверить доступность узла сети? Для проверки доступности узла сети можно использовать команду ping. Эта команда отправляет ICMP-запросы на указанный IP-адрес или доменное имя и ожидает ответа. Если узел доступен, он отправляет ответ, и вы увидите время отклика. Если узел недоступен, вы получите сообщение об ошибке.

Пример использования команды в командной строке: ping 192.168.1.1

Также можно использовать другие инструменты, такие как traceroute (или tracert в Windows), чтобы определить маршрут, по которому проходят пакеты к узлу, и выявить возможные проблемы в сети.

Выводы

Установил инструмент моделирования конфигурации сети Cisco Packet Tracer, ознакомился с его интерфейсом.

Список литературы

1. 802.1D-2004 - IEEE Standard for Local and Metropolitan Area Networks. Media Access Control (MAC) Bridges : тех. отч. / IEEE. — 2004. — С. 1—

2. — DOI: 10.1109/IEEESTD.2004.94569. — URL: <http://ieeexplore.ieee.org/servlet/opac?punumber=9155>.
3. 802.1Q - Virtual LANs. — URL: <http://www.ieee802.org/1/pages/802.1Q.html>.
4. A J. Packet Tracer Network Simulator. — Packt Publishing, 2014. — ISBN 9781782170426. — URL: https://books.google.com/books?id=eVOcAgAAQBAJ&dq=cisco+packet+tracer&hl=es&source=gbs_navlinks_
4. Cotton M., Vegoda L. Special Use IPv4 Addresses : RFC / RFC Editor. — 01.2010. — С. 1—11. — № 5735. — DOI: 10.17487/rfc5735. — URL: <https://www.rfc-editor.org/info/rfc5735>.
5. Droms R. Dynamic Host Configuration Protocol : RFC / RFC Editor. — 03.1997. — С. 1—45. — № 2136. — DOI: 10.17487/rfc2131. — URL: <https://www.ietf.org/rfc/rfc2131.txt%20https://www.rfc-editor.org/info/rfc2131>.
6. McPherson D., Dykes B. VLAN Aggregation for Efficient IP Address Allocation, RFC 3069. — 2001. — URL: <http://www.ietf.org/rfc/rfc3069.txt>.
7. Moy J. OSPF Version 2 : RFC / RFC Editor. — 1998. — С. 244. — DOI: 10.17487/rfc2328. — URL: <https://www.rfc-editor.org/info/rfc2328>.
8. NAT Order of Operation. — URL: <https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/6209-5.html>.
9. NAT: вопросы и ответы / Сайт поддержки продуктов и технологий компании Cisco. — URL: https://www.cisco.com/cisco/web/support/RU/9/92/92029_nat-faq.html.
10. Neumann J. C. Cisco Routers for the Small Business A Practical Guide for IT Professionals. — Apress, 2009.
11. Odom S., Nottingham H. Cisco Switching: Black Book. — The Coriolis Group,
12. — ISBN 9781576107065. — URL: <http://books.google.sk/books?id=GYsLAAAACAAJ>.
13. Tetz E. Cisco Networking All-in-One For Dummies. — Indianapolis, Indiana : John Wiley & Sons, Inc., 2011. — (For Dummies). — URL: <http://www.dummies.com/store/product/Cisco-Networking-All-in-One-For-Dummies.productCd-0470945583.html>.
14. ГОСТ Р ИСО/МЭК 7498-1-99. — «ВОС. Базовая эталонная модель. Часть
15. Базовая модель». — ОКС: 35.100.70. — Действует с 01.01.2000. — URL: <http://protect.gost.ru/v.aspx?control=7&id=132355>.
16. Кларк К., Гамильтон К. Принципы коммутации в локальных сетях Cisco. — М. : Вильямс, 2003. — (Cisco Press Core Series). — ISBN 5-8459-0464-1.
17. Королькова А. В., Кулябов Д. С. Архитектура и принципы построения современных сетей и систем телекоммуникаций. — М. : Издательство РУДН, 2009.
18. Королькова А. В., Кулябов Д. С. Прикладные протоколы Интернет и www. Курс лекций. — М. : РУДН, 2012. — ISBN 9785209049500.
19. Королькова А. В., Кулябов Д. С. Прикладные протоколы Интернет и www. Лабораторные работы. — М. : РУДН, 2012. — ISBN 9785209049357.
20. Королькова А. В., Кулябов Д. С. Сетевые технологии. Лабораторные работы. — М. : РУДН, 2014. — ISBN 785209056065.
21. Куроуз Д. Ф., Росс К. В. Компьютерные сети. Нисходящий подход. — 6-е изд. — М. : Издательство «Э», 2016. — (Мировой компьютерный бестселлер).

22. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101. — М. : Вильямс, 2017. — (Cisco Press Core Series). — ISBN 978-5-8459-1906-9.
23. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101. Маршрутизация и коммутация. — М. : Вильямс, 2016. — (Cisco Press Core Series).
24. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. — 5-е изд. — Питер : Питер, 2017. — (Учебник для вузов). — ISBN 978-5-496-01967-5.
25. Сети и системы передачи информации: телекоммуникационные сети / К. Е. Самуйлов [и др.]. — М. : Изд-во Юрайт, 2016. — ISBN 978-5-9916-7198-9.
26. Таненбаум Э., Уэзеролл Д. Компьютерные сети. — 5 изд. — Питер : Питер, 27. — (Классика Computer Science). — ISBN 978-5-496-00831-0.
28. Хилл Б. Полный справочник по Cisco. — М. : Вильямс, 2009. — ISBN 978-5-8459-1309-8.
29. Цикл статей «Сети для самых маленьких». — URL: <http://linkmeup.ru/blog/11.html>.
30. Часто задаваемые вопросы технологии NAT / Сайт поддержки продуктов и технологий компании Cisco. — URL: https://www.cisco.com/c/ru_ru/support/docs/ip/network-address-translation-nat/26704-nat-faq00.html.