

Федеральное государственное бюджетное образовательное учреждение высшего
образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)

09.03.01 Информатика и вычислительная техника

Профиль: Программное обеспечение средств
вычислительной техники и автоматизированных
систем

**Отчёт по лабораторной работе №3
по теме «Изучение среды GNS3»
по дисциплине «Сети ЭВМ и телекоммуникации»**

по направлению 09.03.01 «Информатика и вычислительная техника»,
направленность (профиль) – «Программное обеспечение средств вычислительной техники
и автоматизированных систем», квалификация – бакалавр,
программа академического бакалавриата,
форма обучения – очная, год начала подготовки (по учебному плану) – 2016

Выполнил: студент ф-та ИВТ 3 курса гр. ИП-611

/ Макаревич А.А. /

Проверил: ст. преподаватель кафедры ВС

/ Крамаренко К.Е. /

Новосибирск, 2019

Введение

Цель лабораторной работы: получить навыки использования среды моделирования GNS3. Подготовить среду для выполнения курсовой работы..

Задачи: - установить среду моделирования GNS3 и произвести начальную конфигурацию добавив маршрутизатор CISCO и два пустых контейнера с виртуальными машинами от VirtualBox;

- собрать макет локальной сети, как показано на Рисунок 1;
- исходя из того, что для функционирования создаваемой сети нам выделен диапазон адресов 10.255.0.0/16, определить сколько подсетей нам необходимо задать;
- настроить все интерфейсы всех маршрутизаторов и статическую маршрутизацию. Убедиться, что имеется связь между всеми сетевыми интерфейсами всех маршрутизаторов;
- запустить все модельные устройства (показав, что пустые контейнеры тоже работают, но выдают ошибку загрузки из-за отсутствия операционной системы);
- используя анализатор Wireshark, продемонстрировать принцип работы ping между двумя маршрутизаторами, расположенными в разных подсетях (необходимо показать все генерируемые пакеты в прямом и обратном пути при одном запросе ping);
- убедиться, что наша среда имеет связь со средой другого студента используя реальную физическую сеть.

Предмет исследования: конфигурируемая сеть, исследуемая компьютерным имитационным моделированием.

Средства, используемые при проведении исследования: среда моделирования компьютерных сетей, использующих сетевое оборудование, функционирующее на базе процессоров с архитектурой MIPS. К таким сетевым устройствам относятся, в том числе, большинство сетевых коммутаторов и маршрутизаторов, производимых компанией CISCO – GNS (Graphical Network Simulator).

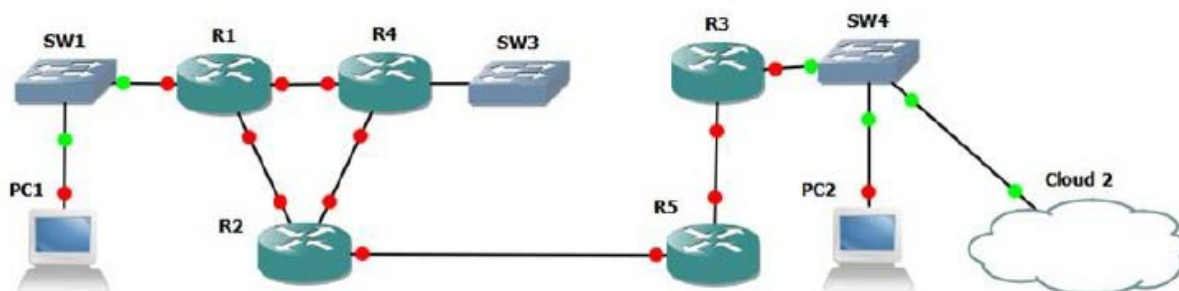


Рисунок 1. Конфигурация моделируемой компьютерной сети.

Выполнение работы

1. Установить среду моделирования GNS3 и произвести начальную конфигурацию добавив маршрутизатор CISCO и два пустых контейнера с виртуальными машинами от VirtualBox.

