Лабораторная работа № 4. Изучение маршрутизации с использованием Cisco Packet Tracer

Данная лабораторная работа предназначена для ознакомления с статической и динамической настройкой маршрутизации в сети, по средства программы Cisco Packet Tracer.

Для успешного выполнения лабораторной работы необходимо:

- наличие программы cisco packet tracer (далее CPT) версии не ниже 7.1 с наличием Router-PT-Empty;
- понимание работы маршрутизаторов;
- знание основных команд для настройки маршрутизаторов.

1. Постановка задачи

Имеется частная сеть 192.168.0.0/24, которая представлена на рисунке 1. Необходимо разбить данную сеть на подсети в соответствии с топологией сети так, чтобы максимально полезно расходовать сетевые адреса.

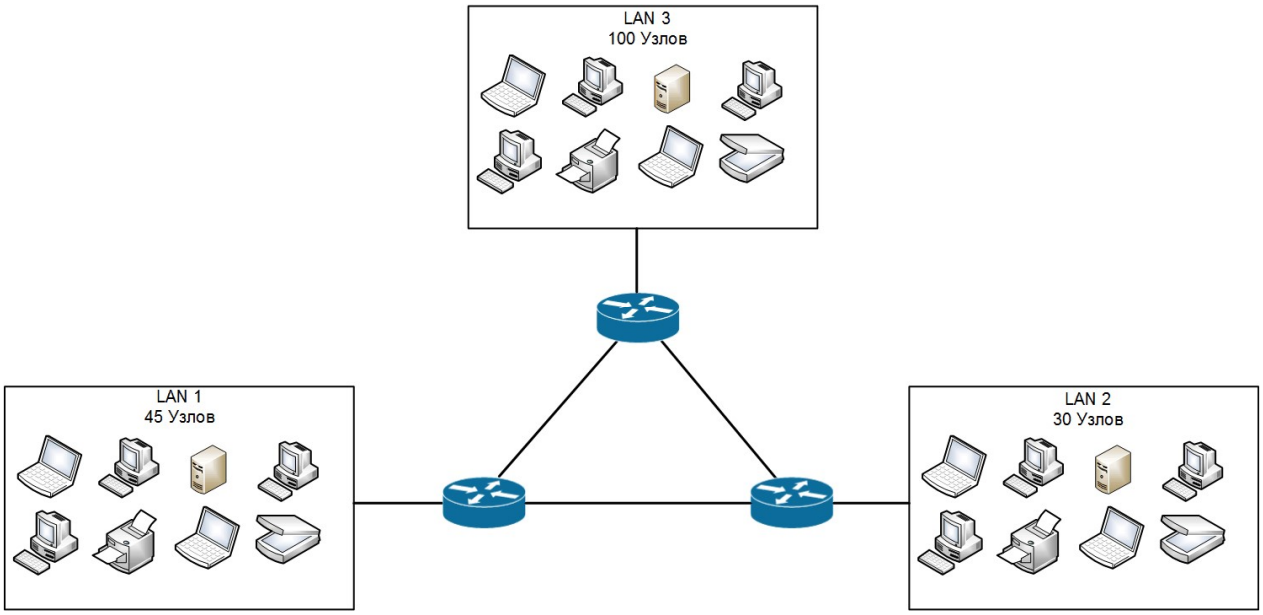

Рисунок 1 - Схема сети

1.1. Разбейте сеть на подсети, и полученный результат внесите в таблицу 1. Объясните принцип деления сети. Результат покажите преподавателю.

Таблица 1 - Разбиение сети

Название сети	Сеть	Первый IP - адрес	Последний IP - адрес	Маска	Общее количество адресов в сети
LAN1					
LAN2					
…					

В лабораторной работе используется маршрутизатор Router-PT-Empty. Среди перечней маршрутизаторов он отображается как Generic. Данный маршрутизатор изначально имеет только два интерфейса – AUX и Console. Для добавления Fast-Ethernet и Gigabit Ethernet необходимо выключить маршрутизатор (цифра 1), перетянуть необходимый интерфейс (цифра 2) и вставить в пустую ячейку (цифра 3), как показано на рисунке 2. Для удобства возможно изменение зума (цифра 4). После добавления необходимых интерфейсов не забудьте включить маршрутизатор.

