

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению лабораторных работ
по дисциплине «Программно-аппаратные средства защиты информации»
для студентов направления подготовки
10.03.01 «Информационная безопасность»
Направленность (профиль)
«Организация и технологии защиты информации (по отрасли или в сфере
профессиональной деятельности)»

Ставрополь
2026

Содержание:

ЛАБОРАТОРНАЯ РАБОТА № 1-3

Общие сведения о программно-аппаратных средствах защиты информации 3

ЛАБОРАТОРНАЯ РАБОТА № 4-6 Хранение аутентифицирующей информации в открытых компьютерных системах. 36

ЛАБОРАТОРНАЯ РАБОТА № 7-8 Развитие технологий межсетевого экранирования.....50

ВВЕДЕНИЕ

1. Цель и задачи освоения дисциплины

Дисциплина «Программно-аппаратные средства защиты информации» относится к профессиональному циклу образовательной программы направления подготовки 10.03.01 Информационная безопасность, направленность (профиль) «Организация и технологии защита информации (по отрасли или в сфере профессиональной деятельности)».

Цель освоения дисциплины: подготовка выпускника к деятельности, связанной с эксплуатацией и обслуживанием аппаратуры и оборудования, содержащего современные средства вычислительной техники, получение основополагающих знаний о программно-аппаратных средствах защиты информации в операционных системах, вычислительных сетях и системах управления базами данных, средствах антивирусной защиты.

Задачами дисциплины являются:

1. Формирование требований к системе управления ИБ конкретного объекта;
2. Проектирование системы управления ИБ конкретного объекта.
3. Эффективное управление ИБ конкретного объекта.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИД-3 ОПК-9 Выбирает оптимальный вариант использования навыков и методик применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности	-демонстрирует знания устройства и принципов работы криптографических средств защиты информации, применяемых в компьютерных системах и сетях; -устанавливает, настраивает и интегрирует криптографические средства защиты информации в компьютерных системах и сетях

ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ИД-1 ОПК-10 Использует методологический базис теории защиты информации, используемый при разработке формировании политики информационной безопасности	- использует федеральные, отраслевые и ведомственные нормативные документы для формирования политики информационной безопасности; - использует нормативно-правовые документы при разработке положений, приказов, инструкций и других документов, реализующих политику информационной безопасности; - способен принимать участие в организации работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты информации
---	--	--

ПЛАНЫ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

ЛАБОРАТОРНАЯ РАБОТА № 1-3

Тема: Инициализация цус и пу цус апкш «континент»

1.Цель работы :

1. Инициализация ЦУС и ПУ ЦУС.
2. Приобретение практических навыков настройки ЦУС и ПУ ЦУС.

Формируемые компетенции: ОПК-9, ОПК-10.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал, посвящённый настройке туннеля VPN GRE по схеме «точка-точка».
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

3. Распределение времени занятия:

Всего: 270 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 70 мин

1. Инициализация и настройка ЦУС и ПУ ЦУС 70 мин

Проверка выполнения практического занятия 10 мин

Заключительная часть 3 мин

4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

4.1. Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

4.2. Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию;

- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;

- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

4.3. Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

6. Программное обеспечение

АПКШ «Континент», виртуальная машина VmWare Workstation

7. Основные теоретические сведения

См. рекомендованную к ознакомлению литературу по изучаемой дисциплине

8. Литература

1. James Boney, Cisco IOS in a Nutshell, O'Reilly, 2010
2. Wendell Odom, Interconnecting Networking Devices Cisco, Part 2, Cisco Press, 2010

