МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению практических работ
по дисциплине

СЕТЕВЫЕ ТЕХНОЛОГИИ CISCO

Направление подготовки	**10.03.01 Информационная безопасность**
Профиль	Комплексная защита объектов информатизации
Квалификация выпускника	бакалавр
Форма обучения	очная
Учебный план	2020 г.

Пятигорск, 2020 г.

ВВЕДЕНИЕ

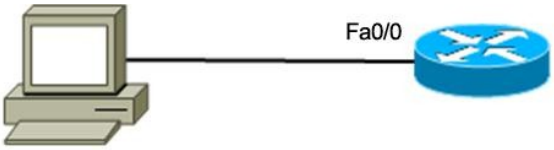
Методические указания содержат курс лабораторных работ по дисциплине «Сетевые технологии cisco» направленный на изучение принципов функционирования и элементной базы вычислительных систем.

Содержащиеся в данном пособии сведения теории, методические указания и рекомендации по выполнению практических работ позволяют использовать его в качестве дополнительного пособия для закрепления курса лекций

СОДЕРЖАНИЕ

Практическая работа 1. Удаленная настройка сетевых устройств

Настройка удаленного маршрутизатора с помощью протокола SSH



Прямой кабель	
Кабель последовательной передачи данных	
Консольный (перевернутый)	
Перекрестный кабель	

Цели

- Настроить маршрутизатор на прием SSH-подключений.
- Настроить клиентские SSH-приложения на ПК.
- Установить подключение к маршрутизатору с интегрированными службами Cisco с помощью протокола SSH версии 2.
- Проверить текущую конфигурацию.

Предварительная информация/подготовка

В прошлом для удаленной настройки сетевых устройств в основном использовался протокол Telnet. Однако такие протоколы, как Telnet, не предусматривают ни аутентификацию, ни шифрование сведений между клиентом и сервером Telnet. В результате для перехвата паролей и сведений о настройках может использоваться сетевой перехватчик.

Протокол SSH — это сетевой протокол, служащий для установки безопасного подключения эмуляции терминала к маршрутизатору или иному сетевому устройству. Протокол SSH шифрует все сведения, которые поступают по сетевому каналу и предусматривает аутентификацию удаленного компьютера. Протокол SSH все больше заменяет Telnet — именно его выбирают сетевые специалисты в качестве средства удаленного входа в систему. Чаще всего протокол SSH служит для входа на удаленный компьютер и выполнения команд, однако он также может передавать файлы с помощью связанных протоколов SFTP или SCP.

Чтобы протокол SSH заработал, взаимодействующие сетевые устройства должны его поддерживать. В этой практической работе необходимо включить SSH-сервер в настраиваемом маршрутизаторе, после чего следует подключиться к маршрутизатору, используя ПК с установленным клиентом SSH. Для работы в локальной сети подключение обычно устанавливается с помощью Ethernet и IP-адреса. Сетевыми устройствами, соединенными с помощью других типов каналов, например, последовательного порта, также можно управлять через протокол SSH, при условии, что они поддерживают IP-адресацию. Подобно протоколу Telnet, SSH- это внутриполосной Интернет-протокол на базе TCP/IP.

В этой практической работе можно использовать команды Cisco SDM или интерфейса командной строки Cisco IOS для настройки протокола SSH в маршрутизаторе.

Маршрутизатор с интегрированным функциями Cisco 1841 поддерживает использование протокола SSH версий 1 и 2, причем версия 2 предпочтительнее. Клиентом SSH, используемым в этой практической работе, является PuTTY, который можно загрузить бесплатно.

Cisco SDM поддерживается многими маршрутизаторами Cisco и версиями программного обеспечения Cisco IOS. Многие последние маршрутизаторы Cisco поставляются с установленным SDM. Если используется маршрутизатор 1841, SDM (и SDM Express) предустановлены. В этой практической работе предполагается использование маршрутизатора Cisco 1841. Можно использовать другую модель маршрутизатора, если она поддерживает SDM. Если используется маршрутизатор, поддерживающий SDM, на котором SDM не установлен, последнюю версию можно загрузить бесплатно по этому адресу: http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm

Перейдя по указанной ссылке, просмотрите или загрузите документ «Загрузка и установка маршрутизатора и диспетчера устройств защиты Cisco» (Downloading and Installing Cisco Router and Security Device Manager). В этом документе содержатся инструкции по установке SDM на маршрутизатор. В нем указаны конкретные номера моделей и версии IOS, которые поддерживают SDM, а также необходимый объем памяти.

Примечание. Если для настройки протокола SSH вы используете SDM, перед выполнением этой практической работы необходимо закончить работу 5.2.3, «Настройка маршрутизатора с интегрированными сетевыми службами с использованием SDM Express». В этой практической работе предполагается, что на маршрутизаторе уже была проведена базовая настройка.

Примечание. Если вы работаете с маршрутизатором, на котором SDM не установлен, воспользуйтесь командами интерфейса командной строки Cisco IOS для настройки протокола SSH. Указания предоставлены для настройки протокола SSH вручную с помощью команд интерфейса командной строки Cisco IOS для маршрутизаторов без запуска SDM в шаге 2 этой практической работы. Чтобы выполнить основную настройку маршрутизатора см. практическую работу 5.3.5 «Настройка основных параметров маршрутизатора с помощью интерфейса командной строки IOS».

Примечание. Маршрутизаторы SDM с удаленным файлом начальной конфигурации. Если для маршрутизатора SDM удалена начальная конфигурация, при перезагрузке маршрутизатора SDM он перестает отображаться по умолчанию. Необходимо будет создать базовые настройки маршрутизатора с использованием команд операционный системы IOS. См. процедуру в конце этой практической работы или обратитесь к преподавателю.

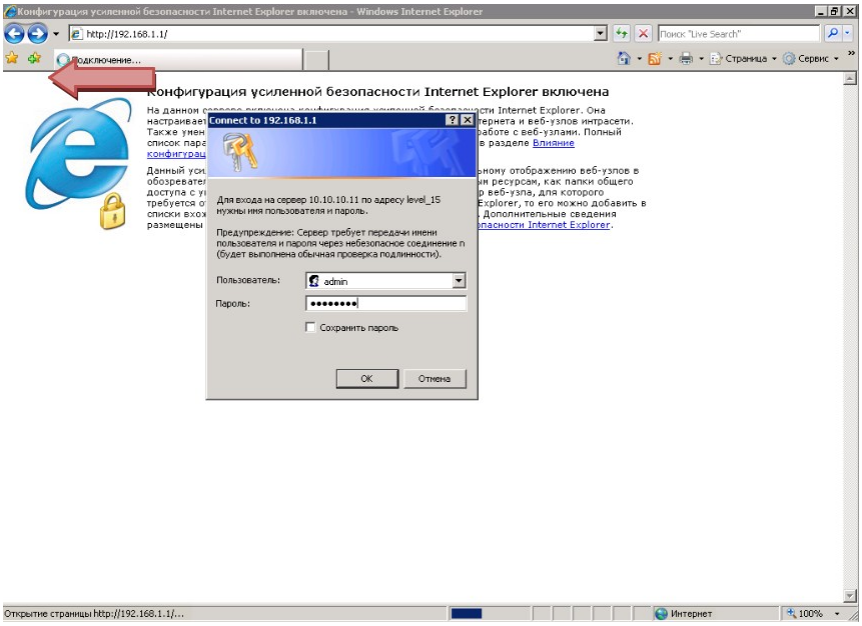
Необходимо использовать следующие ресурсы:

- маршрутизатор Cisco 1841 ISR с установленным SDM версии 2.4 (важно: см. Примечание 2 к шагу 1);
- (дополнительно) другая модель маршрутизатора Cisco с установленным SDM;
- (дополнительно) другая модель маршрутизатора Cisco без установленного SDM (ОС IOS версии 12.2 или выше должна поддерживать протокол SSH);
- компьютер с Windows XP и Internet Explorer 5.5 (или выше) и SUN Java Runtime Environment (JRE) версии 1.4.2_05 или более поздней (или Java Virtual Machine (JVM) 5.0.0.3810);
- последний выпуск клиента putty.exe, установленный на ПК и доступный на рабочем столе;
- прямой или перекрещенный кабель Ethernet 5-ой категории (для SDM и SSH);
- (дополнительно) консольный кабель, если маршрутизатор необходимо настроить с помощью интерфейса командной строки;
- доступ к командной строке ПК;
- доступ к сетевой конфигурации TCP/IP ПК.

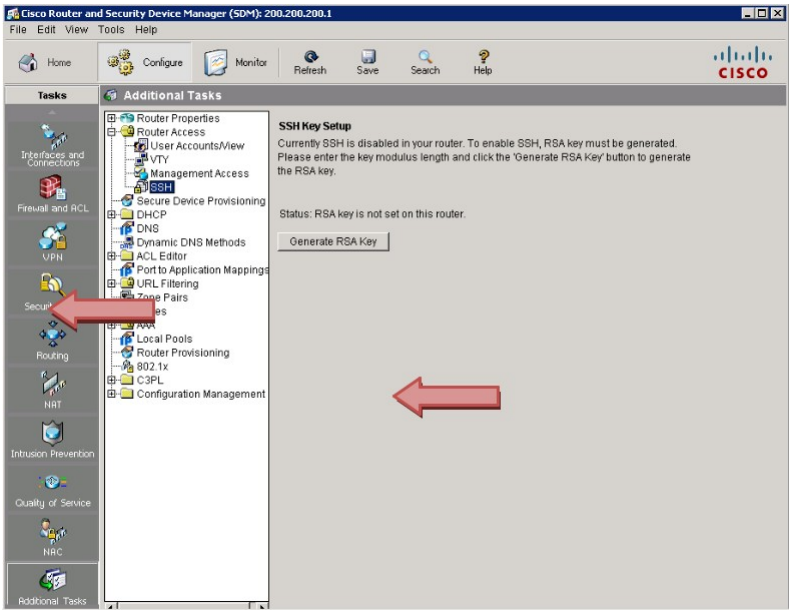
Шаг 1. Настройка маршрутизатора с интегрированными функциями (ISR) на примем SSH-подключений с помощью SDM

Примечание. Если на маршрутизаторе не установлен SDM: При настройке маршрутизатора, где не установлен SDM, на использование протокола SSH прочитайте сведения шага 1 о том, как происходит настройка протокола SSH в виде отдельной задачи при использовании SDM, после чего перейдите к шагу 2; в противном случае выполните шаг 1 и перейдите к шагу 3.

a. Откройте веб-обозреватель и подключитесь к http://192.168.1.1. После появления приглашения введите в качестве имени пользователя **admin** и **cisco123** в качестве пароля. Нажмите **OK**. Начнется загрузка Cisco SDM.

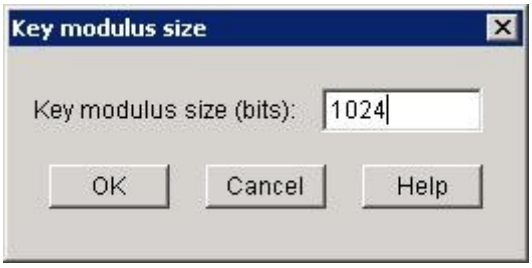


б. После загрузки SDM нажмите кнопку **Configure (настройка)** на панели инструментов. В области задач выберите **Additional Tasks (дополнительные задачи)**. В области дополнительных задач разверните **Router Access (доступ к маршрутизатору)** и щелкните задачу **SSH**. Затем нажмите кнопку **Generate RSA Key (создать ключ RSA)**.



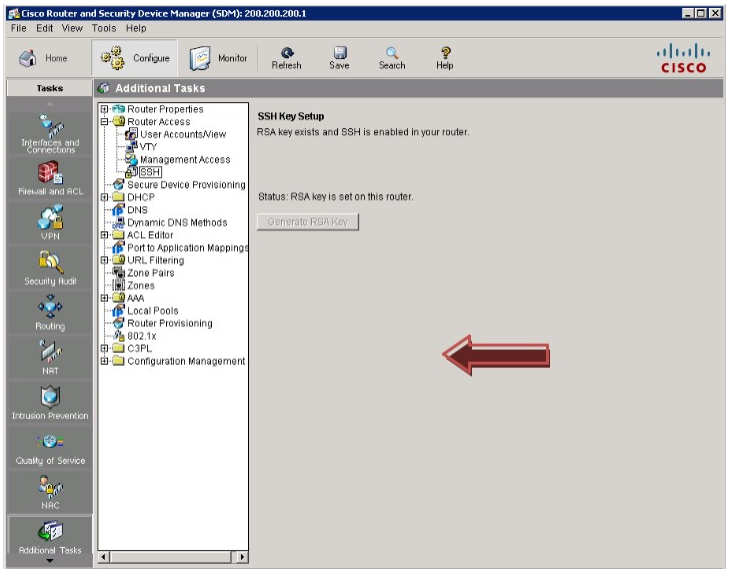
Примечание. Если протокол SSH уже настроен: Если в сообщении настройки ключа **SSH** говорится: «Ключ RSA уже существует, и протокол SSH включен на вашем маршрутизаторе», а **статусом** является «Ключ RSA установлен на этом маршрутизаторе», возможно, это из-за того, что вы выполнили практическую работу 5.2.3 «Настройка маршрутизатора с интегрированными сетевыми службами с помощью SDM Express». Как вы помните, в той практической работе при настройке безопасности одним из рекомендованных параметров безопасности по умолчанию был «Усилить безопасность на этом компьютере». Если этот флажок установлен, протокол SSH автоматически настраивается для доступа к маршрутизатору, а также предусматривается заголовок для предупреждения о злоумышленниках, устанавливается минимальная длина пароля и ограничивается количество неудачных попыток входа.

в. В диалоговом окне размера ключа введите размер ключа, равный **1 024** бит. Нажмите **OK**.

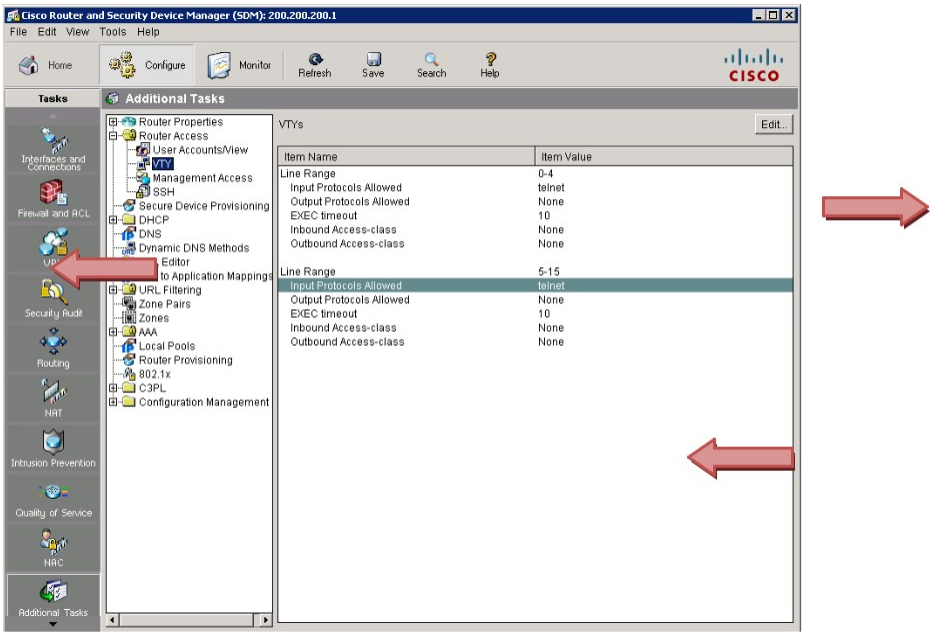


г. В диалоговом окне Enter SSH Credentials (Ввод учетных данных для протокола SSH) введите имя пользователя **admin** и пароль **cisco123**. Нажмите **OK**.

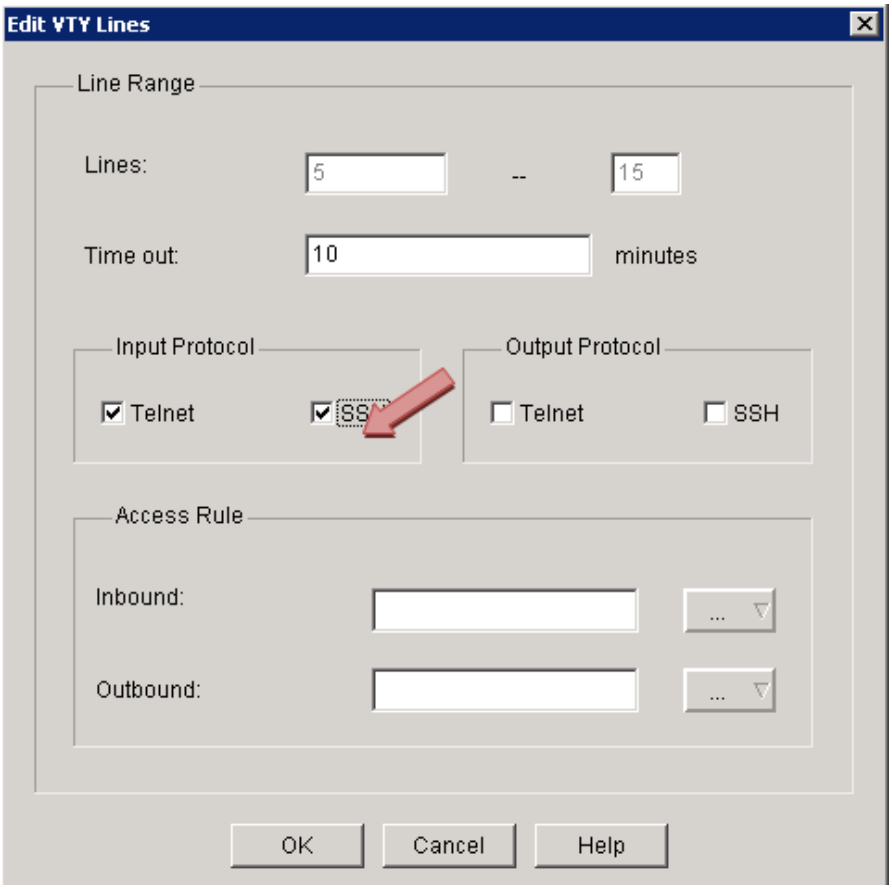
д. Обратите внимание на то, что ключ RSA (Rivest, Shamir, and Adelman) теперь включен на маршрутизаторе.



e. В области дополнительных задач выберите параметр **VTY**. Выберите **Input Protocols Allowed** (разрешить входные протоколы), после чего нажмите кнопку **Edit (изменить)**.

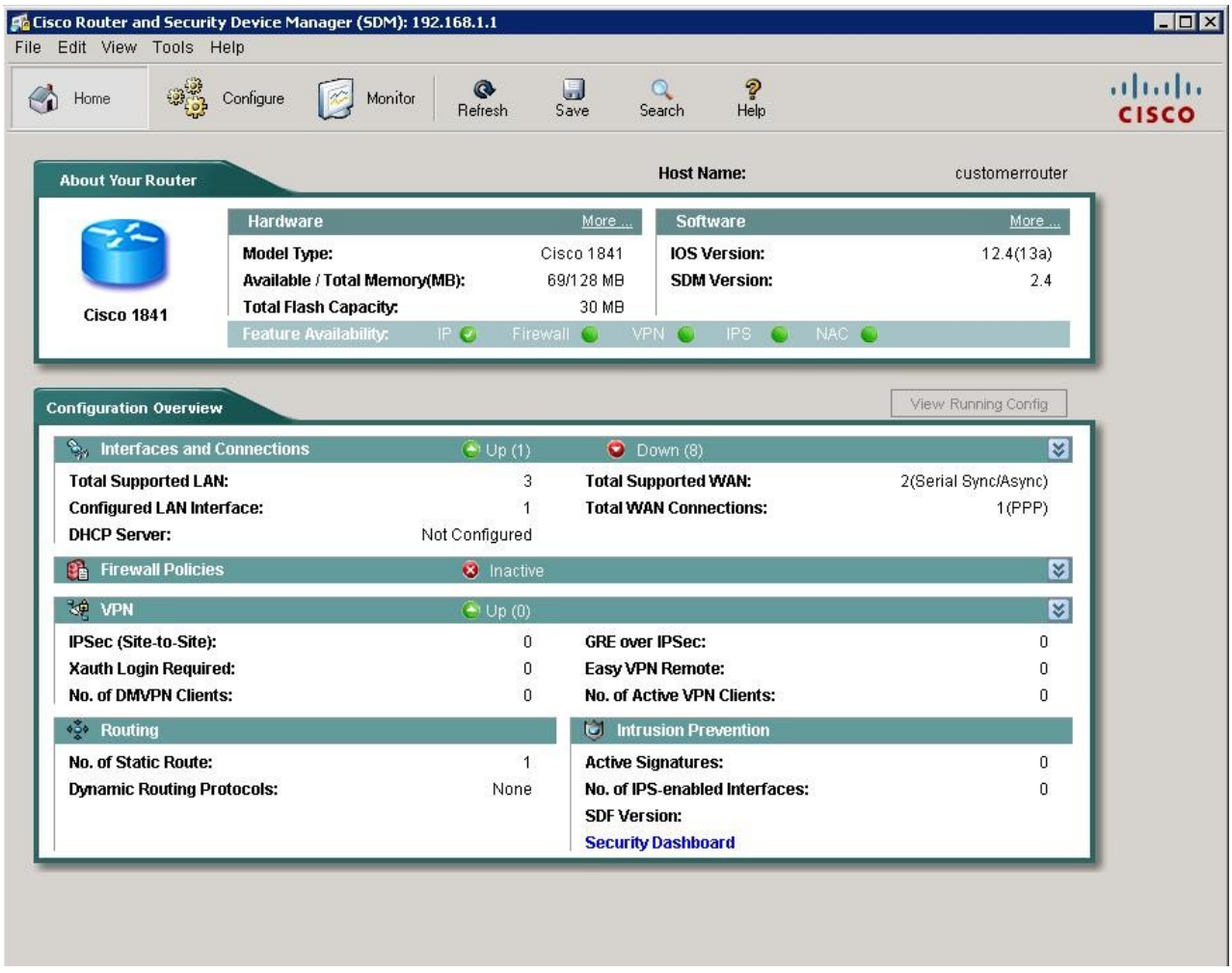


ж. Поставьте флажок рядом с протоколом **SSH** и нажмите **OK**.



з. Когда откроется окно Commands Delivery Status (состояние отправки команд), щелкните **OK**.

и. Закройте Cisco SDM, щелкнув **X** в верхнем правом углу окна.



к. Щелкните **Yes (да),** чтобы подтвердить закрытие SDM.

Шаг 2. (НЕ ОБЯЗАТЕЛЬНО) Настройка протокола SSH на маршрутизаторе без SDM

Примечание. Если вы настраиваете маршрутизатор для протокола SSH, а SDM уже установлен, можно пропустить шаг 2 и перейти сразу к шагу 3.

а. Если вы настраиваете маршрутизатор на прием SSH-подключений, и при этом SDM не установлен, подключите порт консоли маршрутизатора к ПК и программе HyperTerminal,

как описано в практической работе 5.1.2, «Подача питания на маршрутизатор с интегрированными сетевыми службами».

б. Вход в систему маршрутизатора. В командной строке привилегированного режима EXEC введите команды интерфейса командной строки ОС Cisco IOS, как указано ниже. Эти команды включают не все пароли, которые необходимо назначить. См. Практическую работу 5.3.4 «Настройка основных параметров маршрутизатора с помощью интерфейса командной строки IOS» для дополнительных сведений о параметрах конфигурации.

Примечание. На маршрутизаторе должна быть установлена ОС IOS 12.0 или выше. Например, маршрутизатор — модель Cisco 2620XM с ОС 12.2(7r).

в. Настройте основные сведения о маршрутизаторе и интерфейсе.

```
Router#config terminal
Router(config)#hostname CustomerRouter
CustomerRouter(config)#ip domain-name customer.com
CustomerRouter(config)#username admin privilege 15 password 0
cisco123
CustomerRouter(config)#interface FastEthernet 0/0
CustomerRouter(config-if)#ip address 192.168.1.1 255.255.255.0
CustomerRouter(config-if)#no shutdown
CustomerRouter(config-if)#exit
```

г. Настройте строки удаленного входящего терминала vty на прием протоколов Telnet и SSH:

```
CustomerRouter(config)#line vty 0 4
CustomerRouter(config-line)#privilege level 15
CustomerRouter(config-line)#login local
CustomerRouter(config-line)#transport input telnet
ssh CustomerRouter(config-line)#exit
```

д. Создайте пару ключей шифрования RSA, которая будет служить маршрутизатору для аутентификации и шифрования передаваемых SSH-данных. Введите **768** в качестве количества размера ключа (в битах). По умолчанию равно 512.

```
CustomerRouter(config)#crypto key generate rsa

How many bits in the modulus [512] 768

CustomerRouter(config)#exit
```

е. Убедитесь, что протокол SSH включен, и используется надлежащая версия.

```
CustomerRouter#show ip ssh
```

ж. Введите следующие сведения, исходя из результатов команды **show ip ssh**.

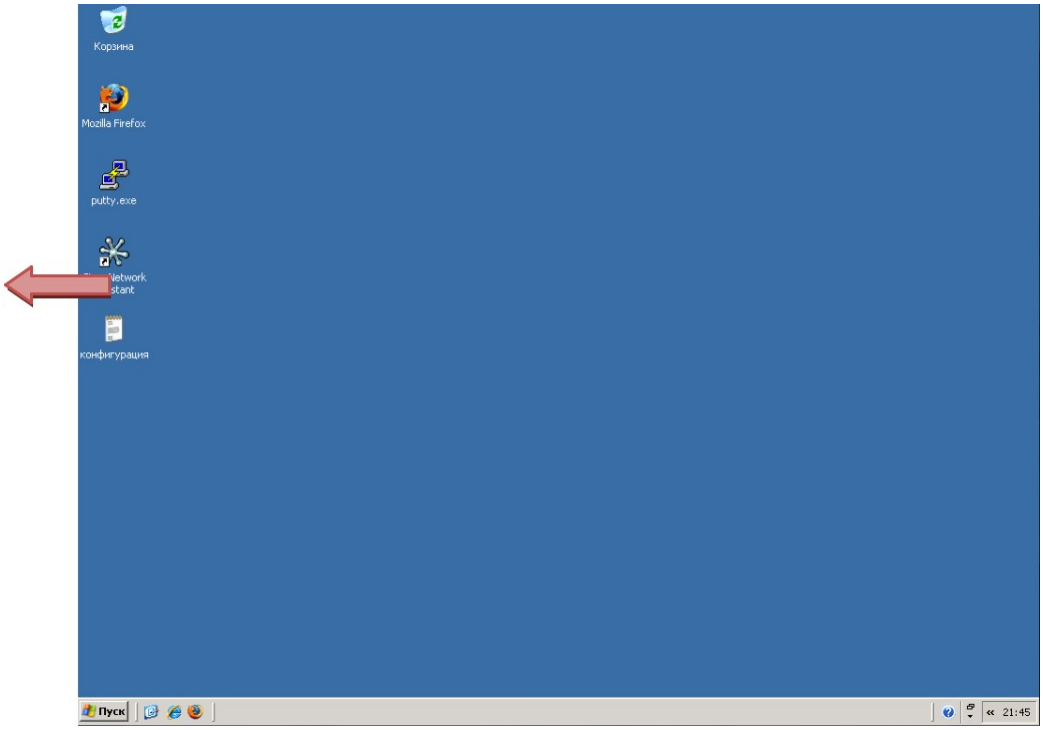
Версия действующего протокола SSH: _____
Время ожидания при аутентификации: _____
Число попыток аутентификации: _____

з. Сохраните текущую конфигурацию в качестве начальной:

```
CustomerRouter#copy running-config startup-config
```

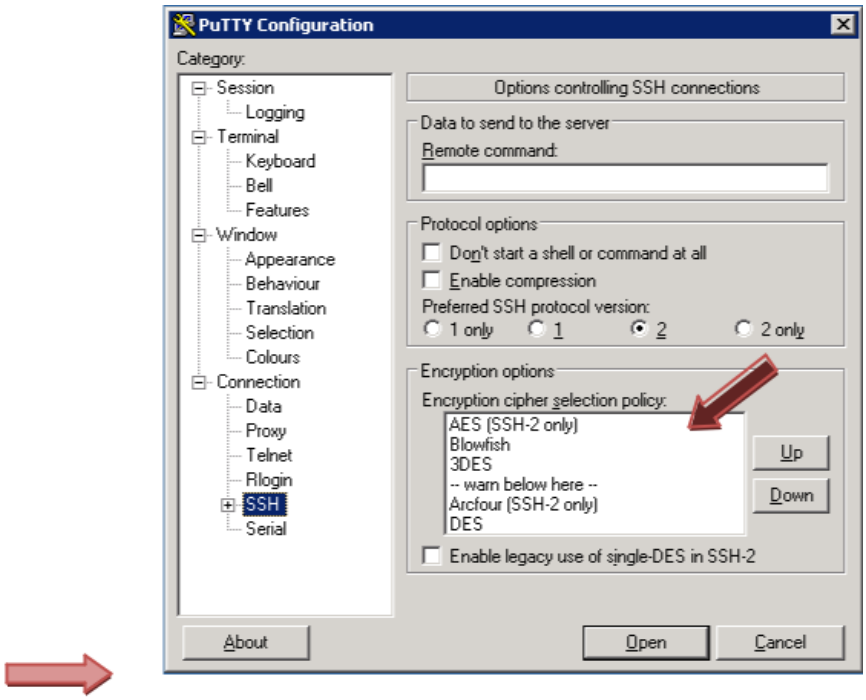
Шаг 3. Настройка клиента SSH и подключение ПК к маршрутизатору с интегрированными сетевыми службами

и. Получите копию putty.exe и разместите приложение на рабочем столе. Запустите PuTTY двойным щелчком мыши по значку **putty.exe**.

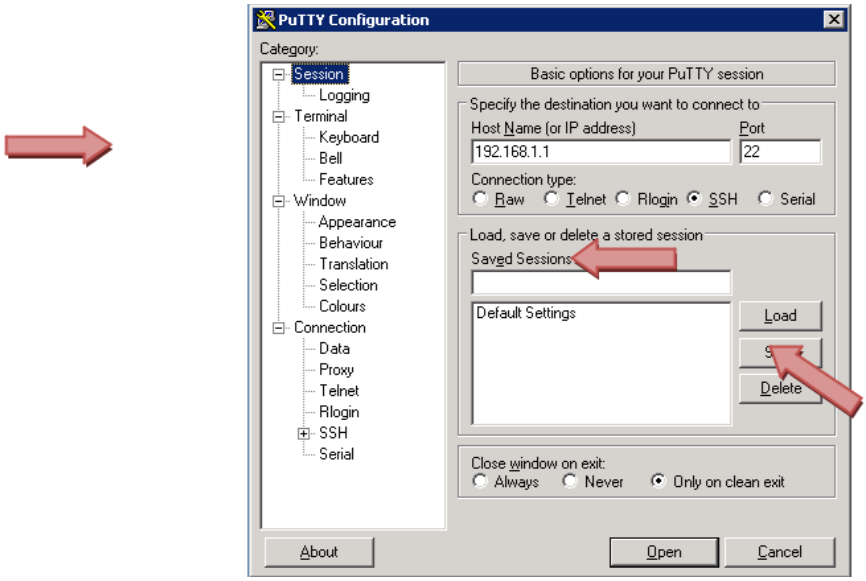


к. В области категорий выберите протокол **SSH** и убедитесь, что в качестве предпочтительной версии протокола SSH установлена версия **2**.

