МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра вычислительной техники

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«17» 01 2022 г

Сеть VPN

Методические указания к лабораторной работе по дисциплинам "Сети и телекоммуникации" и “Защита информации” для студентов, обучающихся по направлению 09.03.01 «Информатика и вычислительная техника»

Курск 2022

УДК 004.7

Составитель С.И.Егоров, Е.А.Грибов

Рецензент
Доктор технический наук, профессор кафедры БМИ Юго-Западного государственного университета *С.А.Филист*

Сеть VPN: методические указания к лабораторной работе по дисциплинам "Сети и телекоммуникации" и "Защита информации" / Юго-Зап. гос. ун-т; сост. С.И.Егоров, *Е.А.Грибов*. Курск, 2022. 6 с.; ил. 3. Библиогр.: 6 с.

Излагаются методические указания по выполнению лабораторной работы на персональной ЭВМ с использованием виртуальной ОС. Изучается сетевой анализатор Network Monitor и настройка сети VPN в сетевой ОС Microsoft Windows Server 2012.

Предназначены для студентов, обучающихся по направлению 09.03.01.

Текст печатается в авторской редакции

Подписано в печать 17.01.2022. Формат 60x84 1/16.

Усл. печ. л. 0,52 Уч.-изд. л. 0,47 Тираж 50 экз. Заказ 43 Бесплатно.

Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Цели работы:

- научиться работать с сетевым анализатором кадров Network Monitor;
- научиться устанавливать и настраивать сети VPN.

Сетевой анализатор Network Monitor, входящий в состав Microsoft Windows Server 2012, используется для анализа и обнаружения проблем в локальной сети. Network Monitor позволяет вести журнал сетевой активности, копию которого можно отослать профессиональным сетевым аналитикам или в службу поддержки. Кроме того, разработчики сетевого программного обеспечения применяют Network Monitor для мониторинга и отладки своих приложений.

Виртуальные частные сети (Virtual Private Networks, VPN) позволяют обеспечить безопасный доступ к ресурсам сети.

В лабораторной работе используется компьютер с установленной на нем системой Windows Server 2012 и компьютер-клиент, введенный в Active Directory.

Задание 1. Установить сетевой анализатор Network Monitor.

Указания к выполнению

1. Запустите виртуальную машину с Windows Server 2012.
2. На рабочем столе запустите двойным кликом файл NM34_x64.exe
3. Следуйте указаниям в окне установщика
4. На экране «**Use Microsoft Update to help your computer secure and up to date**» выберите «**I do not want to use Microsoft Update**» и щелкните **Next**
5. На экране «**Choose Setup Type**» выберите «**Complete**» и щелкните **Next**.
6. На последнем экране нажмите **Install** и дождитесь окончания установки программы и всех её компонентов.

Задание 2. Выполните мониторинг сетевых кадров с помощью Network Monitor.

Указания к выполнению

1. Запустите Network Monitor: **Start** – **All Programs** – **Microsoft Network Monitor** (**Пуск** – **Программы** – **Microsoft Network Monitor**).
2. Запустите мониторинг кадров: меню **Capture** – **Start** (**Запись** – **Запустить**) или клавиша **F10**.
3. Запустите из командной строки сервера утилиту ping и проверьте доступность физического компьютера клиента:

ping 192.168.X.10 ,

X – номер варианта. Сделайте скриншот.

4. Остановите мониторинг в Network Monitor: меню **Capture** – **Stop** или клавиша **F11.** Просмотрите информацию о полученных кадрах: меню **Capture** – **Display Captured Data** (**Запись** – **Отображение собранных данных**) или клавиша **F12**. В окне **Summary** (**Общая информация**) отобразится подробная информация обо всех собранных кадрах. Двойной щелчок на любом кадре откроет подробную статистику по этому кадру (рис. 1). Сделайте скриншот.

