Лабораторная работа № 10.  
Сетевой анализатор Network Monitor и сети VPN

**Цели работы:**

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

**Связь с проектом**

Сетевой анализатор Network Monitor, 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. Допустим, декан факультета захотел иметь защищенное соединение с сервером, т. е. такое соединение, сообщения по которому не могут быть прочитаны даже при перехвате сообщения. Решением данной задачи является настройка VPN.

**Задание 1**. Установить сетевой анализатор Network Monitor.

**Указания к выполнению**

1. Запустите виртуальную машину с Windows Server 2008.
2. Запустите программу установки сетевого анализатора Network Monitor, расположенную в папке с заданием к лабораторной работе.
3. В окне мастера установки нажмите **Next** (**Далее**), затем отметьте пункт согласия с условиями лицензионного соглашения (**I accept the terms n the License Agreement**) и снова нажмите **Next** (**Далее**).
4. В следующем окне выберите пункт **I do not want to use Microsoft Update** (**Я не хочу использовать обновления Microsoft**) и нажмите **Next** (**Далее**).
5. В окне выбора типа установки щелкните по пункту **Typical** (**Стандартная**) и нажмите **Install** (**Установить**).
6. Дождитесь окончания установки и нажмите **Finish** (**Завершить**).
7. Появится окно конфигурирования Network Monitor.

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

**Указания к выполнению**

1. Запустите Microsoft Network Monitor через меню **Пуск** (**Start**).
2. Запустите мониторинг кадров: выберите в меню **New** **Capture** (**Новый захват**)**,** а затем пункт **Start** (**Старт**).
3. Окно Network Monitor содержит следующие элементы (Рис. 5):

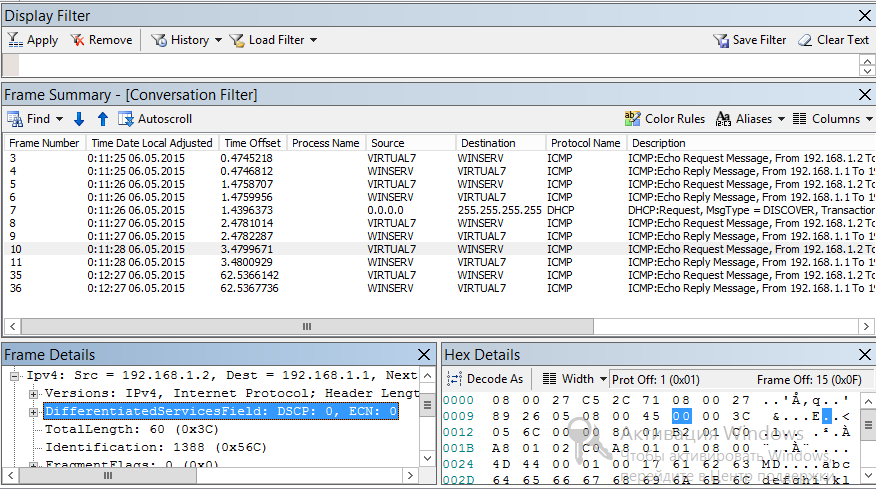


Рис. 5. Элементы окна Network Monitor

Network Monitor отображает общую статистику отслеживаемого трафика, в том числе следующую информацию:

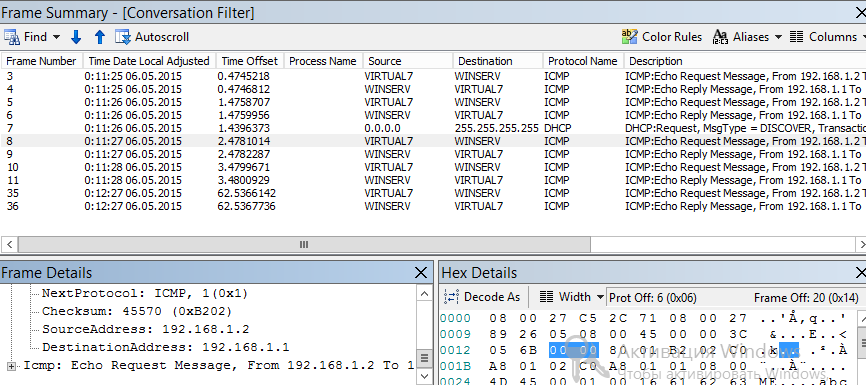
1. сведения о широковещательных кадрах (**Broadcast**);
2. сведения о многоадресных кадрах (**Multicast**);
3. статистику использования сети;
4. количество полученных байт в секунду;
5. количество полученных кадров в секунду и т. д.
6. Запустите из командной строки утилиту ping и проверьте доступность клиентского компьютера:

Изображение выглядит как текст

Автоматически созданное описание

ping 192.168.1.10

1. Остановите мониторинг в Network Monitor: меню **Stop**. Просмотрите информацию о полученных кадрах. В окне **Frame Summary** (**Общая информация о кадре**) отобразится подробная информация обо всех собранных кадрах. Двойной щелчок на любом кадре откроет подробную статистику по этому кадру (рис. 6).



Окно общей информации

Окно подробной информации Окно информации в шестнадцатеричном виде

Рис. 6. Элементы окна Summary

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

* + **Frame** – номер кадра;
  + **Time** – время захвата кадра;
  + **Src MAC Addr** – МАС-адрес источника;
  + **Dst MAC Addr** – МАС-адрес приемника;
  + **Protocol** – протокол, передавший кадр;
  + **Description** – описание кадра;
  + **Src Other Addr** – имя источника;
  + **Dst Other Addr** – имя приемника;
  + **Type Other Addr** – тип протокола нижнего уровня.

При проверке достижимости узла 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.

**Задание 3**. Перехват текстовых сообщений.

**Указания к выполнению**

1. С помощью Network Monitor можно просматривать информацию, передаваемую по сети, если она незашифрована. В этом задании осуществим отправку текстового сообщения с помощью команды net send и перехватим её, используя Network Monitor.
2. Запустите мониторинг кадров в Network Monitor.