Примечание. Клиент Putty будет производить подключение, даже если на сервере SSH будет запущена SSH-версия 1.

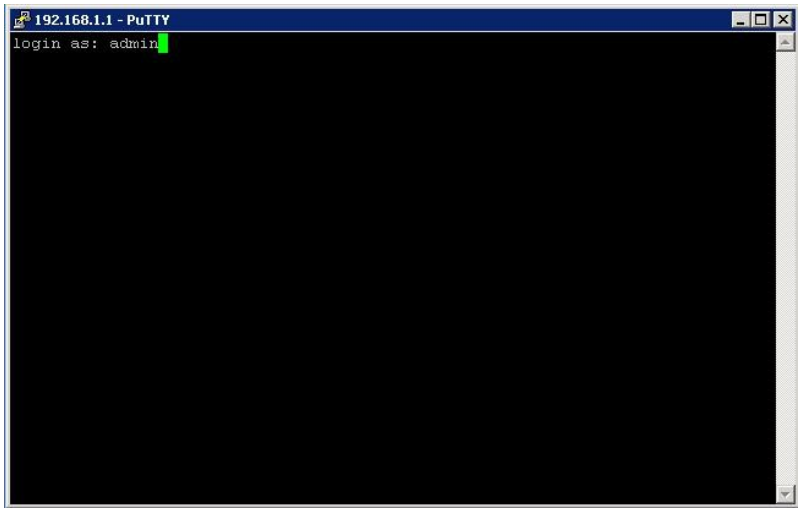


л. В области категорий выберите **Session (сеанс)** и введите IP-адрес интерфейса ЛВС маршрутизатора **—** 192.168.1.1. Убедитесь, что для типа подключения выбран протокол SSH. Щелкните **Open (открыть)**.

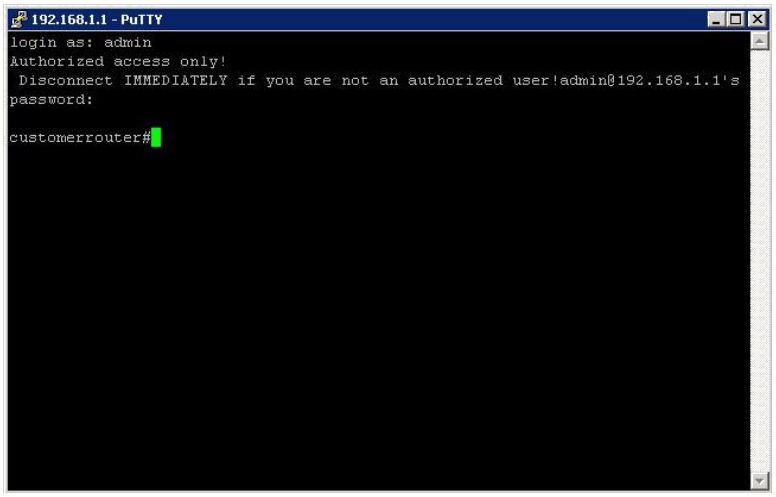


м. Когда в Cisco 1841 ISR подключение к SSH-службе с помощью клиента SSH создается впервые, ключ подключения сохраняется в кэш-памяти локального реестра компьютера. В окне PuTTY Security Alert (предупреждение о защите PuTTY) щелкните **Yes (да)**, чтобы продолжить.

н. В приглашении входа в систему введите имя пользователя администратора **(admin)** и нажмите **ВВОД**.



о. В командной строке пароля введите пароль администратора (**cisco123)** и нажмите **ВВОД**.

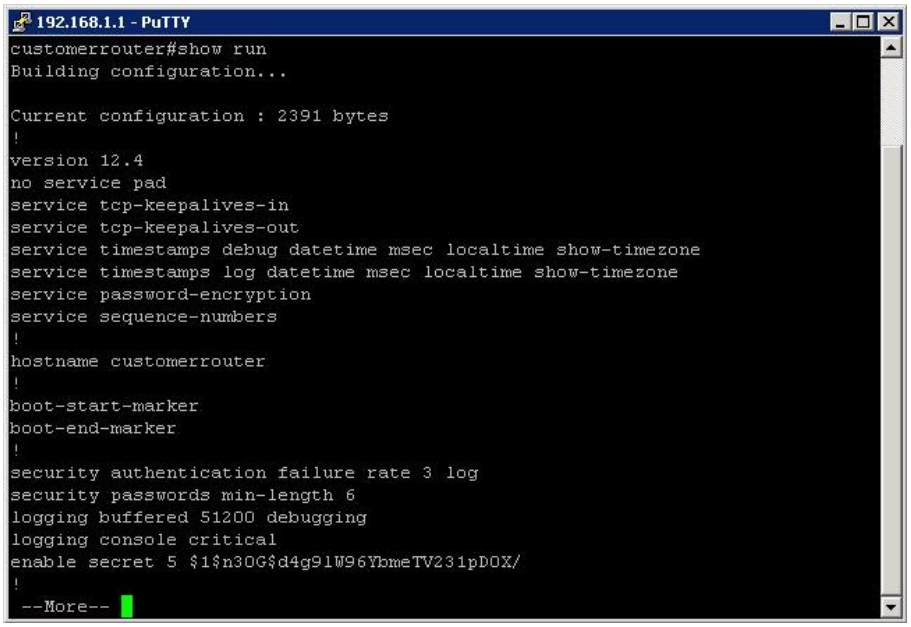


Шаг 4. Проверка конфигурации маршрутизатора Cisco 1841 с интегрированными сетевыми службами

а. Чтобы проверить конфигурацию маршрутизатора, введите **show run** в командной строке привилегированного режима и нажмите **ВВОД**.

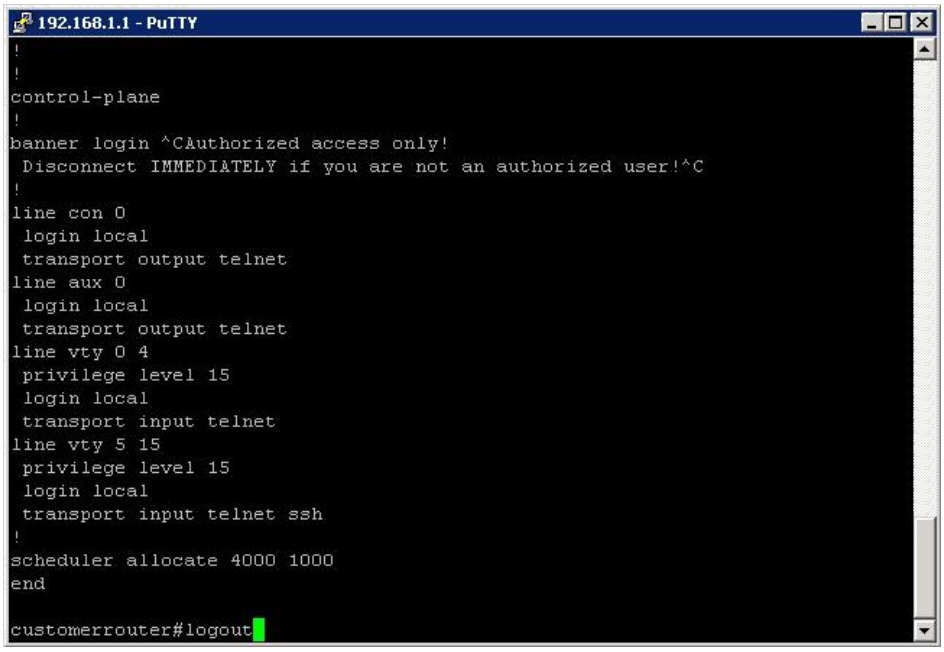
Примечание. Нет необходимости переключаться с пользовательского режима на привилегированный, поскольку после назначения настроек в SDM Express и SDM привилегированный режим становится режимом по умолчанию.

б. Нажмите клавишу **ПРОБЕЛ**, чтобы прокрутить текущую конфигурацию маршрутизатора.



Шаг 5. Выход из маршрутизатора Cisco 1841 с интегрированными сетевыми службами

Чтобы выйти из маршрутизатора после завершения проверки конфигурации, введите команду **logout** в командной строке привилегированного режима и нажмите **ВВОД**.



Шаг 6. Вопросы для повторения

а. Назовите преимущества и недостатки протоколов Telnet и SSH.

_____

_____

б. Каков порт по умолчанию для протокола SSH? _____ Каков порт по умолчанию для Telnet? _____

_____

_____

в. Какая версия ОС Cisco IOS была отображена в текущей конфигурации?

_____

_____

Практическая работа 2 Работа с IP маршрутизацией и протоколами маршрутизации

Создание схемы сети на основе таблиц маршрутизации

Цели

- Истолковать выходные данные маршрутизаторов;
- Определить сети и IP-адреса для каждого маршрутизатора;
- Составить схему сетевой топологии;
- Продумать и составить документ о внедрении сети.

Предварительная информация/подготовка

В этой практической работе необходимо создать схему сетевой топологии, исходя только из результата команды **show ip route** двух маршрутизаторов. Команда **show ip route** отображает текущее состояние таблицы маршрутизации. Маршрутизаторы M1 и M2 напрямую подключены к ГВС-каналу и оба работают по протоколу динамической маршрутизации. Кроме ГВС-канала,
каждый из маршрутизаторов подключен к своим локальным сетям.

Шаг 1. Анализ записей таблицы маршрутизации для маршрутизатора M1

г. Проанализируйте результаты команды **show ip route** от маршрутизатора M1 представленные ниже.

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M
- mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA -
OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
       * - candidate default, U - per-user static route, o -
ODR
       P - periodic downloaded static

route Gateway of last resort is not set

C    172.17.0.0/16 is directly connected, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C192.168.2.0/24 is directly connected, FastEthernet0/1
R192.168.3.0/24 [120/1] via 172.17.0.2, 00:00:17, Serial0/0
R    192.168.4.0/24 [120/1] via 172.17.0.2, 00:00:17, Serial0/0
```

д. Сколько сетей известны маршрутизатору M1? _____

е. Сколько сетей подключено напрямую к этому маршрутизатору? _____

ж. О скольких сетях сведения были получены от другого маршрутизатора? _____

з. Используя коды в начале результатов команды show ip route, скажите, что означает «R»? Данные об этой сети были получены через протокол маршрутизации; сеть не связана напрямую с интерфейсом этого маршрутизатора.

и. Какому устройству принадлежит IP-адрес 172.17.0.2 в маршрутах, определенных через протокол RIP? _____

к. К какому устройству относится Serial0/0 и что оно обозначает в маршрутах, полученных по протоколу RIP? _____

Шаг 2. Анализ записей таблицы маршрутизации для маршрутизатора M2

л. Проанализируйте результаты команды **show ip route** от маршрутизатора M2 представленные ниже.

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M
- mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA -
OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
       * - candidate default, U - per-user static route, o -
ODR
       P - periodic downloaded static

route Gateway of last resort is not set

C    172.17.0.0/16 is directly connected, Serial0/0
R    192.168.1.0/24 [120/1] via 172.17.0.1, 00:00:17, Serial0/0
R192.168.2.0/24 [120/1] via 172.17.0.1, 00:00:17, Serial0/0
C192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, FastEthernet0/1
```

м. Сколько сетей известны маршрутизатору M2? _____

н. Сколько сетей подключено напрямую к этому маршрутизатору? _____

о. О скольких сетях сведения были получены от другого маршрутизатора? _____

п. Какому устройству принадлежит IP-адрес 172.17.0.1 в маршрутах, определенных через протокол RIP? _____

р. К какому устройству относится Serial0/0 и что оно обозначает в маршрутах, полученных по протоколу RIP? _____

Шаг 3. Документирование интерфейсов маршрутизаторов и IP-адресов

c. Пользуясь результатами команды **show ip route** от маршрутизаторов M1 и M2, заполните таблицу, указав имя маршрутизатора, имена всех используемых интерфейсов и их IP-адреса и маски подсетей. Используйте первый доступный IP-адрес для каждого из интерфейсов локальной сети FastEthernet.

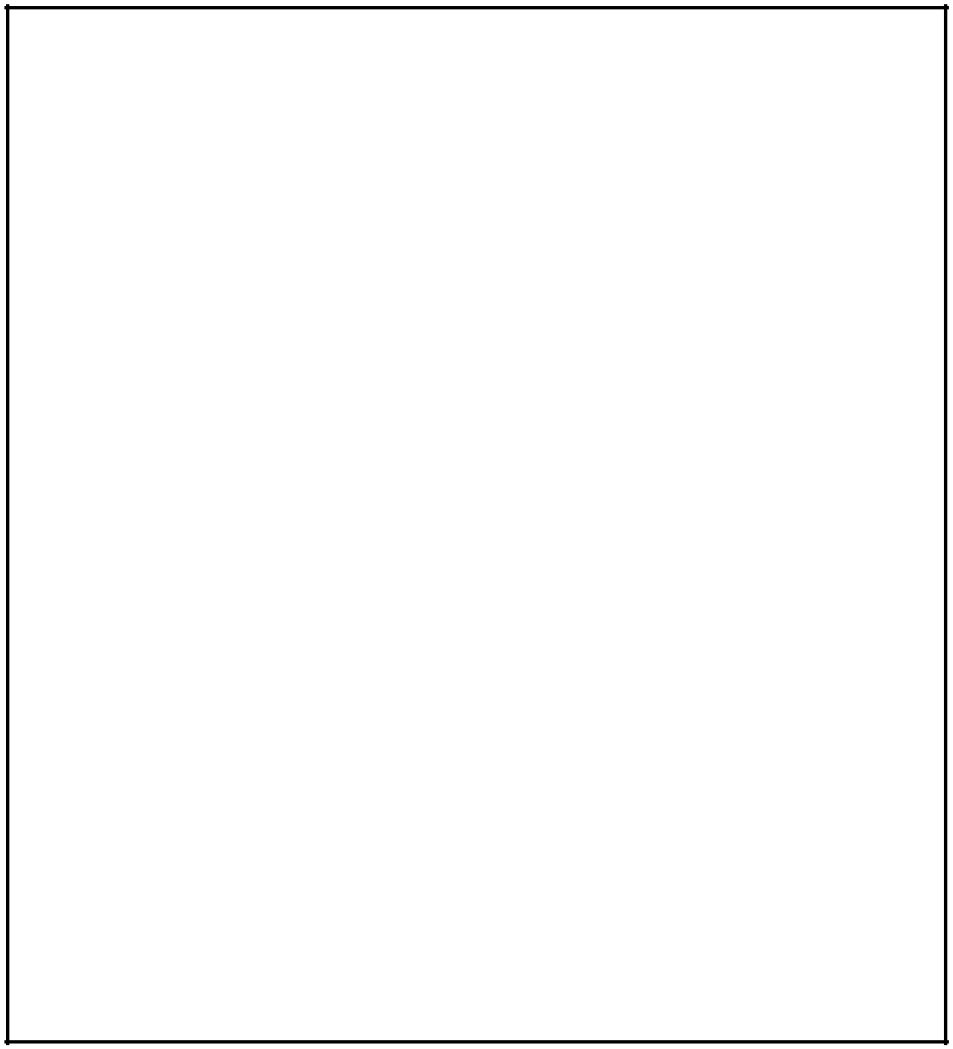
Название устройства	**Интерфейс**	**IP-адрес**	**Маска подсети (десятичное представл. с точками и /xx)**
M1			
M1			
M1			
M2			
M2			
M2			

т. Исходя из этого примера, скажите, можно ли на основе таблиц маршрутизации определить точный IP-адрес всех интерфейсов маршрутизатора? ____

у. Какие IP-адресы интерфейсов маршрутизаторов можно определить на основе таблиц маршрутизации? _____

Шаг 4. Создание схемы сетевой топологии.

На основе результатов команды **show ip route** от маршрутизаторов M1 и M2, а также введенных вами сведений таблицы нарисуйте топологию сети. Обязательно включите все устройства, подключения, интерфейсы, IP-адреса, маски подсетей и номера сетей.



Шаг 5. Вопросы для повторения

а. Как вы думаете, что случится с записями в таблице маршрутизации для M1, если одна из сетей Ethernet маршрутизатора M2 будет отключена?

_____

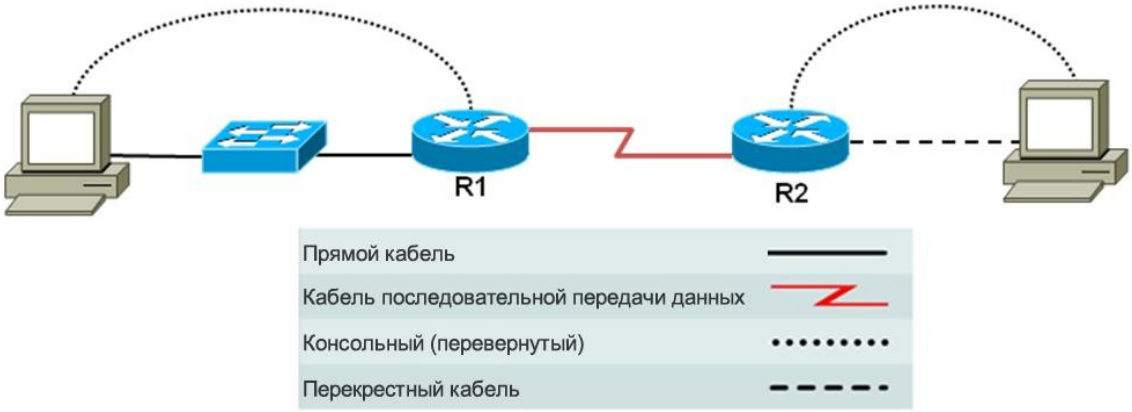
_____

б. Как вы думаете, что случится с записями в таблицах маршрутизации для M1 и M2, если последовательный интерфейс в M2 будет отключен?

_____

_____

Конфигурация RIP и ее проверка



Обозначение маршрутизатора	Название маршру-тизатора	Адрес интерфейса Fast Ethernet 0	Адрес последовательного интерфейса 0	Тип интерфейса	Маска подсети для обоих интерфейсов
Маршрутизатор 1	M1	172.16.0.1	172.17.0.1	DCE	255.255.0.0
Маршрутизатор 2	M2	172.18.0.1	172.17.0.2	DTE	255.255.0.0

Задача

- Реализовать маршрутизацию RIP и убедиться, что выполняется динамическая замена сетевых маршрутов.

Основная информация/подготовка

Организуйте сеть, аналогичную той, что изображена на диаграмме выше. Можно использовать любой маршрутизатор или сочетание маршрутизаторов, соответствующее требованиям интерфейса на диаграмме (например, маршрутизаторы 800, 1600, 1700, 1800, 2500 или 2600). См. таблицу в конце этой практической работы для определения правильных идентификаторов интерфейса с учетом оборудования в аудитории. В зависимости от модели маршрутизатора выходные данные могут несколько отличаться от выходных данных, приведенных в этой практической работе. Предполагается, что все этапы этой практической работы следует выполнить для каждого из маршрутизаторов, если не указано иное.

До начала практической работы начните сессию Гипертерминала.

ПРИМЕЧАНИЕ. До перехода к следующему шагу выполните для каждого маршрутизатора инструкции по удалению и перезагрузке, приведенные в конце этой практической работы.

Необходимо использовать следующие ресурсы:

- два маршрутизатора, каждый из которых имеет интерфейс Ethernet и последовательный интерфейс (по возможности не следует использовать SDM-маршрутизаторы, поскольку требуемая начальная конфигурация SDM удаляется при удалении начальной конфигурации);
- два компьютера с установленной системой Windows XP;
- прямой кабель Ethernet 5-ой категории (между ПК1 и коммутатором);
- перекрещенный кабель Ethernet 5-ой категории (между ПК2 и маршрутизатором M1);
- нуль-модемный кабель для последовательного порта;
- консольные кабели (от ПК1 и ПК2 к маршрутизаторам M1 и M2);
- доступ к командной строке ПК;
- доступ к сетевой конфигурации TCP/IP ПК.

Шаг 1. Создайте сеть и настройте маршрутизаторы

ф. Создайте сеть, как изображено на диаграмме топологии.

х. В режиме глобальной конфигурации настройте имена узлов, как изображено на схеме в диаграмме топологии. Далее настройте интерфейсы в соответствии со схемой. Можно использовать либо интерфейс командной строки, либо графический пользовательский интерфейс диспетчера устройств защиты, если он имеется.

ПРИМЕЧАНИЕ. При возникновении сложностей с основной конфигурацией маршрутизатора см. практическую работу 5.3.5. В этой практической работе приведены инструкции по использованию интерфейса командной строки Cisco IOS.

Шаг 2. Проверьте записи таблицы маршрутизации

а. Используйте команду **show ip route** для просмотра таблицы IP-маршрутизации маршрутизатора M1:

```
R1>show ip route
<output omitted>
Gateway of last resort is not set
C 172.16.0.0/16 is directly connected, FastEthernet0/0 C
172.17.0.0/16 is directly connected, Serial0/0/0
```

б. Что означает символ «C» слева от сетевых записей 172.16.0.0 и 172.17.0.0 в таблице маршрутизации?

_____

Шаг 3. Настройте на маршрутизаторах протокол маршрутизации

Существует две версии RIP: версия 1 и версия 2. В этой конфигурации необходимо указать вторую версию RIP (RIPv2), поскольку это самая последняя версия. На некоторых маршрутизаторах версия RIPv2 выбирается по умолчанию, но в этом случае не следует считать это аксиомой.

а. В режиме глобальной конфигурации введите на маршрутизаторе M1 следующие команды:

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 172.16.0.0
R1(config-router)#network 172.17.0.0
R1(config-router)#exit
R1(config)#exit
```

б. Сохраните конфигурацию маршрутизатора M1:

```
R1#copy running-config startup-config
```

в. В режиме глобальной конфигурации введите на маршрутизаторе M2 следующие команды:

```
R2(config)#router rip version 2
R2(config-router)#version 2
R2(config-router)#network 172.17.0.0
R2(config-router)#network 172.18.0.0
R2(config-router)#exit
R2(config)#exit
```

г. Сохраните конфигурацию маршрутизатора M2:

```
R2#copy running-config startup-config
```

Шаг 4. Настройте правильный IP-адрес, маску подсети и шлюз по умолчанию для узлов

а. Настройте для узла, подсоединенного к маршрутизатору M1, IP-адрес, маску подсети и шлюз по умолчанию, совместимые с IP-адресом интерфейса Fast Ethernet (172.16.0.0).

б. Настройте для узла, подсоединенного к маршрутизатору M2, IP-адрес, маску подсети и шлюз по умолчанию, совместимые с IP-адресом интерфейса Fast Ethernet (172.18.0.0).

в. Убедитесь в том, что межсетевое взаимодействие осуществляется, послав эхо-запрос на интерфейс Fast Ethernet другого маршрутизатора.

г. Можно ли с узла, подсоединенного к маршрутизатору M1, послать эхо-запрос на интерфейс Fast Ethernet маршрутизатора M2?

_____

д. Можно ли с узла, подсоединенного к маршрутизатору M2, послать эхо-запрос на интерфейс Fast Ethernet маршрутизатора M1?

_____

е. Если ответы на оба вопроса отрицательны, выполните поиск и устранение ошибок в конфигурации маршрутизатора. После этого повторно выполните эхо-запрос, пока ответы на оба вопроса не станут утвердительными. Обязательно проверьте физические кабели на наличие неисправностей, а также неверные подключения, чтобы убедиться, что используются кабели подходящего типа.

Шаг 5. Отобразите таблицы маршрутизации для каждого маршрутизатора

а. В режиме полного доступа или в привилегированном режиме EXEC изучите записи таблицы маршрутизации, введя на маршрутизаторе M1 команду **show ip route**.

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M
- mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA -
OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF
NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2,
E-EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia
- IS-IS inter area
       * - candidate default, U - per-user static route, o -
ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    172.17.0.0/16 is directly connected, Serial0/0
C    172.16.0.0/16 is directly connected, FastEthernet0/0
R 172.18.0.0/16 [120/1] via 172.17.0.2, 00:00:17,
Serial0/0
```

б. Какие записи содержатся в таблице маршрутизации маршрутизатора M1?

_____

_____

в. Что означает символ «C» слева от сетевой записи 172.18.0.0 в таблице маршрутизации?

_____

г. Что означает для этого сетевого маршрута «via 172.17.0.2»?

_____

д. Что означает для этого сетевого маршрута «Serial0/0»?

_____

е. Изучите таблицы маршрутизации, введя на маршрутизаторе M2 команду **show ip route**.

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M
- mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA -
OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia
- IS-IS inter area
       * - candidate default, U - per-user static route, o -
ODR
       P - periodic downloaded static

route Gateway of last resort is not set

C    172.17.0.0/16 is directly connected, Serial0/0
R    172.18.0.0/16 [120/1] via 172.17.0.2, 00:00:13, Serial0/0
C    172.18.0.0/16 is directly connected, FastEthernet0/0
```

ж. Какие записи содержатся в таблице маршрутизации маршрутизатора M2?

_____

_____

Шаг 6. Используйте процедуру отладки для наблюдения за обменом данными по протоколу RIP

Используя команду **debug ip rip**, можно в реальном времени наблюдать процесс обмена данными и передачу обновлений между маршрутизаторами, на которых используется протокол RIP.

ПРИМЕЧАНИЕ. При запуске команды отладки значительно повышается нагрузка на процессор маршрутизатора. По возможности не используйте команду отладки в производственной сети.

а. На маршрутизаторе M1 в привилегированном режиме EXEC введите команду **debug ip rip**. Изучите процесс обмена маршрутами между двумя маршрутизаторами. Выходные данные должны выглядеть аналогично данным, приведенным здесь.

```
R1#debug ip rip
RIP protocol debugging is on
R1#
00:51:28: RIP: sending v2 update to 224.0.0.9 via Serial0/0
(172.17.0.1)
00:51:28: RIP: build update entries
00:51:28:       172.16.0.0/16 via 0.0.0.0, metric 1, tag 0
00:51:49: RIP: received v2 update from 172.17.0.2 on Serial0/0
00:51:49:      172.18.0.0/16 via 0.0.0.0 in 1 hops
00:51:57: RIP: sending v2 update to 224.0.0.9
via FastEthernet0/0 (172.16.0.1)
00:51:57: RIP: build update entries
00:51:57:       172.17.0.0/16 via 0.0.0.0, metric 1, tag 0
00:51:57:       172.18.0.0/16 via 0.0.0.0, metric 2, tag 0
```

б. Для прекращения процедуры отладки введите команду **undebug all**.