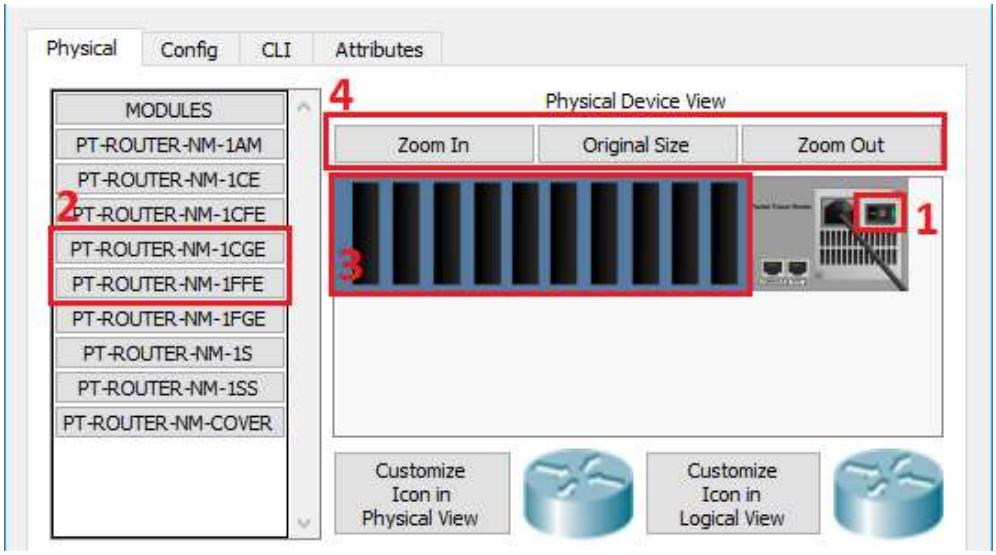

Рисунок 2 - Добавление новых интерфейсов на маршрутизатор

1.2. Соберите сеть в CPT так, как показано на рисунке 3. Для соединения ПК с маршрутизатором используйте автоматический выбор типа кабеля.