9. Методические рекомендации по выполнению лабораторной работы

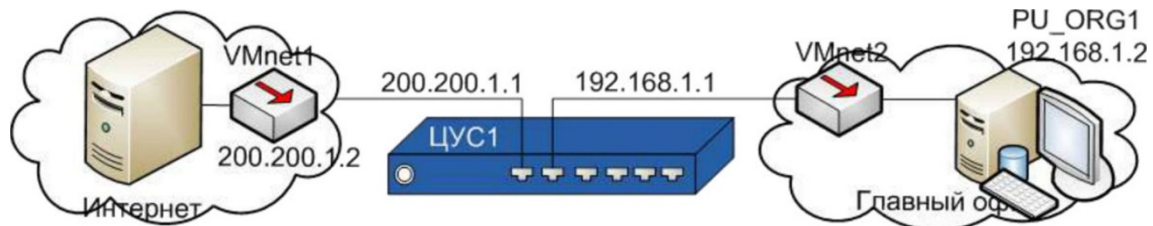


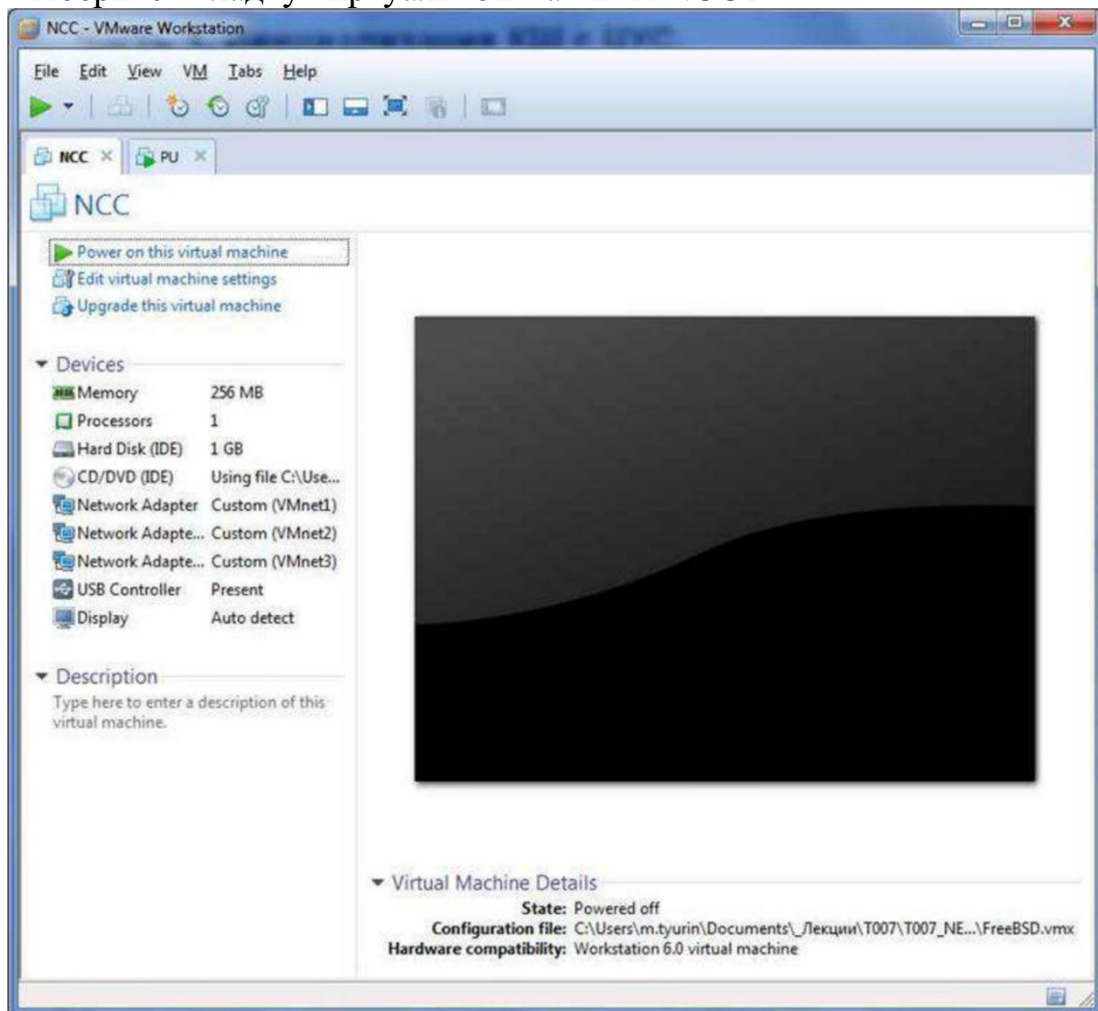
Рисунок 1 - Топология

9.1 Методические пояснения и рекомендации по выполнению первого вопроса

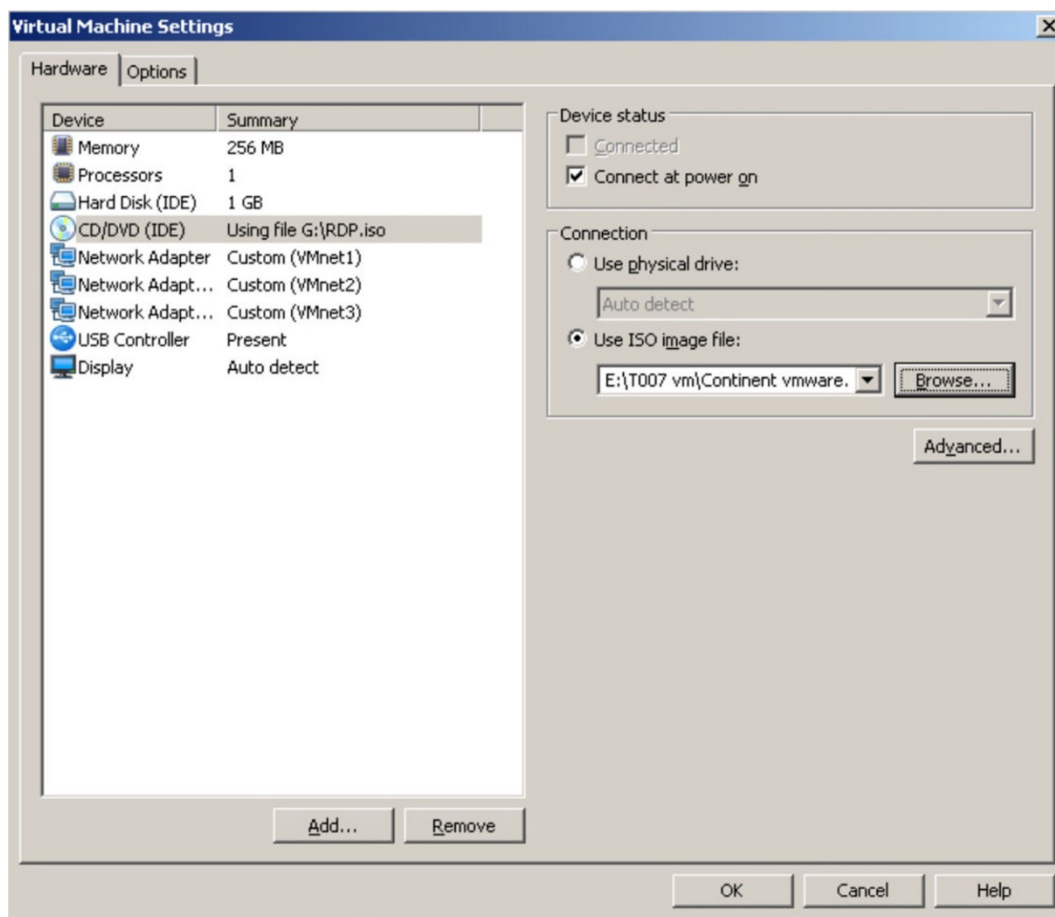
Вопрос 1 Инициализация КШ с ЦУС.