```
R1#undebug all
All possible debugging has been turned off
R1#
```

в. Через какой интерфейс маршрутизатор M1 передает и получает обновления? _____

г. Почему метрика маршрута на адрес 172.17.0.0 равна 1, а метрика маршрута на адрес 172.18.0.0 равна 2?

_____Выйдите из системы, введя команду **exit**, и выключите маршрутизатор.

Шаг 7. Вопросы для повторения

а. Что, по вашему мнению, случится с таблицей маршрутизации на маршрутизаторе M1 при нарушениях в работе сети Ethernet на маршрутизаторе M2?

_____

_____

б. Что, по вашему мнению, произойдет, если на маршрутизаторе M1 настроить использование версии RIPv1, а на маршрутизаторе M2 настроено использование версии RIPv2?

_____

_____

Удаление и перезагрузка маршрутизатора

а. Перейдите к привилегированному режиму EXEC, введя команду **enable**:

```
Router>enable
```

б. В привилегированном режиме EXEC введите команду **erase startup-config**:

```
Router#erase startup-config
```

После этого отображается следующее сообщение:

```
Erasing the nvram filesystem will remove all files! Continue?
[confirm]
```

в. Для подтверждения нажмите **«Ввод»**.

После этого отображается:

```
Erase of nvram: complete
```

г. В привилегированном режиме EXEC введите команду **reload**:

```
Router(config)#reload
```

После этого отображается следующее сообщение:

```
System configuration has been modified. Save? [yes/no]:
```

д. Введите **n**, а затем нажмите **«Ввод»**.

После этого отображается следующее сообщение:

```
Proceed with reload? [confirm]
```

е. Для подтверждения нажмите **«Ввод»**.

Сначала отображается следующий ответ:

```
Reload requested by console.
```

После перезагрузки маршрутизатора отображается следующее сообщение:

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

ж. Введите **n**, а затем нажмите **«Ввод»**.

После этого отображается следующее сообщение:

```
Press RETURN to get started!
```

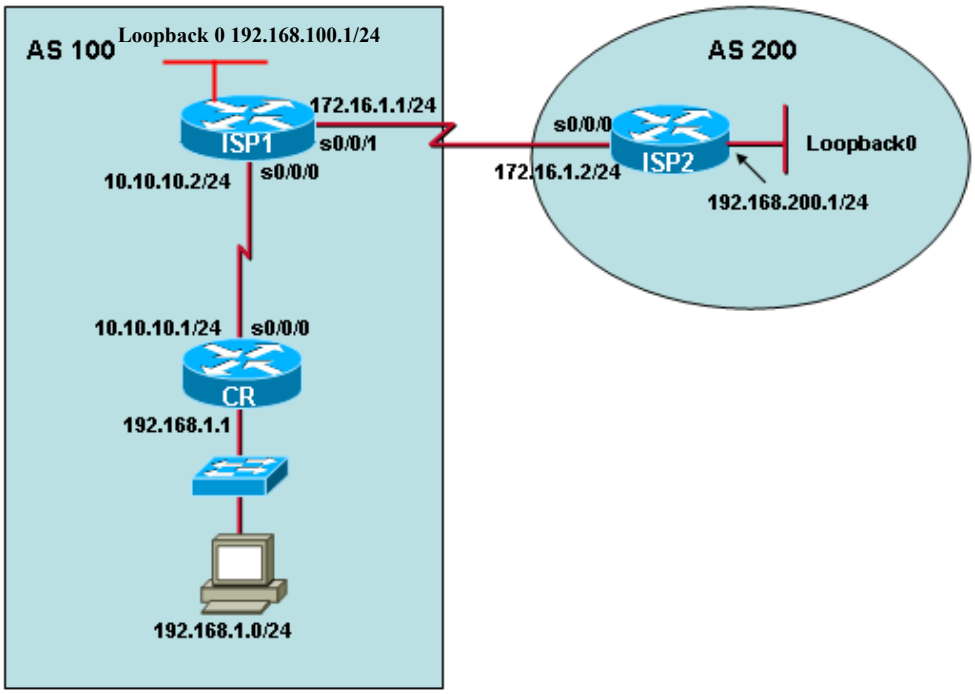
з. Нажмите **«Ввод»**.

Маршрутизатор готов к выполнению практической работы.

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet №1**	**Интерфейс Ethernet №2**	**Последовательный интерфейс №1**	**Последовательный интерфейс №2**
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)

Чтобы точно узнать, каким образом настроен маршрутизатор, посмотрите на интерфейсы. Это позволит определить тип маршрутизатора, а также число используемых интерфейсов. Невозможно эффективно перечислить все сочетания настроек для маршрутизатора каждого класса. Здесь приводятся идентификаторы возможных комбинаций интерфейсов в устройстве. Эта схема интерфейсов не включает в себя никакие другие типы интерфейса, даже если в определенном маршрутизаторе такой имеется. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это официальное сокращение, которое можно использовать в команде Cisco IOS для обозначения интерфейса.

Настройка протокола BGP для использования маршрутизации по умолчанию



Задачи

- Настроить на маршрутизаторе клиента внутреннюю сеть, которая будет объявлена Поставщиком услуг Интернета 1 с использованием протокола BGP.
- Настроить протокол BGP для обмена информацией маршрутизации между поставщиком услуг Интернета 1 (ISP1) в AS 100 и поставщиком услуг Интернета 2 (ISP2) в AS 200.

Основная информация/подготовка

Небольшой компании необходим доступ к Интернету. Они договорились о предоставлении услуг с местным поставщиком услуг Интернета (ISP1). Поставщик услуг Интернета (ISP1) подключается к Интернету через другого поставщика услуг Интернета (ISP2), используя внешний протокол маршрутизации. Самым популярным протоколом маршрутизации, используемым в Интернете между разными поставщиками услуг Интернета, является протокол BGP4. В этой практической работе необходимо подключить маршрутизатор клиента к поставщику услуг Интернета, используя маршрут по умолчанию, а поставщик услуг Интернета ISP1 должен подключиться к поставщику услуг Интернета ISP2 через протокол BGP4.

Необходимо использовать следующие ресурсы:

- маршрутизатор клиента (1841 или другой);
- коммутатор (дополнительно, если между ПК и маршрутизатором клиента используется перекрещенный кабель);
- 2 маршрутизатора поставщиков услуг Интернета (1841 или другие маршрутизаторы, поддерживающие протокол BGP);
- ПК, на котором установлена программа эмуляции терминала;
- консольный кабель для настройки маршрутизаторов;
- доступ к командной строке ПК;
- доступ к сетевой конфигурации TCP/IP ПК.

На ПК начните сессию гипертерминала для связи с каждым маршрутизатором.

ПРИМЕЧАНИЕ. Перейдите к инструкциям по удалению и перезагрузке маршрутизатора в конце этой практической работы. До продолжения работы выполните эти шаги для всех маршрутизаторов, используемых в этой практической работе.

ПРИМЕЧАНИЕ. Маршрутизаторы SDM. Если для маршрутизатора SDM удалена начальная конфигурация, при перезагрузке маршрутизатора SDM он перестает отображаться по умолчанию. Необходимо создать основную конфигурацию маршрутизатора с использованием команд IOS. См. процедуру в конце этой практической работы или обратитесь к преподавателю.

Шаг 1. Настройте на каждом из маршрутизаторов основные сведения

а. Создайте и настройте сеть в соответствии с диаграммой топологии, но не настраивайте протокол маршрутизации. При необходимости см. инструкции по настройке имени узла, паролей и адресов интерфейсов в практической работе 5.3.5. «Настройка основных параметров маршрутизатора с использованием интерфейса командной строки IOS».

б. Настройте IP-адрес и маску подсети узла в сети клиента таким образом, чтобы они были полностью совместимы с интерфейсом FastEthernet маршрутизатора CR с использованием шлюза по умолчанию 192.168.1.1.

в. Для проверки подключения между соединенными напрямую маршрутизаторами используйте команду **ping**. Смог ли маршрутизатор CR получить доступ к маршрутизатору ISP2? _____ Смог ли узел клиента получить доступ к ISP1? _____

г. Настройте интерфейс loopback, используя IP-адрес для маршрутизаторов ISP1 и ISP2, как изображено на диаграмме топологии. Интерфейс loopback — это виртуальный интерфейс, имитирующий реальную сеть для проведения тестирования. Настройте интерфейс Loopback на маршрутизаторе ISP1.

```
ISP1>enable
ISP1#configure terminal
ISP1(config)#interface loopback0
ISP1(config-if)#ip address 192.168.100.1 255.255.255.0
```

д. Настройте интерфейс Loopback на маршрутизаторе ISP2.

```
ISP2>enable
ISP2#configure terminal
ISP2(config)#interface loopback0
ISP2(config-if)#ip address 192.168.200.1 255.255.255.0
```

Шаг 2. Настройте маршрут по умолчанию и статический маршрут

и. На маршрутизаторе CR настройте маршрут по умолчанию таким образом, чтобы пользователи получили доступ к поставщику услуг Интернета ISP1:

```
CR(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
```

б. На маршрутизаторе ISP1 настройте статический маршрут обратно в сеть клиента:

```
ISP1(config)#ip route 192.168.1.0 255.255.255.0 10.10.10.1
```

в. Протестируйте подключение, послав эхо-запрос с узла к поставщику услуг Интернета по адресу 10.10.10.2.

ПРИМЕЧАНИЕ. При невозможности послать эхо-запрос выполните, при необходимости, поиск и устранение проблем настройки и подключения маршрутизатора и ПК.

Шаг 3. Настройте на маршрутизаторах обоих поставщиков услуг Интернета протокол BGP

а. Настройте протокол BGP на маршрутизаторе ISP1:

```
ISP1(config)#router bgp 100
ISP1(config-router)#neighbor 172.16.1.2 remote-as 200
ISP1(config-router)#network 192.168.1.0
ISP1(config-router)#network
192.168.100.0 ISP1(config-router)#end
ISP1#copy running-config startup-config
```

ПРИМЕЧАНИЕ. Всегда рекомендуется часто сохранять конфигурацию, особенно после завершения основных шагов процесса настройки.

б. Настройте протокол BGP на маршрутизаторе ISP1:

```
ISP2(config)#router bgp 200
ISP2(config-router)#neighbor 172.16.1.1 remote-as 100
ISP2(config-router)#network
192.168.200.0 ISP2(config-router)#end
ISP2#copy running-config startup-
```

config Шаг 4. Просмотрите таблицы маршрутизации

Настройка протокола BGP завершена. Проверьте таблицы маршрутизации для каждого маршрутизатора

ПРИМЕЧАНИЕ. Выходные данные могут слегка различаться в зависимости от используемой модели маршрутизатора.

a. `ISP2#show ip route`

```
Codes: C — connected, S — static, I — IGRP, R — RIP, M
— mobile, B — BGP
       D — EIGRP, EX — EIGRP external, O — OSPF, IA —
OSPF inter area
       N1 — OSPF NSSA external type 1, N2 — OSPF NSSA external
type 2
       E1 — OSPF external type 1, E2 — OSPF external type 2, E
— EGP
       i — IS-IS, L1 — IS-IS level-1, L2 — IS-IS level-2, ia
— IS-IS inter area
       * — candidate default, U — per-user static route, o —
ODR
       P — periodic downloaded static

route Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Serial0/0
C    192.168.200.0/24 is directly connected, Loopback0
B192.168.1.0/24 [20/0] via 172.16.1.1, 00:40:38
B    192.168.100.0/24 [20/0] via 172.16.1.1, 00:40:38
```

1) Имеется ли в таблице маршрутизации ISP2 адрес сети 192.168.1.0? _____
2) Какая буква отображается слева от записи для 192.168.1.0? ____
3) Что означает эта буква? _____
4) Есть ли в таблице маршрутизации сеть 192.168.100.0? _____
5) Какой маршрутизатор объявил сеть 192.168.1.0? _____

б. ISP1#**show ip route**

к. Codes: C — connected, S — static, I — IGRP, R — RIP, M — mobile, B — BGP

л. D — EIGRP, EX — EIGRP external, O — OSPF, IA — OSPF inter area

м. N1 — OSPF NSSA external type 1, N2 — OSPF NSSA external type 2

н. E1 — OSPF external type 1, E2 — OSPF external type 2, E — EGP

о. i — IS-IS, L1 — IS-IS level-1, L2 — IS-IS level-2, ia — IS-IS inter area

п. * — candidate default, U — per-user static route, o — ODR

р. P — periodic downloaded static route

с.

т. Gateway of last resort is not set

у.

ф. 172.16.0.0/24 is subnetted, 1 subnets

х. C 172.16.1.0 is directly connected, Serial0/1

ц. B 192.168.200.0/24 [20/0] via 172.16.1.2, 00:33:45 ч.

10.0.0.0/24 is subnetted, 1 subnets

ш. C 10.10.10.0 is directly connected, Serial0/0

щ. S 192.168.1.0/24 [1/0] via 10.10.10.1

ы. C 192.168.100.0/24 is directly connected, Loopback0

э.

1) О какой сети (сетях) поставщик услуг Интернета ISP1 узнал от поставщика услуг Интернета ISP2? _____

2) Каким образом поставщик услуг ISP1 узнал о сети 192.168.1.0?

_____

_____

3) Объявляет ли ISP1 какие-либо сети на маршрутизатор клиента? _____

в. CR#**show ip route**

```
Codes: C — connected, S — static, I — IGRP, R — RIP, M
— mobile, B — BGP
       D — EIGRP, EX — EIGRP external, O — OSPF, IA —
OSPF inter area
       N1 — OSPF NSSA external type 1, N2 — OSPF NSSA external
type 2
       E1 — OSPF external type 1, E2 — OSPF external type 2, E
— EGP
       i — IS-IS, L1 — IS-IS level-1, L2 — IS-IS level-2, ia
— IS-IS inter area
       * — candidate default, U — per-user static route, o —
ODR
       P — periodic downloaded static route

Gateway of last resort is 10.10.10.2 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.10.10.2
```

1) Почему сети 192.168.100.0 и 192.168.200.0 отсутствуют в таблице маршрутизации маршрутизатора CR?

Шаг 5. Проверьте подключения

а. Направьте эхо-запрос с узла в сети Ethernet клиента на интерфейс Loopback поставщика услуг Интернета ISP2.

б. Направьте эхо-запрос с маршрутизатора ISP2 на узел в сети Ethernet клиента.

ПРИМЕЧАНИЕ. При невозможности послать эхо-запрос выполните, при необходимости, поиск и устранение проблем настройки и подключения маршрутизатора и ПК.

Шаг 6. Просмотр сведений BGP на маршрутизаторе поставщика услуг Интернета

а. На маршрутизаторе ISP1 просмотрите маршрутизацию BGP.

```
ISP1#show ip bgp
BGP table version is 4, local router ID is 192.168.100.1
Status codes: s suppressed, d damped, h history, * valid,
> best,
i — internal
Origin codes: i — IGP, e — EGP, ? — incomplete

   Network          Next Hop            Metric LocPrf Weight
Path
*> 192.168.1.0      10.10.10.1               0         32768
i
*> 192.168.100.0    0.0.0.0                  0         32768
i
*> 192.168.200.0    172.16.1.2               0             0

200 i
```

б. На маршрутизаторе ISP2 просмотрите маршрутизацию BGP.

```
ISP2#show ip bgp
BGP table version is 4, local router ID is 192.168.200.1
Status codes: s suppressed, d damped, h history, * valid,
> best,
i — internal
Origin codes: i — IGP, e — EGP, ? — incomplete

   Network          Next Hop            Metric LocPrf Weight
Path
*> 192.168.1.0      172.16.1.1               0             0
100 i
*> 192.168.100.0    172.16.1.1               0             0
100 i
*> 192.168.200.0    0.0.0.0                  0         32768

i
```

Шаг 7. Вопросы для повторения

Почему ISP1 не объявляет никакие сети на маршрутизатор клиента?

_____

_____

Удаление и перезагрузка маршрутизатора

а. Перейдите к привилегированному режиму EXEC, введя команду **enable**.

```
Router>enable
```

в. В привилегированном режиме EXEC введите команду **erase startup-config**.

```
Router#erase startup-config
```

После этого отображается следующее сообщение:

```
Erasing the nvram filesystem will remove all files! Continue?
[confirm]
```

г. Для подтверждения нажмите **«Ввод»**.

После этого отображается:

```
Erase of nvram: complete
```

д. В привилегированном режиме EXEC введите команду **reload**.

```
Router(config)#reload
```

После этого отображается следующее сообщение:

```
System configuration has been modified. Save? [yes/no]:
```

е. Введите **n**, а затем нажмите **«Ввод»**.

После этого отображается следующее сообщение:

```
Proceed with reload? [confirm]
```

ж. Для подтверждения нажмите **«Ввод»**.

Сначала отображается следующий ответ:

```
Reload requested by console.
```

После перезагрузки маршрутизатора отображается следующее сообщение:

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

з. Введите **n**, а затем нажмите **«Ввод»**.

После этого отображается следующее сообщение:

```
Press RETURN to get started!
```

и. Нажмите **Enter**.

Маршрутизатор готов к выполнению практической работы.

Практическая работа 3. Службы поставщиков

услуг Изменение файла HOSTS (УЗЛЫ) в Windows

Задание

- Изменить локальный файл HOSTS (УЗЛЫ) в ОС Windows PC, чтобы отобразить имя на IP-адрес, упростив тем самым идентификацию.

Предварительная информация/подготовка

Вы работаете в компании ИСП. Вас посылают на объект клиента для поиска и устранения неполадок, касающихся одного из серверов клиента. Известно, что есть пользователь сети, которому постоянно необходим доступ к серверу для администрирования веб-сайта, разрабатываемого компанией. На текущий момент у клиента нет локальных серверов, выполняющих функцию связи имени с IP-адресом сервера. Однако веб-сайту, над которым работает клиент, требуется использование имени в URL-адресе, чтобы клиент мог получить надлежащий к нему доступ. Поскольку это единственная рабочая станция, которой необходим доступ к серверу на основе имени, вы решаете использовать файл HOSTS (УЗЛЫ) на рабочей станции под управлением Windows, чтобы устранить проблему с разрешением имени. Вы намерены изменить локальный файл HOSTS (УЗЛЫ) и добавить отображение имени для веб-сервера. Вы проверите функциональные возможности разрешения имени с помощью команды **ping** из приглашения для ввода команд.

Требуются следующие ресурсы:

- ПК, работающий под управлением Windows XP;
- Права администратора на этом ПК.

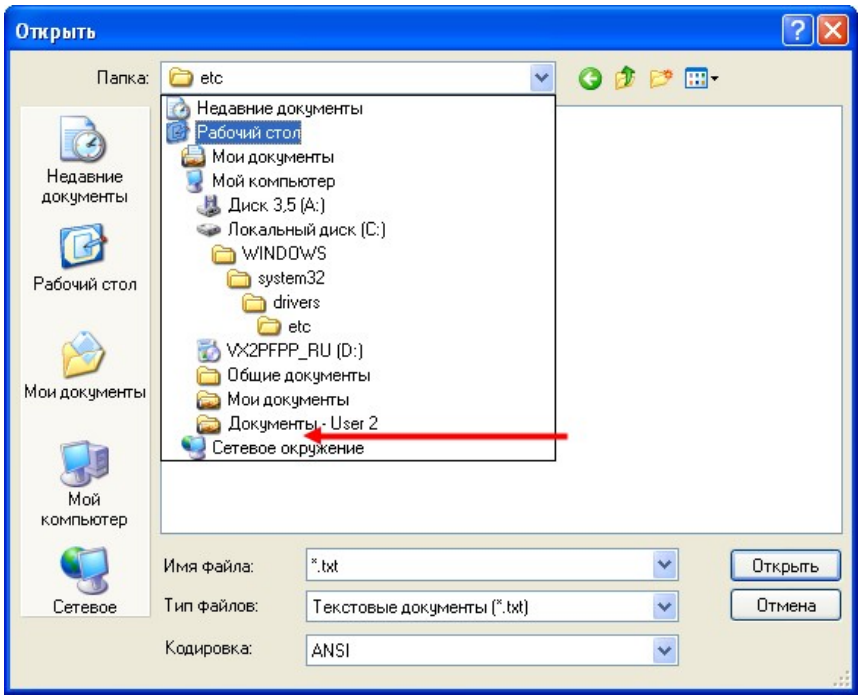
ПРИМЕЧАНИЕ. Вид экрана вашей ОС Windows может несколько отличаться от того, что представлен здесь, но процедура аналогична.

Шаг 1. Обнаружение файла HOSTS (УЗЛЫ) в Windows

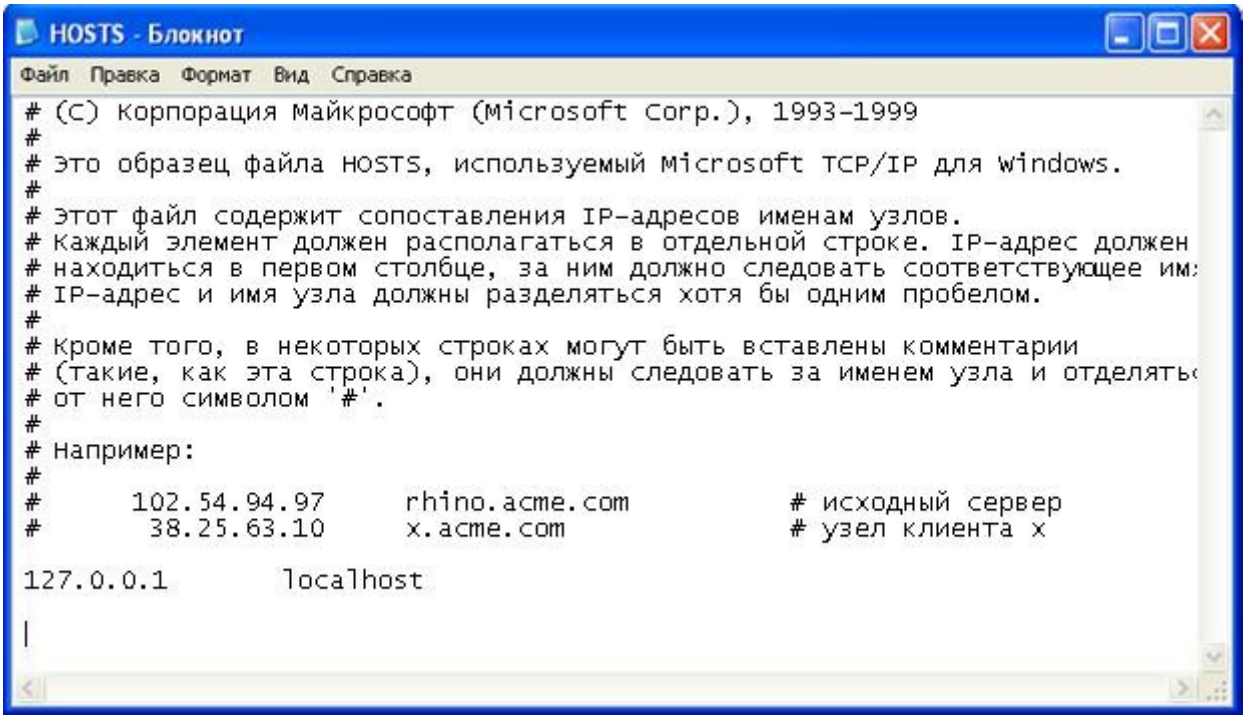
ю. Нажмите кнопку **Start (пуск)** и выберите **All Programs > Accessories (программы > Стандартные)**, после чего выберите программу **Notepad (блокнот)**.

я. В Notepad (блокнот) выберите **File > Open (файл > открыть)**. Измените **Files of Type** (**файлы типа)** на **All Files** (**все файлы)**, чтобы отобразить нетекстовые файлы. Перейдите по адресу C:\WINDOWS\SYSTEM32\DRIVERS\ETC.

аа. Выберите файл **HOSTS (УЗЛЫ)** и щелкните **Open (открыть)**.

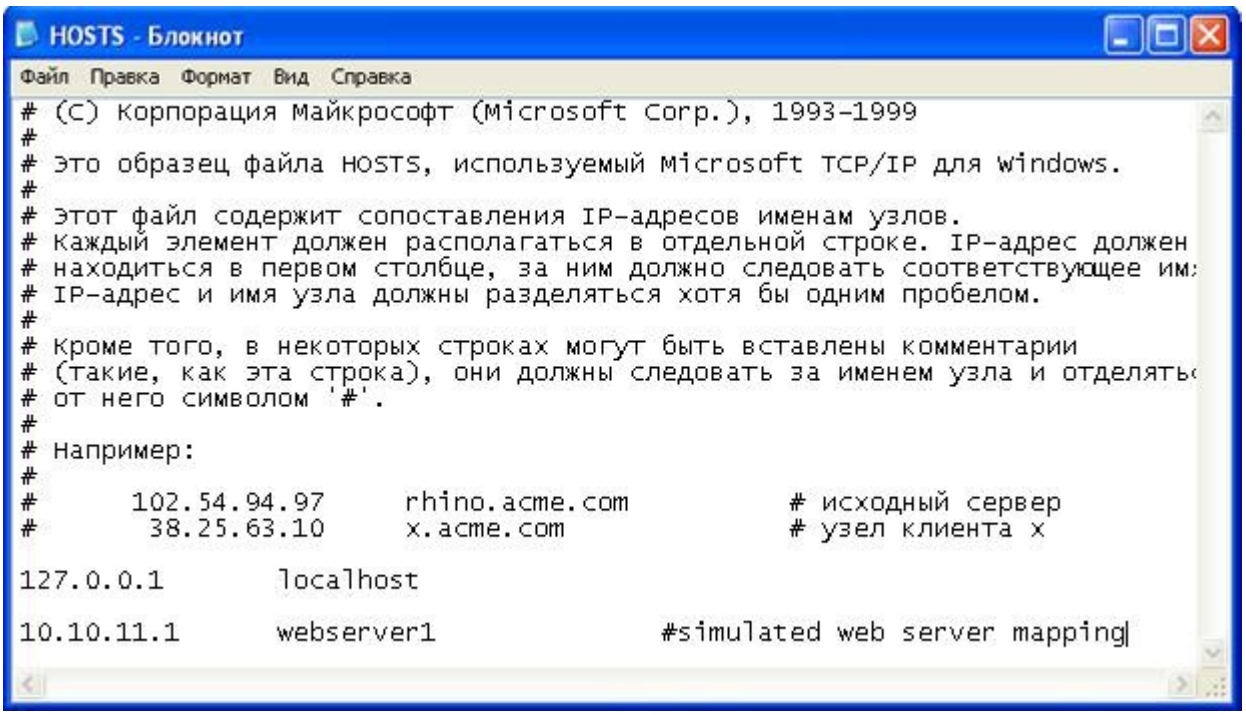


В Notepad (блокнот) откроется файл **HOSTS (УЗЛЫ)**.



Шаг 2. Изменение файла HOSTS (УЗЛЫ)

бб. В нижней части файла **HOSTS (УЗЛЫ)** находится перечень узлов, которые уже внесены. Добавьте новую запись для веб-сервера. Введите **10.10.11.1**, нажмите клавишу **Tab** и введите **webserver1**. Снова нажмите клавишу **Tab** и добавьте комментарий, перед которым ставится символ #. Символ # служит для обозначения комментария.



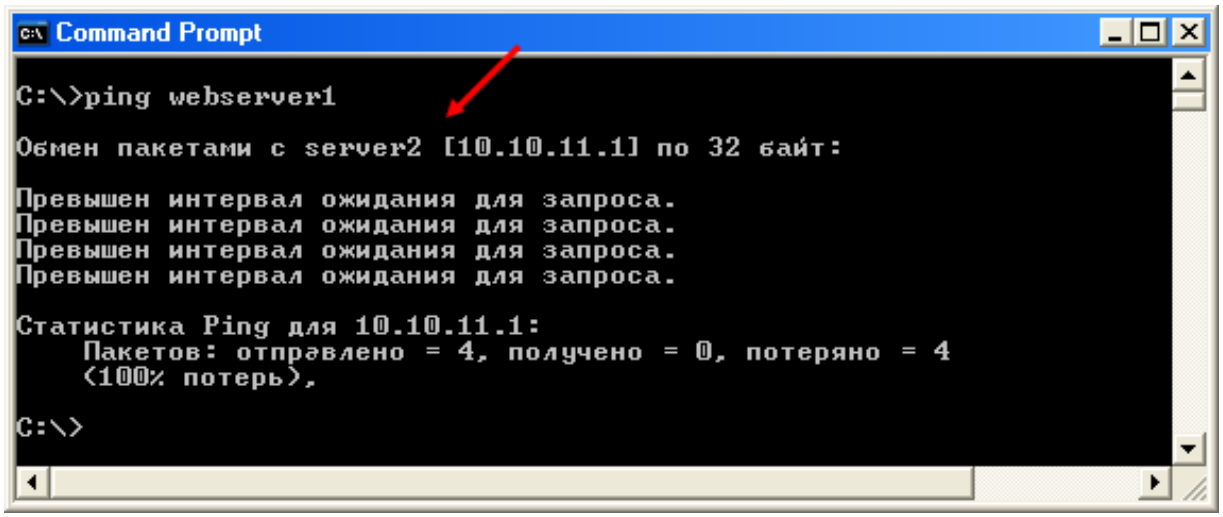
вв. Сохраните обновленный файл **HOSTS (УЗЛЫ)**.

Шаг 3. Проверка отображения нового имени

гг. Чтобы появилось приглашение для ввода команды, щелкните **Start (пуск)** и нажмите кнопку **Run (выполнить)**. В диалоговом окне **Run (выполнить)**, введите **CMD** и нажмите **OK**. Кроме того, чтобы открыть командное окно, можно выбрать **Start** > **All Programs** > **Accessories** > **Command Prompt (пуск** > **программы** > **стандартные** > **командная строка)**.

дд. В окне командной строки введите **ping webserver1** и нажмите клавишу **ВВОД**.

Имя **webserver1** было преобразовано в **10.10.11.1** непосредственно перед отправкой соответствующих эхо-запросов. Это означает, что файл **HOSTS (УЗЛЫ)** был успешно изменен и функционирует должным образом в процессе разрешения имен на данной рабочей станции. Поскольку эта процедура была имитацией, и в реальности webserver1 не существует, узел назначения недоступен. Если бы webserver1, доступный из данного узла, существовал, он, скорее всего, ответил бы на эхо-запрос.



Шаг 4. Вопросы для повторения

ее. Какие еще файлы расположены в папке **\ETC** с файлом **HOSTS (УЗЛЫ)**?

_____

_____

жж. Какой символ служит для обозначения комментария в файле **HOSTS (УЗЛЫ)**?

_____

Изучение кэшированной информации DNS на сервере Windows DNS Server

Задача

- Просмотреть кэшированную информацию DNS на сервере Windows DNS server после выполнения запроса DNS, поиск которого выполняется.

Основная информация/подготовка

В этой практической работе требуется изучить сведения, кэшированные на локальном DNS-сервере после выполнения поиска. На DNS-сервере можно будет увидеть настроенные корневые серверы. Кроме того, будет виден кэшированный верхний уровень и записи узлов на каждом уровне после завершения поиска. Важно понимать, что весь процесс поиска сведений с использованием разных уровней иерархии DNS выполняется всего лишь за доли секунды.

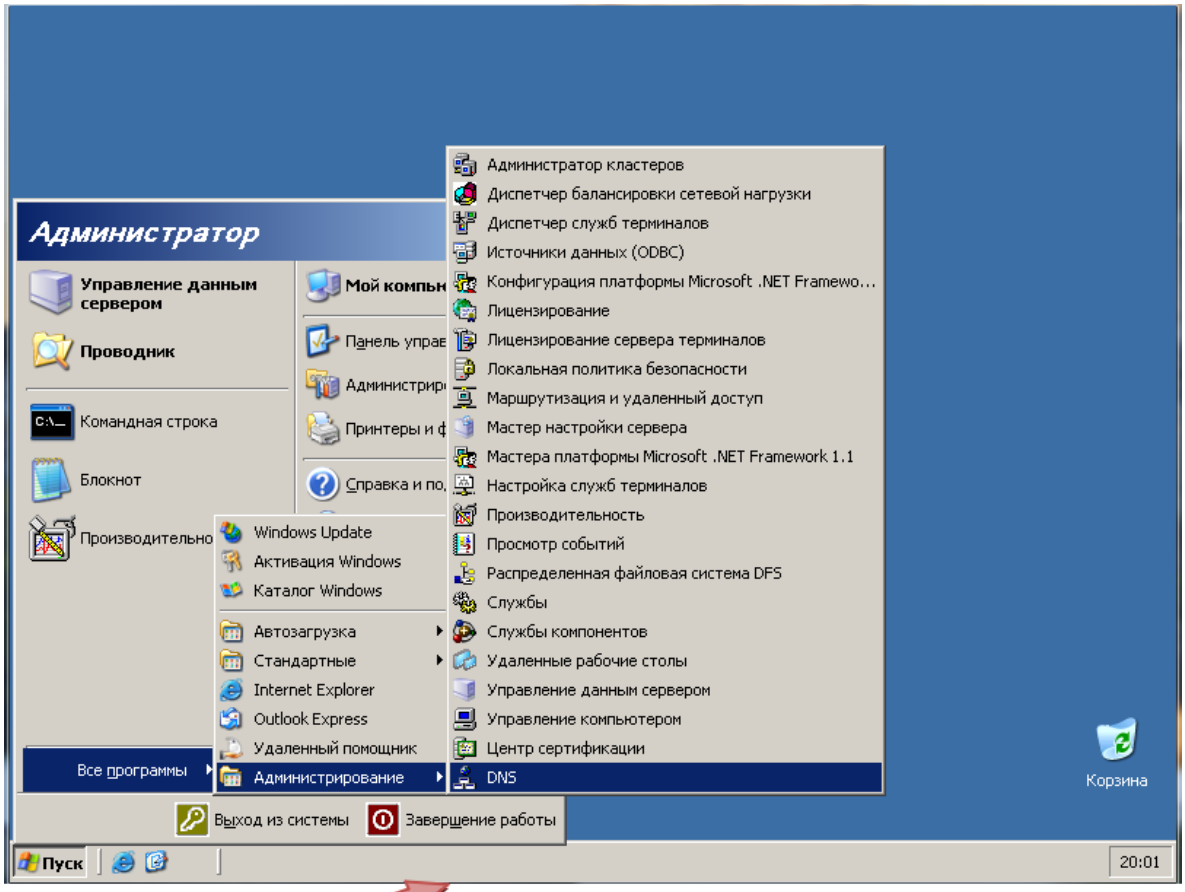
Необходимо использовать следующие ресурсы:

- сервер Windows 2003 Server, на котором запущен DNS;
- административный доступ к серверу;
- подключение к Интернету.

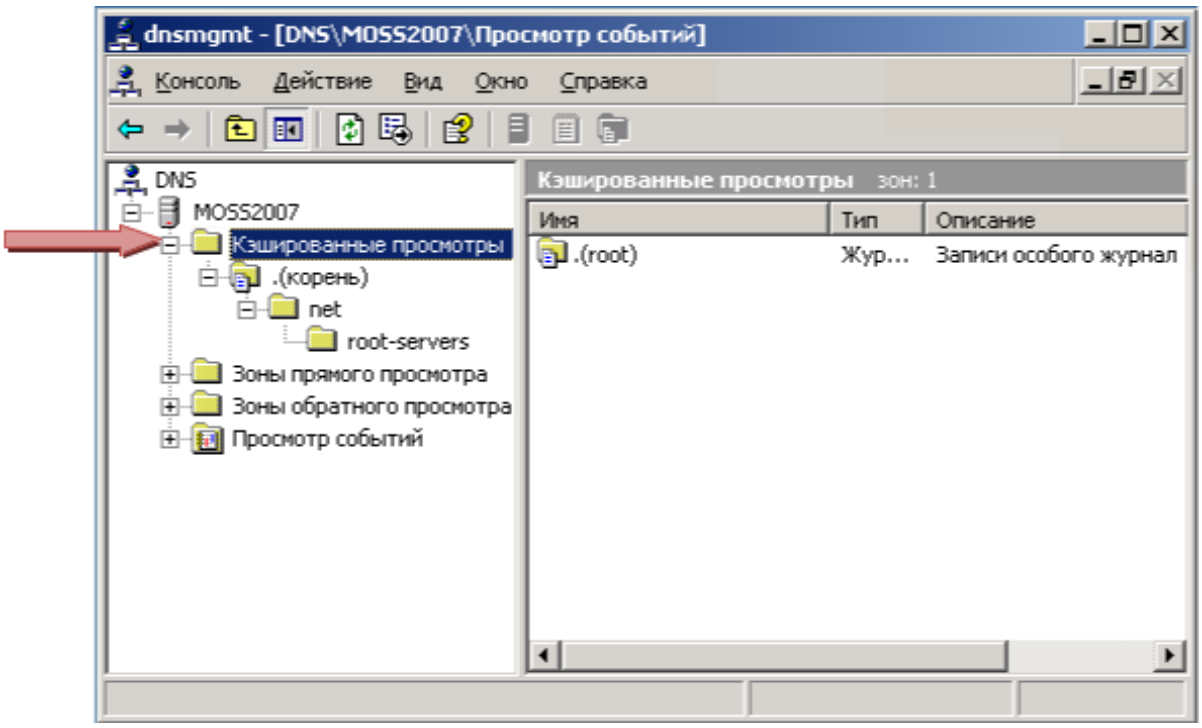
ПРИМЕЧАНИЕ. При отсутствии доступа к серверу Windows DNS преподаватель может продемонстрировать выполнение этой практической работы. Если отсутствует оборудование для выполнения этой практической работы, или ее невозможно продемонстрировать, прочтите все шаги практической работы, чтобы лучше понять DNS и функционирование DNS-серверов.

Шаг 1. Используйте средство администрирования Windows Server DNS

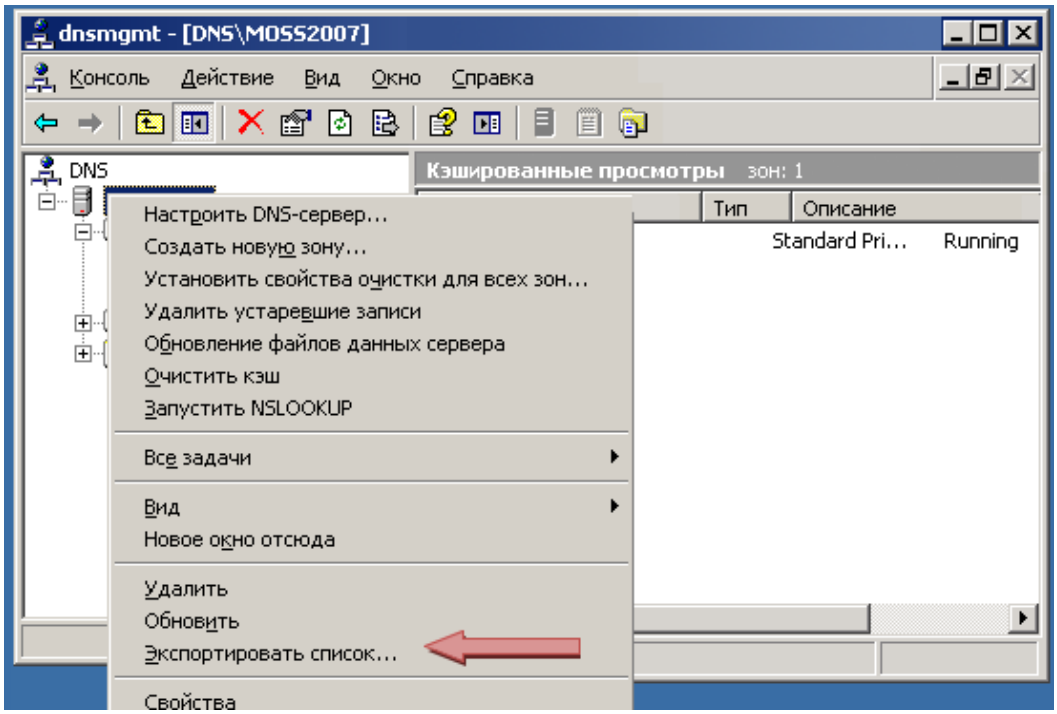
зз. Щелкните **«Пуск» > «Все программы»** > **«Администрирование»**, а затем щелкните **«DNS»** для запуска средства администрирования DNS.



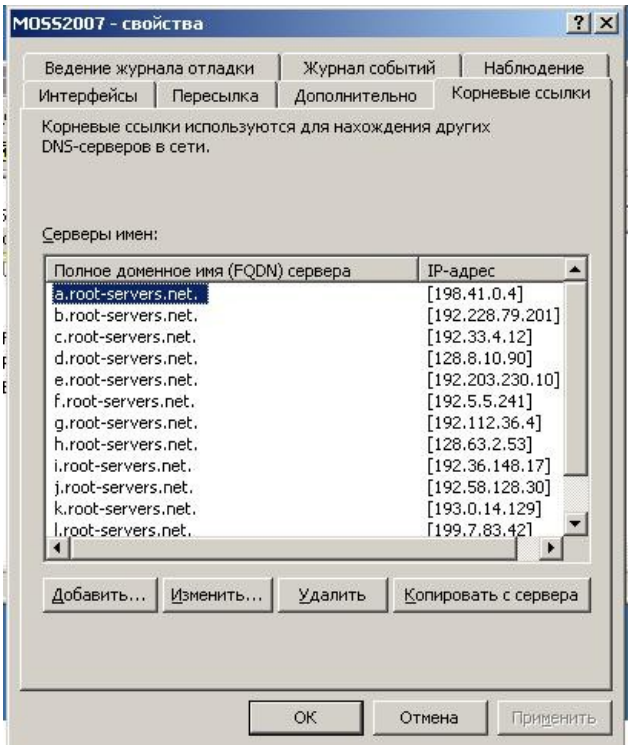
ии. Разверните папку **«Cached Lookups»** и все вложенные папки, чтобы убедиться в отсутствии кэшированных результатов поиска.



кк. После этого убедитесь, что сервер настроен для использования корневых каталогов в Интернете, щелкнув правой кнопкой по серверу DNS, а затем щелкнув **«Свойства»**.

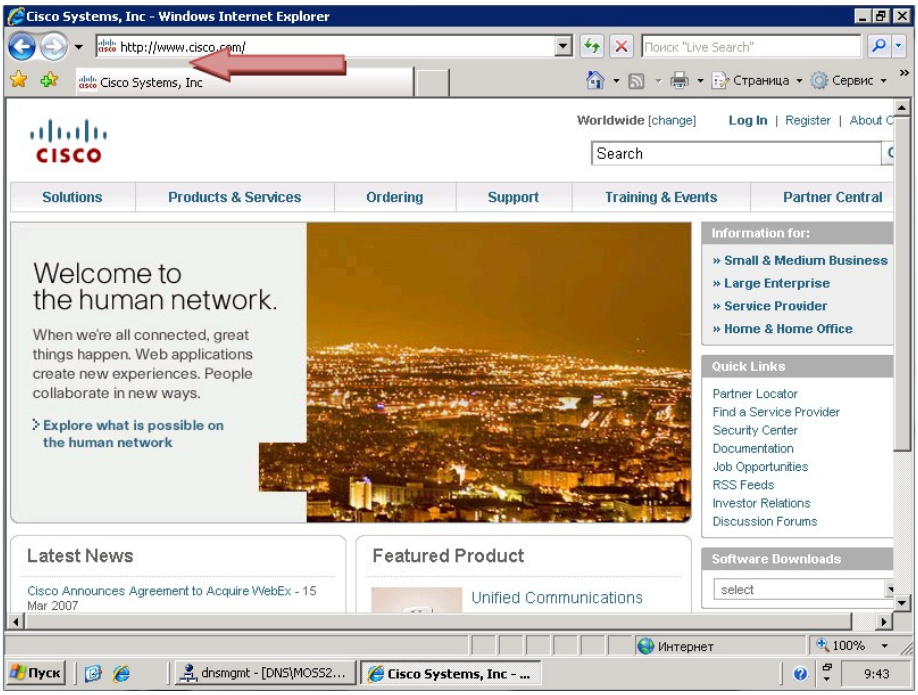


лл. В диалоговом окне **«Свойства»** выберите вкладку **«Корневые ссылки»** и убедитесь в наличии «Root servers» (корневых серверов). Щелкните **«ОК»**, чтобы закрыть диалоговое окно **«Свойства»**.



Шаг 2. Выполните поиск DNS

На DNS-сервере откройте обозреватель Internet Explorer и перейдите по адресу http://www.cisco.com. Закройте веб-обозреватель после открытия веб-страницы.



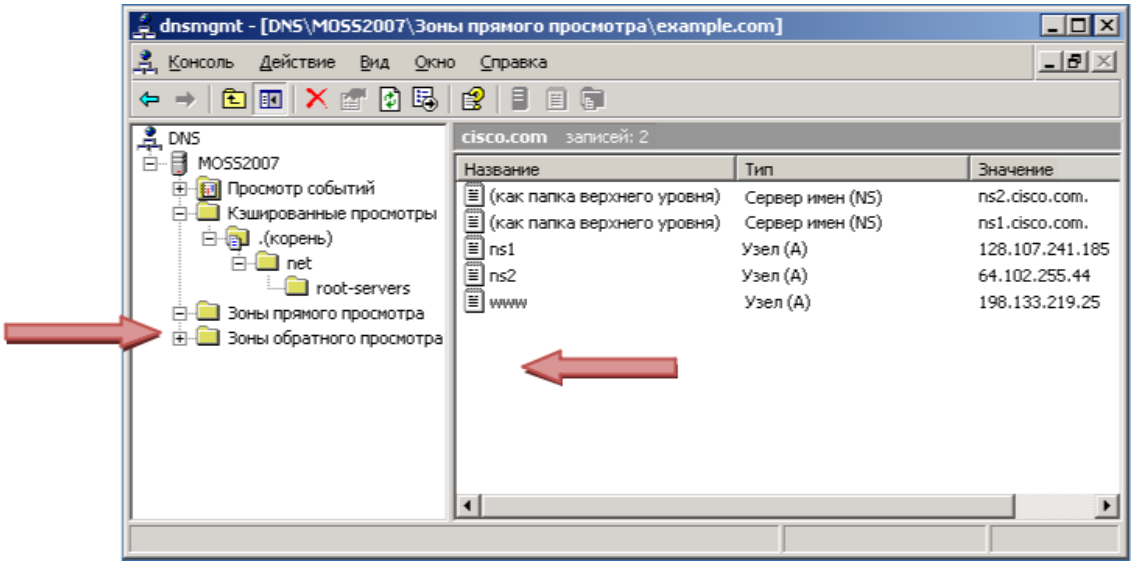
Шаг 3. Изучите кэшированные записи DNS

a. Switch back to the DNS Administrative tool.Вернитесь к средству администрирования DNS.

б. В корневой папке **«Cached Lookups»** щелкните кнопку **«Обновить»** на панели инструментов.

в. Разверните все вложенные папки, расположенные ниже папки **«Cached Lookups»**, чтобы отобразить все кэшированные записи DNS.

Обратите внимание, что теперь структура папок развернута до папки «Cisco». В папке «Cisco» обратите внимание на две записи, относящиеся к серверу имен (Name Server), которые указывают на два сервера имен, управляющих DNS- зоной Cisco.com. Так же обратите внимание на запись «Host» для www, направляющую на адрес 198.133.219.25.



Шаг 4. Вопросы для повторения

г. DNS-сервер был вынужден послать запрос на серверы доменных имен cisco.com, чтобы разрешить имя сервера (www.cisco.com) на IP-адрес. Что, по вашему мнению, произойдет при следующем посещении этого веб-узла через несколько минут?

_____

_____

д. Что произойдет, если не запрашивать этот веб-узел в течение более длительного периода времени?

_____
_____

Создание основной и вторичной зон обратного просмотра

Задача

- Создать основную и вторичную зоны обратного просмотра на DNS-серверах Windows?

Предварительная информация/подготовка

По запросу вы должны внедрить DNS-зону для клиента, который зарегистрировал домен второго уровня в сети Интернет. Клиент намерен разместить DNS-зону на двух отдельных серверах. Вы отправляетесь на объект, чтобы настроить зону на каждом из двух DNS-серверов. Один сервер будет выступать в роли основного DNS-сервера, тогда как другой — в качестве вторичного.

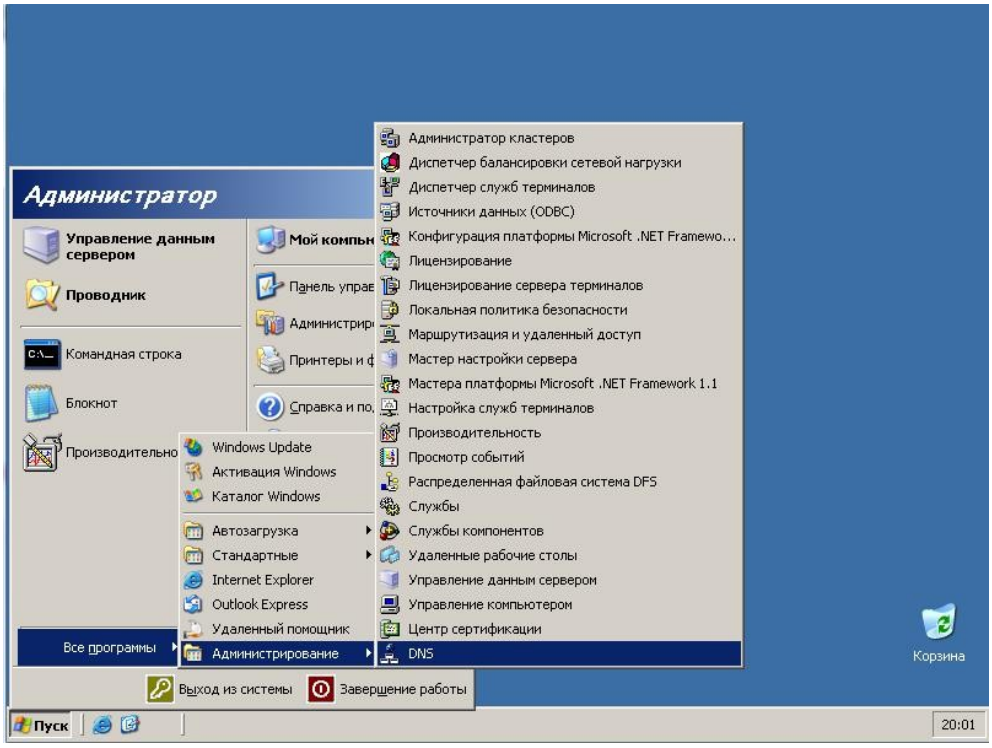
Требуются следующие ресурсы:

- Серверы Windows 2003 Server, на котором запущена служба DNS;
- Административный доступ к серверам;
- Подключение к Интернет.

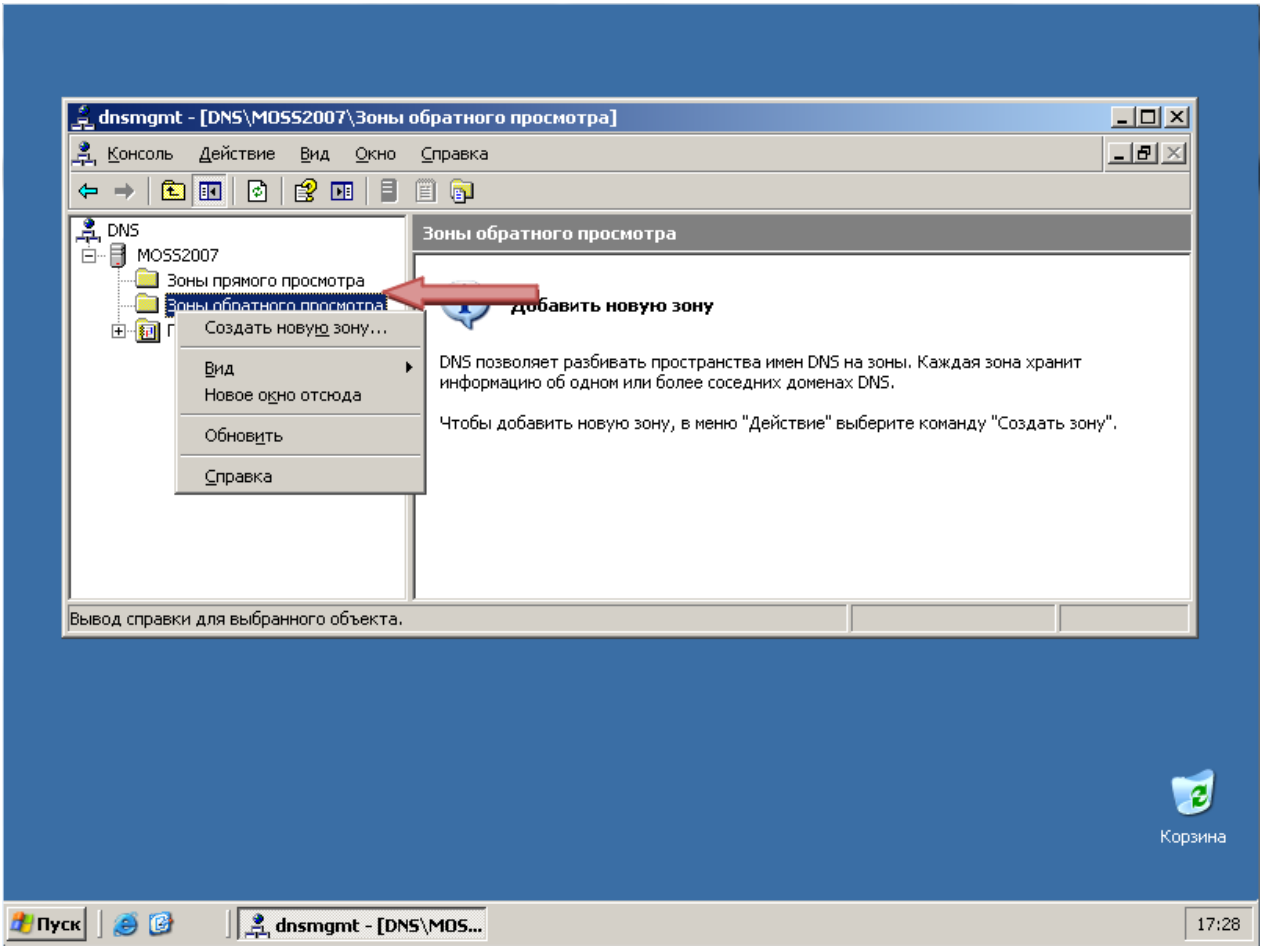
ПРИМЕЧАНИЕ. При отсутствии доступа к серверу Windows DNS преподаватель может продемонстрировать выполнение этой практической работы. Если отсутствует оборудование для выполнения этой практической работы, или ее невозможно продемонстрировать, прочтите все шаги практической работы, чтобы лучше понять DNS и функционирование DNS-серверов.

Шаг 1. Создание основной зоны обратного просмотра в Windows

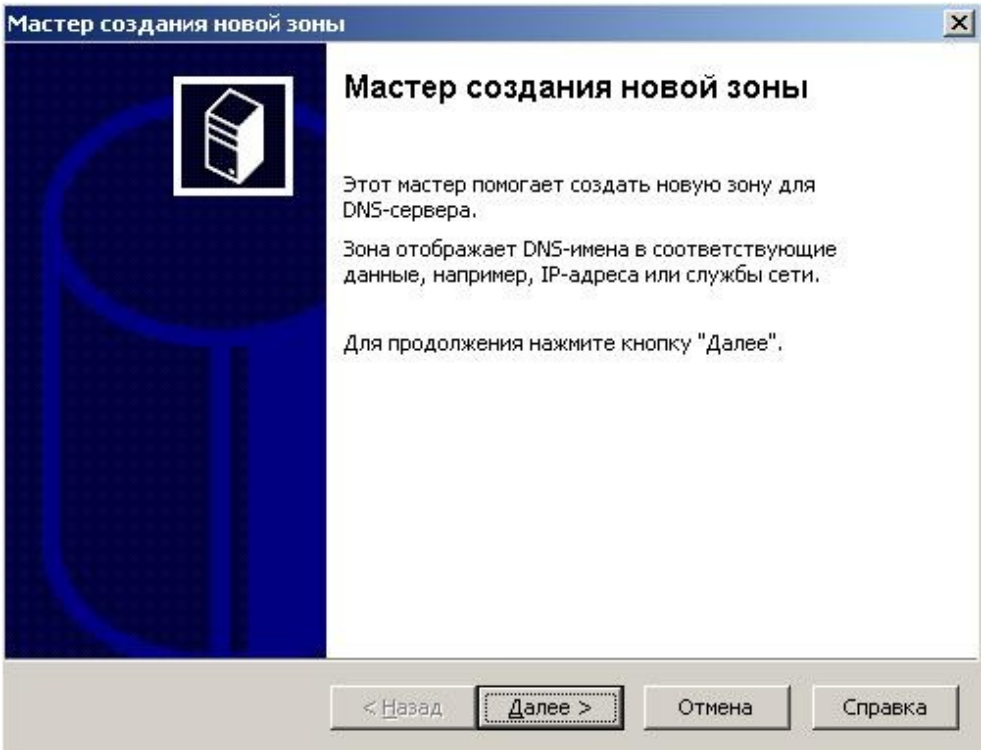
е. Щелкните **Пуск > Все программы** > **Администрирование**, а затем щелкните **DNS** для запуска средства администрирования DNS.



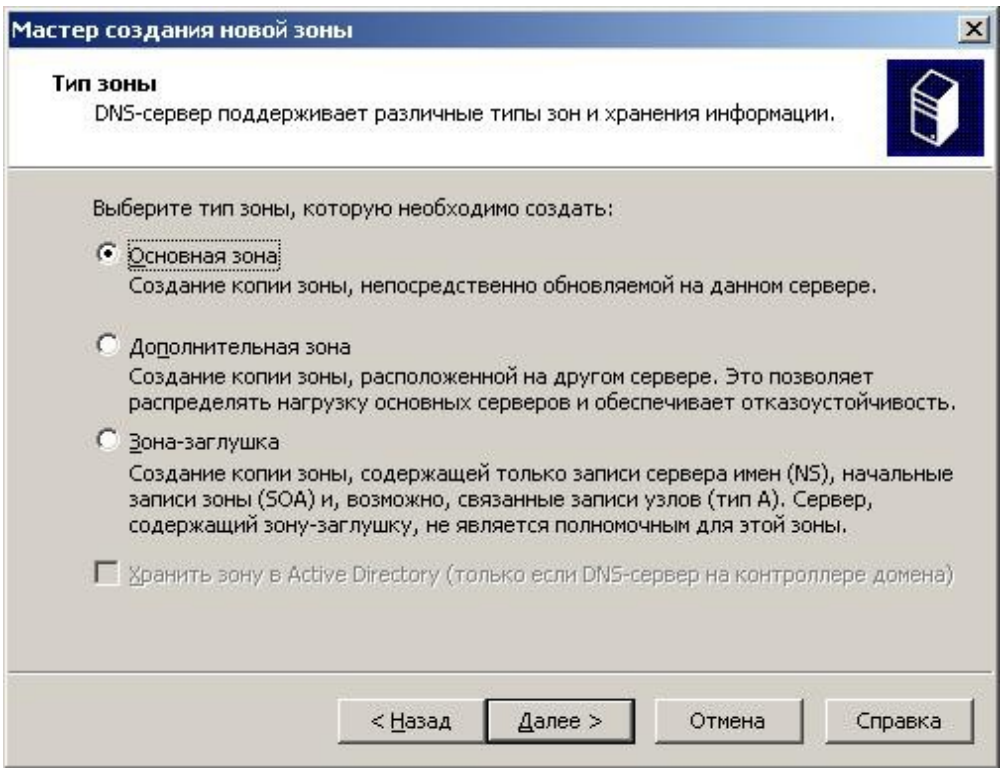
ж. Щелчком правой мыши выберите **Forward Lookup Zones (зоны обратного просмотра)**, после чего щелкните **New Zone (новая зона)**.



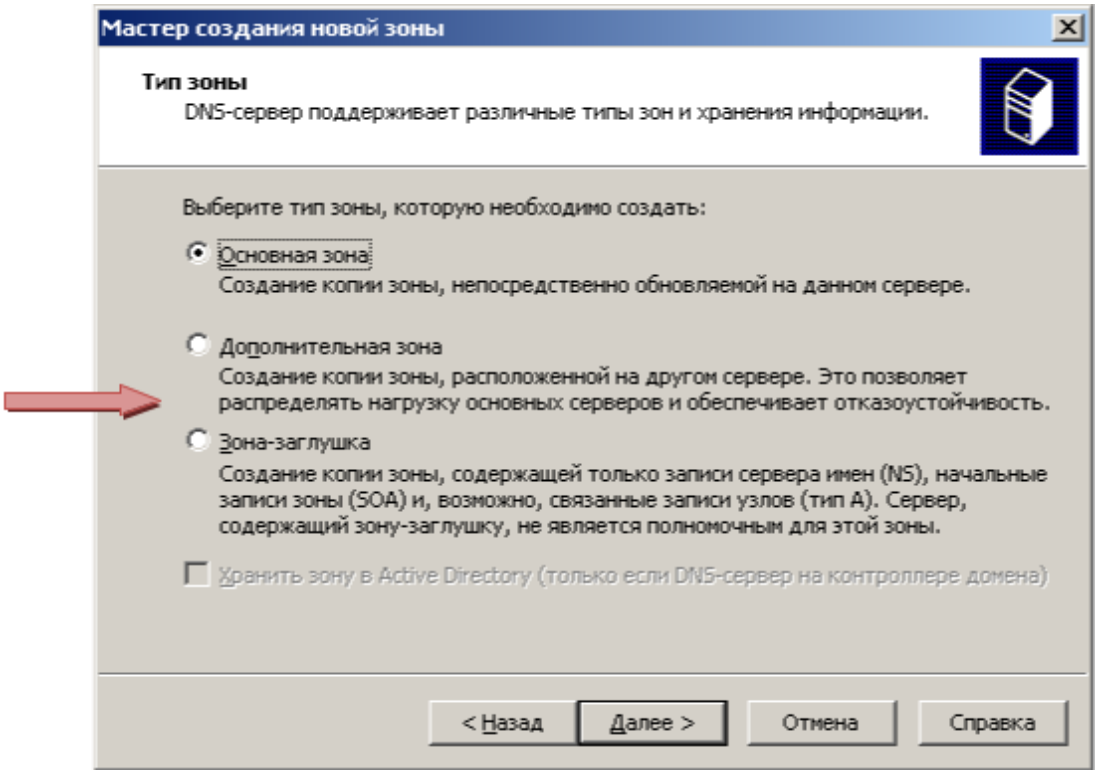
з. Когда появится окно **мастера новых зон** щелкните **Next (далее)**.



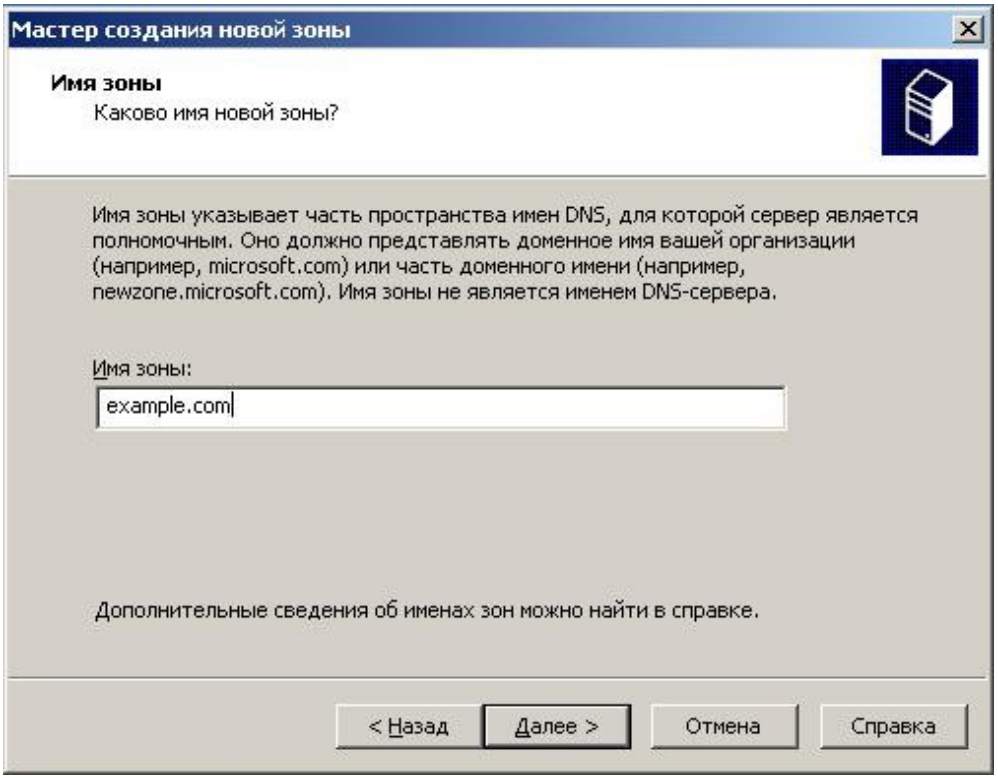
и. По умолчанию переключатель будет установлен в положение **Primary zone (основная зона)**. Щелкните **Next (далее)**, чтобы создать основную зону.



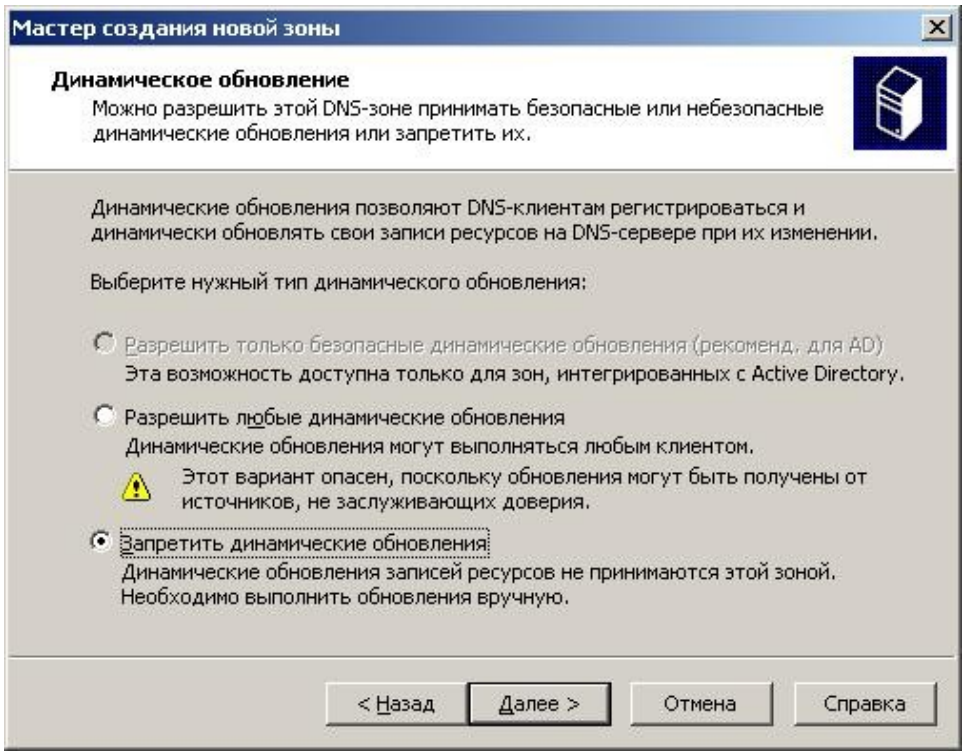
к. Введите доменное имя, **example.com**, в поле с именем зоны и щелкните **Next (далее)**.



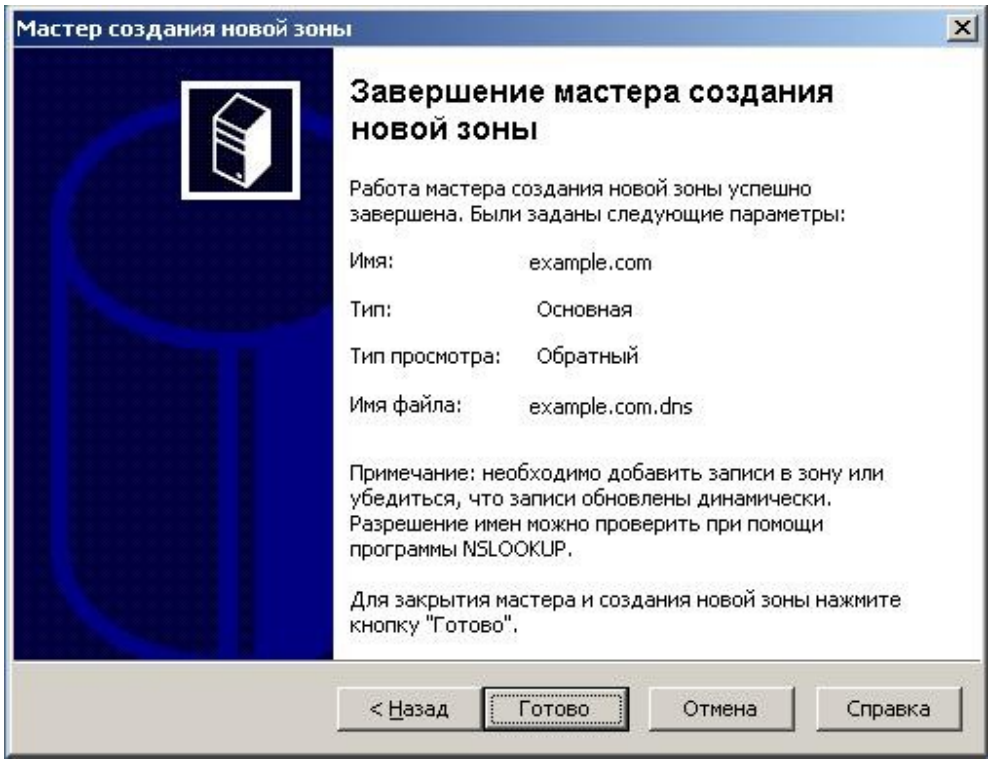
л. Щелкните **Next (далее)**, чтобы создать новый файл с этим именем.



м. Обратите внимание на возможность включения динамических обновлений. Она отключена по умолчанию в целях безопасности. Вам ее включать необходимости нет. Нажмите **Next** (**далее**).

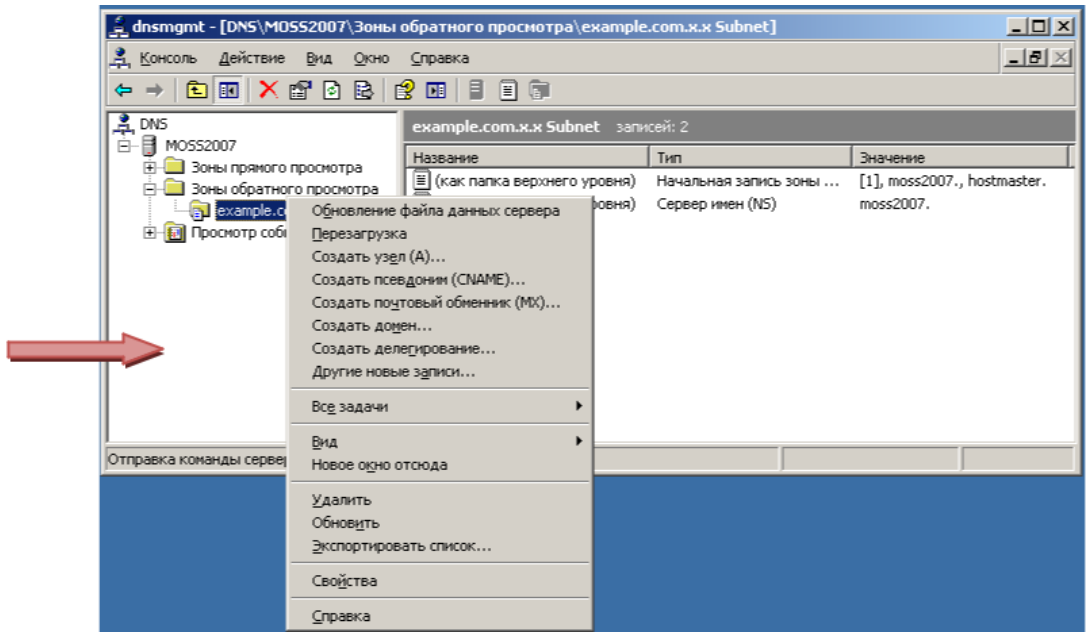


н. Нажмите кнопку **Finish (готово)**, чтобы создать основную зону обратного просмотра.

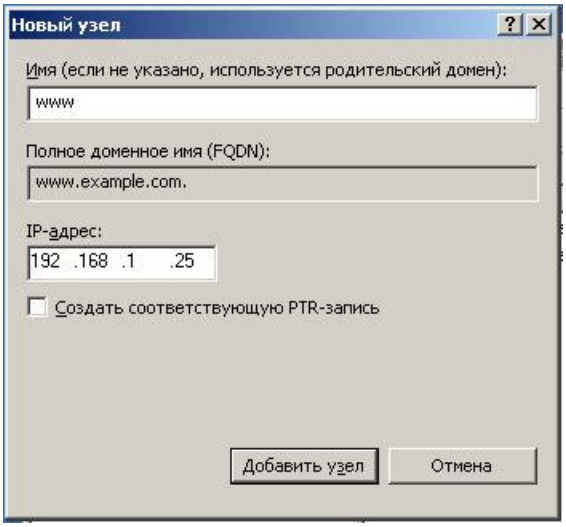


Шаг 2. Добавление записи об узле в основную зону обратного просмотра

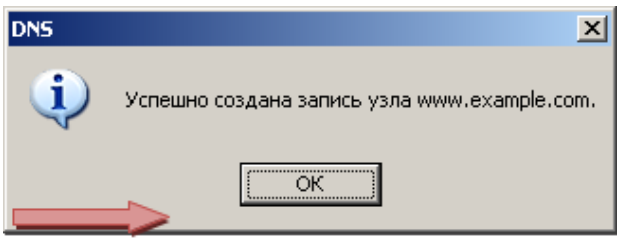
o. Правой кнопкой мыши щелкните зону обратного просмотра **example.com** и выберите **New Host (A) (создать узел (A))**.



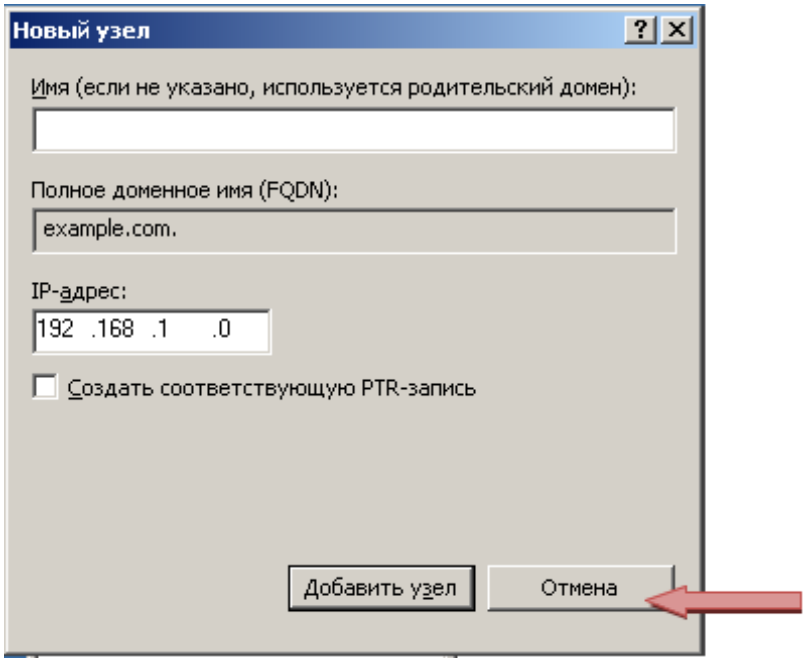
п. В поле имени введите **www**. В поле IP-адреса введите **192.168.1.25**. Сохраните значения по умолчанию для других параметров. При этом будет создан узел с именем www.example.com, которое будет преобразовано в 192.168.1.25. Нажмите внизу кнопку **Add Host (добавить узел)**.



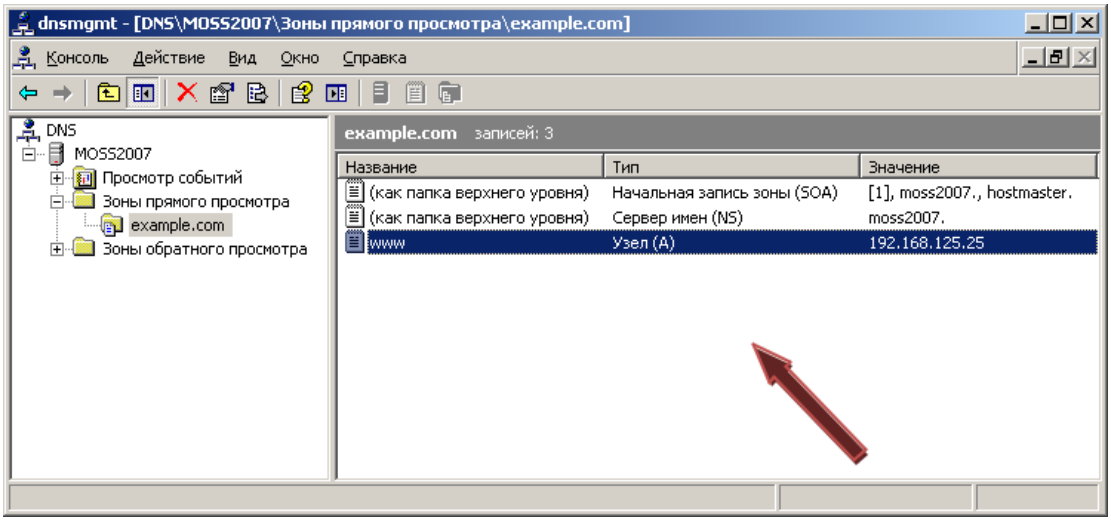