2. Соберите макет локальной сети, как показано на Рисунок 1.

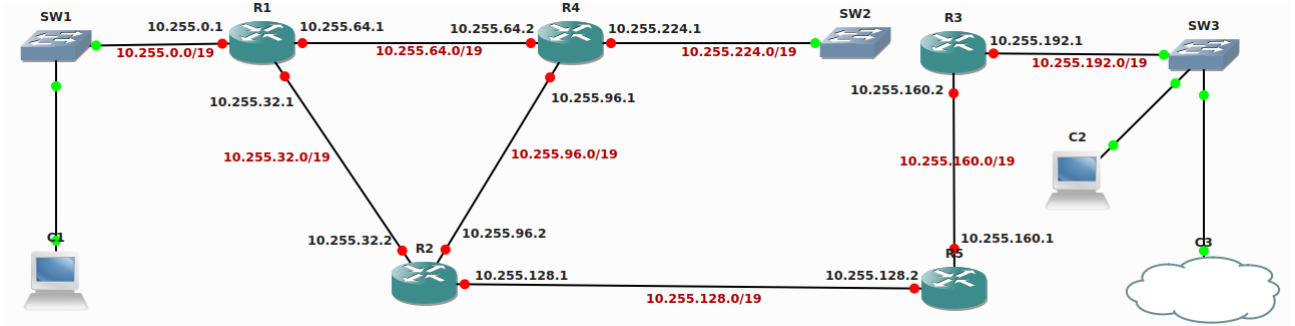


Рисунок 2. Конфигурация макета локальной сети.

3. Исходя из того, что для функционирования создаваемой сети Вам выделен диапазон адресов 10.255.0.0/16, определить сколько подсетей Вам необходимо задать.

Необходимо задать 8 подсетей

10.255.0.0/19
10.255.32.0/19
10.255.64.0/19
10.255.96.0/19
10.255.128.0/19
10.255.160.0/19
10.255.192.0/19
10.255.224.0/19

4. Настройте все интерфейсы всех маршрутизаторов и статическую маршрутизацию. Убедитесь, что имеется связь между всеми сетевыми интерфейсами всех маршрутизаторов.

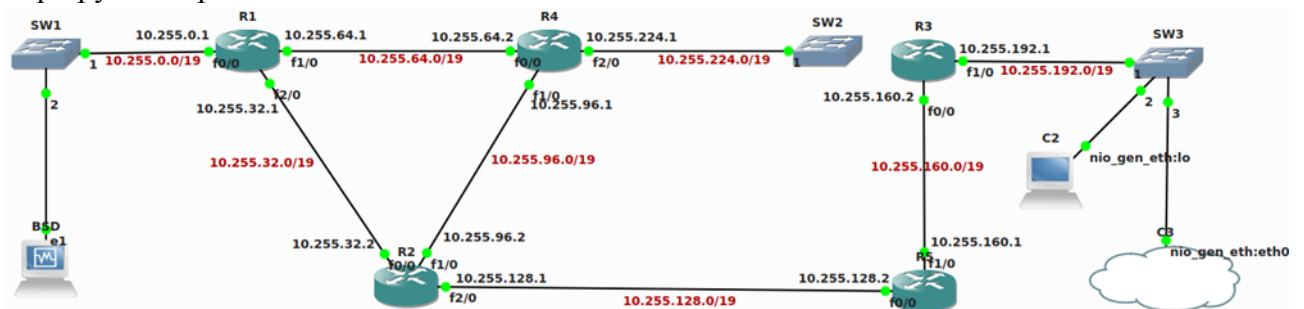


Рисунок 3. Настройка интерфейсов маршрутизаторов и статической маршрутизации.