Изображение выглядит как текст

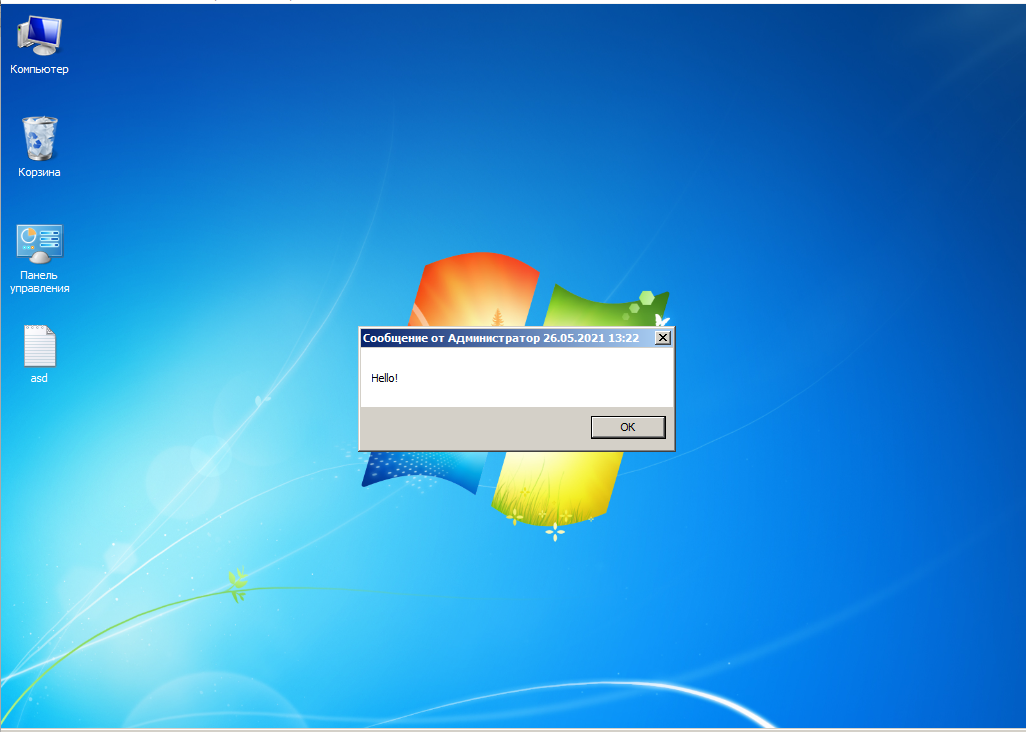
Автоматически созданное описание

1. Из командной строки на сервере отправьте текстовое сообщение на клиентский компьютер с помощью команды msg:

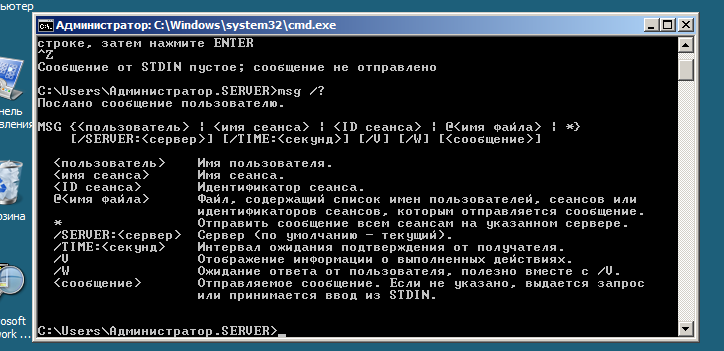
msg \* /server:192.168.1.10 Hello!

Изображение выглядит как текст

Автоматически созданное описание



1. Изучите справку по команде msg, чтобы понять, какие параметры были указаны при отправке сообщения.



1. После передачи сообщения остановите мониторинг кадров. Откройте окно **Frame Summary** для просмотра собранных кадров:

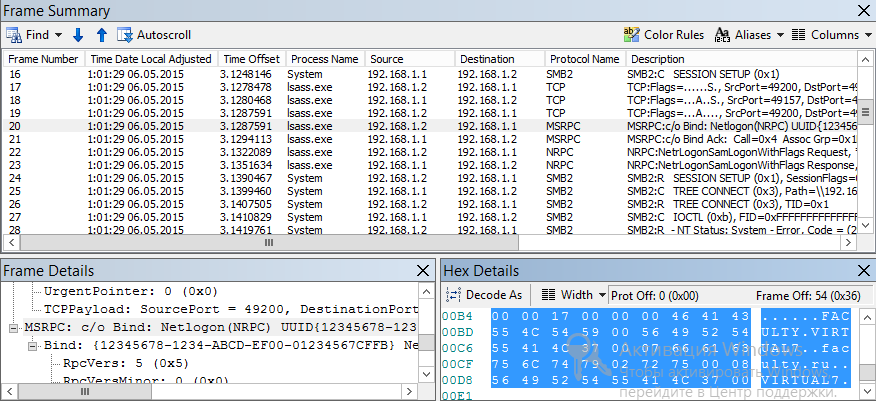


Рис. 7. Перехват текстового сообщения

В одном из кадров можно прочитать посланное сообщение[[1]](#footnote-1).