р. Нажмите **OK**.



c. Щелкните **Done (добавить узел)**.



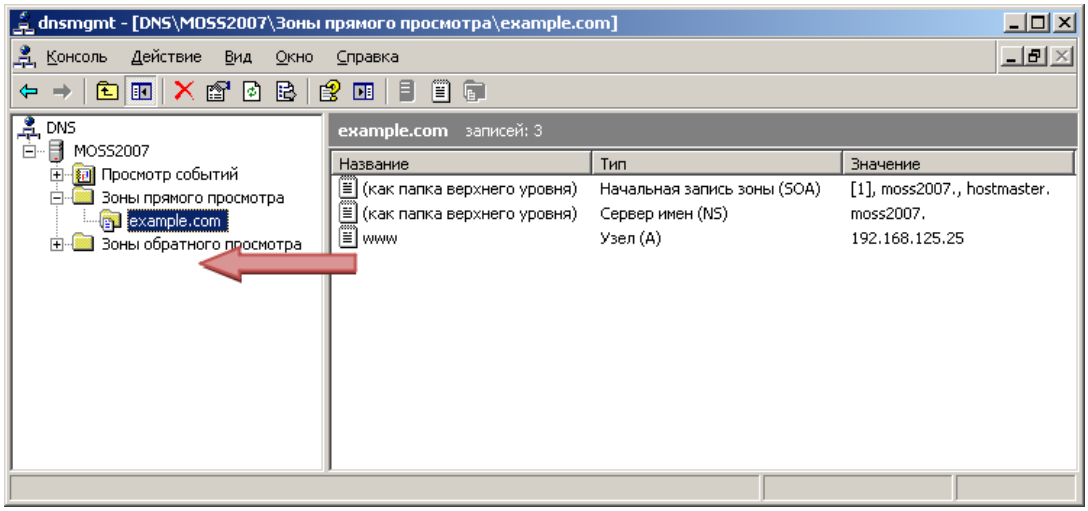
Эта запись узла теперь находится в вашей зоне DNS.



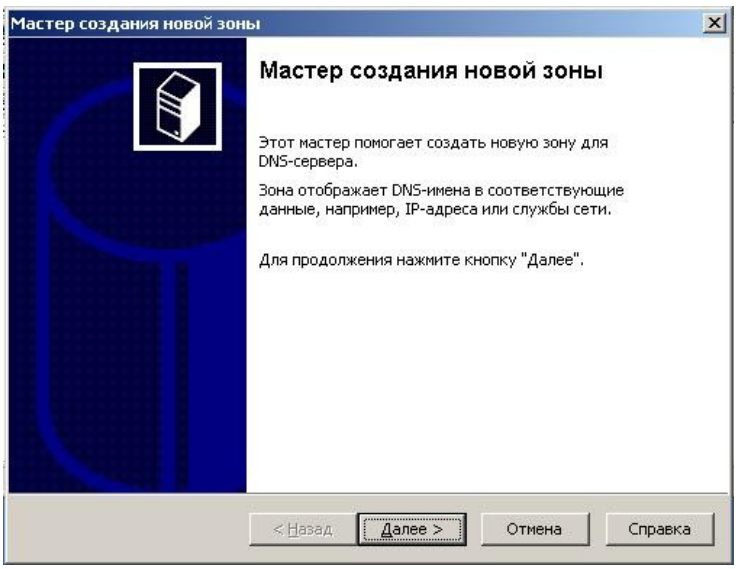
Шаг 3. Создание вторичной зоны обратного просмотра

а. На втором DNS-сервере Windows запустите инструмент администрирования DNS. Следуйте указаниям шага 1.

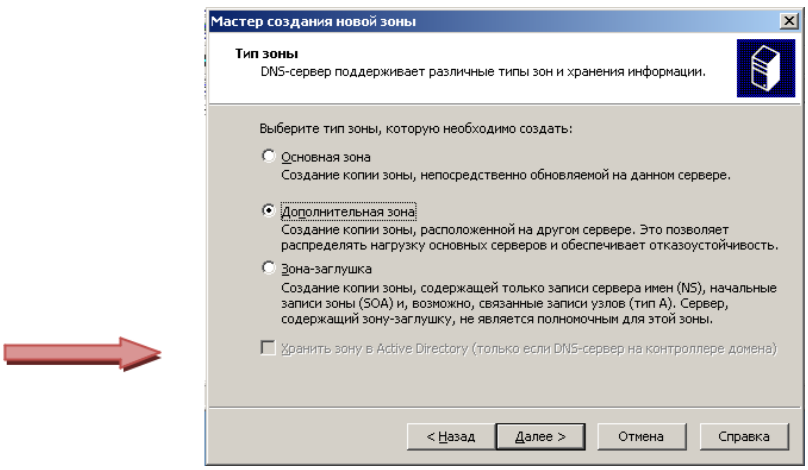
б. Щелчком правой кнопки мыши выберите **Forward Lookup Zones (зоны обратного просмотра)**, после чего щелкните **New Zone (новая зона)**.



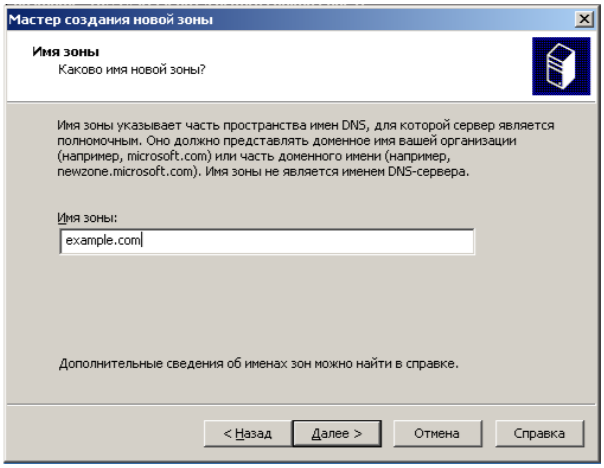
в. Когда появится окно **мастера новых зон** щелкните **Next (далее)**.



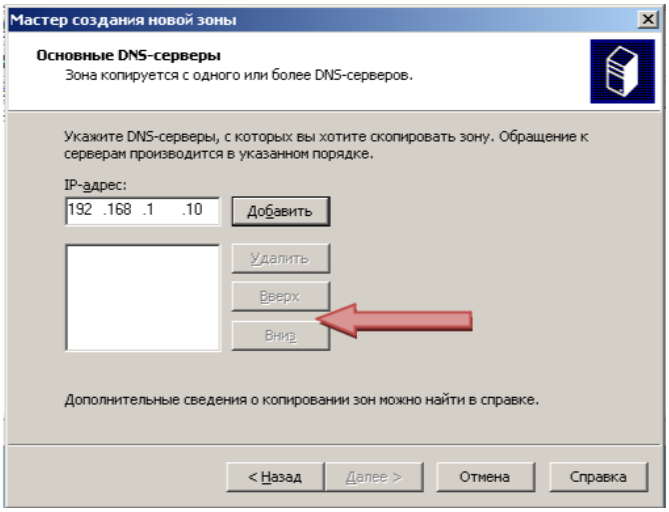
г. Установите переключатель в позицию **Secondary zone (дополнительная зона)** и нажмите **Next** (**далее**).



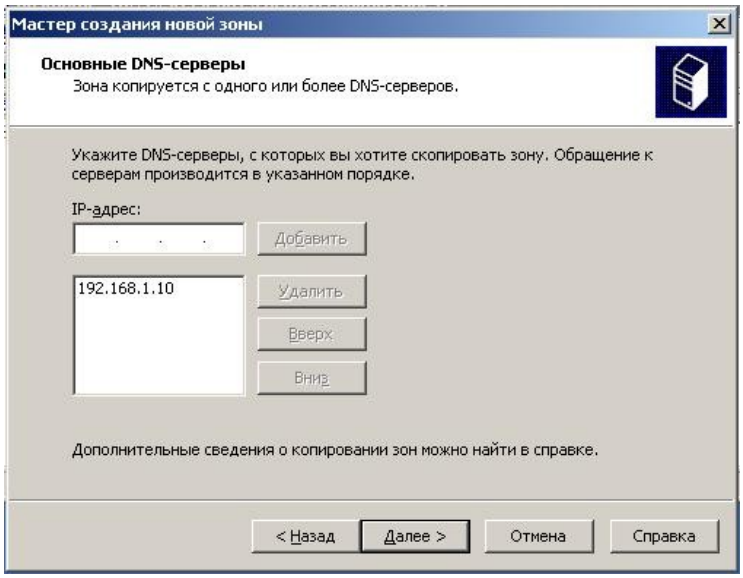
д. В поле имени зоны введите **example.com**, после чего нажмите **Next. (далее)**.



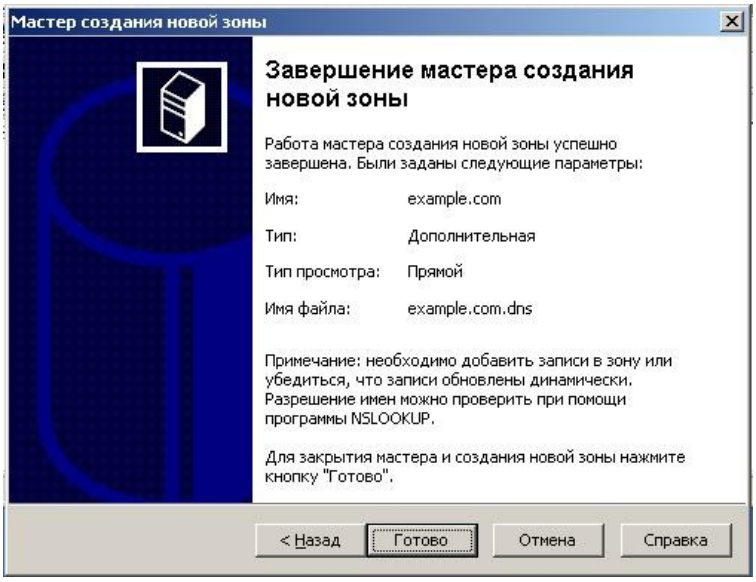
е. В поле IP-адреса введите **192.168.1.10**, это будет IP-адресом основного сервера. Потом нажмите кнопку **Add (добавить)**.



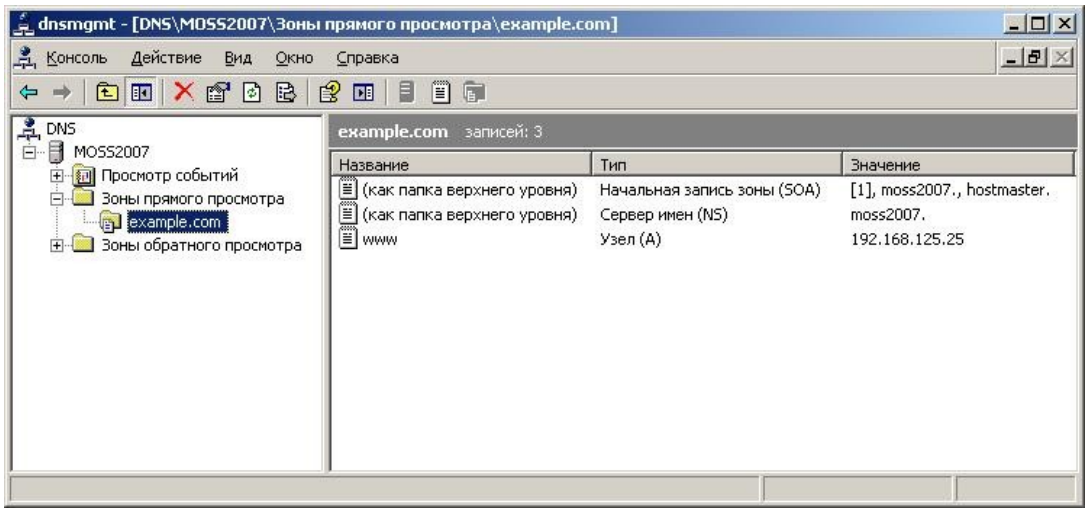
ж. Нажмите кнопку **Next (далее)**.



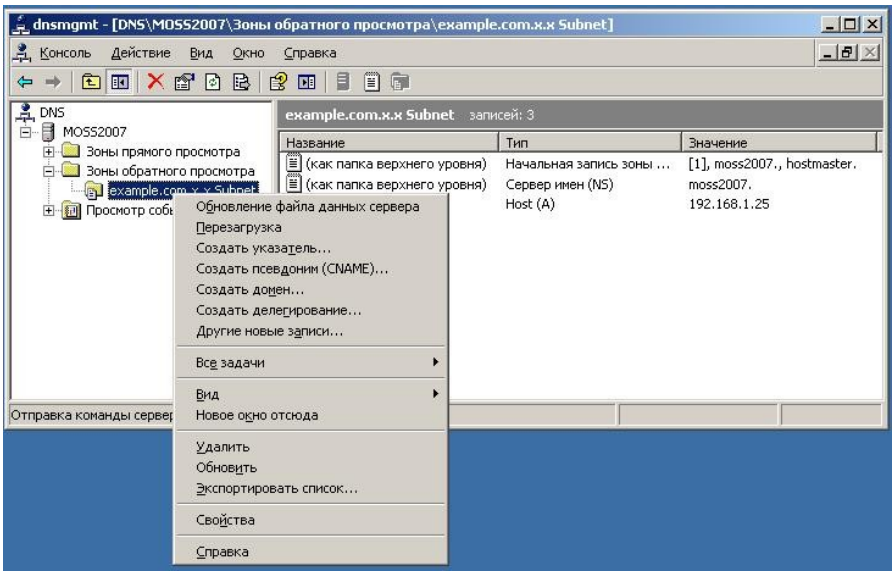
з. Нажмите кнопку **Finish (готово)**.



и. При просмотре вторичной зоны обратите внимание на то, что запись узла www, созданная на основном сервере, была перемещена на вторичный сервер.



к. Чтобы убедиться, что это вторичная зона и предназначена только для чтения, щелкните правой кнопкой мыши зону и вы увидите, что возможность создания записей отсутствует.



Шаг 4. Вопросы для повторения

Назовите основное преимущество размещения основного и вторичного DNS-сервера в зоне.

_____

Практическая работа 4. Обязанности поставщиков услуг Интернета

Обеспечение безопасности локальных и переданных данных

Задачи

- Использовать разрешения файловой системы новой технологии Windows (NTFS) для обеспечения безопасности локальных данных на компьютере с операционной системой Windows XP Professional edition.
- Использовать обозреватель Explorer 7 для получения доступа к безопасным веб-узлам.

Основная информация/подготовка

Эта практическая работа состоит из двух частей. Эти части можно выполнять вместе или независимо друг от друга.

Часть 1. Обеспечение безопасности локальных данных

В части 1 требуется обеспечить безопасность данных на компьютере с использованием файловой системы NTFS.

Ситуация. Два пользователя, работающих в небольшой компании, совместно используют рабочую станцию. Конфиденциальные данные хранятся локально на жестком диске компьютера. Вас попросили помочь защитить данные таким образом, чтобы к этим данным мог получить доступ только один локальный пользователь. Вы должны обеспечить безопасность локальных данных с использованием разрешений NTFS.

Компьютер используют два локальных пользователя, Боб и Джо. Боб требует изменить доступ к папке с названием «Bob's Files» (Файлы Боба), расположенной в папке с названием «Local Data on the C drive» (Локальные данные на диске C). Джо не получит доступ к папке «Bob's Files».

Часть 2. Определение безопасного канала обмена данными при передаче данных через Интернет

В части 2 необходимо использовать обозреватель Internet Explorer для определения безопасных и незащищенных веб-узлов.

Ситуация. Вы отвечаете за обучение конечных пользователей, работающих в небольшой фирме, безопасному доступу к веб-узлам. Необходимо обучить конечных пользователей способам отличать полезный и безопасный веб-узел от опасного веб-узла.

Необходимо использовать следующие ресурсы:

- компьютер с ОС Windows XP Professional и административным доступом;
- файловая система NTFS на компьютере и функция простого общего доступа к файлам отключены (в разделе меню «Свойства папки» в Проводнике);
- предварительно настроенные учетные записи пользователей Боба и Джо;
- подключение к Интернету.

Часть 1. Обеспечение безопасности локальных данных

Шаг 1. Обеспечьте безопасность папки, содержащей файлы Боба

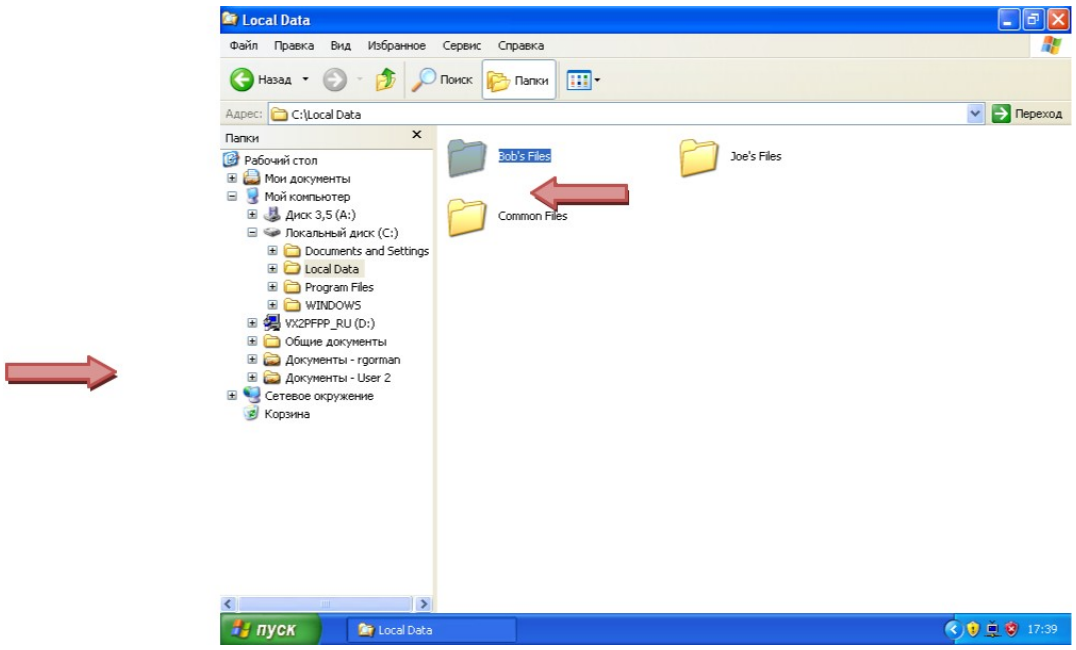
а. Войдите в систему Windows XP компьютера как администратор.

б. From the **Accessories** menu, launch Windows Explorer.Из меню **«Стандартные»** запустите Проводник.

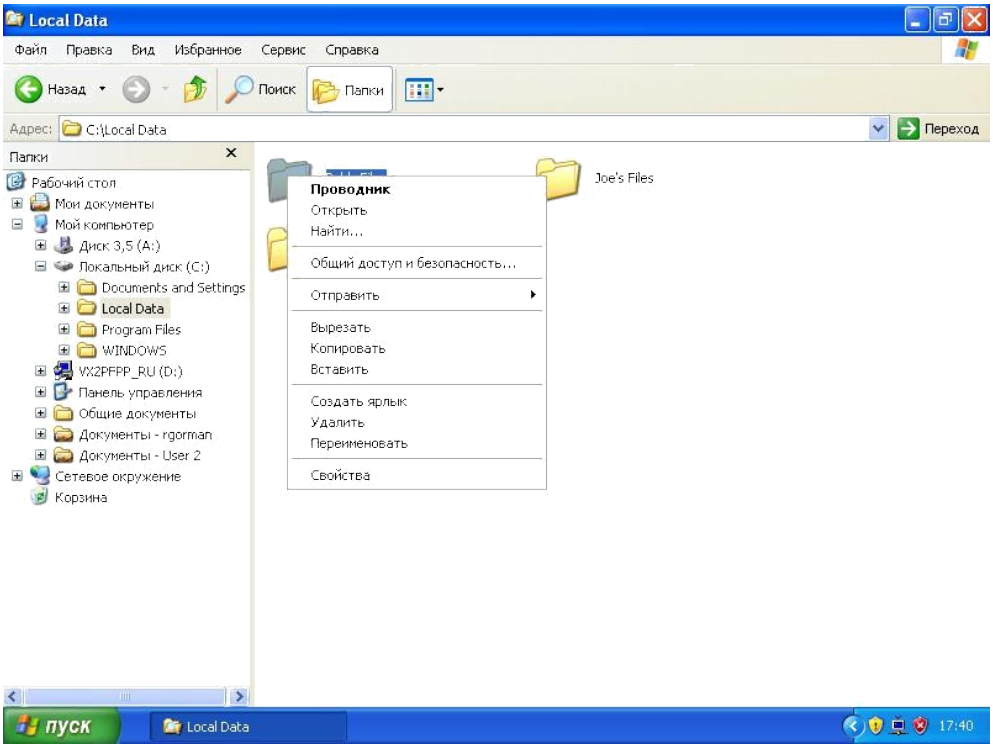
в. С использованием Проводника создайте папку на локальном диске (C:) и назовите ее **«Local Data»**. В меню **«Файл»** щелкните **«Создать»**, а затем щелкните **«Папку»**.

г. Щелкните папку **«Local Data»**, а затем щелкните правой кнопкой мыши по пустой области в правой части экрана. Щелкните **«Создать»**, а затем щелкните **«Папку»** и создайте папку с именем **«Bob's Files»**. Повторите эту процедуру и создайте папки **«Common Files»** (Общие файлы) и **«Joe's Files»** (Файлы Джо).

д. Перейдите к папке **«Local Data»**, в которой можно видеть папку **«Bob's Files»**.

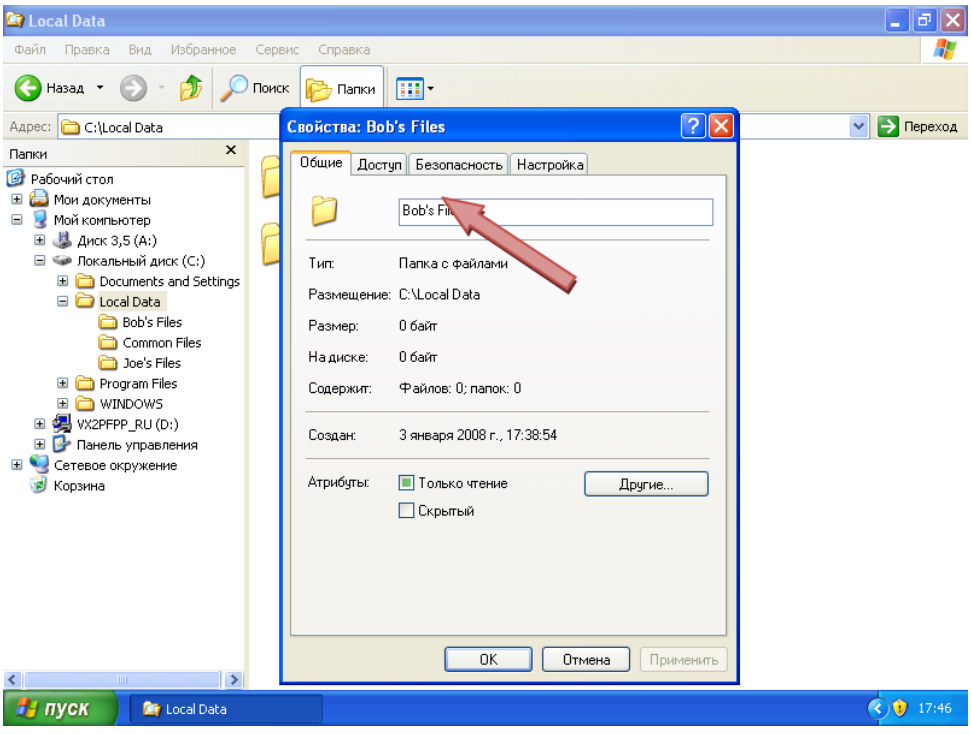


е. Щелкните правой кнопкой мыши папку **«Bob's Files»** и выберите **«Свойства»**.

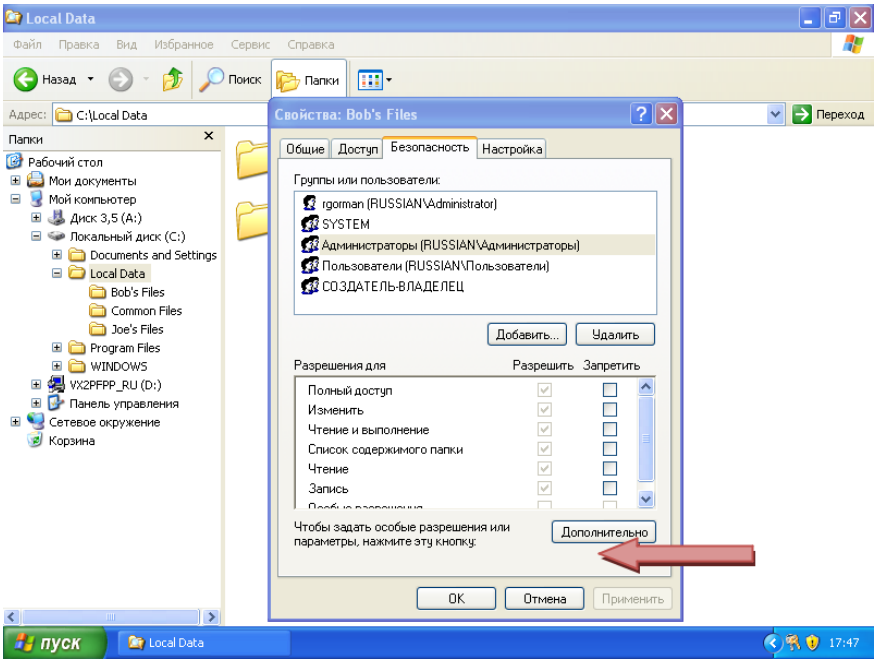


ж. В диалоговом окне **«Свойства: Bob's Files»** щелкните вкладку **«Безопасность»**.

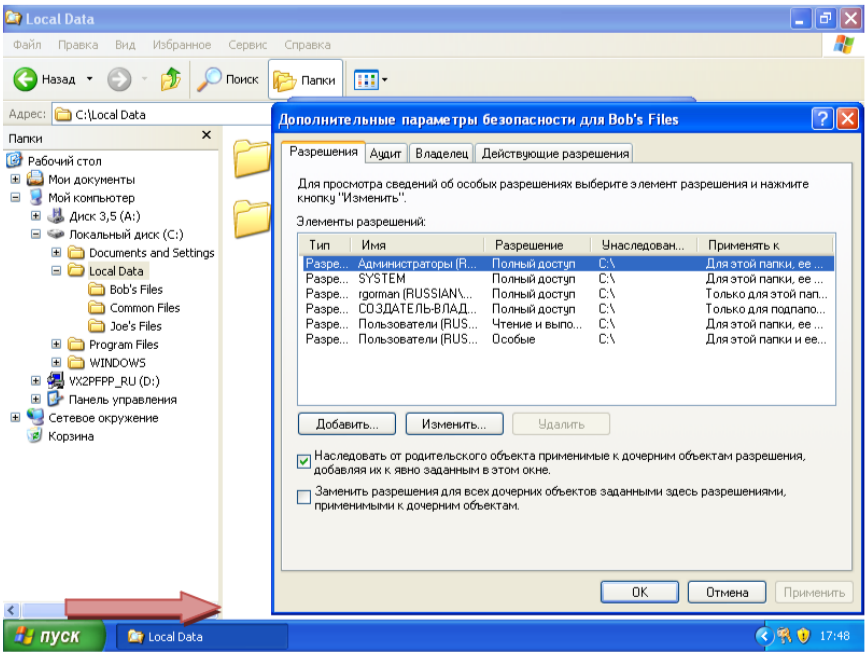
ПРИМЕЧАНИЕ. Необходимо работать с диском, на котором установлена файловая система NTFS. В противном случае вкладка **«Безопасность»** не отображается.



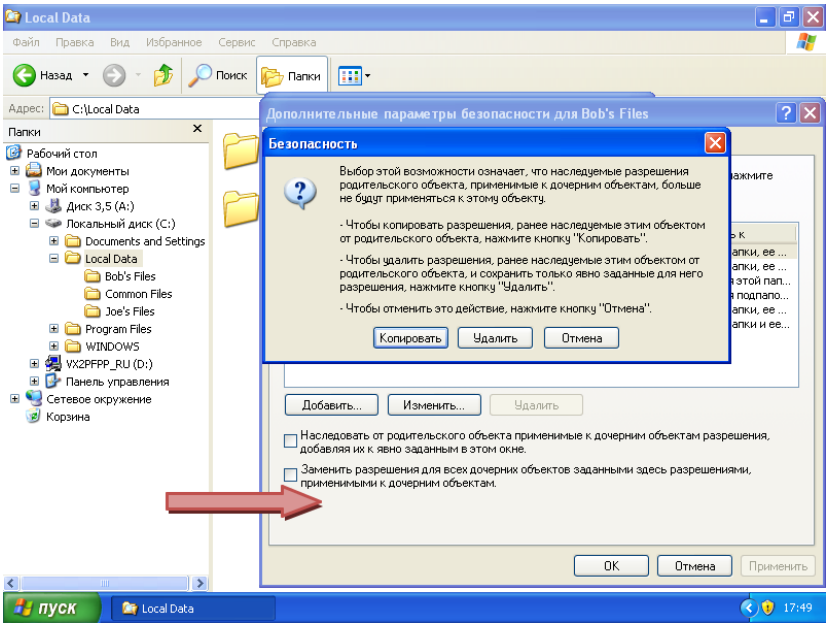
з. Обратите внимание, что разрешения недоступны, и их изменить нельзя. Это ограничение установлено в силу разрешений, унаследованных от родительской папки. Для обеспечения безопасности папки необходимо отключить унаследованные разрешения. На вкладке **«Безопасность»** щелкните кнопку **«Дополнительно»**.



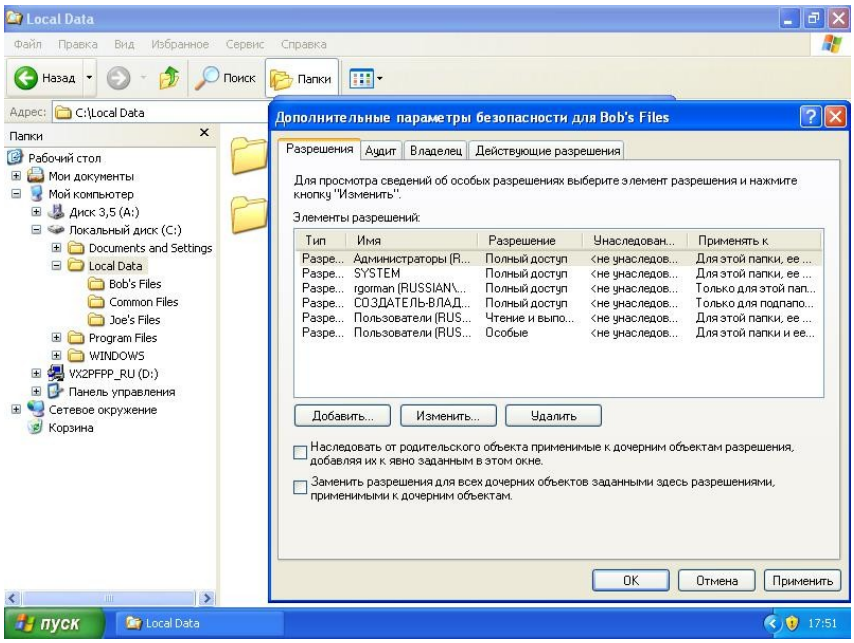
и. Снимите флажок рядом с параметром «Наследовать от родительского объекта применимые к дочерним объектам разрешения».



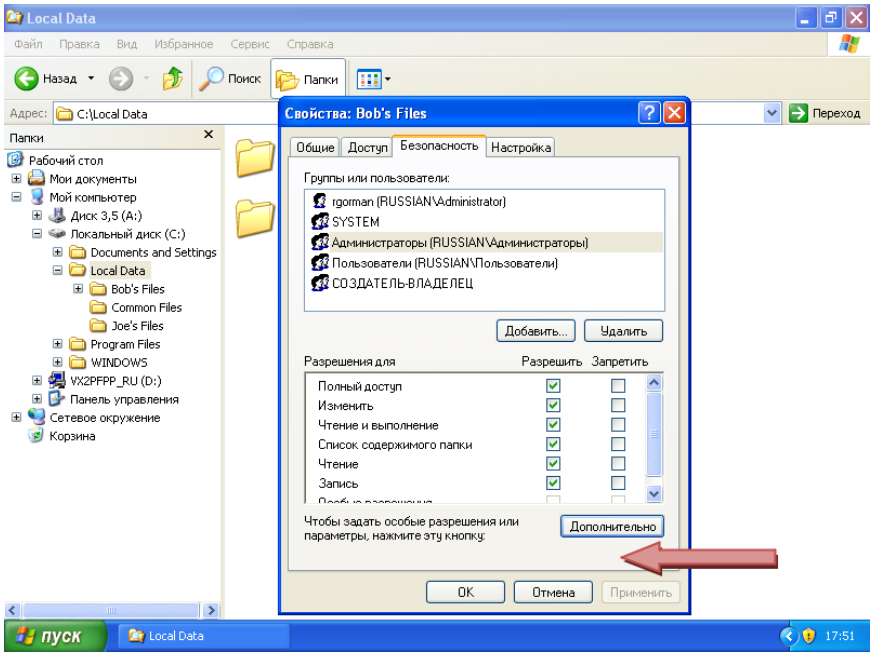
к. Щелкните **«Копировать»** для сохранения существующих разрешений.



л. Щелкните **«OK»**.

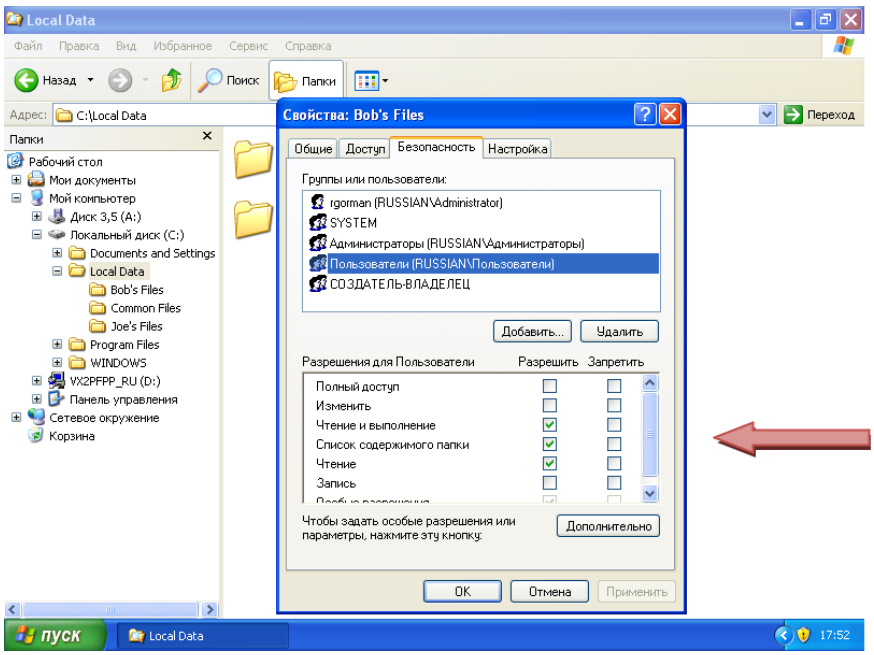


Теперь наследование отключено, и можно приступать к изменению разрешений.

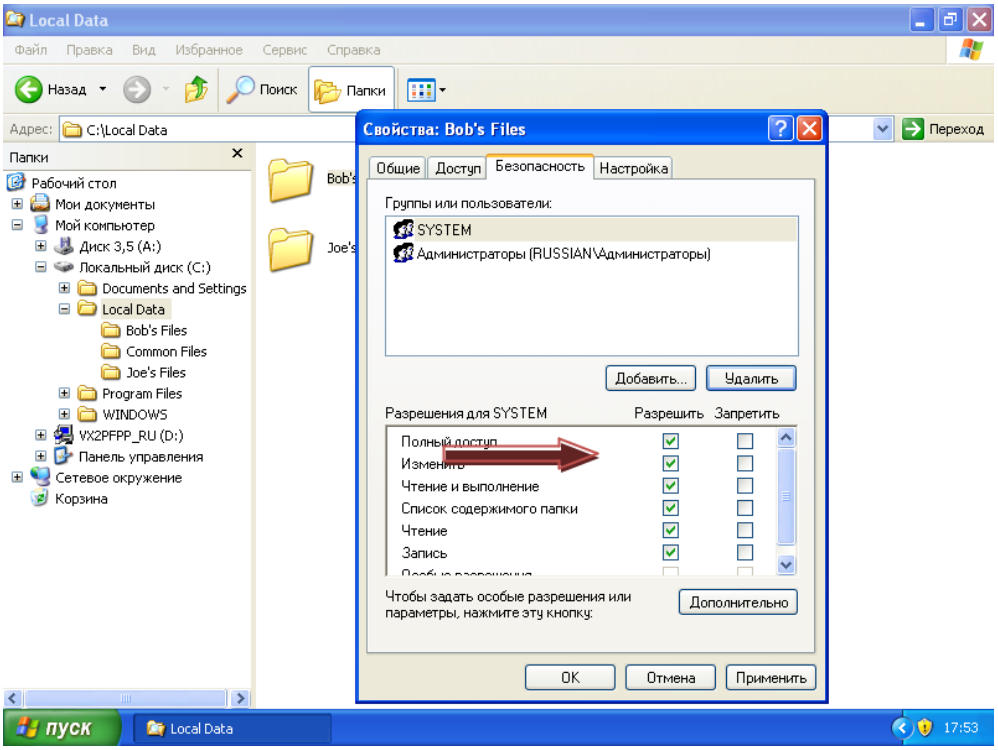


м. Выберите группу **«Users»** и щелкните **«Удалить»**. Продолжайте выбирать других оставшихся пользователей и группы, кроме групп «Administrators» и «SYSTEM», а затем щелкните **«Удалить»**.

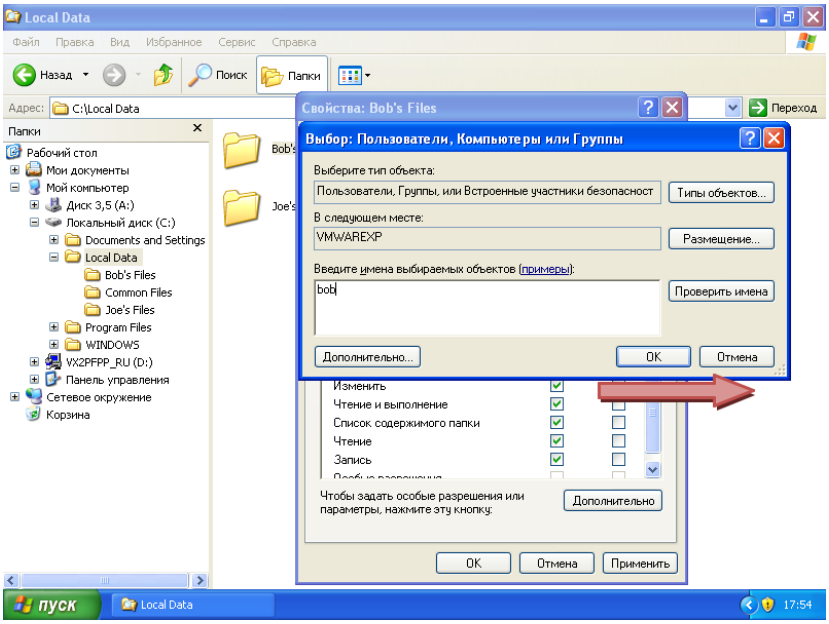
ПРИМЕЧАНИЕ. Группы «SYSTEM» и «Administrators» всегда должны получать полный доступ к каталогам и файлам, чтобы обеспечить резервное копирование, восстановление и сканирование этих файлов системами компьютера.



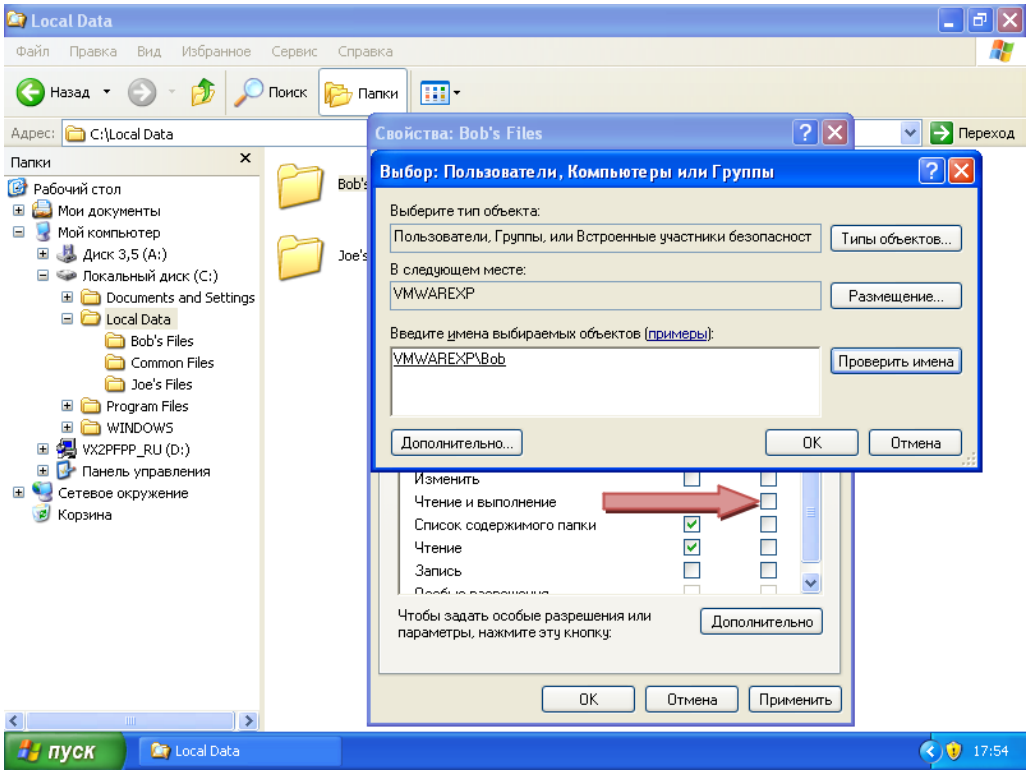
н. Теперь добавьте к списку Боба. Щелкните **«Добавить»**.



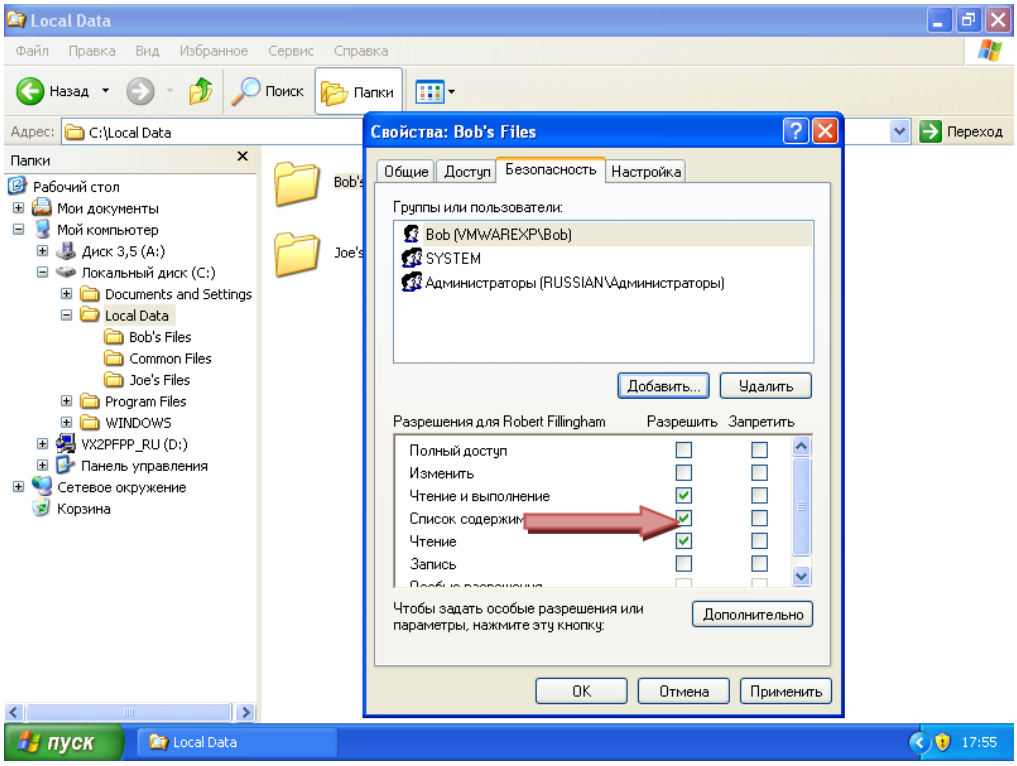
о. Введите в текстовом поле **«Bob»** и щелкните кнопку **«Проверка имен»** для проверки его учетной записи.



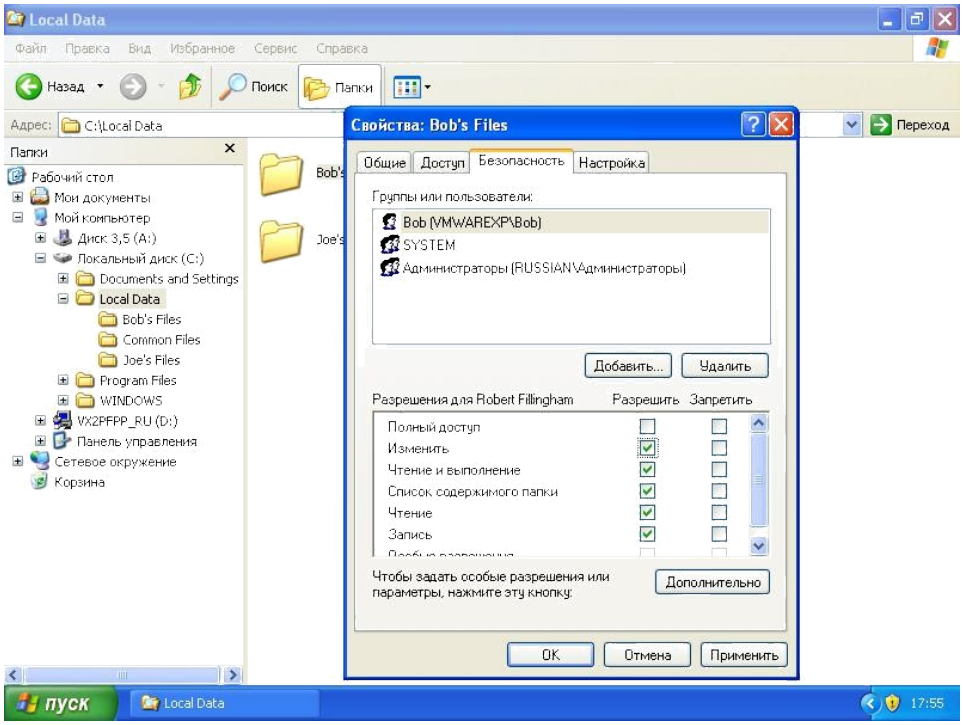
п. После завершения проверки щелкните **«OK»**.



p. Теперь Боб добавлен к списку. Обратите внимание, что в настоящее время у него есть разрешения «Чтение и выполнение», «Список содержимого папки» и «Чтение». Поскольку Бобу необходимо создавать новые файлы и удалять существующие, дайте ему разрешение «Изменение». Установите флажок в столбце **«Разрешить»** рядом с **«Изменение»**.

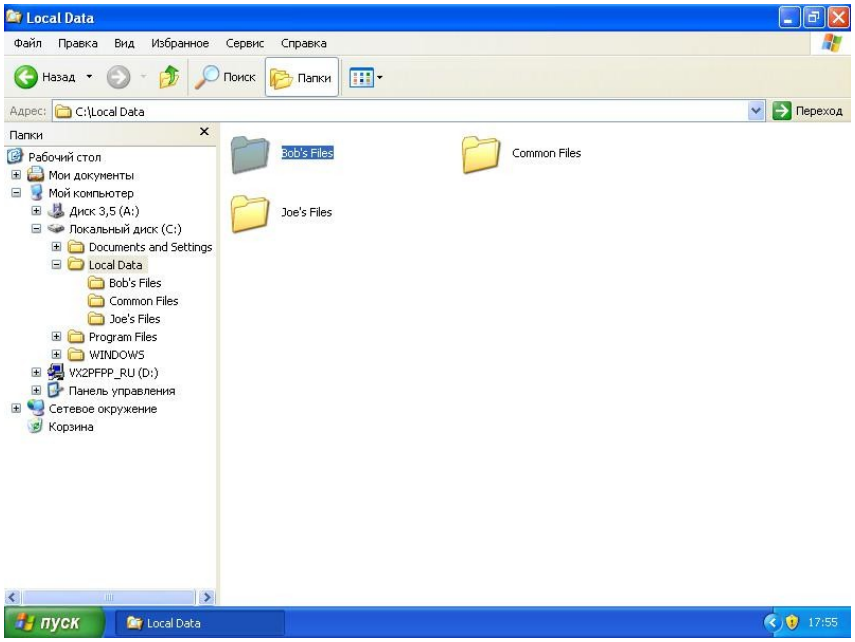


c. После присвоения Бобу разрешения на изменения щелкните **«OK»**, чтобы задать безопасность.

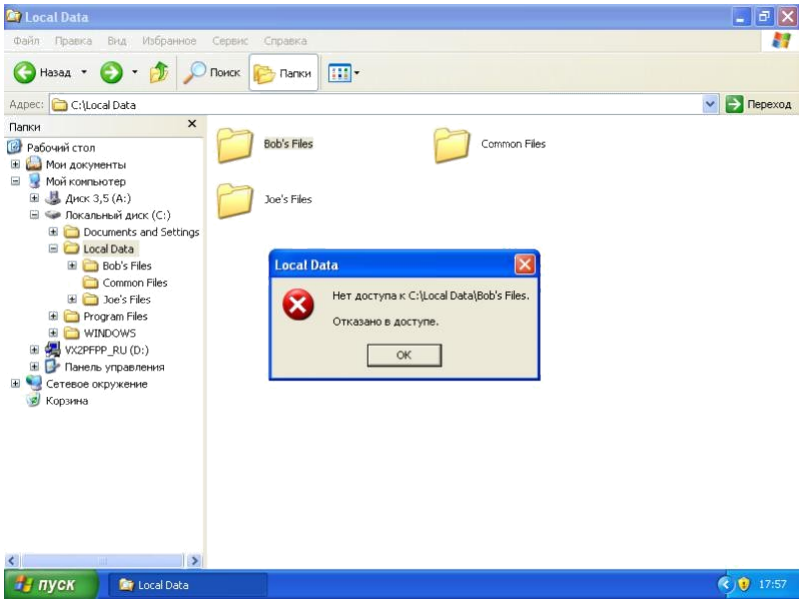


Шаг 2. Протестируйте доступ Джо к файлам Боба

т. Войдите в локальный компьютер как Джо и попытайтесь получить доступ к каталогу **«Bob's Files»**.



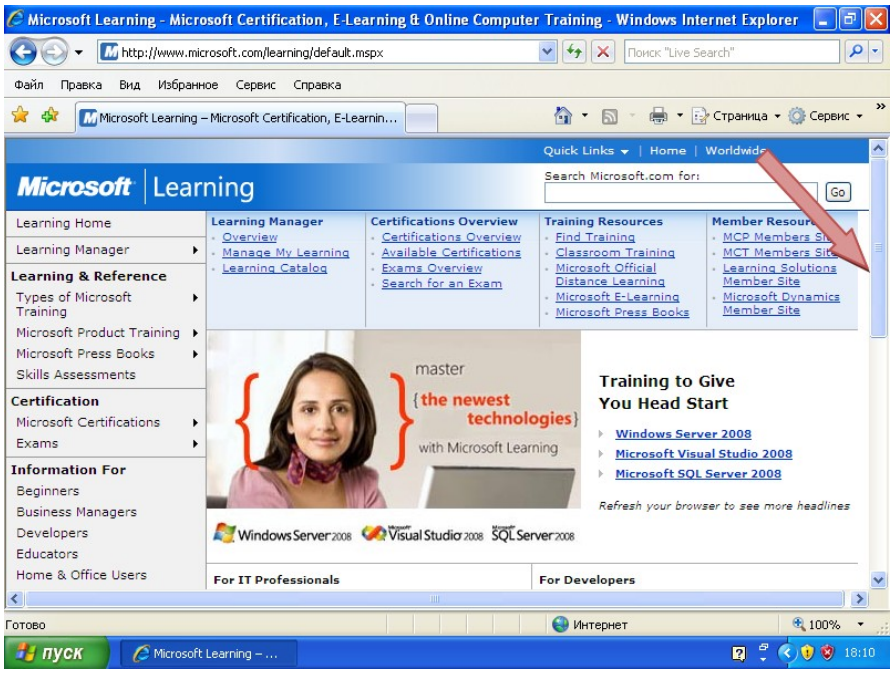
у. Обратите внимание на всплывающее диалоговое окно, в котором сообщается, что у Джо нет разрешения на доступ к этим файлам. Поскольку Джо не имеет административного доступа на ПК, он не может получить доступ к папке «Bob's Files».



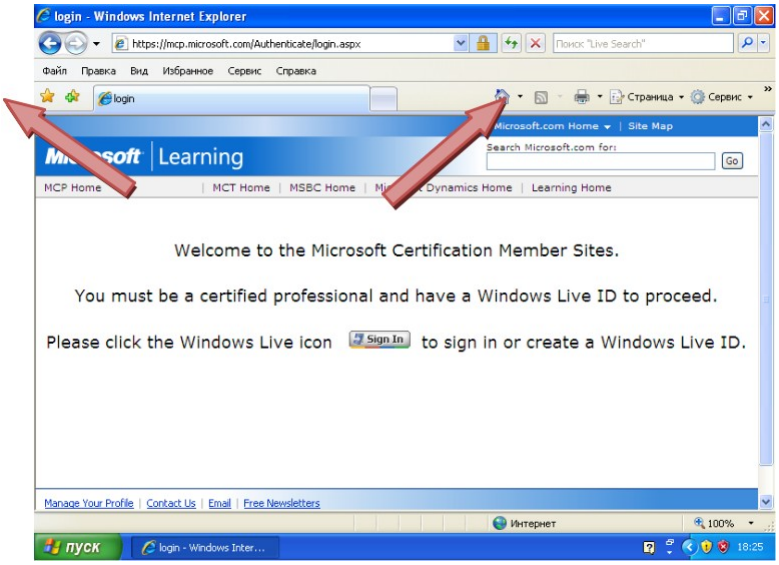
Часть 2. Определение безопасного канала обмена данными при передаче данных через Интернет

Шаг 1. Определите безопасную веб-страницу

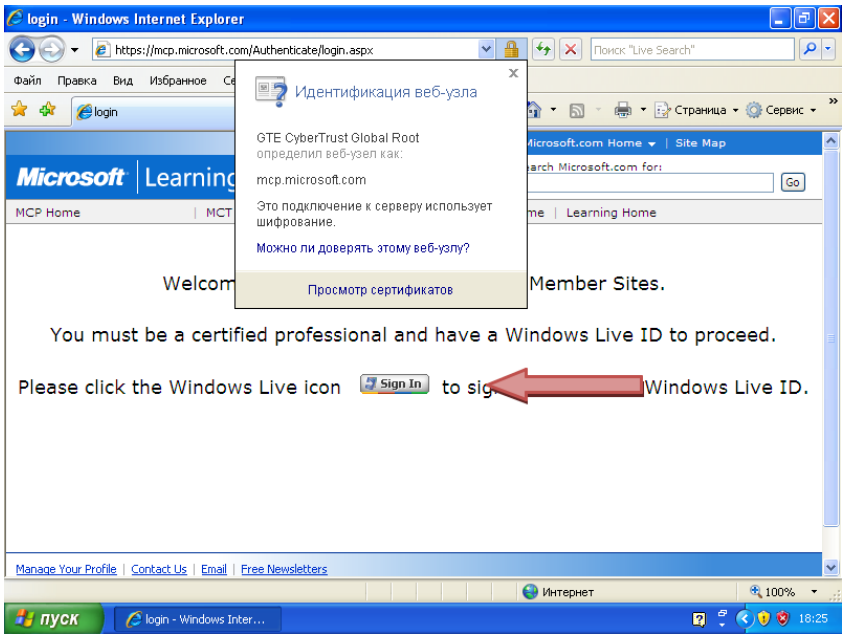
a. Запустите обозреватель Internet Explorer и перейдите к веб-узлу http://www.microsoft.com/learning. Этот узел является типичной незащищенной страницей. Щелкните ссылку «**MCP Members Site**».



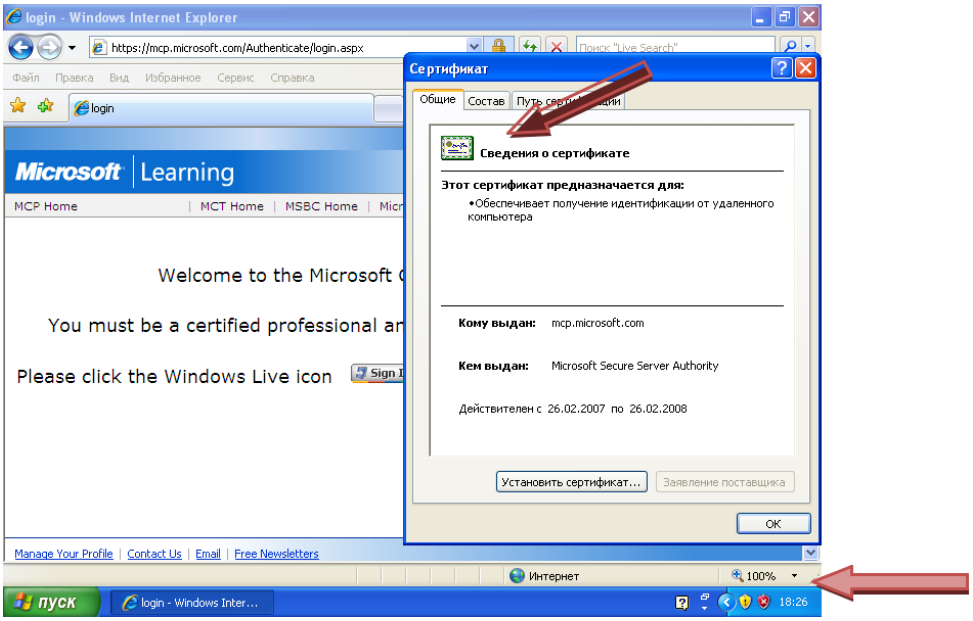
ф. Обратите внимание, что URL-адрес изменился с HTTP на HTTPS. HTTPS — это защищенная версия HTTP, где для обеспечения безопасности используется протокол SSL. Обратите внимание также на значок **замка**, расположенный справа от URL-адреса. Наличие значка **замка** означает, что веб-узел является защищенным. Щелкните значок **замка** для отображения дополнительных сведений о защищенном веб-узле.



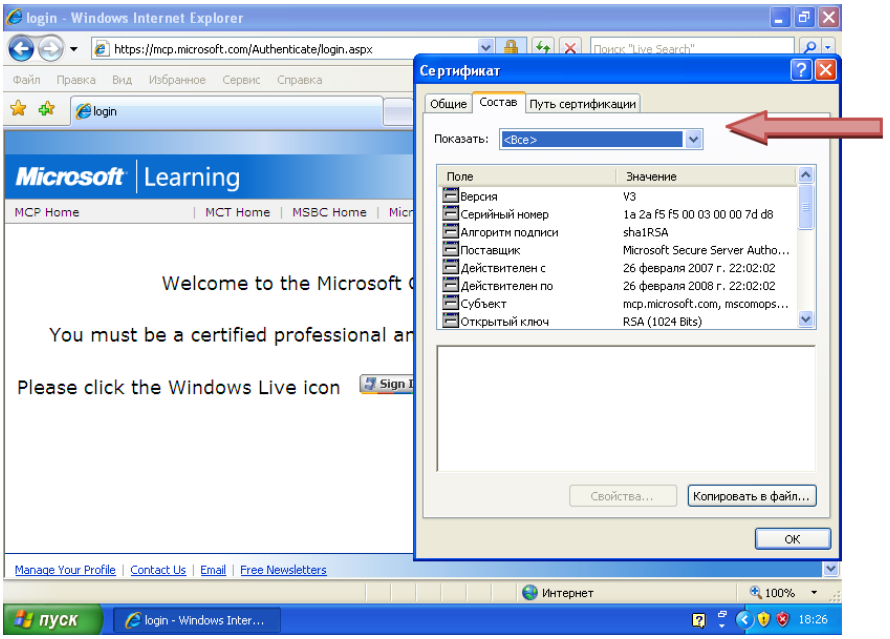
x. Во всплывающем окне отображаются сведения о поставщике сертификата безопасности для этого веб-узла. В нем также указано, что подключение к серверу защищено. Щелкните ссылку **«View certificates»** (Просмотр сертификатов) в нижней части всплывающего окна.



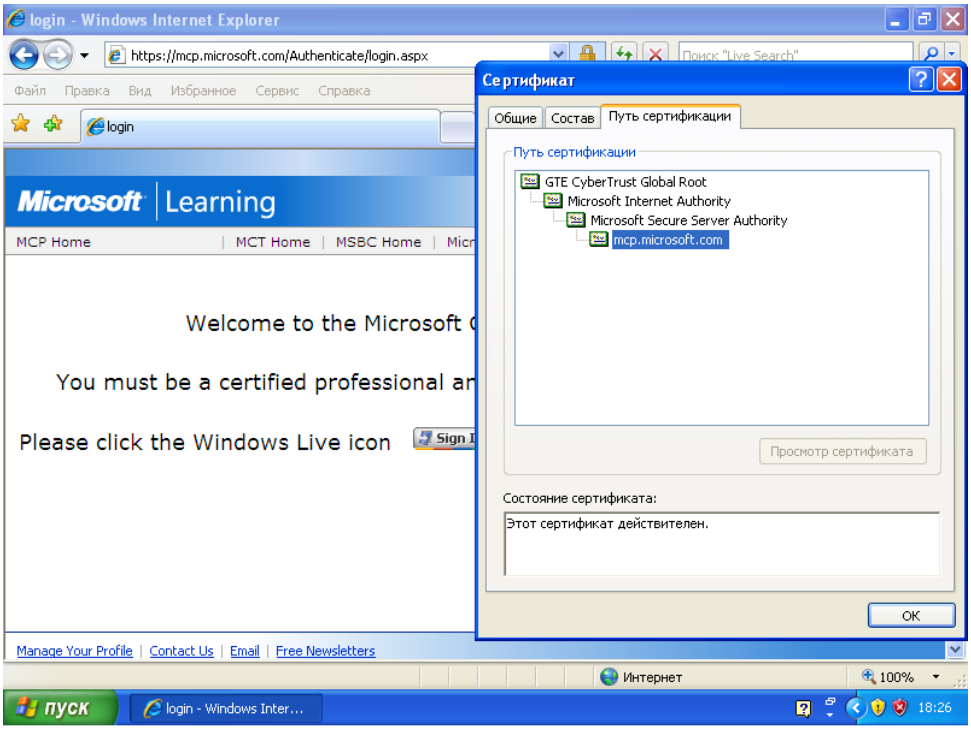
ц. Открывается окно сертификата, в котором отображается установленный на веб-сервере сертификат, позволяющий ему использовать протокол SSL. Обратите внимание на диапазон дат **«Valid from»** (Срок действия) внизу. Сертификаты действительны только в течение указанного периода времени, а затем их необходимо обновлять. Процесс обновления гарантирует, что администраторы веб-сервера непрерывно проверяют свои серверы в центре сертификации, выдавшем сертификат. Для получения дополнительных сведений щелкните вкладку **«Details»** (Сведения).



ч. На вкладке **«Details»** отображаются сведения о сертификате. Щелкните вкладку **«Certification Path»** (Путь сертификации).

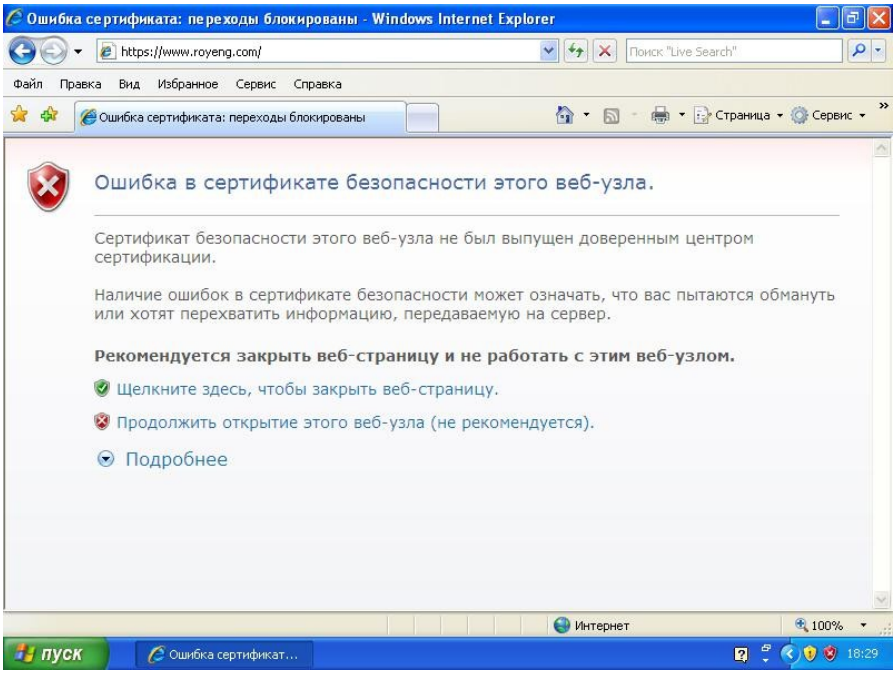


ш. На вкладке **«Certification Path»** отображается иерархический список центров сертификации, уполномоченных выдавать сертификаты веб-серверов. Щелкните **«OK»**, чтобы закрыть окно сертификата.



Шаг 2. Изучите предупреждение о защищенном доступе к ненадежному источнику

a. Если сертификат безопасности, предъявленный веб-узлом, был получен из ненадежного источника, в обозревателе Internet Explorer отображается следующий экран , предупреждающий о проблеме. Предлагается возможность закрыть веб-страницу или перейти к веб-узлу.