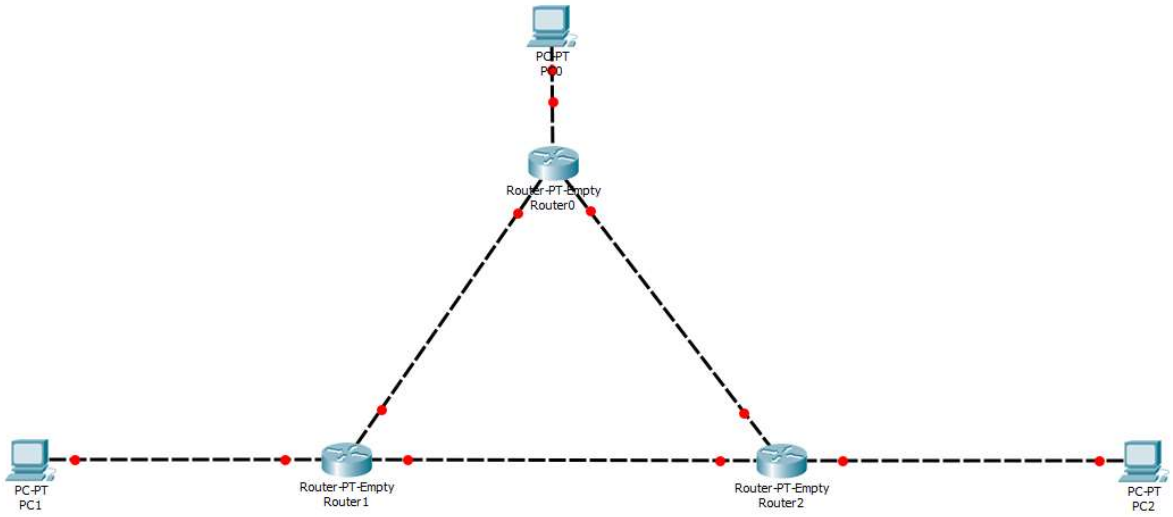

Рисунок 3 - Вид сети в cisco packet tracer

1.3. Произведите настройку ПК, задайте IP-адрес ПК и IP-адрес основного шлюза.

1.4. Произведите предварительную настройку маршрутизатора, настройте все интерфейсы (ip address…), настройте доступ к маршрутизатору (создайте локального пользователя), создайте пароль для входа в привилегированный режим и создайте сообщение при подключении к маршрутизатору.

1.5. Проверьте доступность ближайших маршрутизаторов к ПК с помощью команды ping.

1.6. Проверьте доступность маршрутизаторов между собой, с помощью команды ping.

1.7. Просмотрите таблицу маршрутизации на всех устройствах, какие записи там есть?

1.8. Сохраните схему в файл Шаблон.pkt, в дальнейшем она понадобится для реализации динамической и статической маршрутизации.

2. Статическая маршрутизация

Статическая маршрутизация - вид маршрутизации, при котором маршруты указываются в явном виде при конфигурации маршрутизатора. Вся

маршрутизация при этом происходит без участия каких-либо протоколов маршрутизации.

2.1. Скопируйте .pkt файл, сохраненный ранее и переименуйте его в Статический.pkt.

2.2. На всех маршрутизаторах настройте статическую маршрутизацию с помощью команды ip route. При создании статических маршрутов воспользуйтесь следующим рисунком для заполнения метрики – рисунок 4, где цифрами обозначены значения метрики. Для PC0 метрику выберите сами. На каких устройствах какие маршруты были созданы? В отчёт включите таблицу маршрутизации для каждого узла в схеме.

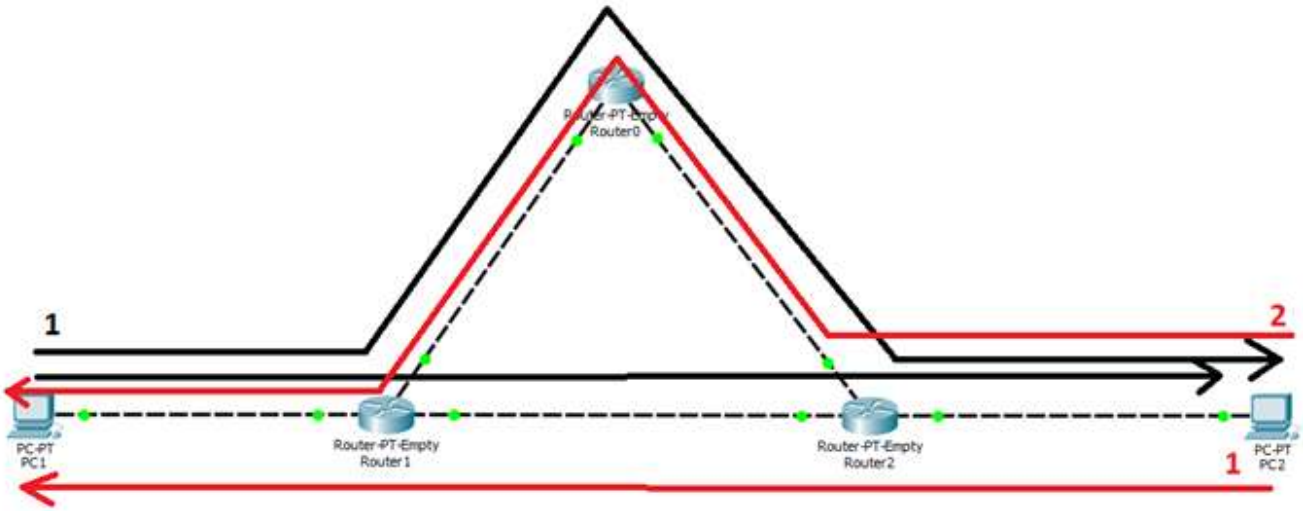

Рисунок 4 - Метрика

2.3. Проверьте доступность каждого компьютера с PC0, PC1, PC2 с помощью команды ping.