1. Запустите VmWare Workstation

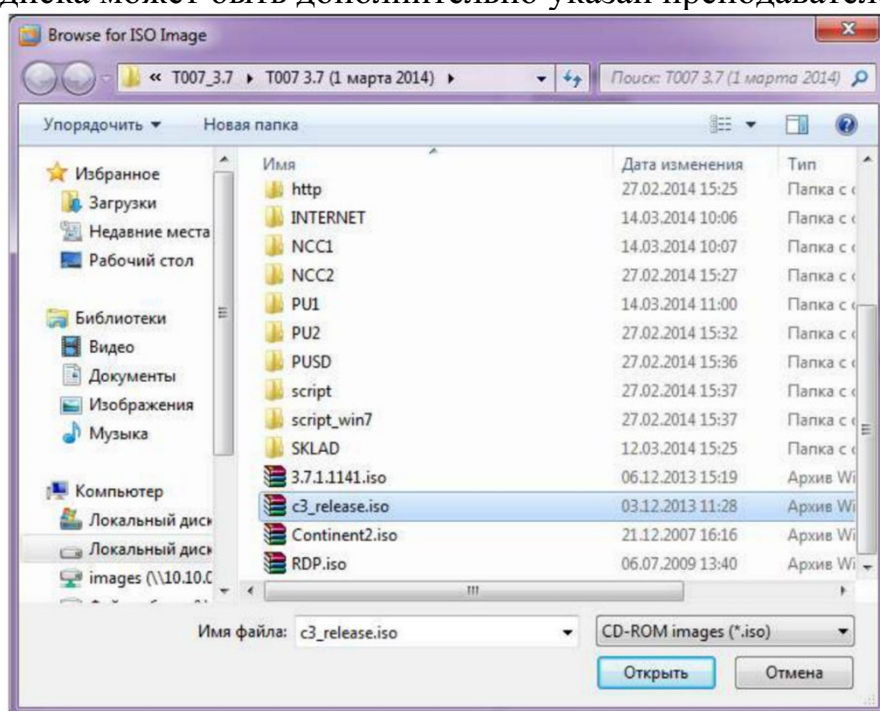
Выберите вкладку виртуальной машины NCC1



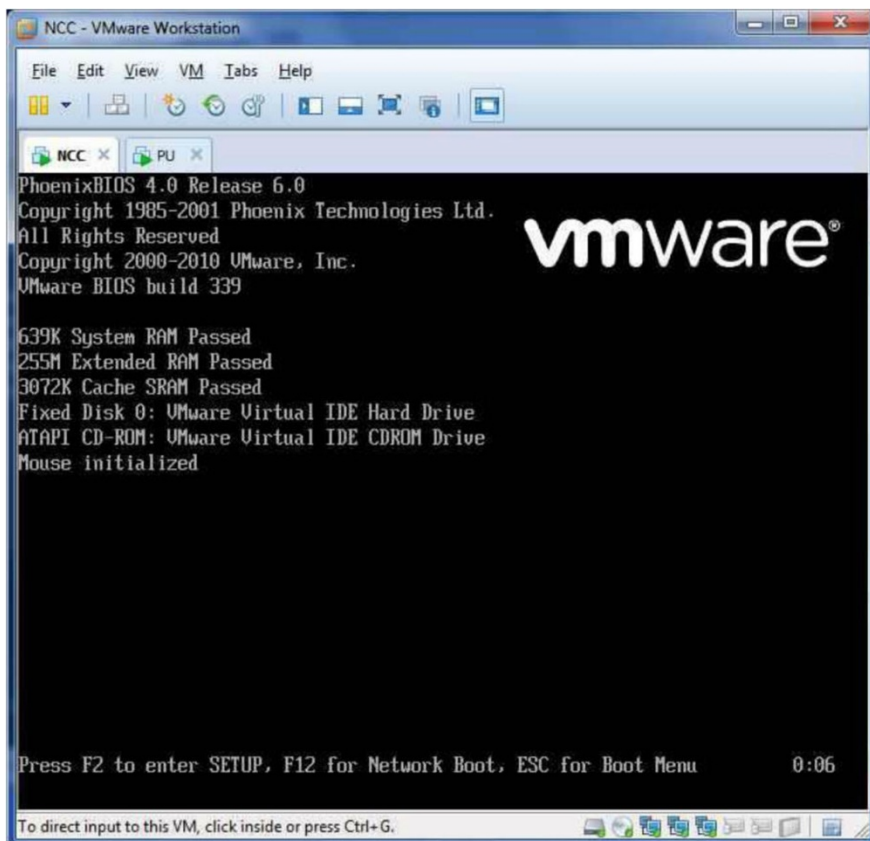
2. Назначьте в качестве CD образ C3_rel0as6.iso (при изменении версии образ диска может быть дополнительно указан преподавателем) для этого выполните двойное нажатие мышкой на CD.
В открывшемся окне нажмите кнопку Browse



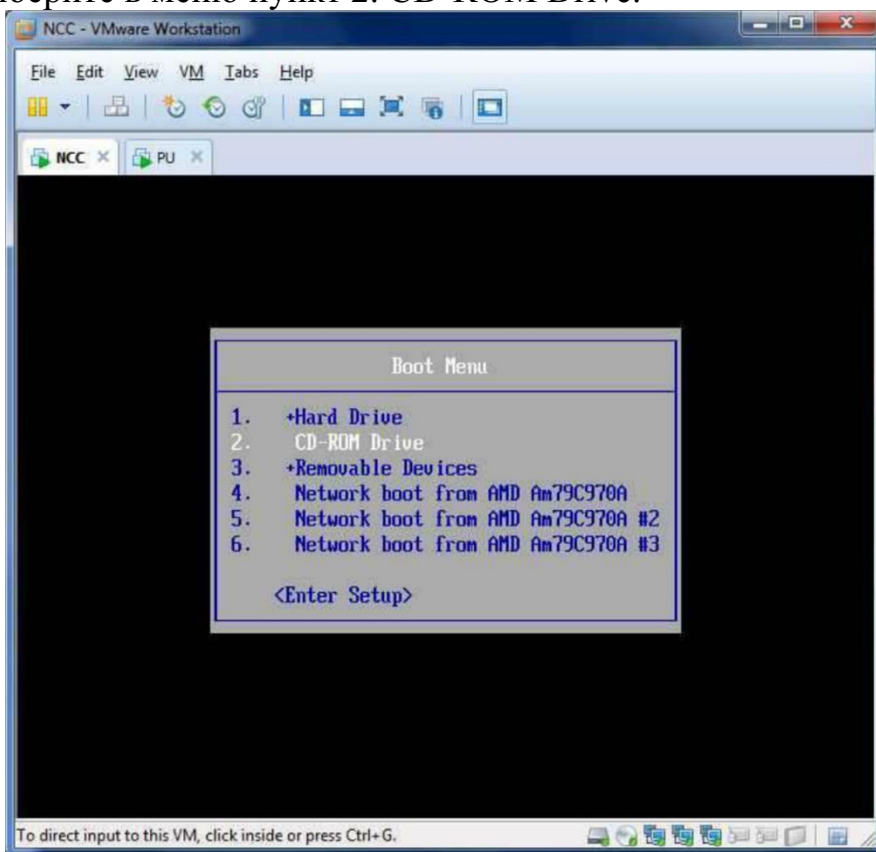
3. Выберите соответствующий образ диска «c3_release.iso» (при изменении версии образ диска может быть дополнительно указан преподавателем)



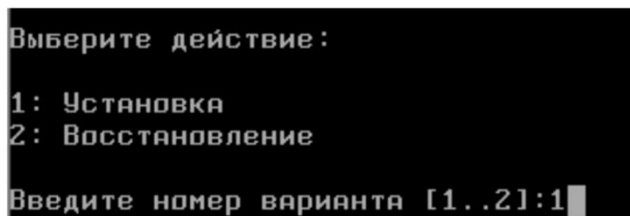
Запустите виртуальную машину.