б. Нельзя доверять серверу или предлагаемому на нем контенту, если нет точных данных, что этот веб-узел является законным. При переходе по пути сертификации, как описано ранее, не отображается список надежных центров сертификации. Возможно, это защищенный веб-узел (HTTPS), но он сам себя сертифицировал, не прибегая к услугам уполномоченного центра сертификации.

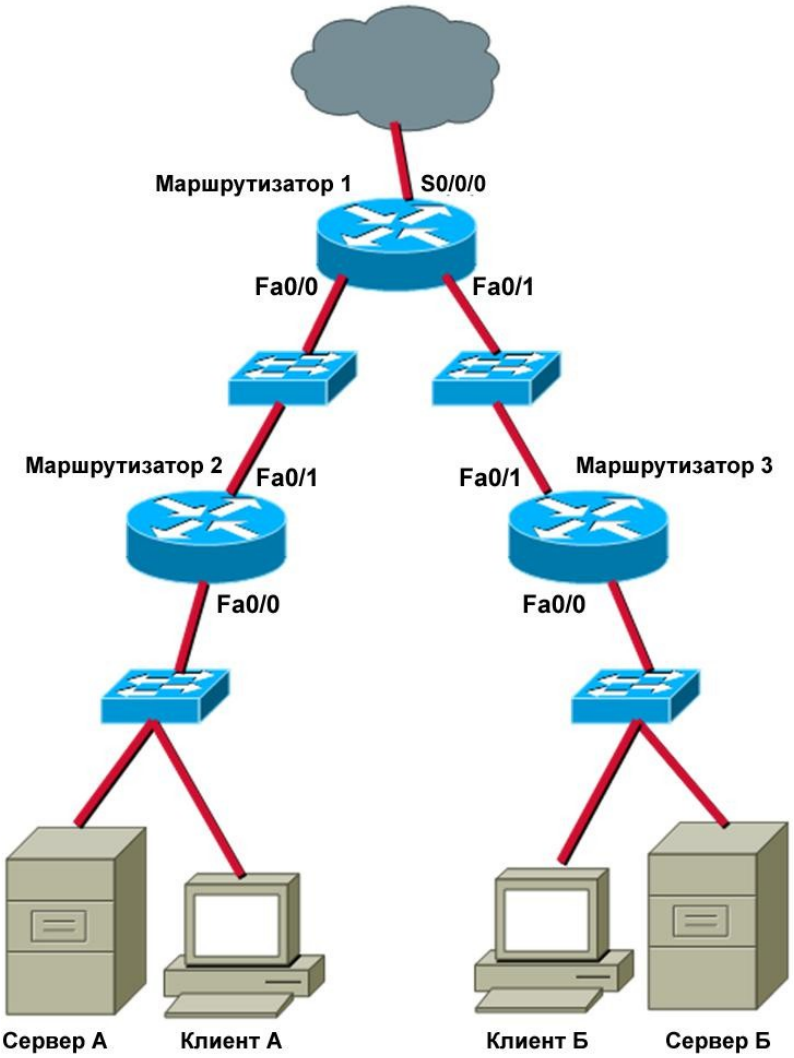
Планирование списков доступа и фильтров портов

Задача

- На основе составленной схемы сети определите места, где необходимо внедрение списков доступа и фильтров портов для защиты сети.

Исходные данные

Представьте, что вы специалист службы поддержки, отправленный на объект для работы с текущей сетью корпоративного клиента, которому необходимо снизить угрозу нарушений сетевой безопасности.



Определение мест для размещения списков доступа

Шаг 1. Ограничение клиента А одной сетью

Вас просят ограничить доступ клиента А только подсетью, к которой он в текущий момент подключен. Клиенту А необходим доступ к серверу А, но сеть Интернет и сервер в должны быть ему недоступны. Где следует разместить список доступа?

Маршрутизатор	Интерфейс	Разрешить или отклонить?	Входной или выходной фильтр?	Основание

Шаг 2. Ограничить доступ к серверу А для клиента А, но разрешить доступ к серверу в и к сети Интернет

Вас попросили запретить доступ клиенту в к серверу А, но клиенту в требуется доступ к сети Интернет и к серверу В. Где следует разместить список доступа?

Маршрутизатор	Интерфейс	Разрешить или отклонить?	Входной или выходной фильтр?	Основание

Шаг 3. Разрешить доступ к маршрутизаторам, использующим только протокол SSH, исключительно клиенту А

Вас попросили ограничить доступ к маршрутизаторам только клиентом А, который будет выполнять функции управляющего ПК для этих маршрутизаторов. Вам необходимо ограничить доступ только протоколом SSH от клиента А и предотвратить доступ Telnet. Где следует разместить список доступа?

Подсказка. Для контроля доступа протокола SSH и Telnet к маршрутизаторам требуется несколько интерфейсов на нескольких маршрутизаторах.

Маршрутизатор	Интерфейс	Входной или выходной фильтр?	Порт	Разрешить или отклонить?	Основание

Изучение универсального защитного программного продукта

Задача

- Изучить универсальный защитный программный пакет, который удовлетворяет требованиям малых предприятий.

Исходные данные

Вам необходимо рекомендовать универсальный защитный программный пакет малому предприятию. На предприятии обеспокоены возможностью заражения вирусами и вредоносным ПО, поскольку ранее возникали такие проблемы. Кроме того, клиент намерен централизовать управление универсальным защитным решением. Клиенту необходимо, чтобы все предупреждения универсального защитного продукта приходили на один адрес, а также он хочет получать предупреждения по электронной почте в случае, если произошло заражение.

Шаг 1. Определение трех продуктов

С помощи сети Интернет изучите продукты от трех различных производителей, отвечающие требованиям малых предприятий. Универсальный защитный продукт должен обладать следующими свойствами:

- антивирусная защита;
- защита от шпионского ПО;
- защита от вредоносных программ;
- централизованное управление;
- предупреждения по электронной почте.

Компания	Продукт

Шаг 2. Сравнение цен

После определения трех различных продуктов, отвечающих требованиям клиента, сравните их цены. На предприятии предусмотрены 27 рабочих станций и 3 сервера. Чтобы получить общую стоимость, не забудьте включить затраты на приобретение лицензий для всех компьютерных систем. Проанализируйте стоимость и предоставьте перечень всех компонентов, включенных общую стоимость.

Компания	Продукт	Цена

Практическая работа 5. Поиск и устранение неисправностей в сети Объяснение договора об уровне обслуживания

Задачи

- Описать назначение договора об уровне обслуживания.
- Рассмотреть общие требования клиента по договору об уровне обслуживания.
- Проанализировать образец договора об уровне обслуживания и ответить на вопросы, относящиеся к его содержанию и соответствию потребностям заказчика.

Основная информация/подготовка

Договор об уровне обслуживания — это формальное соглашение между клиентом и поставщиком услуг. В договоре об уровне обслуживания определены типы и уровни обслуживания, на получение которых клиент может рассчитывать, а также штрафы, которые, возможно, предусмотрены в случае несоблюдения договора. В этой практической работе необходимо понять назначение договора о сервисном обслуживании, а также какие требования клиента он может гарантировать. После этого необходимо проанализировать образец договора об уровне обслуживания между поставщиком услуг Интернета и компанией среднего размера и ответить на вопросы в отношении положений этого договора об уровне обслуживания. Можно работать индивидуально или в небольших группах.

Необходимо использовать следующий ресурс:

- Образец договора об уровне обслуживания (в этой практической работе).

Шаг 1. Рассмотрите типичные потребности клиента

Среднестатистический клиент предъявляет следующие требования к договору об уровне обслуживания. Эти требования необходимо включить в договор об уровне обслуживания с поставщиком услуг.

- **Описание услуги:** описание объема предоставляемых услуг и время, когда услуги необходимы. Здесь также описывается время, когда эта услуга не включена в договор об уровне обслуживания. Описанные услуги, как правило, предоставляются типичным малым и средним производственным компаниям: служба электронной почты, электронная система обмена данными, оперативный финансовый учет, безопасная поддержка удаленных сотрудников, удаленные инструментальные средства и системы контроля, услуги по резервному копированию и восстановлению данных.
- **Доступность:** описание доступности каждой услуги в часах в день и в днях в месяц, когда услуга может быть доступна.
- **Производительность:** описание пикового и внепикового распределения объема данных, который клиент предполагает генерировать для каждой услуги.
- **Надежность:** описание коэффициента надежности, требуемого для каждой услуги.
- **Отслеживание и оповещение о времени отклика:** описание требований к производительности пользователей каждой из услуг.
- **Безопасность:** описание политик обеспечения безопасности клиента в отношении к услугам, предоставляемым ему в соответствии с договором об уровне обслуживания.
- **Цикл финансовых операций:** описание цикла финансовых операций клиента.

- **Штрафы за перерыв в обслуживании:** расчет предварительных потерь клиента в случае перерыва в обслуживании для каждой из услуг, предоставляемых клиенту в соответствии с договором об уровне обслуживания.
- **Затраты:** таблица издержек, оплаченных клиентом в прошлом за услуги, предоставляемые в соответствии с другим договором об уровне обслуживания.

Шаг 2. Проанализируйте образец договора о сервисном обслуживании и определите его основные компоненты

а. Прочтите образец договора об уровне обслуживания, приведенный далее и ответьте на следующие вопросы о его содержании, обязанностях поставщика услуг Интернета и требованиях клиента.

б. Может ли поставщик услуг Интернета в соответствии с этим соглашением считаться ответственным за повреждение оборудования, принадлежащего клиенту, или за потерю данных, произошедших в результате случайных действий сотрудников поставщика услуг Интернета или других лиц? _____

в. Какие примеры одноразовых услуг приведены в договоре об уровне обслуживания?

_____

г. Какие примеры постоянно оказываемых услуг приведены в договоре об уровне обслуживания?

_____

д. На какое время планируется выполнение технического обслуживания, требующего простоя оборудования? За сколько рабочих дней поставщик услуг Интернета должен уведомить

o запланированном простое оборудования?

_____

е. Что делает система сетевого мониторинга поставщика услуг Интернета при обнаружении ошибки?

_____

ж. Какова заявленная доступность системных администраторов в случае системной ошибки?

_____

з. Что такое «контроль использования» и каким образом поставщик услуг Интернета предоставляет эту услугу?

_____

и. Если принять во внимание серьезность проблемы и время отклика поставщика услуг Интернета, то в чем заключается разница в отклике между «Уровнем 1 — обычное рабочее время» и «Уровнем 3 — обычное рабочее время».

_____

к. На чем основано назначение штрафов за перерыв в обслуживании?

_____

(Образец)

Соглашение об уровне обслуживания

Между

[Клиентом]

и

ISP Services Vendor, Inc.

датированное [дата]

I. Общие положения договора об уровне обслуживания

В этом договоре об уровне обслуживания подтверждается соглашение между [Клиентом] и поставщиком услуг Интернета ISP Services Vendor, Inc. (ISPSV) на предоставление услуг Интернета. В нем определяется список предоставляемых услуг, уровни обслуживания, обмен информацией и цены. Это соглашение вступает в силу [начальная дата] и действительно до [конечная дата], если иное не будет указано в поправках. Все положения считаются действительными до внесения соответствующих изменений в поправках к договору.

К договору можно вносить поправки в любое время по договоренности между сторонами. При значительных изменениях в услугах может потребоваться некоторое время для их осуществления. Время введения в действие поправки указывается в этой поправке. Для внесения изменений в договор, приводящих к изменению в оплате услуг, может потребоваться 30 дней.

Каждая из сторон может расторгнуть данное соглашение в целом или частично, уведомив об этом за 30 дней. Договор об уровне обслуживания пересматривается ежегодно. В зависимости от изменения уровня обслуживания может измениться стоимость обслуживания.

II. Гарантии и обязанности

Цель ISPSV — обеспечить высококачественные и экономичные услуги Интернета жителям района.

В соответствии с данным договором об уровне обслуживания берем на себя обязательство защищать оборудование и поддерживаемые данные от намеренного повреждения со стороны сотрудников ISPSV или других лиц, получивших от ISPSV доступ к оборудованию. Однако мы не несем ответственность за повреждение оборудования, принадлежащего Клиенту, или потерю данных в результате случайных действий сотрудников поставщика услуг Интернета или других лиц.

III. Услуги, предоставляемые [Клиенту]

В следующей таблице указаны услуги, включаемые в этот договор об уровне обслуживания. Цены на услуги определяются, исходя из модели ценообразования ISPSV, и прилагаются как поправка к этому договору об уровне обслуживания.

	Услуга	Комментарии
	Одноразовые услуги	