2.4. Посмотрите таблицу маршрутизации на каждом маршрутизаторе, какие запись там появились? Все ли маршруты там есть?

2.5. Перейдите в режим симуляции и отправьте ICMP пакет с PC1 на PC2, по какому маршруту двигался пакет?

2.6. Повторите предыдущий пункт несколько раз, какие изменения вы видите?

2.7. Повторите действия, но отправляйте ICMP пакет с PC2 на PC1, опишите маршруты, которые используются.

2.8. Удалите кабель между Router1 и Router2. Отправьте ICMP пакте с PC1 на PC2. Получилась ли это сделать? Изменилась ли таблица маршрутизации?

2.9. Добавьте в схему четвёртый маршрутизатор, который подключается к Router1 и Router2. За маршрутизатором разместите ПК. Добейтесь доступности PC4 для всех остальных ПК. В отчет внесите последовательность команд и то, на каких устройствах их нужно вводить.

3. Динамическая маршрутизация

Динамическая маршрутизация — вид маршрутизации, при котором таблица маршрутизации редактируется программно.

При динамической маршрутизации происходит обмен маршрутной информацией между соседними маршрутизаторами, в ходе которого они сообщают друг другу, какие сети в данный момент доступны через них. Информация обрабатывается и помещается в таблицу маршрутизации.

Существует несколько видов протоколов динамической маршрутизации. Рассмотрим один из наиболее распространённых - Routing Information Protocol (RIP).

3.1. Скопируйте .pkt файл, сохраненный ранее и переименуйте его в Динамический.pkt.

3.2. Настройте динамическую маршрутизацию с помощью команд:

```
router rip
version 2
passive-interface
network
no auto-summary
```

3.3. Просмотрите таблицу маршрутизации на каждом маршрутизаторе.

3.4. В режиме симуляции отправьте ICMP пакет, по какому пути идет пакет?

3.5. С PC1 через командную сроку выполните команду ping –t к PC2. Удалите кабель между Router1 и Router2, через какое время соединение восстановилось? Посмотрите таблицу маршрутизации, есть ли изменения?

3.6. Удалите кабель между Router0 и Router2, через какое время ответ о недоступности PC2 стал приходить с другого IP-адреса? Посмотрите таблицу маршрутизации, есть ли изменения? Объясните данный механизм работы протокола RIP.

3.7. Восстановите схему обратно.

3.8. Добавьте в схему четвёртый маршрутизатор, который подключается к Router1 и Router2. За маршрутизатором разместите ПК. Добейтесь доступности PC4 для всех остальных ПК. В отчет внесите последовательность команд и то, на каких устройствах их нужно вводить.

3.9. Сравните объем команд который нужно вести для внедрения четвёртого маршрутизатора в схему с статической и динамической маршрутизацией.

Лабораторная работа № 5. Изучение маршрутизации с использованием Graphical Network Simulator-3

Данная лабораторная работа предназначена для ознакомления и изучения основы работы с эмулятором оборудования Cisco GNS3.

Для успешного выполнения лабораторной работы необходимо:

- убедиться в наличии прав администратора на рабочем компьютере;
- наличие программы GNS3;
- наличие образа маршрутизатора c7200;
- наличие программы WireShark;
- наличие программы tftp32(64);
- наличие программ SnmpGet, SnmpWalk, SnmpSet;
- понимание работы маршрутизаторов;
- знание основных команд для настройки маршрутизаторов.