4. Передайте управление в ее окно, щелкнув на нем левой кнопкой мышки.
 Включите меню автозагрузки, нажав ESC.
 Выберите в меню пункт 2. CD-ROM Drive.



- Нажмите <Enter>. Начнется загрузка ОС с предъявленного носителя.
 5. По окончании базовой загрузки ОС на экране появится запрос:



```
Выберите действие :  
1: Установка  
2: Восстановление  
Введите номер варианта [1..2]:1
```

6. Появится запрос:

Установка «Континент»

продолжить? (y/n):

7. Введите "y" и нажмите <Enter>.

На экране появится предупреждение:

***** Внимание * *****

ВСЕ данные на жестком диске будут БЕЗВОЗВРАТНО ПОТЕРЯНЫ
продолжить? (y/n):

8. Введите "y" и нажмите клавишу <Enter>.

На экране появится запрос:

Введите идентификатор криптошлюза: 1

Введите 1 и нажмите <Enter>.

9. На экране появится меню выбора варианта установки:

Выберите вариант установки:

- 1: Шлюз;
- 2: Шлюз с сервером доступа;
- 3: ЦУС ;
- 4: ЦУС с сервером доступа;
- 5: ДА;
- 6: АРМ генерации ключей.

Введите номер варианта [1...6]: 3

Введите 3 : ЦУС и нажмите <Enter>.

10. На экране появятся строка конфигурации данного КШ и меню выбора варианта

установки аппаратной конфигурации: выберите "3: IPC-25 (MS-9830)"

```
Введите номер варианта [1..6]:3
1: IPC-10 (MS-S088)
2: IPC-25 (MS-92D9)
3: IPC-25 (MS-9830)
4: IPC-100 (G560)
5: IPC-100 (MS-92E3)
6: IPC-400 (MS-9297)
7: IPC-400 (MS-S021)
8: IPC-1000 (IBM x3650M2)
9: IPC-1000 (MS-9297)
10: IPC-1000 (MS-S021)
11: IPC-1000F (MS-S021)
12: IPC-1000F (MS-9297)
13: IPC-1000F2 (MS-9297)
14: IPC-1000F2 (MS-S021)
15: IPC-1010 (MS-9297)
16: IPC-3034 (MS-S021)
17: IPC-3000F (MS-S021)
Введите номер варианта [1..17]:
```

11. Начнется копирование файлов. При успешном завершении установки программного

обеспечения на экране появится сообщение:

После чего сразу же осуществится плановая автоматическая перезагрузка компьютера.

После загрузки операционной системы на экране появится сообщение:

Криптографический шлюз "Континент"

Конфигурация: ЦУС

Начальная конфигурация ЦУС .

Обнаруженные интерфейсы :

Номер	Имя
-------	-----

1	1e3
---	-----

2	tun O
---	-------

Укажите номер внешнего интерфейса : 1

Примечание:

- Имена интерфейсов, отображаемые на экране в строке сообщений, соответствуют именам, указанным на корпусе КШ рядом с соответствующим разъемом.
- Интерфейс tunO предназначен для настройки подключения к внешним сетям по протоколу PPPoE.

11 .Введите **1** и нажмите **<Enter>**.

На экране появится запрос:

Введите внешний IP адрес шлюза:200.200.1.1/24

12. Введите внешний IP-адрес данного КШ - **200.200.1.1/24**

(адрес вводится в формате <адрес>/<префикс>). Нажмите **<Enter>**.

Продолжить (y/п)?

13. Введите "y" и нажмите **<Enter>**. На экране появится пронумерованный

список

внутренних интерфейсов данного криптографического шлюза:

Интерфейсы:

ы:

Номер	Имя
-------	-----

2	1e1
---	-----

3	1e2
---	-----

4	1e3
---	-----

5	tun0
---	------

Укажите номер внутреннего интерфейса.

Если их несколько — того, к которому подключается АРМ администратора : 2

14. Введите **2**. Нажмите **<Enter>**.

На экране появится запрос:

Введите внутренний IP адрес шлюза:192.168.1.1/24

15. Введите IP-адрес данного интерфейса в локальной сети **192.168.1.1/24**.

16. Нажмите **<Enter>**.

После того как параметры интерфейсов определены, на экране появится запрос:

Введите адрес маршрутизатора по умолчанию:200.200.1.2

17. Введите IP-адрес маршрутизатора по умолчанию **200.200.1.2**, Нажмите клавишу

<Enter>. ЦУС сохранит информацию о конфигурации в базе данных, после чего на экране появится указание:

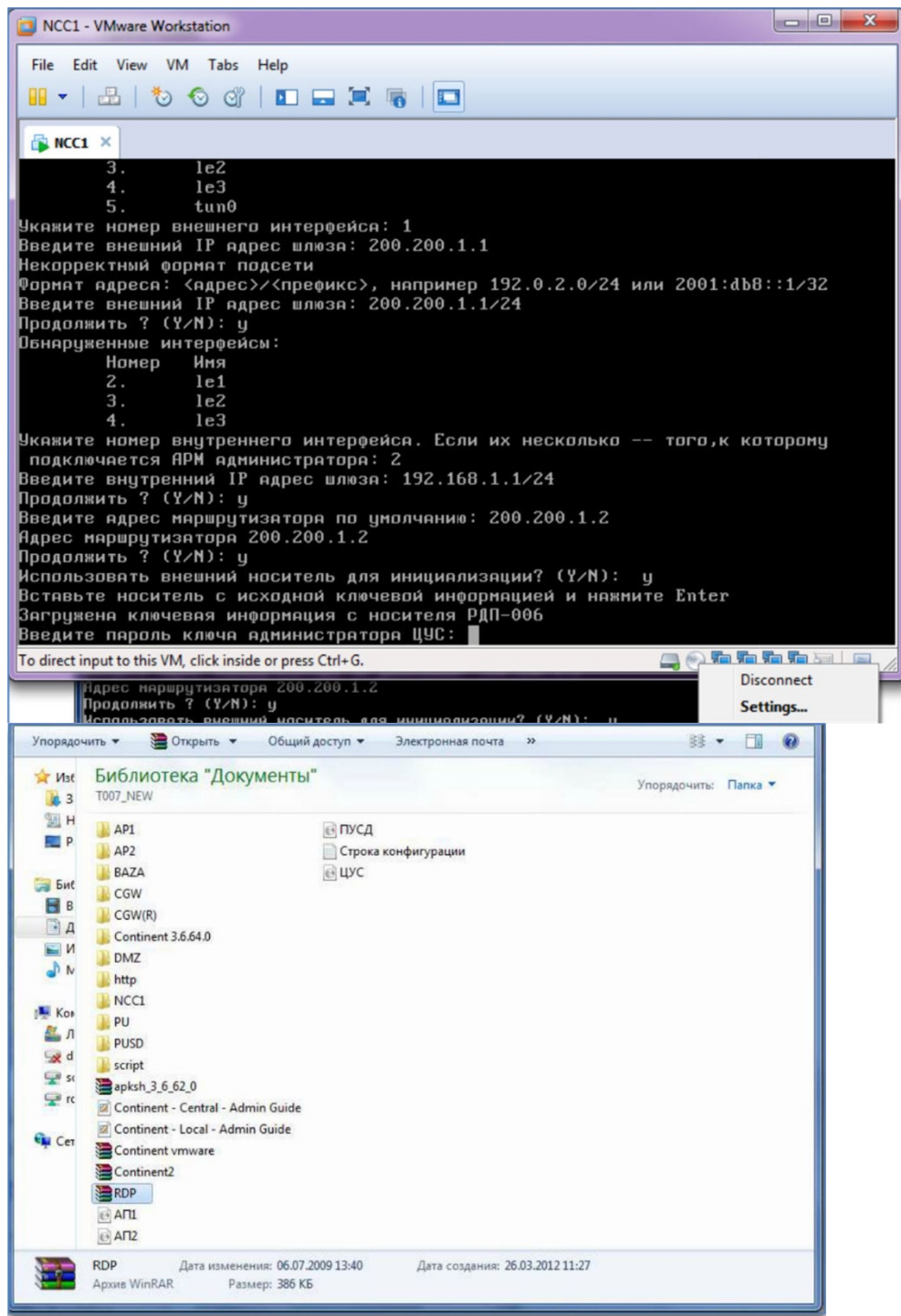
Использовать внешний носитель для инициализации ? (Y/N) Y

Примечание:

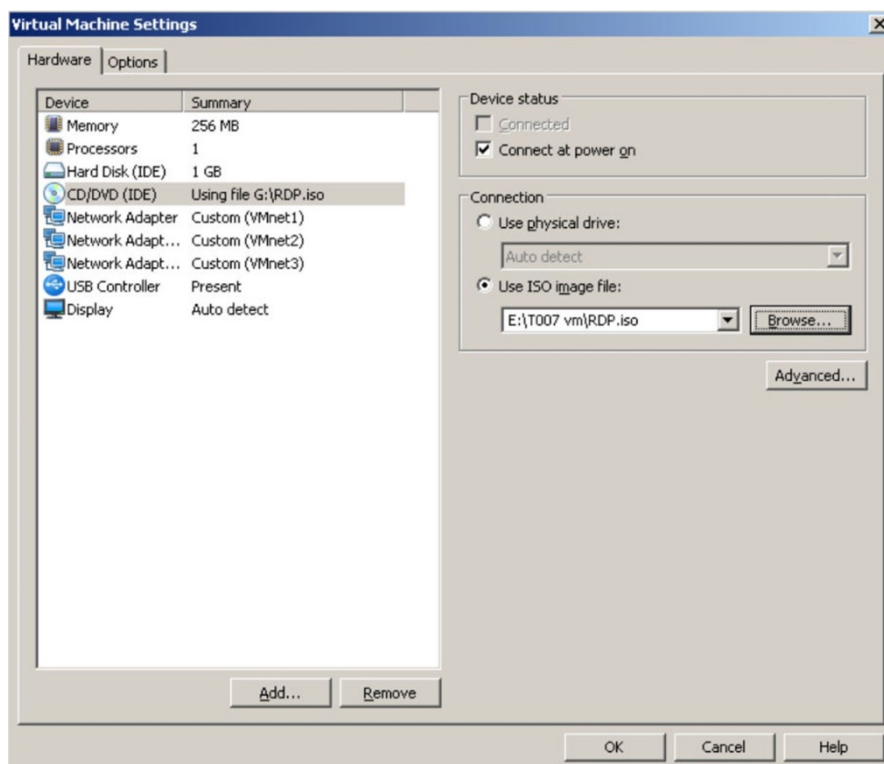
- при использовании в качестве источника исходной ключевой информации ПАК "Соболь" введите "п"
- при использовании ключевого блокнота РДП-006 введите "у"

18. Введите «**y**» и нажмите клавишу **<Enter>**.

Вставьте носитель с исходной ключевой информацией и нажмите Enter



19. Предъявите носитель с исходной ключевой информацией для этого подключите к виртуальной машине образ **RDP.iso**



Нажмите клавишу <Enter>.

Исходный ключевой материал будет загружен в ЦУС. По окончании данной операции на экране появится сообщение:

Введите пароль административного ключа

20. Введите пароль. Внимание - пароль не отображается. (Длина пароля 1-8 символов.

Разрешено использование любых символов, кроме кириллицы. Этот пароль будет

использован для шифрования административного ключа и в дальнейшем понадобится

для запуска программы управления ЦУС). Нажмите клавишу <Enter>.