R1:

```
interface FastEthernet0/0
ip address 10. 255. 0. 1 255. 255. 224. 0
interface FastEthernet1/0
ip address 10. 255. 64. 1 255. 255. 224. 0
interface FastEthernet2/0
ip address 10. 255. 32. 1 255. 255. 224. 0
ip route 10. 255. 96. 0 255. 255. 224. 0 10. 255. 32. 2
```

```

ip route 10.255.128.0 255.255.224.0 10.255.32.2
ip route 10.255.160.0 255.255.224.0 10.255.32.2
ip route 10.255.192.0 255.255.224.0 10.255.32.2
ip route 10.255.224.0 255.255.224.0 10.255.64.2

```

R2:

```

interface FastEthernet0/0
ip address 10.255.32.2 255.255.224.0
interface FastEthernet1/0
ip address 10.255.96.2 255.255.224.0
interface FastEthernet2/0
ip address 10.255.128.1 255.255.224.0
ip route 10.255.0.0 255.255.224.0 10.255.32.1
ip route 10.255.64.0 255.255.224.0 10.255.32.1
ip route 10.255.160.0 255.255.224.0 10.255.128.2
ip route 10.255.192.0 255.255.224.0 10.255.128.2
ip route 10.255.224.0 255.255.224.0 10.255.96.1

```

R3:

```

interface FastEthernet0/0
ip address 10.255.160.2 255.255.224.0
interface FastEthernet1/0
ip address 10.255.192.1 255.255.224.0
ip route 10.255.0.0 255.255.224.0 10.255.160.1
ip route 10.255.32.0 255.255.224.0 10.255.160.1
ip route 10.255.64.0 255.255.224.0 10.255.160.1
ip route 10.255.96.0 255.255.224.0 10.255.160.1
ip route 10.255.128.0 255.255.224.0 10.255.160.1
ip route 10.255.224.0 255.255.224.0 10.255.160.1

```

R4:

```

interface FastEthernet0/0
ip address 10.255.64.2 255.255.224.0
interface FastEthernet1/0
ip address 10.255.96.1 255.255.224.0
interface FastEthernet2/0
ip address 10.255.224.1 255.255.224.0
ip route 10.255.0.0 255.255.224.0 10.255.64.1
ip route 10.255.32.0 255.255.224.0 10.255.96.2
ip route 10.255.128.0 255.255.224.0 10.255.96.2
ip route 10.255.160.0 255.255.224.0 10.255.96.2
ip route 10.255.192.0 255.255.224.0 10.255.96.2

```

R5:

```

interface FastEthernet0/0
ip address 10.255.128.2 255.255.224.0
interface FastEthernet1/0

```

```

ip address 10.255.160.1 255.255.224.0
ip route 10.255.0.0 255.255.224.0 10.255.128.1
ip route 10.255.32.0 255.255.224.0 10.255.128.1
ip route 10.255.64.0 255.255.224.0 10.255.128.1
ip route 10.255.96.0 255.255.224.0 10.255.128.1
ip route 10.255.192.0 255.255.224.0 10.255.160.2
ip route 10.255.224.0 255.255.224.0 10.255.128.1

```

```

-----
R1#ping 10.255.192.1

```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.255.192.1, timeout is 2 seconds:

...!!

Success rate is 40 percent (2/5), round-trip min/avg/max = 12/26/40 ms

```

R1#ping 10.255.192.1

```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.255.192.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/36/44 ms

s

```

-----
R3#ping 10.255.224.1

```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.255.224.1, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 36/43/52 ms

```

-----
R3#ping                                     10.255.0.1

```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.255.0.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 48/58/64 ms

5. Запустите все модельные устройства (показав, что пустые контейнеры тоже работают, но выдают ошибку загрузки из-за отсутствия операционной системы).