**Задание 4**. Установка сервера виртуальной частной сети (VPN).

**Указания к выполнению**

1. В предыдущем задании мы убедились, что передача текстовой информации в незашифрованном виде по открытым сетям небезопасна. Решением данной проблемы является организация виртуальных частных сетей VPN.
2. Установите VPN-сервер. Для этого следует открыть Диспетчер серверов и добавить роль **Удаленный доступ**, если эта роль не была ранее добавлена, а также службу данной роли **DirectAccess** и **VPN**

Изображение выглядит как текст

Автоматически созданное описание

1. В оснастке **mmc** откройте **Routing and Remote Access** (**Маршрутизация и удаленный доступ**).
2. В контекстном меню сервера выберите пункт **Configure and Enable Routing and Remote Access** (**Сконфигурировать и активировать маршрутизацию и удаленный доступ**). В окне мастера **Routing and Remote Access Server Setup Wizard** выберите пункт **Custom configuration** (**Особая конфигурация**). Установите флажок **VPN access** (**Доступ к VPN**). На предложение запустить службу нужно ответить **Yes** (**Да**).

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

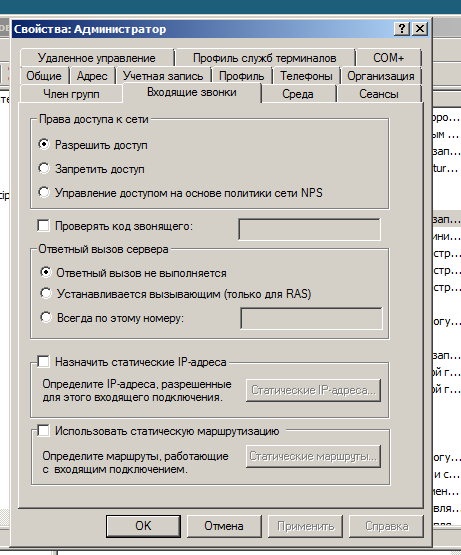
Автоматически созданное описание

1. 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** (**Статический пул адресов**). Нажмите кнопку **Add** (**Добавить**), введите начальный и конечный адреса диапазона, например 192.168.2.1 – 192.168.2.10 и нажмите **ОК**.

Изображение выглядит как текст

Автоматически созданное описание

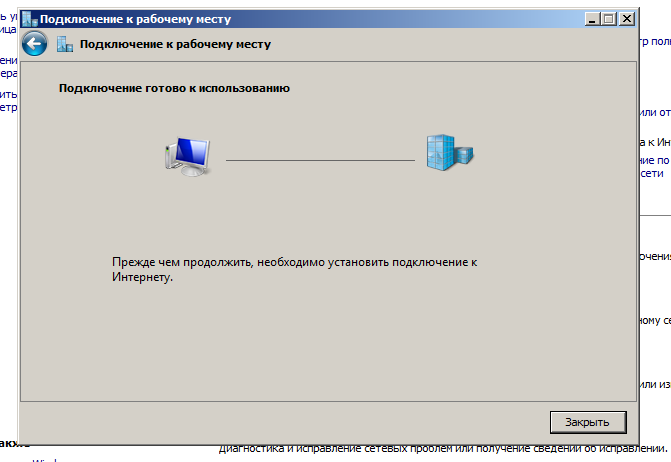
1. Следующим шагом будет активизация возможности удаленного подключения у одной из учетных записей. Откройте оснастку **Active Directory Users and Computers** (**Пользователи и компьютеры** **Active Directory**), выберите любую из существующих учетных записей (например, **Administrator** (**Администратор**)). В контекстном меню учетной записи выберите пункт **Properties** (**Свойства**), перейдите на вкладку **Dial-in (Входящие звонки**), в разделе **Права доступа к сети** выберите пункт **Allow access** (**Разрешить доступ**), щелкните **ОК**.



**Задание 5**. Настройка VPN-клиента.

**Указания к выполнению**

1. Для получения доступа к ресурсам удаленного компьютера следует настроить клиента VPN. Запустите виртуальную машину с Windows 7 (те же действия при наличии разрешений можно выполнять на физическом компьютере).
2. Зайдите в **Центр управления сетями и общим доступом**. По центру в разделе **Изменение сетевых параметров** выберите **Настройка нового подключения или сети**.
3. В **Мастере новых подключений** выберите **Подключить к рабочему месту**, затем – **Использовать мое подключение к Интернету (VPN) – Отложить настройку подключени к Интернету**  В следующем окне следует ввести IP-адрес VPN-сервера (192.168.1.1). Нажмите кнопку **Создать**. VPN-клиент настроен.