1. Установка и настройка программы

Graphical Network Simulator (далее GNS3) —программа-эмулятор, которая позволяет комбинировать виртуальные и реальные устройства, используемые для моделирования сложных сетей, эмулируя все основные компоненты устройств, в том числе процессор, память и устройства ввода/вывода. Эмулятор создает модель маршрутизатора и запускает внутри реальную операционную систему Cisco IOS, получая таким образом полнофункциональный маршрутизатор.

1.1. Установите программу GNS3, образ для установки получите у преподавателя. Выберете для установки все компоненты. После установки перезагрузите компьютер.

1.2. Запустите программу GNS3 с правами Администратора. При первом запуске программы появится окно, в котором необходимо выбрать пункт Run only legacy IOS on my computer и нажмите далее. При настройке Host binding выберете 127.0.0.1 и нажмите далее. При появлении окна с созданием нового проекта все настройки оставьте по умолчанию.

После запуска программы появится главное окно программы GNS3, с элементами пользовательского интерфейса приведенными на рисунке 1.

Пользовательский интерфейс программы состоит из следующих элементов:

- меню программы;
- панель инструментов, содержащая ярлыки для быстрого доступа к часто используемым элементам программы;
- окно выбора типа сетевого устройства;
- рабочая область;
- окно консоли управления эмулятором маршрутизаторов;
- окно топологии сети, отображающее состояние объектов сети и связи между ними;
- окно управления захватом трафика, отображающее точки съема сетевого трафика.

1.3. Добавьте образ маршрутизатора, для этого внизу области 3 нажмите New appliance template. В появившемся окне выберете Add an IOS router using a real IOS image и нажмите OK. Далее укажите путь до образа в формате .image. Нажимайте далее пока не дойдете до настройки интерфейсов. Выберете для slot 0 – C7200-IO-2FE, для slot 1 – PA-GE, для slot 2 – PA-GE (при добавлении нового маршрутизатора он будет иметь 2 FastEthernet и 2 GigabitEthernet интерфейса) и нажмите далее. На следующем этапе нажмите кнопку Idle-PC finder и дождитесь успешного определения значения Idle-PC (необходимо для ограничения нагрузки на ЦП) и нажмите Finish.