На экране появится сообщение:

Повторите пароль

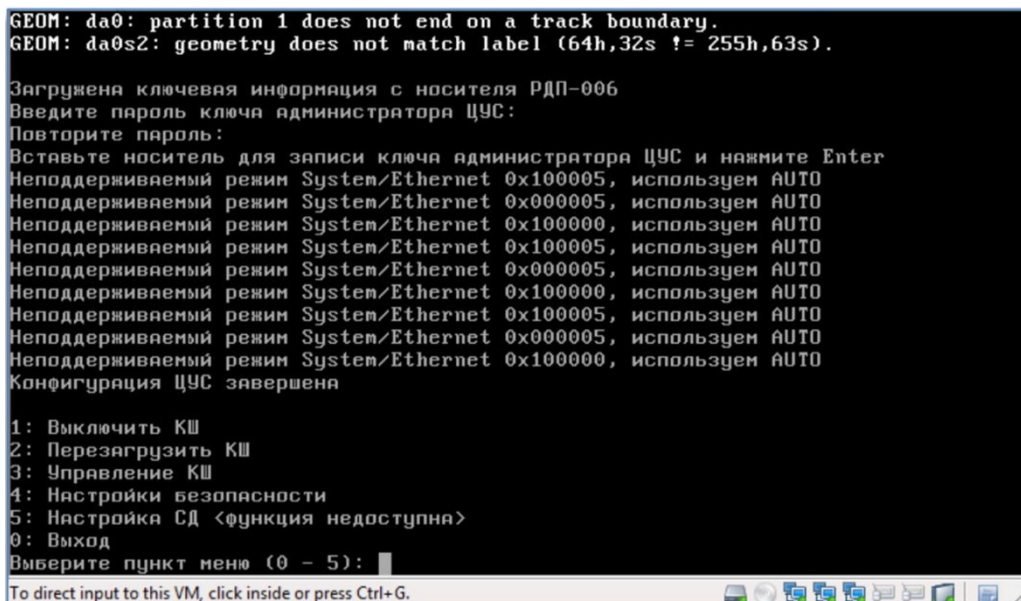
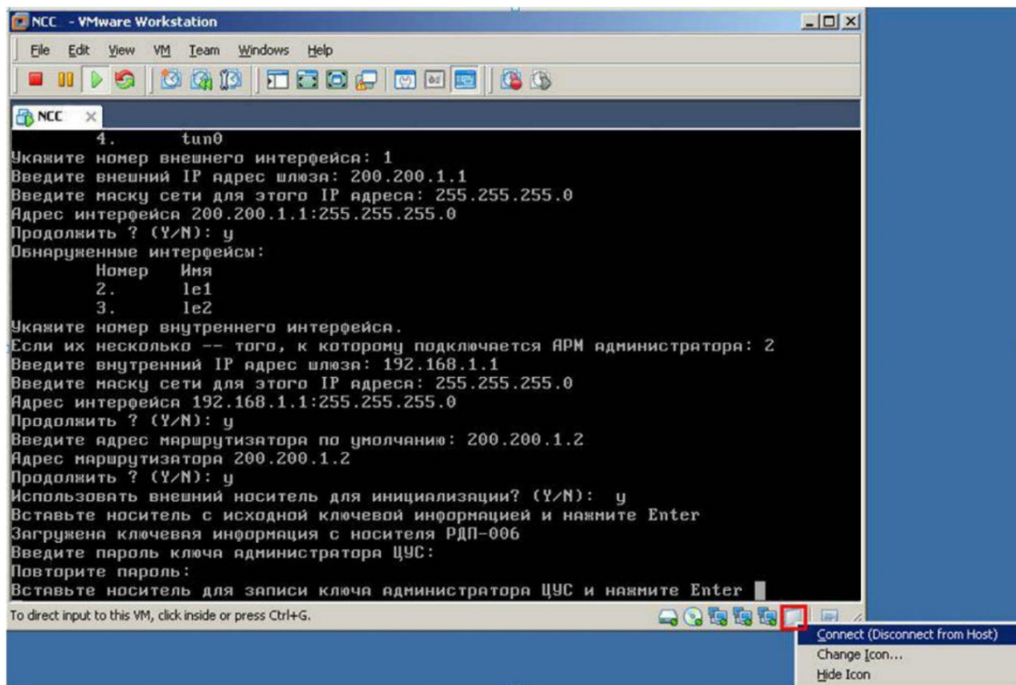
21. Введите пароль повторно и нажмите клавишу <Enter>.

На экране появится сообщение:

Вставьте носитель для записи административного ключа и нажмите Enter

Предъявите носитель для записи административного ключа. Виртуальной машине

необходимо предоставить USB Flash.



22. Нажмите клавишу <Enter>.

При успешной записи ключа на носитель на экране появится главное меню:

1. Выключить КШ
2. Перезагрузить КШ
3. Управление КШ
4. Настройки безопасности
5. Настройка СД

О. Выход

Выберите пункт меню (0-5):

Если в течение 5 секунд после появления последнего сообщения клавиша <Enter>

нажата не будет, ЦУС автоматически завершит процедуру инициализации.

После завершения инициализации на экране появится сообщение:

Успешный запуск <Дата, Время>

9.5 Методические пояснения и рекомендации по выполнению второго вопроса

Вопрос 2 Установка Программы управления и Агента

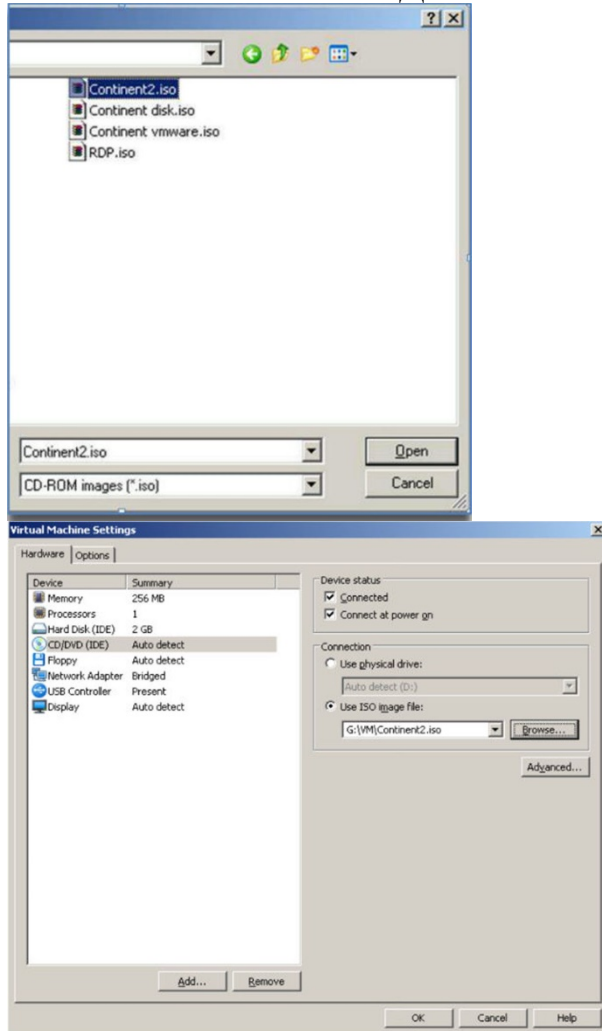
Запуск программы установки

1. Загрузите виртуальную машину **РШ**. Пройдите аутентификацию:

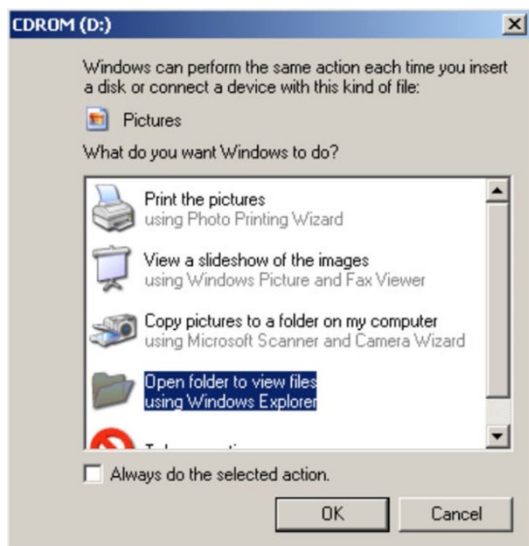
User name: Administrator

Password: 1111

Установите MSDE2000. Для этого подключите к виртуальной машине образ



В виртуальной машине в появившемся окне выберите **Open folder to view files** и нажмите **Ok** **Continent2.iso**.



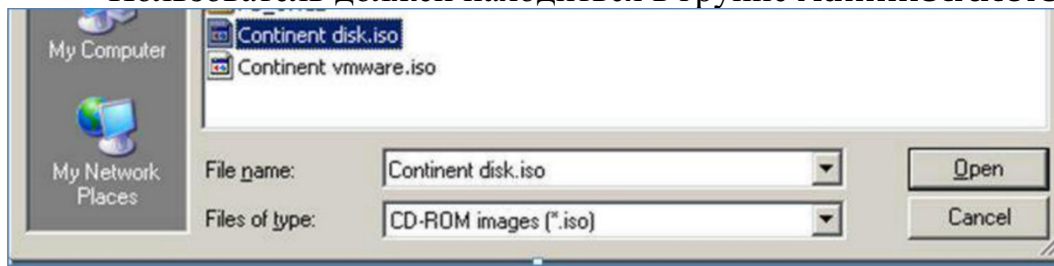
Перейдите «D:\Tools\MSDE2000», запустите setup.exe. После установки **перезагрузите** операционную систему виртуальной машины и войдите под учетной записью **Administrator** (*<дальнейшие действия должны совершаться от имени этой учетной записи>*)

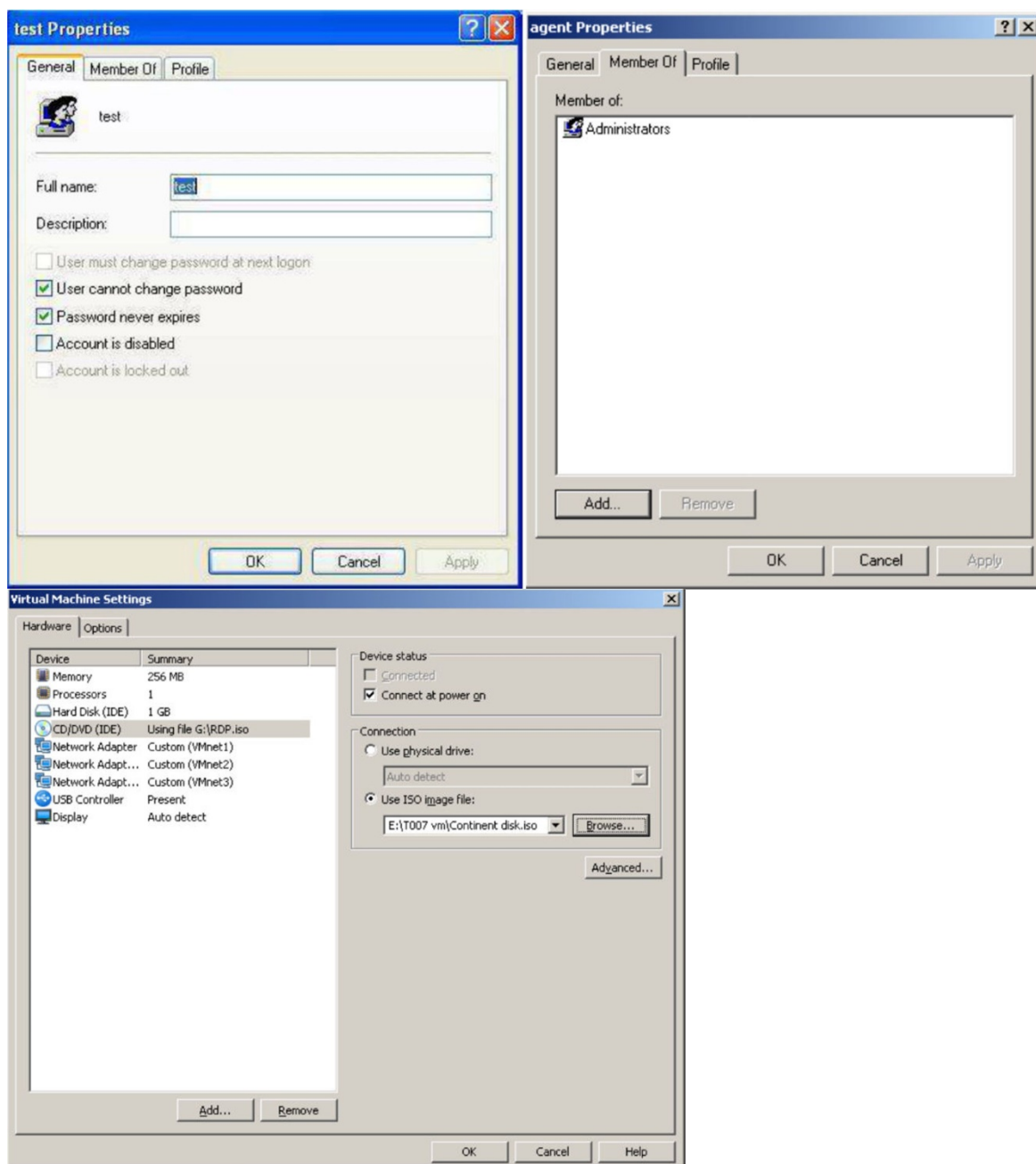
Создайте пользователя ОС: пользователь “**test**”, и поместите его в группу **Administrators**.