	Установка стойки и компьютера	
	Реализация системы резервного копирования	
	Настройка межсетевого экрана	
	Постоянные услуги	
	Хостинг сервера	
	Резервное копирование и восстановление данных	
	Системное администрирование ОС Unix	
	Системное администрирование ОС Windows	
	Администрирование приложений	

IV. Доступность системы

Системы должны быть доступны 7 дней в неделю, 24 часа в сутки за исключением запланированных через определенные периоды времени процедур технического обслуживания, требующих простоя

оборудования. График технического обслуживания с простоем оборудования обсуждается с каждым клиентом. Такое обслуживание выполняется между 19:00 и 7:00. Клиенты должны быть уведомлены о запланированном простое оборудования, по меньшей мере, за три (3) рабочих дня.

Профессиональные системные администраторы дежурят в офисе поставщика услуг Интернета по рабочим дням с 7:00 до 19:00. В случае системных ошибок можно вызвать дежурного системного администратора 7 дней в неделю, 24 часа в сутки.

V. Мониторинг системы

Для всех систем, расположенных на площадях поставщика услуг Интернета, проводится базовый мониторинг работы системы, регулярно выполняющий тестирование ее работоспособности. При обнаружении ошибки система мониторинга вызывает дежурного системного администратора.

Внешний мониторинг работы можно осуществить, заключив соглашение с компанией ExternalAlertServices, осуществляющей внешний мониторинг. При заключении такого соглашения эта услуга оплачивается клиентом (примерно 25 долларов США в месяц).

Контроль использования предоставляет пользователям статистические данные об обращениях к веб-узлам. Для этой цели поставщик услуг Интернета использует сервер WebTrends. Данные с сервера WebTrends ежемесячно предоставляются клиентам.

VI. Системные уведомления

Поставщик услуг Интернета предоставляет ряд списков адресов электронной почты для каждого сервера и приложения. Включение в эти списки определяется и регулируется клиентом. К этим спискам относятся:

- **[system]-info**

  Уведомление о зарегистрированных системой сообщениях о рабочем состоянии системы.

- **[system]-announce**

  Получение всех сообщений поставщика услуг Интернета о запланированном техническом обслуживании, простоях системы и других событиях.

- **[system]-[application]-info**

  Уведомление о зарегистрированных системой сообщениях о рабочем состоянии приложения.

- **[system]-[application]-announce**

  Получение всех сообщений поставщика услуг Интернета о запланированном техническом обслуживании, простоях системы и других событиях.

VII. Процесс управления изменениями

Все просьбы внести изменения в системы или приложения, вносимые клиентом или сотрудниками ISPSV, должны быть одобрены в процессе управления изменениями. Этот процесс начинается с подачи запроса начать процесс управления изменениями поставщика услуг Интернета. Запросы регистрируются, а затем посылаются по электронной почте уполномоченному Клиенту для получения одобрения. Клиент выражает одобрение или отвергает запрос по электронной почте.

За исключением экстренных ситуаций, запросы не выполняются без получения одобрения со стороны Клиента. В случае экстренной ситуации необходимо как можно быстрее связаться с клиентом и проинформировать его об изменениях.

o Методы обмена информацией

Стандартные запросы

Все стандартные вопросы об изменении учетных записей и другие неэкстренные запросы необходимо подавать через процесс управления изменениями поставщика услуг Интернета. В запрос необходимо включить:

- имя клиента;
- название системы;
- название приложения;
- суть запроса;
- необходимая дата изменений;
- серьезность проблемы (уровень 1, 2, 3 или 4).

Экстренные запросы

Необходимо подавать экстренные запросы либо лично, либо через горячую линию поставщика услуг Интернета по номеру (123) 456-7890. Если звонок перенаправляется на голосовую почту, оставьте сообщение, указав свое имя и телефон, по которому можно перезвонить. Дежурный системный администратор будет в течение 5 минут уведомлен о звонке и перезвонит.

Конфликты

Если проблемы не решаются к удовлетворению клиента с использованием перечисленных выше методов, клиент может потребовать ответа, обратившись к руководству ISP VENDOR в следующем порядке: 1. Директор филиала, 2. Директор по маркетингу, 3. Президент.

o Права для обработки запросов системы

Мы поддерживаем четыре списка для предоставления пользователям полномочий. Эти списки содержатся в приложении к документу клиента:

Список пользователей с базовыми правами

Список тех, кто может добавлять людей и удалять их из остальных списков.

Список пользователей с правом изменения учетной записи

Список тех, кто может потребовать изменения учетной записи.

Список пользователей с правом изменения системы

Список тех, кто может потребовать изменения системы.

Список пользователей с правом изменения приложений

Список тех, кто может потребовать изменения приложений.

VIII. Серьезность проблемы и время отклика

ISPSV реагирует на проблемы в соответствии со следующими уровнями их серьезности:

Серьезность проблемы	Начальное время отклика	Последующие мероприятия с Клиентом
Уровень 1 — обычное рабочее время	Ответ клиенту в течение 30 минут с момента уведомления, 100% времени.	Каждый час
Уровень 1 — нерабочее время	Ответ клиенту в течение 1 часа с момента уведомления, 95% времени	Каждый час
Уровень 2 — обычное	Ответ клиенту в течение 4 часов с момента	Каждый день

рабочее время	уведомления, 100% времени	
Уровень 3 — обычное рабочее время	Ответ клиенту в течение 1 рабочего дня с момента уведомления, 100% времени.	Каждую неделю
Уровень 4 — обычное рабочее время	Ответ клиенту в течение 3 рабочих дней с момента уведомления, 100% времени.	Каждый месяц

o Уровень серьезности 1:

Серьезные последствия для деятельности: определяется как проблема, приведшая к полному прерыванию обслуживания производственной среды Клиента, работа продолжаться не может. Временные решения для обеспечения тех же функций невозможны, и их невозможно найти достаточно быстро для сведения к минимуму последствий для работы Клиента. Проблема имеет одну или более из следующих характеристик:

- большое число пользователей не могут получить доступ к системе;
- не доступны существенно важные функции. Приложение не может продолжать работу из-за неработоспособности важной функции, невозможно обеспечить безопасность или резервное копирование данных и т.д.

o Уровень серьезности 2:

Значительные последствия для деятельности: этот термин применим, когда обработка данных выполняется, но производительность существенно снижена и/или работа системы значительно ограничена. Обходное решение невозможно, но работу можно продолжать в ограниченном режиме. Проблема имеет одну или более из следующих характеристик:

- внутренняя программная ошибка, приведшая к сбою системы, но возможна перезагрузка или восстановление;
- серьезное снижение производительности;
- недоступны некоторые важные функции, но система может продолжать работу в ограниченном режиме.

o Уровень серьезности 3:

Незначительные последствия для деятельности: проблема, которая привела к минимальной потере в предоставлении услуг. Последствия этой проблемы минимальны, или она вызвала неудобство (например, необходимость ручного перезапуска для восстановления функций продукта). Проблема имеет одну или более из следующих характеристик:

- программная ошибка, для устранения которой у Клиента есть приемлемые обходные пути;
- незначительное снижение производительности;
- программная ошибка, для устранения которой необходимо вручную редактировать конфигурацию или файлы сценария, связанные с этой проблемой.

o Уровень серьезности 4:

Нет последствий для производительности: проблема не вызвала перерыва в обслуживании и никак не препятствует использованию системы. Проблема имеет одну или более из следующих характеристик:

- модернизация программного обеспечения, для которой у Клиента есть приемлемые решения;
- ошибка в документации.

IX. Штрафы за перерыв в обслуживании

Уровень серьезности	Затронутые услуги	Оценка штрафной

проблемы		суммы

X. Политики поставщика услуг Интернета

См. все политики, включая обеспечение безопасности, управление изменениями, запланированное техническое обслуживание, процедуры резервного копирования и восстановления данных, политику целевого пользования и требования к аппаратному обеспечению, в документации ISPSV.

XI. Оплата услуг

ISPSV выставляет счета ежемесячно, непосредственно снимая согласованную сумму с соответствующего счета в счет оплаты предоставленных услуг.

XII. Подписи

Этот договор об уровне обслуживания был прочитан и принят уполномоченными представителями ISPSV и [Клиента]

Подпись (ISPSV) Дата	Подпись ([Клиента]) Дата
Имя	Имя
Должность	Должность

Приложение 1. Услуги и цены

Система или приложение	Услуги	Цена

Приложение 2. Список контактных лиц при запросах системы

Имя	Адрес электронной почты	Рабочий телефон	Мобильный телефон	Домашний телефон
Контактное лицо с базовыми правами				
Изменение учетной записи				
Системные изменения				
Изменение приложения				

Сбор сетевых данных с помощью программы Wireshark

Цели

- выполнить сбор сетевого трафика с помощью программы Wireshark, чтобы ознакомиться с интерфейсом и средой Wireshark;
- проанализировать трафик для веб-сервера;
- создать фильтр для ограничения сбора сетевых данных пакетами ICMP.
- отправить эхо-запрос удаленному узлу, чтобы понаблюдать за работой фильтра пакетов ICMP в ходе сбора сетевых данных.

Предварительная информация/подготовка

В этой практической работе вы установите программу Wireshark, широко известный анализатор сетевых протоколов и средство мониторинга. Программа Wireshark собирает все пакеты, отправленные или полученные сетевой интерфейсной платой (NIC) компьютера. Ее можно установить либо в аудитории, либо дома на ПК. Вам он понадобиться для отслеживания и просмотра разных типов сетевых протоколов и трафика. Ранее программа Wireshark была известна под именем Ethereal.

Программа Wireshark поставляется бесплатно и доступна по адресу www.wireshark.org. Установщик программы, wireshark-setup-0.99.5.exe, должен быть доступен на локальном сервере сетевой академии.

Практическую работу можно выполнять индивидуально, по парам или в группе.

Требуются следующие ресурсы:

- ПК под управлением ОС Windows XP с сетью Ethernet и хотя бы двумя узлами;
- программа Wireshark версии 0.99.5 (или самая последняя версия);