Все контейнеры работают и не выдают ошибок из-за присутствия операционной системы.

```

64 bytes from 10.255.192.1: icmp_seq=305 ttl=252 time=42.444 ms
64 bytes from 10.255.192.1: icmp_seq=306 ttl=252 time=42.173 ms
64 bytes from 10.255.192.1: icmp_seq=307 ttl=252 time=41.828 ms
64 bytes from 10.255.192.1: icmp_seq=308 ttl=252 time=50.832 ms
64 bytes from 10.255.192.1: icmp_seq=309 ttl=252 time=50.284 ms
64 bytes from 10.255.192.1: icmp_seq=310 ttl=252 time=49.229 ms
64 bytes from 10.255.192.1: icmp_seq=311 ttl=252 time=48.052 ms
64 bytes from 10.255.192.1: icmp_seq=312 ttl=252 time=47.395 ms
64 bytes from 10.255.192.1: icmp_seq=313 ttl=252 time=47.050 ms
64 bytes from 10.255.192.1: icmp_seq=314 ttl=252 time=46.606 ms
64 bytes from 10.255.192.1: icmp_seq=315 ttl=252 time=46.283 ms
64 bytes from 10.255.192.1: icmp_seq=316 ttl=252 time=45.065 ms
64 bytes from 10.255.192.1: icmp_seq=317 ttl=252 time=64.870 ms
64 bytes from 10.255.192.1: icmp_seq=318 ttl=252 time=53.676 ms
64 bytes from 10.255.192.1: icmp_seq=319 ttl=252 time=43.363 ms

```

Рисунок 4. Запуск модельных устройств

Пинг с устройства BSD (10.255.0.100) ip 10.255.192.1

6. Используя анализатор Wireshark, продемонстрируйте принцип работы ping между двумя маршрутизаторами, расположенными в разных подсетях (необходимо показать все генерируемые пакеты в прямом и обратном пути при одном запросе ping).

No.	Time	Source	Destination	Protocol	Length	Info
5	13.149325	10.255.0.100	10.255.192.1	ICMP	98	Echo (ping) request id=0x1a75, seq=0/0, ttl=253 (reply in 6)
6	13.164414	10.255.192.1	10.255.0.100	ICMP	98	Echo (ping) reply id=0x1a75, seq=0/0, ttl=254 (request in 5)

▼ Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)

Encapsulation type: Ethernet (1)

Arrival Time: Mar 9, 2018 13:53:53.150985000 +07

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1520578433.150985000 seconds

[Time delta from previous captured frame: 3.637162000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 13.149325000 seconds]

Frame Number: 5

Frame Length: 98 bytes (784 bits)

Capture Length: 98 bytes (784 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:icmp:data]

[Coloring Rule Name: ICMP]

[Coloring Rule String: icmp || icmpv6]

▼ Ethernet II, Src: ca:07:36:c8:00:38 (ca:07:36:c8:00:38), Dst: ca:09:36:da:00:00 (ca:09:36:da:00:00)

Destination: ca:09:36:da:00:00 (ca:09:36:da:00:00)

Source: ca:07:36:c8:00:38 (ca:07:36:c8:00:38)

Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 10.255.0.100, Dst: 10.255.192.1

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 84

Identification: 0x9dfd (40445)

► Flags: 0x00

Fragment offset: 0

Time to live: 253

Protocol: ICMP (1)

Header checksum: 0x4948 [validation disabled]

[Header checksum status: Unverified]

Source: 10.255.0.100

Destination: 10.255.192.1

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

► Internet Control Message Protocol

0000 ca 09 36 da 00 00 ca 07 36 c8 00 38 08 00 45 00 ..6...6..8...E.

0010 00 54 9d fd 00 00 fd 01 49 48 0a ff 09 64 0a ff .T.....IH...d..

0020 c0 01 08 00 60 f1 1a 75 00 00 85 6e 54 d2 35 65 .d..h..u...nT.Se

0030 bd 2e b8 3e 71 83 09 16 99 91 4f 02 aa c8 ef a3 ...>q...0....

0040 87 69 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 .i.....!"#\$%

0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,-./012345

0060 36 37

Рисунок 5. Демонстрация принципа работы ping между двумя маршрутизаторами (прямой путь).