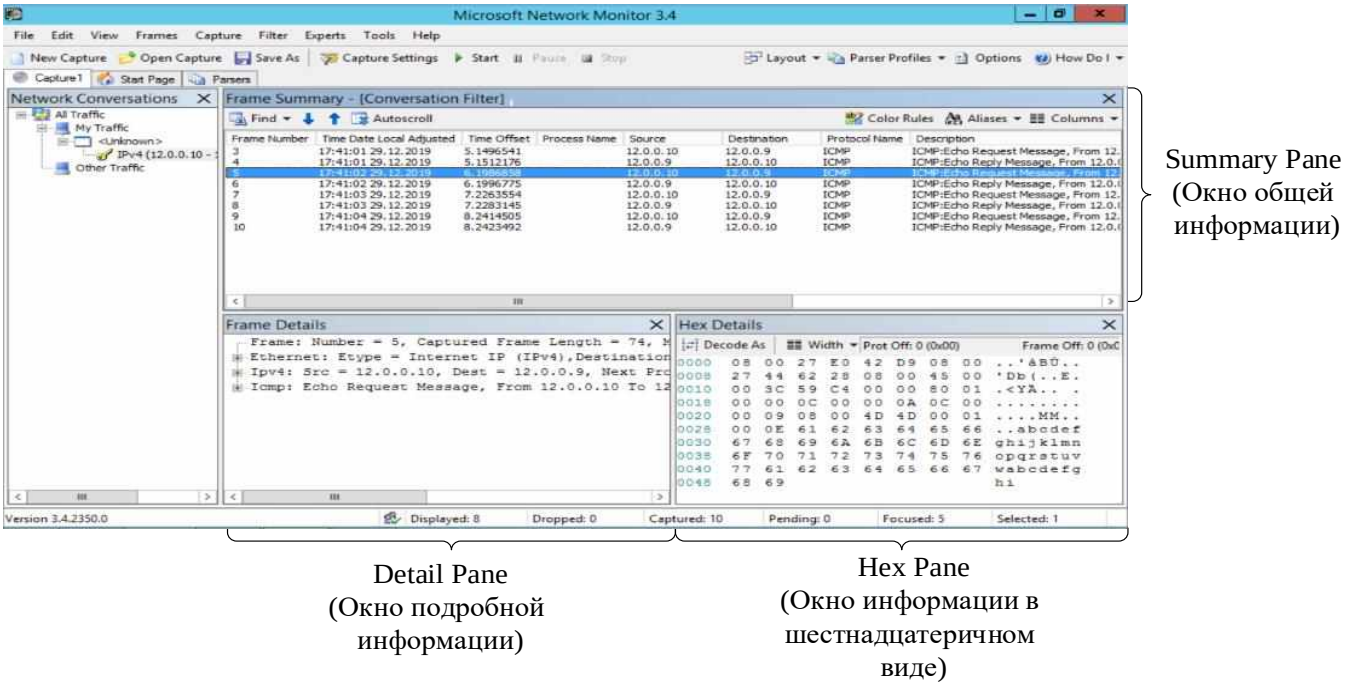

Рис. 1. Элементы окна Summary

В окне **Summary Pane** (**Окно общей информации**) отображается:

- **Frame** – номер кадра;
- **Time Date Local Adjusted** – время захвата кадра;
- **Time Offset** – длительность передачи/приема
- **Source** –IP-адрес источника;
- **Destination** –IP-адрес приемника;
- **Protocol Name** – протокол, передавший кадр;
- **Description** – описание кадра;

На рисунке видно, что Network Monitor захватил 10 кадров:

- Первый кадр – широковещательный ARP-запрос на разрешение указанного в ping IP-адреса.
- Второй кадр – ARP-ответ на запрос, содержащий требуемый IP-адрес.
- Следующие восемь кадров – эхо-пакеты протокола ICMP и ответы на них. Обратите внимание на данные, передаваемые в эхо-пакете. Сделайте скриншот.

Задание 3. Установка сервера виртуальной частной сети (VPN).

Указания к выполнению

1. Установите VPN-сервер. Для этого следует открыть оснастку: **Пуск – Диспетчер серверов – Управление – Добавить роли и компоненты – Удаленный доступ – DirectAccess и VPN(RAS).** Дождаться окончания установки.

2. В Диспетчере серверов в уведомлениях нажмите «Открыть мастера первоначальной настройки» компонента «Настройка удаленного доступа»

3. В появившемся окне мастера выберите «Развернуть только VPN»

4. Итак, VPN-сервер установлен и запущен. Сейчас следует установить диапазон IP-адресов, которые VPN-сервер может назначать VPN-клиентам. В контекстном меню сервера выберите пункт **Properties** (**Свойства**). Перейдите на вкладку IPv4, выберите **Static address pool** (**Диапазон статических адресов**). Нажмите кнопку **Add** (**Добавить**), введите начальный и конечный адреса диапазона, например 192.168.100+X.2 – 192.168.100+X.10 и нажмите **ОК**.