- подключение к сети Интернет (не обязательно, но желательно);
- доступ к командной строке ПК;
- доступ к сетевой конфигурации TCP/IP ПК.

Шаг 1. Установка и запуск программы Wireshark

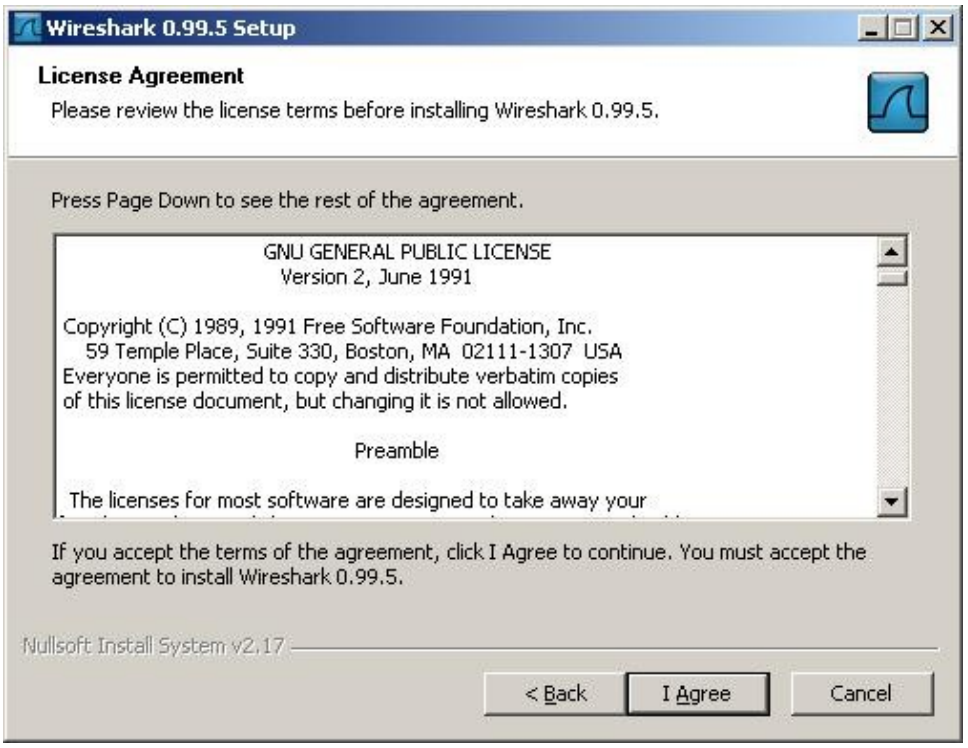
Если программа Wireshark загружалась на ПК ранее, перейдите в папку с программой Wireshark **Start > All Programs > Wireshark > Wireshark (пуск > программы > Wireshark > Wireshark)** и щелкните значок приложения.

Если ранее программа Wireshark не устанавливалась, выполните следующие действия:

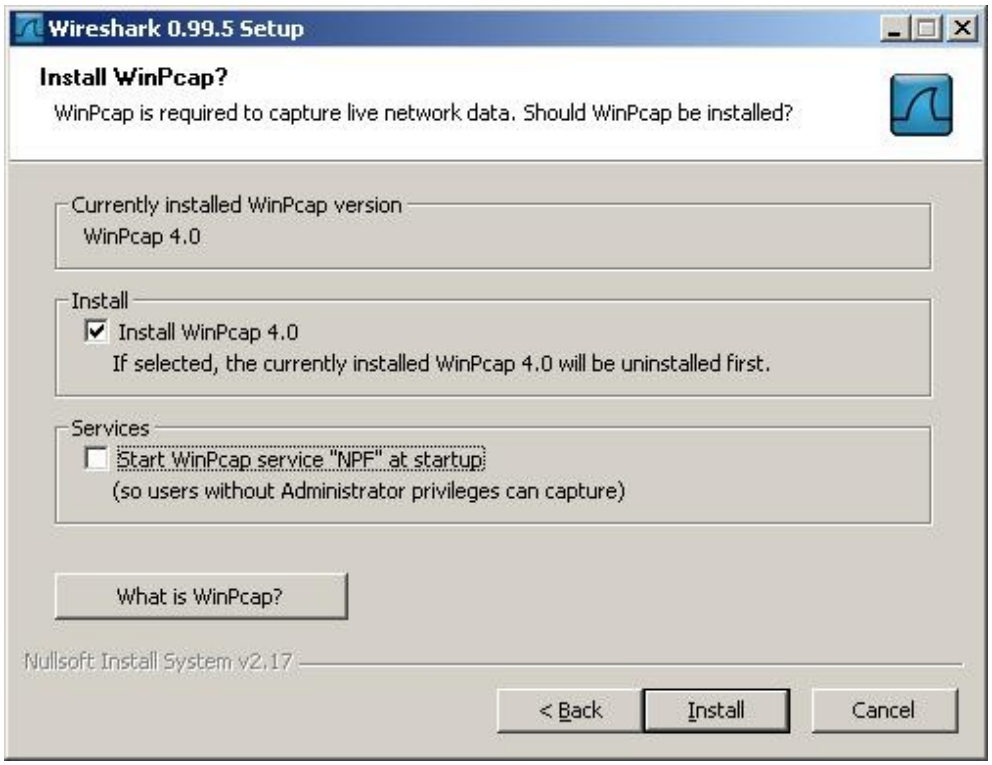
а. Указав путь в локальной сети до установщика программы Wireshark, wireshark-setup-0.99.5.exe, загрузите установщик на рабочий стол ПК.

б. Щелкните установщик два раза и следуйте его подсказкам, принимая значения по умолчанию.

2) Нажмите кнопку **I Agree** (принять).



3) Убедитесь, что на ПК установлен WinPcap. В WinPcap входит драйвер для поддержки сбора пакетов. Программа Wireshark использует эту библиотеку для сбора динамических сетевых данных в Windows.



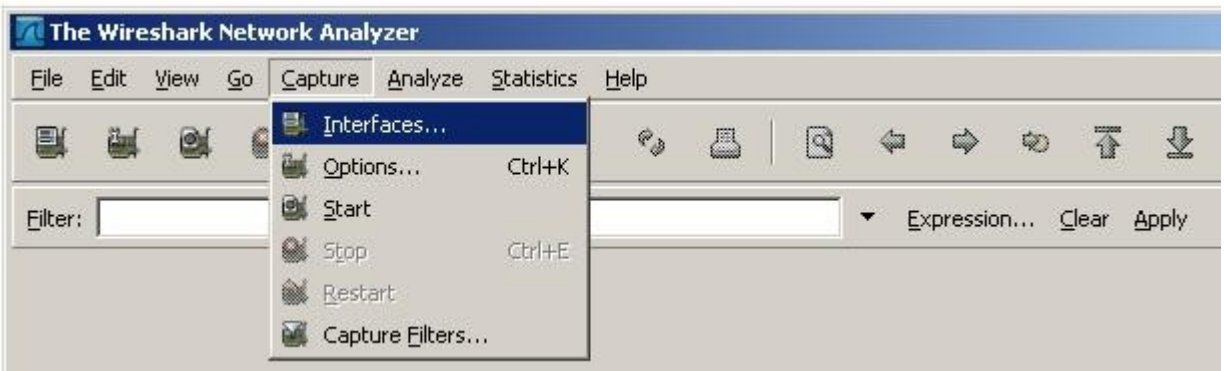
в. Щелкните **Install (установить)** и следуйте подсказкам до конца процесса установки.

г. После установки программы установите соответствующий флажок, чтобы запустить программу Wireshark.

Шаг 2. Выбор интерфейса для сбора пакетов

д. Запустите приложение Wireshark.

е. В меню **Capture (сбор)** выберите пункт **Interfaces (интерфейсы)**.

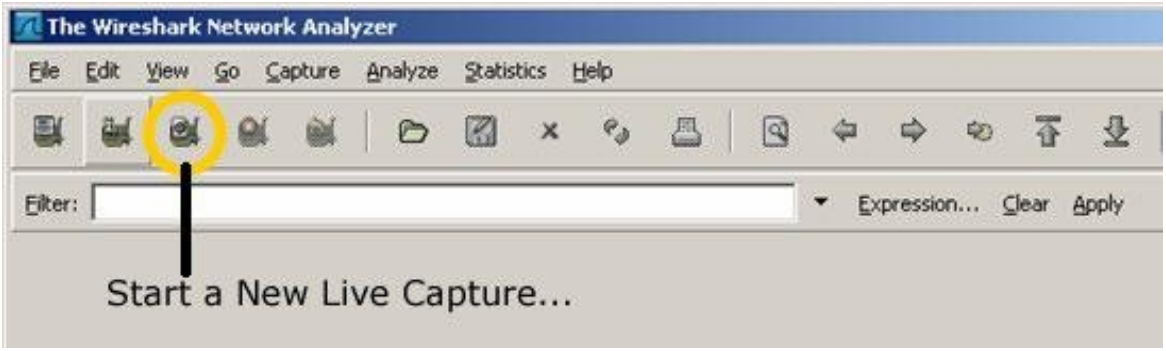


4) Нажмите кнопку **Start** (пуск) для интерфейса Ethernet (NIC), который требуется использовать для сбора сетевого трафика.

Шаг 3. Запуск сбора сетевых данных

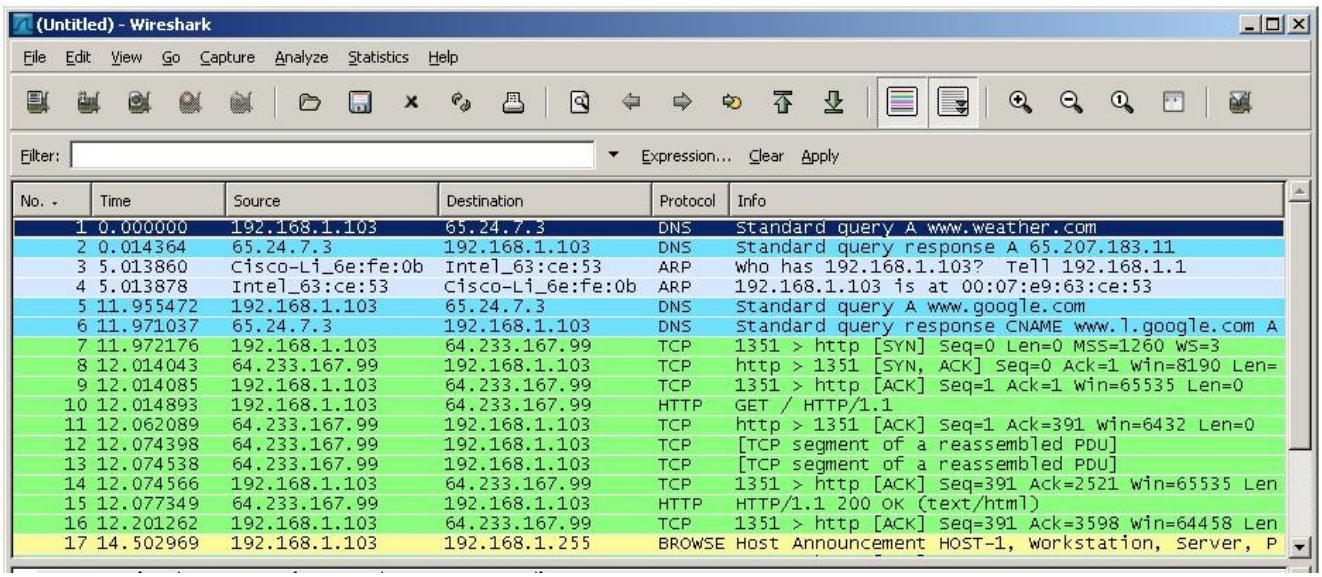
ж. Прокрутите меню и просмотрите панель инструментов в интерфейсе запуска Wireshark.

з. Нажмите кнопку **New Live Capture** (новый сбор динамических данных) и просмотрите сведения, собранные Wireshark. Пусть сбор данных продолжается в течение нескольких минут, чтобы вы могли понаблюдать за различными типами трафика в сети.



Шаг 4. Анализ сведений о веб-трафике (не обязательно)

и. Если существует подключение к сети Интернет, откройте веб-обозреватель и перейдите в узел www.google.com. Сверните окно Google и вернитесь в Wireshark. Должен быть отображен трафик, схожий с тем, что представлен ниже. Найдите столбцы **Source**, **Destination** и **Protocol** (источник, адрес назначения и протокол) на экране Wireshark.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.103	65.24.7.3	DNS	Standard query A www.weather.com
2	0.014364	65.24.7.3	192.168.1.103	DNS	Standard query response A 65.207.183.11
3	5.013860	Cisco-Li_6e:fe:0b	Intel_63:ce:53	ARP	Who has 192.168.1.103? Tell 192.168.1.1
4	5.013878	Intel_63:ce:53	Cisco-Li_6e:fe:0b	ARP	192.168.1.103 is at 00:07:e9:63:ce:53
5	11.955472	192.168.1.103	65.24.7.3	DNS	Standard query A www.google.com
6	11.971037	65.24.7.3	192.168.1.103	DNS	Standard query response CNAME www.l.google.com A
7	11.972176	192.168.1.103	64.233.167.99	TCP	1351 > http [SYN] Seq=0 Len=0 MSS=1260 WS=3
8	12.014043	64.233.167.99	192.168.1.103	TCP	http > 1351 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=
9	12.014085	192.168.1.103	64.233.167.99	TCP	1351 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
10	12.014893	192.168.1.103	64.233.167.99	HTTP	GET / HTTP/1.1
11	12.062089	64.233.167.99	192.168.1.103	TCP	http > 1351 [ACK] Seq=1 Ack=391 Win=6432 Len=0
12	12.074398	64.233.167.99	192.168.1.103	TCP	[TCP segment of a reassembled PDU]
13	12.074538	64.233.167.99	192.168.1.103	TCP	[TCP segment of a reassembled PDU]
14	12.074566	192.168.1.103	64.233.167.99	TCP	1351 > http [ACK] Seq=391 Ack=2521 Win=65535 Len
15	12.077349	64.233.167.99	192.168.1.103	HTTP	HTTP/1.1 200 OK (text/html)
16	12.201262	192.168.1.103	64.233.167.99	TCP	1351 > http [ACK] Seq=391 Ack=3598 Win=64458 Len
17	14.502969	192.168.1.103	192.168.1.255	BROWSE	Host Announcement HOST-1, Workstation, Server, P

5) Подключение к серверу Google начнется с отправки запроса на DNS-сервер для поиска
IP-адреса сервера. IP-адрес сервера назначения, по всей вероятности, начнется с 64.x.x.x. Каковы источник и адрес назначения первого пакета, отправленного на сервер Google?

_____

к. Откройте еще одно окно веб -обозревателя и перейдите в базу данных **ARIN Whois** http://www.arin.net/whois/ или воспользуйтесь другим средством поиска **whois** и введите IP-адрес сервера назначения. Какой организации назначен этот IP-адрес?

_____

л. Какие протоколы служат для подключения к веб-серверу и доставки веб-страницы в ваш локальный узел? _____

м. Каким цветом выделяется трафик между вашим узлом и веб-сервером Google?

_____

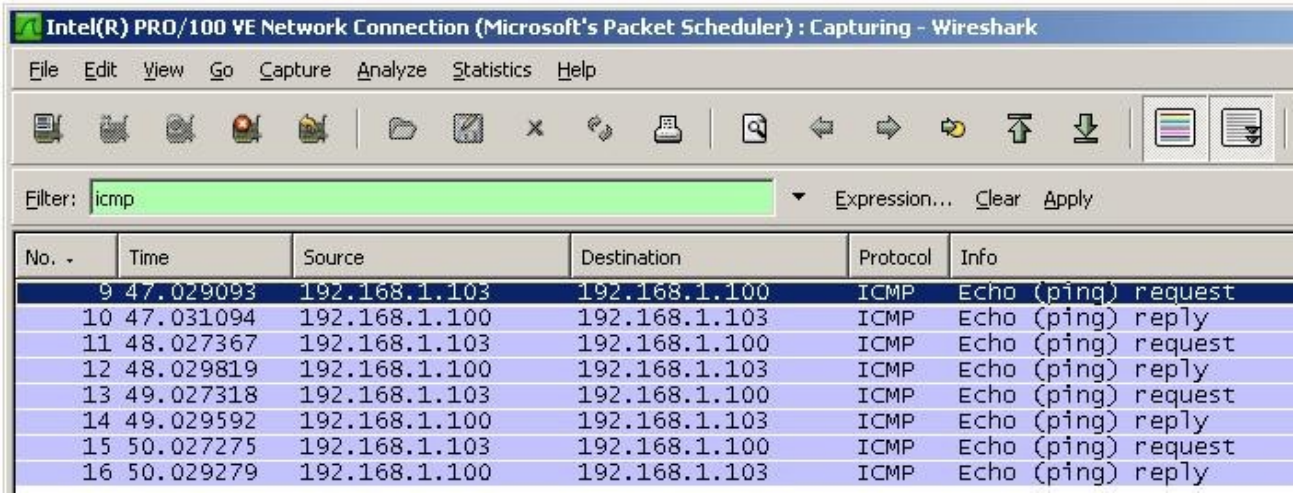
Шаг 5. Фильтрация сбора сетевых данных

н. Откройте окно командной строки, выбрав **Start > All Programs > Run (пуск > программы > выполнить)** и введя **cmd**. Либо щелкните **Start > All Programs > Accessories (пуск > все программы > стандартные > командная строка)**.

о. Отправьте эхо-запрос по IP-адресу узла в вашей локальной сети и понаблюдайте за процессами в окне сбора Wireshark. Прокрутите вниз и вверх окно, в котором отображается трафик. Какие используются типы протоколов?

_____

п. В текстовом поле **Filter (фильтр)** введите **icmp** и щелкните **Apply** (применить). Протокол управления сообщениями в Интернет (ICMP) — это протокол, используемый эхо-запросом для проверки сетевого подключения к другому узлу.



р. Какой трафик отображается при вводе команды icmp в текстовое поле **Filter** (фильтр)?

_____

с. Щелкните **Filter (фильтр):** Кнопка **Expression (выражение)** в окне Wireshark. Прокрутите список вниз и просмотрите возможности фильтрации. Есть ли в списке протоколы TCP, HTTP, ARP и другие? _____

Шаг 6. Вопросы для повторения

т. В поле фильтра отображены сотни фильтров: Возможность выражения. В больших сетях может быть много разных типов трафика в огромных объемах. Какие три фильтра из длинного списка, вы думаете, могут быть наиболее эффективны для сетевого администратора?

_____

у. Программа Wireshark это средство для внеполосного или внутриполосного мониторинга сетей? _____. Поясните свой ответ.

_____

_____

Планирование решения резервного копирования

Задача

- Исходя из бизнес-сценария, составьте план соответствующего решения для резервирования.

Предварительная информация/подготовка

К вам поступил запрос на предоставление плана и предложения, связанных с решением резервирования для малого корпоративного клиента ИСП, на которого вы работаете. Малое предприятие обеспокоено потерями ценных корпоративных данных, в частности, последние три года случались потери данных из-за сбоев аппаратного обеспечения и пользовательских ошибок. Они хотят, чтобы в решение был встроен план наискорейшего восстановления данных. Клиент готов взять на себя локальные административные функции по мониторингу и управлению локальной системой резервного копирования.

Текущие требования данных:

Сервер 1: 50 Гб;

Сервер 2: 100 Гб;

Сервер 3: 10 Гб.

Исходя из текущего роста объемов данных, компания прогнозирует ежегодный десятипроцентный рост общего объема данных.

Компания отдает предпочтение решению резервного копирования, которое позволит им создавать ежедневные резервные копии на протяжении 4 недель и дополнительно выполнять ежемесячное архивирование на протяжении 12 месяцев. Кроме того, они бы предпочли решение со сроком службы 5 лет при сохранении им своих функциональных возможностей.

ПРИМЕЧАНИЕ. Следует учесть, что они не приобрести ленточный автозагрузчик или библиотечную систему, что означает, что емкость резервного носителя должна быть достаточной, чтобы разместить все данные в одном устройстве.

Шаг 1. Выбор носителя и аппаратного обеспечения для резервного копирования

Ориентируясь на типы носителей, представленные в этом курсе, с помощью сети Интернет определите подходящий носитель с емкостью, отвечающей требованиям предприятия. Кроме того, необходимо узнать стоимость приобретения дополнительного аппаратного обеспечения на случай необходимости и стоимость носителя. Также на основе прошлых требований определите количество носителей для резервного копирования. Введите свои рекомендации в таблицу, представленную далее:

ПРИМЕЧАНИЕ. Стандартные рабочие часы в компании — с 8.00 до 18:00 с понедельника по пятницу, но работники могут начинать работу в 7:00 и оставаться до 20:00. Поэтому было решено, что резервное копирование возможно только после 22:00 и должно завершаться до 6:00. Оборудование и носители для резервного копирования должны предусматривать скорость достаточную для копирования всех данных со всех серверов за указанный период времени.

Оборудование / носитель	Цена	Количество

Шаг 2. Разработка плана и порядка резервного копирования

После того, как вы определились с носителем для резервного копирования, пришло время составить предложение относительно резервного копирования и установить порядок управления предприятием своей системой резервного копирования. Необходимо решить, какой тип резервного копирования лучше всего подходит предприятию и как лучше всего спланировать замену носителей. На предприятии должен быть предусмотрен порядок действий, который прост и легок для исполнения. Носители должны быть оснащены соответствующими ярлыками, чтобы клиент знал, что копируется в тот или иной день. Предлагаемый вами план должен выполнять всем потребностям клиента. Кроме того, обозначьте другие нерешенные проблемы или вопросы, которые необходимо обсудить для определения удачного решения для клиента. Опишите свой план, заполнив следующие пункты:

a. Опишите рекомендованное оборудование и обоснуйте свой выбор:

_____

_____

_____

_____

_____

б. Опишите размещение оборудования в сети и скорость его сетевого канала:

_____

_____

_____

_____

в. Опишите используемый носитель резервного копирования и обоснуйте его выбор:

_____

_____

_____

_____

г. Опишите график резервного копирования:

_____

_____

_____

_____

д. Опишите порядок резервного копирования и восстановления данных, в том числе: тип резервного копирования (обычный, разностное, инкрементное), процедуру его тестирования, какого рода обслуживание требует оборудование. Как будут помечены записи и где будут храниться записи после резервного копирования. Если возникнет необходимость в восстановлении резервных копий, каков порядок действий, используемый для файла, папки, диска (если требуется, воспользуйтесь дополнительными листами)?

_____

_____

_____

_____

_____

_____

_____