5	13.149325	10.255.0.100	10.255.192.1	ICMP	98	Echo (ping) request id=0x1a75, seq=0/0, ttl=253 (reply in 6)
6	13.164414	10.255.192.1	10.255.0.100	ICMP	98	Echo (ping) reply id=0x1a75, seq=0/0, ttl=254 (request in 5)

▼ Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)

Encapsulation type: Ethernet (1)

Arrival Time: Mar 9, 2018 13:53:53.166074000 +07

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1520578433.166074000 seconds

[Time delta from previous captured frame: 0.015089000 seconds]

[Time delta from previous displayed frame: 0.015089000 seconds]

[Time since reference or first frame: 13.164414000 seconds]

Frame Number: 6

Frame Length: 98 bytes (784 bits)

Capture Length: 98 bytes (784 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:icmp:data]

[Coloring Rule Name: ICMP]

[Coloring Rule String: icmp || icmpv6]

▼ Ethernet II, Src: ca:09:36:da:00:00 (ca:09:36:da:00:00), Dst: ca:07:36:c8:00:38 (ca:07:36:c8:00:38)

Destination: ca:07:36:c8:00:38 (ca:07:36:c8:00:38)

Source: ca:09:36:da:00:00 (ca:09:36:da:00:00)

Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 10.255.192.1, Dst: 10.255.0.100

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 84

Identification: 0x9dfd (40445)

► Flags: 0x00

Fragment offset: 0

Time to live: 254

Protocol: ICMP (1)

Header checksum: 0x4848 [validation disabled]

[Header checksum status: Unverified]

Source: 10.255.192.1

Destination: 10.255.0.100

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

► Internet Control Message Protocol

0000 ca 07 36 c8 00 38 ca 09 36 da 00 00 08 00 45 00 ..6..8..6....E.

0010 00 54 9d fd 00 00 fe 01 48 48 0a ff c0 01 0a ff .T.....HH.....

0020 00 64 00 00 68 f1 1a 75 00 00 85 6e 54 d2 35 65 .d..h..u...nT.Se

0030 bd 2e b8 3e 71 83 09 16 99 91 4f 02 aa c8 ef a3 ...>q...0....

0040 87 69 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 .i.....!"#\$%

0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,-./012345

0060 36 37

Рисунок 6. Демонстрация принципа работы ping между двумя маршрутизаторами (обратный путь).

При передаче пакета от роутера к роутеру меняется MAC назначения, и не меняется IP назначения, так как меняется канальная среда.

7. Убедитесь, что Ваша среда имеет связь со средой другого студента используя реальную физическую сеть.

Другого студента нет, но через интерфейс <cloud> есть возможность связать физическую и виртуальные сети.

Выводы по проделанной работе:

В результате выполнения лабораторной работы, мы приобрели навыки использования среды моделирования GNS3. Подготовить среду для выполнения курсовой работы, что и требовало наше техническое задание лабораторной работы;

- установить среду моделирования GNS3 и произвести начальную конфигурацию добавив маршрутизатор CISCO и два пустых контейнера с виртуальными машинами от VirtualBox;

- собрать макет локальной сети, как показано на Рисунок 1;

- исходя из того, что для функционирования создаваемой сети нам выделен диапазон адресов 10.255.0.0/16, определить сколько подсетей нам необходимо задать;

- настроить все интерфейсы всех маршрутизаторов и статическую маршрутизацию. Убедиться, что имеется связь между всеми сетевыми интерфейсами всех маршрутизаторов;

- запустить все модельные устройства (показав, что пустые контейнеры тоже работают, но выдают ошибку загрузки из-за отсутствия операционной системы);

- используя анализатор Wireshark, продемонстрировать принцип работы ping между двумя маршрутизаторами, расположенными в разных подсетях (необходимо показать все генерируемые пакеты в прямом и обратном пути при одном запросе ping);

- убедиться, что наша среда имеет связь со средой другого студента используя реальную физическую сеть.

Собственно данные умения и навыки, которые мы смогли получить при выполнении данной лабораторной работы, помогут нам в дальнейших работах и по выполнению нашего курсового проекта по курсу «Сети ЭВМ и телекоммуникации».

Контрольные вопросы

1. Для чего была разработана среда GNS3?

Для программной эмуляции работы сетевых устройств.

2. Какие устройства моделируются в GNS3?

Любые поддерживаемые гипервизором.