5. Следующим шагом будет активизация возможности удаленного подключения у одной из учетных записей. Откройте оснастку **Active Directory Users and Computers** (**Пользователи и компьютеры Active Directory**), выберите любую из существующих учетных записей (например, **Administrator** (**Администратор**)). В контекстном меню учетной записи выберите пункт **Properties** (**Свойства**), перейдите на вкладку **Dial-in (Коммутируемый доступ**), в разделе **Remote Access Permission** (**Dial-in or VPN**) (**Разрешение удаленного доступа (коммутируемый или VPN)**) выберите пункт **Allow access** (**Разрешить доступ**), щелкните **ОК.**

6. Выполнены на сервере команду ipconfig /all и сделайте скриншот.

Задание 4. Настройка VPN-клиента.

Указания к выполнению

1. Для получения доступа к ресурсам удаленного компьютера следует настроить клиента VPN. Запустите виртуальную машину с Windows 8.1 (те же действия при наличии разрешений можно выполнять на физическом компьютере).

2. Откройте окно сетевых подключений (**Пуск** – **Панель управления** – **Сетевые подключения**). Слева в разделе **Сетевые задачи** выберите **Создание нового подключения**. В **Мастере новых подключений** выберите **Подключить к сети на рабочем месте**, затем – **Подключение к виртуальной частной сети.** В следующем окне введите название для подключений (например, «VPN»). Затем нужно выбрать **Не набирать номер для предварительного подключения.** В следующем окне следует ввести IP-адрес VPN-сервера (192.168.X.1). Нажмите кнопку **Готово.** VPN-клиент настроен.

3. Для подключения к VPN-серверу откройте созданное подключение и введите в поле имени пользователя имя той учетной записи, которой вы

разрешили доступ к VPN-серверу. Если задан пароль, введите его. Нажмите кнопку **Подключение**. Если все правильно, должно установиться VPN-подключение, а в правом нижнем углу экрана должен появиться значок подключения.

4. Проверьте параметры подключения. Для этого в контекстном меню подключения выберите пункт **Состояние**. Перейдите на вкладку **Сведения** и выпишите параметры **Тип сервера**, **Проверка подлинности**, **IP-адрес сервера** и **IP-адрес клиента**. Убедитесь, что оба адреса принадлежат тому диапазону, который вы назначили на VPN-сервере.

Задание 5. Попытка перехвата пакетов в VPN-подключении.

Указания к выполнению

1. Запустите из командной строки сервера утилиту ping и пошлите эхо-запросы на VPN-клиент. Используйте IP-адрес клиента, выписанный с вкладки **Сведения VPN-подключения**, например:

2.

ping 192.168.100+X.2

Сделайте скриншот.

3. Остановите мониторинг в Network Monitor: меню **Capture** – **Stop** или клавиша **F11.** Просмотрите информацию о полученных кадрах: меню **Capture** – **Display Captured Data** (**Запись** – **Отображение собранных данных**) или клавиша **F12**. В окне **Summary** (**Общая информация**) отобразится подробная информация обо всех собранных кадрах. Двойной щелчок на любом кадре откроет подробную статистику по этому кадру. Найдите кадр с эхо запросом, разверните заголовки и поле данных, сделайте выводы и скриншот.

Контрольные вопросы

1. Для каких целей используется сетевой анализатор Network Monitor?
2. Какие виды фильтров позволяет применять Network Monitor?
3. Для чего служит VPN?
4. Назовите протоколы аутентификации, применяемые в VPN.
5. Каким образом в соединении VPN можно выбрать протокол соединения – PPTP или L2TP?
6. Как защищаются пакеты, передаваемые по VPN?

Библиографический список

1. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. [Текст] / В. Ф. Шаньгин. - М. : ДМК Пресс, 2012. - 592 с. : ил.
2. Котельников Е.В. Сетевое администрирование на основе Microsoft Windows Server 2003: лабораторный практикум / Е.В. Котельников и Н.А. Кротова. MSDN Academic Alliance, 2007. http://ua.bookfi.org/book/805988