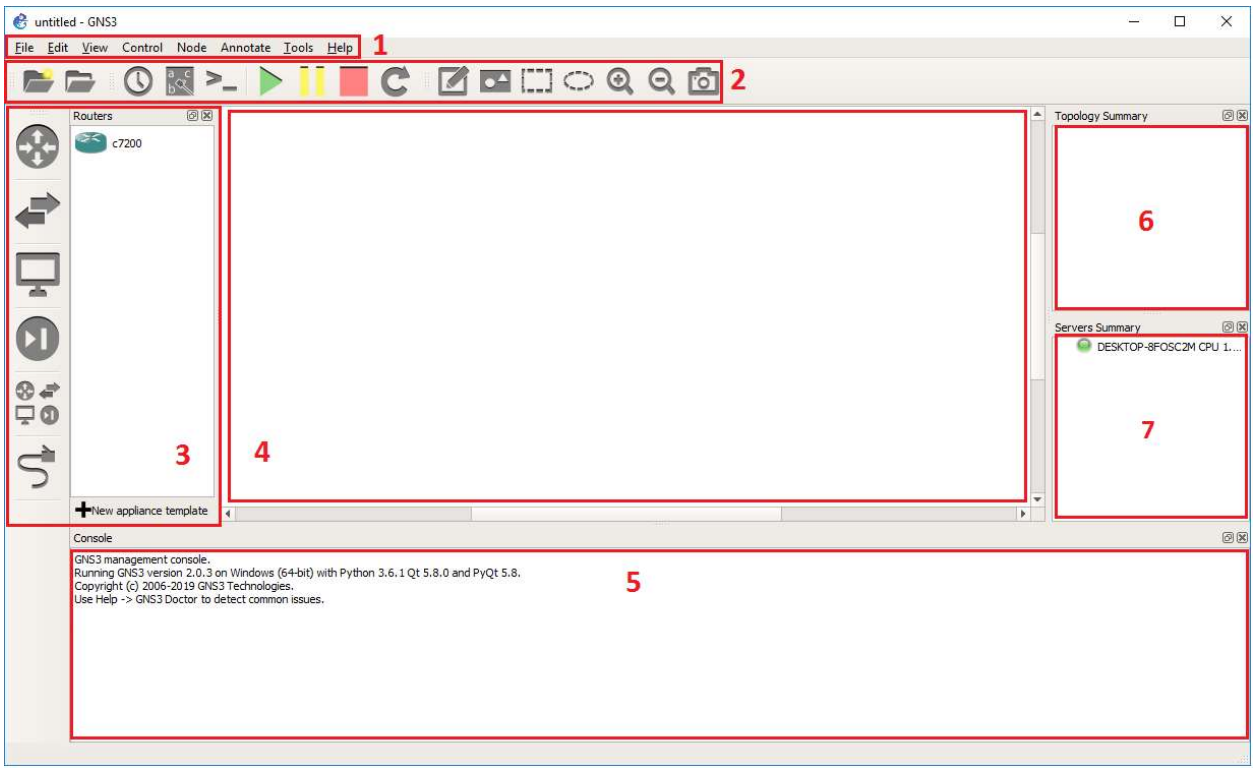

Рисунок 1 - Главное окно программы GNS3

1.4. Соберите схему, показанную на рисунке 2. При подключении R1 к Cloud1 из выпадающего списка нужно выбрать Npcap Loopback Adapter. Для добавления Cloud1 и PC1 на рабочую область, в окне выбора сетевого устройства перейдите на вкладку Browse end Devices, и перетяните Cloud и VPCS.

1.5. На сетевом интерфейсе Npcap Loopback Adapter в Windows задайте статический IP-адрес.

1.6. Запустите программу WireShark и выберете интерфейс Npcap Loopback Adapter.

1.7. На маршрутизаторе R1 включите интерфейс, который соединён с Cloud1.

1.8. Какой пакет удалось захватить после включения интерфейса? Какая информация содержится в этом пакете?

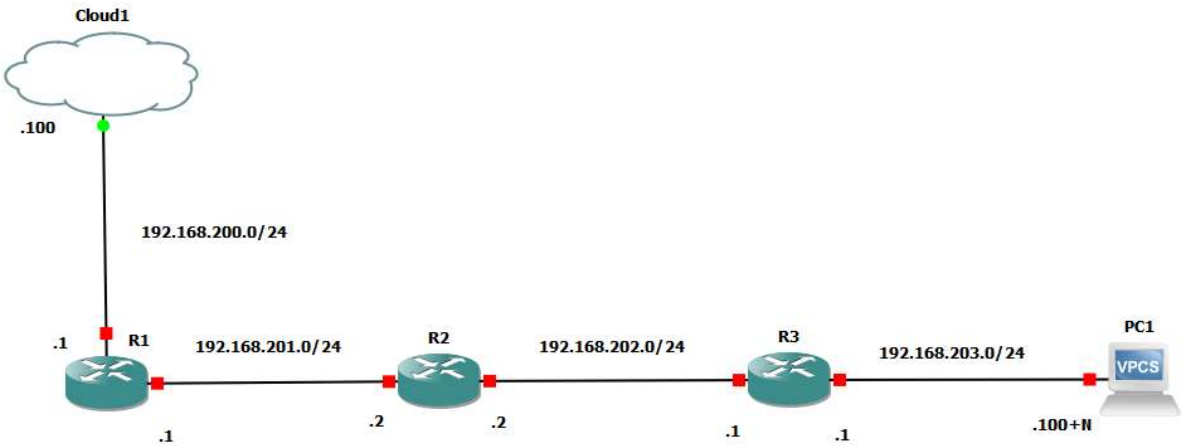

Рисунок 2 - Пример схемы сети

1.9. Настройте необходимые интерфейсы на маршрутизаторах, в соответствии с рис. 2.