3. Что такое Idle-PC?

Параметр Dynamips, определяющий оптимальное значение процессорного времени для виртуальной машины.

4. Как работает протокол ARP?

ARP (англ. Address Resolution Protocol — протокол определения адреса) — протокол канального уровня.

Протокол ARP (address resolution protocol, RFC-826, std-38) решает проблему преобразования IP-адреса в MAC-адрес.

Рассмотрим процедуру преобразования адресов при отправлении сообщения. Пусть одна ЭВМ отправляет сообщение другой. Прикладной программе IP-адрес места назначения обычно известен. Для определения Ethernet-адреса просматривается ARP-таблица. Если для требуемого IP-адреса в ней присутствует MAC-адрес, то формируется и посылается соответствующий пакет. Если же с помощью ARP-таблицы не удастся преобразовать адрес, то выполняется следующее:

1. Всем машинам в сети посылается пакет с ARP-запросом (с широковещательным MAC-адресом).

2. Исходящий IP-пакет ставится в очередь.

Каждая машина, принявшая ARP-запрос, в своем ARP-модуле сравнивает собственный IP-адрес с IP-адресом в запросе. Если IP-адрес совпал, то прямо по MAC-адресу отправителя запроса посылается ответ, содержащий как IP-адрес ответившей машины, так и ее MAC-адрес. После получения ответа на свой ARP-запрос машина имеет требуемую информацию о соответствии IP и MAC-адресов, формирует соответствующий элемент ARP-таблицы и отправляет IP-пакет, ранее поставленный в очередь. Если же в сети нет машины с искомым IP-адресом, то ARP-ответа не будет и не будет записи в ARP-таблицу. Протокол IP будет уничтожать IP-пакеты, предназначенные для отправки по этому адресу.

5. Как получить доступ к консоли конфигурирования маршрутизатора CISCO (продемонстрируйте).

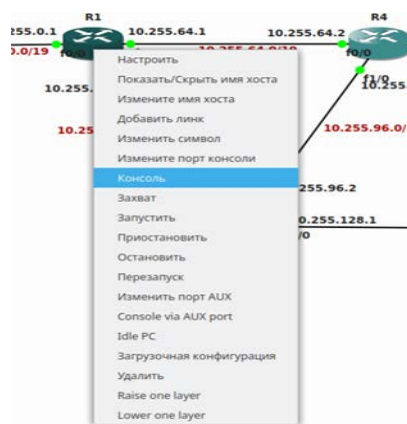


Рисунок 7. Получение доступа к консоли конфигурирования маршрутизатора CISCO.

6. Зачем используется Wireshark?

Программа-анализатор трафика для компьютерных сетей Ethernet и других. Имеет графический пользовательский интерфейс.

7. Можно ли создать сеть, в которой одновременно используются маршрутизаторы CISCO и маршрутизаторы, реализованные на базе персональных компьютеров, функционирующих под управлением сетевых операционных систем (Windows Server, Linux и т.п.)?

Да.

8. Зачем используется библиотека WinPCAP?

Инструмент, работающий в среде Microsoft Windows, позволяющий приложениям захватывать и передавать сетевые пакеты в обход стека протоколов.

9. Что такое Dynamips?

Программный эмулятор маршрутизаторов CISCO.

10. Какие среды виртуализации использует GNS3?

Dynamips, VPCS, KVM (qemu, VirtualBox).

Список использованных источников

1. CISCO Packet Tracer – Networking academy. – Официальный сайт [Электронный ресурс]. – URL: <https://www.netacad.com/web/about-us/cisco-packet-tracer>.
2. Курс лекций Мамоиленко С.Н. «Сети ЭВМ и телекоммуникации».
3. Мамоиленко С.Н., Лабораторная работа № 1 «Знакомство со средой моделирования CISCO Packet Tracer» [Текст]: учеб. пособие / С.Н. Мамоиленко; Сиб. гос. ун-т телекоммуникаций и информатики. - Новосибирск : СибГУТИ, 2016. – 14 с.