1. 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.
2. 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.

Изображение выглядит как текст

Автоматически созданное описание

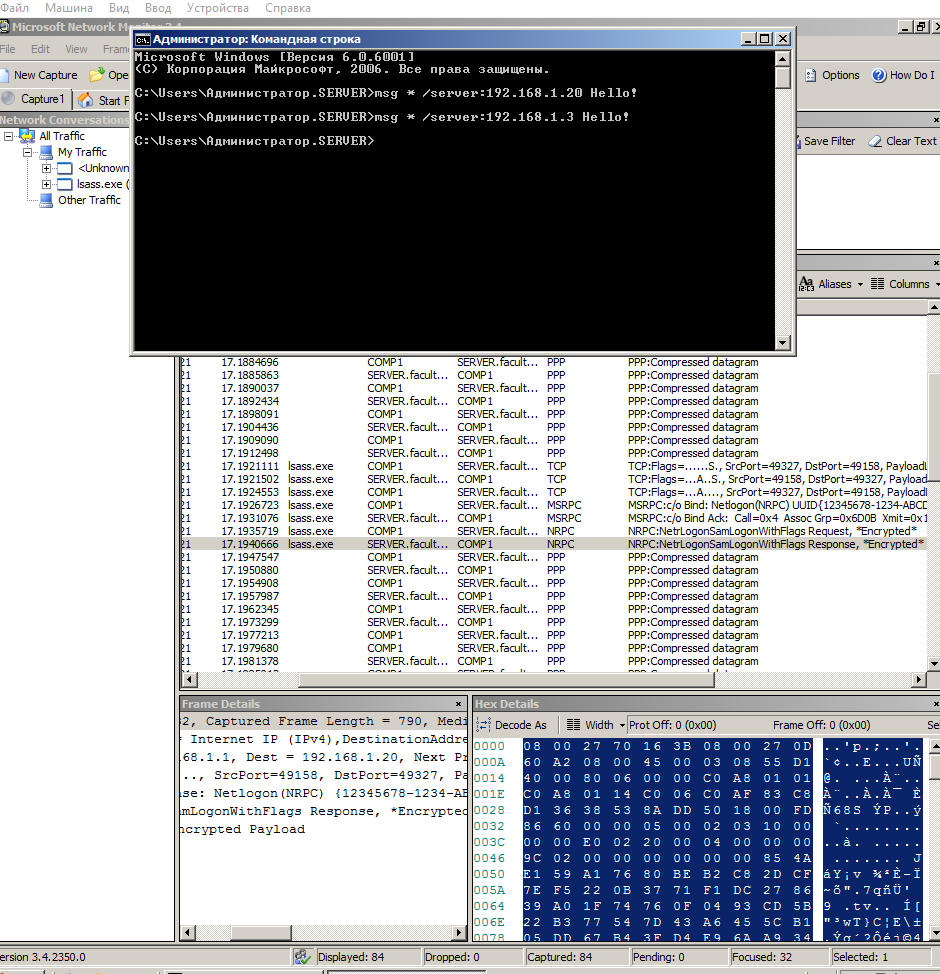
**Задание 6**. Попытка перехвата сообщения в VPN-подключении.

**Указания к выполнению**

1. На виртуальной машине с Windows Server 2008 запустите мониторинг кадров в Network Monitor.
2. Передайте текстовое сообщение на VPN-клиент с помощью команды net send. Используйте IP-адрес клиента, выписанный с вкладки **Сведения VPN-подключения**, например:

msg \* /server:192.168.2.2 Hello!

1. После передачи сообщения остановите мониторинг в Network Monitor. Перейдите в окно **Frame Summary** и попытайтесь найти ваше текстовое сообщение. По результатам сделайте выводы.