1.10. Посмотрите информацию о соседях маршрутизатора R2, полученную по протоколу cdp, с помощью команды show cdp neighbors. Какая информация о соседях представлена?

1.11. Настройте виртуальный PC1 с помощью команды ip <ip>/<mask> <gateway> в соответствии с Рисунок 2, где N номер варианта.

1.12. Настройте маршрутизацию (статическую/динамическую по выбору) с хоста на PC1 и проверьте её с помощью команды ping. Какое значение TTL вы получили, почему? При отсутствии связи с PC1 проверьте таблицу маршрутизации на хосте. При необходимости задать статический маршрут на хосте можно в командной строке с правами администратора с помощью команды route ADD <ip сети> MASK <mask> <gateway>.

2. Изучение протокола SYSLOG

Протокол SYSLOG используется для формирования и отправки простого текстового сообщения от источника на сервер о происходящих изменениях. Поскольку источники сообщений и сервер SYSLOG могут располагаться на разных машинах, это позволяет организовать сбор и хранение сообщений от множества географически разнесенных разнородных источников в едином хранилище (репозитории), что позволяет не имея физического доступа к устройствам получать информацию о событиях, происходящих на них.

2.1. Запустите WireShark и включите захват трафика.

2.2. На маршрутизаторе R3 задайте адрес SYSLOG-сервера с помощью команды logging <host-ip>.

2.3. Запустите программу Tftpd64(32) и перейдите на вкладку Syslog server. В выпадающем меню Server interfaces выберете IPv4 интерфейс Npcap Loopback Adapter

2.4. На маршрутизаторе R3 включите любой из выключенных интерфейсов.

2.5. Посмотрите информацию, которая появилась в программе Tftpd64(32).

2.6. Посмотрите пакеты, которые удалось захватить с помощью WireShark. Какую информацию содержат эти пакеты?

2.7. Не закрывайте программу Tftpd64 в ходе выполнения всей лабораторной работы.

3. Изучение протокола NTP

NTP – протокол для синхронизации времени на устройствах в сети. Обычно в сети присутствует сервер и клиент. Время сервера считается эталонным, и клиент обращается к серверу для синхронизации своего времени.

3.1. На маршрутизаторе R3 из привилегированного режима настройте часовой пояс командой clock timezone и время, с помощью команды clock set.

3.2. Сделайте маршрутизатор R3 NTP-сервером, с помощью команды ntp master.

3.3. Запустите WireShark и включите захват трафика.

3.4. Задайте маршрутизатор R3 в качестве NTP-сервера на хосте, для этого зайдите в Панель управления -> Дата и время -> перейдите на вкладку Время по интернету -> изменить параметры -> задайте IP адрес маршрутизатора R3 -> нажмите кнопку Обновить сейчас.

3.5. Какие пакеты удалось захватить с помощью WireShark? Какую информацию содержит данный пакет?

3.6. В программе Tftpd64(32) на вкладке Syslog server посмотрите какие записи появились. Какая информация в них содержится?

4. Изучение протокола TFTP

Протокол TFTP (Trivial File Transfer Protocol) предназначен для передачи файлов. Применяется для решения задач, связанных с обслуживанием и эксплуатацией сетевого оборудования. Чаще всего используется для загрузки бездисковых рабочих станций и обновления, и резервного копирования конфигурационных файлов и образов ОС (прошивок) на различных сетевых устройствах.

4.1. Запустите WireShark и включите захват трафика.

4.2. Сделайте маршрутизатор R3 TFTP-сервером, который будет предоставлять доступ к файлу текущей конфигурации, с помощью команды tftp-server system:running-config.

4.3. В приложении Tftpd64(32) перейдите на вкладку TFTP client.