**Самостоятельная работа**

* + Сохраняйте в отчет скриншоты основных шагов.

1. Изучите возможности фильтрации кадров в Network Monitor (меню **Filter**). Настройте следующие фильтры:

* захват кадров только между сервером и физическим компьютером;
* захват кадров только по протоколу ARP.

Изображение выглядит как текст

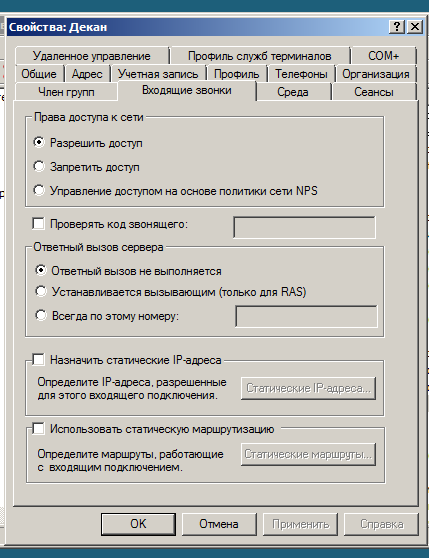
Автоматически созданное описание

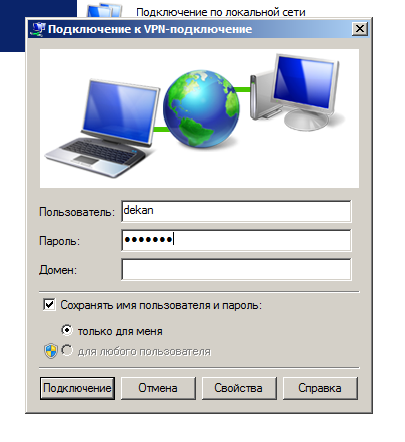
1. Передайте небольшой текстовый файл с расширением **txt** в сети без VPN (например, пользуясь проводником Windows). Попробуйте его перехватить с помощью Network Monitor.

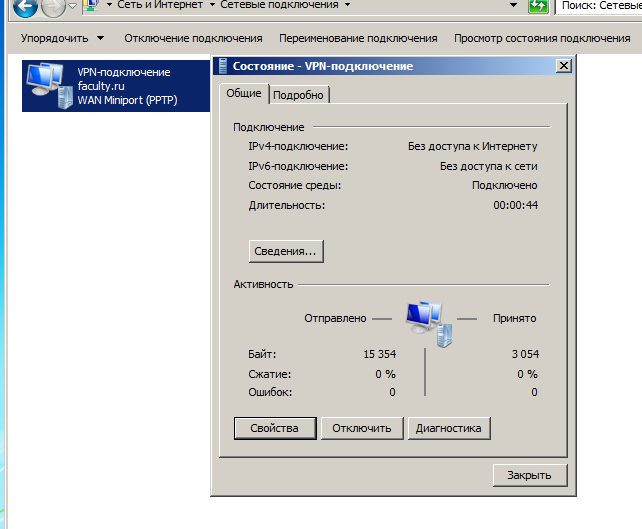
Изображение выглядит как стол

Автоматически созданное описание

1. Настройте доступ к серверу по VPN учетной записи декана факультета.







1. Каким образом для соединения VPN можно выбрать тип используемого протокола аутентификации? Скриншот соответствующего окна поместите в отчет.

Изображение выглядит как текст

Автоматически созданное описание

**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?

1. Если сообщение не удалось отправить, это свидетельствует, скорее всего, о том, что на компьютере, где должно приниматься посылаемое сообщение, невозможно получить информацию о вошедших в систему пользователях. На каждом компьютере, которому будут отправляться сообщения, добавьте в раздел реестра HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server параметр AllowRemoteRPC типа REG\_DWORD равный 1 и перезапустите компьютер. [↑](#footnote-ref-1)