4.4. В поле Host укажите IP-адрес маршрутизатора R3. В поле Local File укажите путь к файлу, в который будет записана текущая конфигурация. В поле Remote File имя файла на маршрутизаторе, который необходимо загрузить(running-config). В поле Block Size значение оставить по умолчанию. Поле Port оставить пустым. После заполнения всех полей нажмите кнопку Get.

4.5. Откройте загруженный файл. Соответствуют ли содержимое файла конфигурации устройства?

4.6. Посмотрите пакеты которые удалось захватить WireShark. Какая информация в них содержится?

4.7. С помощью команды copy tftp://<host-ip>/<filename> nvram:startup-config на маршрутизаторе R3 загрузите с хоста файл с текущей конфигурацией и сохраните его в качестве загрузочной конфигурации. Сравните загрузочную и стартовую конфигурацию устройства.

4.8. В программе Tftpd64(32) на вкладке Syslog server посмотрите появились ли записи?

5. Изучение протокола SNMP

SNMP (Simple Network Management Protocol) — простой протокол сетевого управления. К поддерживающим SNMP устройствам относятся маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемные стойки и другие. Протокол обычно используется в системах сетевого управления для контроля подключённых к сети устройств. SNMP состоит из набора стандартов для сетевого управления, включая протокол прикладного уровня, схему баз данных и набор объектов данных.

5.1. Запустите WireShark и включите захват трафика.

5.2. Сделайте маршрутизатор R3 SNMP-сервером. Для этого создайте группу, которой будет доступна запись с помощью команды snmp-server group <group name> v3 noauth write v1default.

5.3. Создайте пользователя группы, созданной выше с помощью команды snmp-server user <user name> <group name> v3.

5.4. Получите описание устройства R3. Для этого в командной строке Windows запустите программу SnmpGet с параметрами -r:<ip R3> -v:3 -sn:<user name> -o:.1.3.6.1.2.1.1.1.0, где 1.3.6.1.2.1.1.1.0 идентификатор объекта представляющего собой строку содержащую описание системы. Что содержит в себе описание устройства?

5.5. Посмотрите пакеты которые удалось захватить WireShark. Какая информация в них содержится?

5.6. В программе Tftpd64(32) на вкладке Syslog server посмотрите появились ли записи?

5.7. С помощью программы SnmpGet получите значение объекта с идентификатором 1.3.6.1.2.1.1.5.0 – имя устройства. Какое значение получили?

5.8. Измените имя устройства. Для этого в командной строке Windows запустите программу SnmpSet.exe с параметрами -r:<IP R3> -v:3 -sn:<user name> -o:.1.3.6.1.2.1.1.5.0 -val:<new name>, где 1.3.6.1.2.1.1.5.0 идентификатор строки имени устройства.

5.9. Проверьте что имя устройства изменилось с помощью программы SnmpGet.

5.10. Посмотрите пакеты которые удалось захватить WireShark. Какая информация в них содержится?

5.11. В программе Tftpd64(32) на вкладке Syslog server посмотрите появились ли записи?

Также существует программа, позволяющая получить существующие идентификаторы объектов и их типы – SnmpWalk.

5.12. Посмотрите какие идентификаторы доступны в промежутке от 1.3.6.1.2.0 до 1.3.6.1.2.1.1.6.0. Для того в командной строке Windows запустите программу SnmpWalk.exe с параметрами -r:<IP R3> -v:3 -sn:<user name> -os:.1.3.6.1.2.0 -op:.1.3.6.1.2.1.1.6.0

5.13. Посмотрите пакеты которые удалось захватить WireShark. Какая информация в них содержится?

5.14. Используя программу SnmpWalk.exe выполните запись всех идентификаторов объекта в файл, для этого используйте команду SnmpWalk.exe -r:<IP R3> -v:3 -sn:<user name> > <file name>.

5.15. Откройте полученный файл. Выберете любые 10 параметров, найдите информацию о них в интернете и опишите их назначение, результат вставьте в отчет.