В полях Password и Confirm password укажите пароль 1111 (рекомендуется).

Установите галочки:

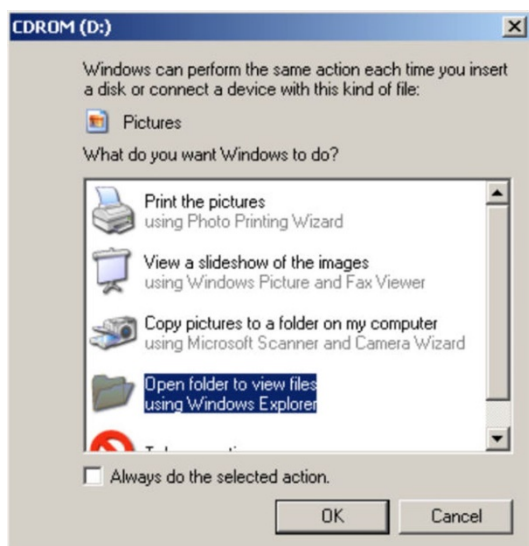
- User cannot change password
- Password never expires
- Пользователь должен находиться в группе **Administrators**.





Подключите образ 3.7.1.1141 .iso (образ установочного диска, с версией программы, рекомендованной преподавателем) к данной виртуальной машине, который находится в папке курса.

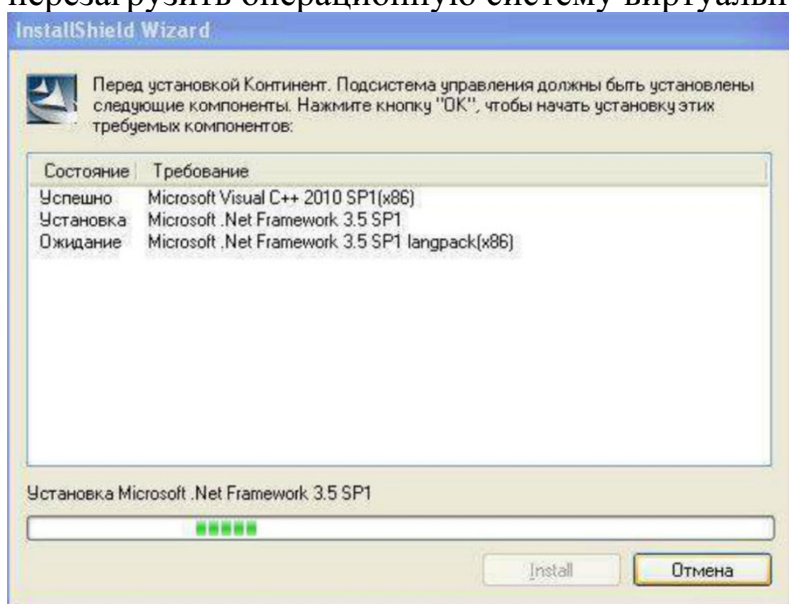
В виртуальной машине в появившемся окне выберете **Open folder to view files** и нажмите «OK»



Перейдите в каталог D:\Setup\Continent\RCP\ и запустите на исполнение файл Setup.exe.

Может потребоваться установка дополнительных компонентов, таких как показано на рисунке. В этом случае необходимо подтвердить установку и дождаться ее окончания.

После окончания установки дополнительных компонентов необходимо перезагрузить операционную систему виртуальной машины.



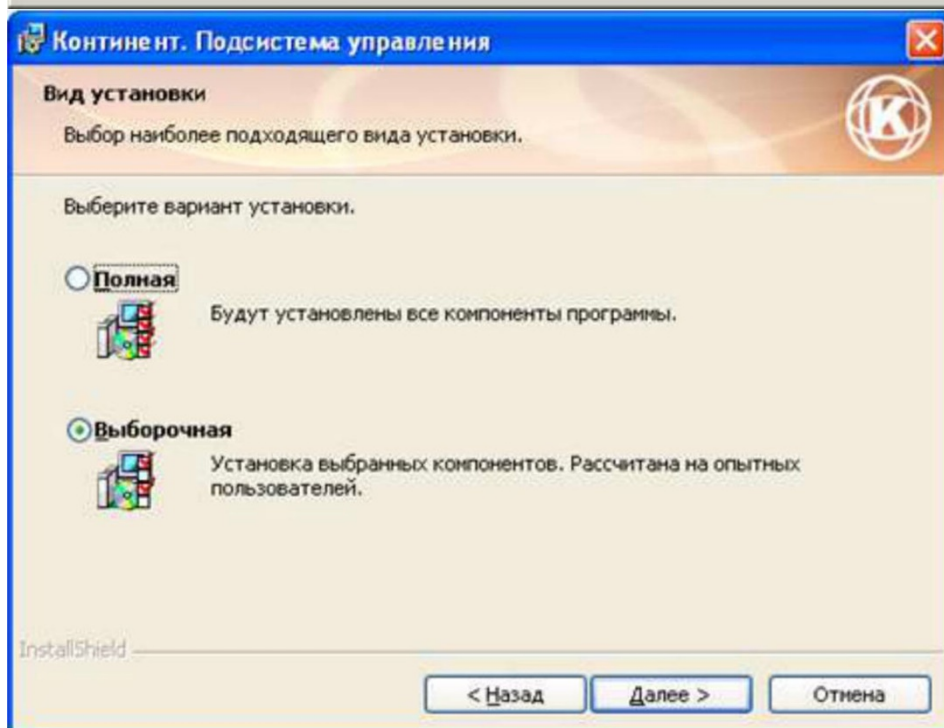
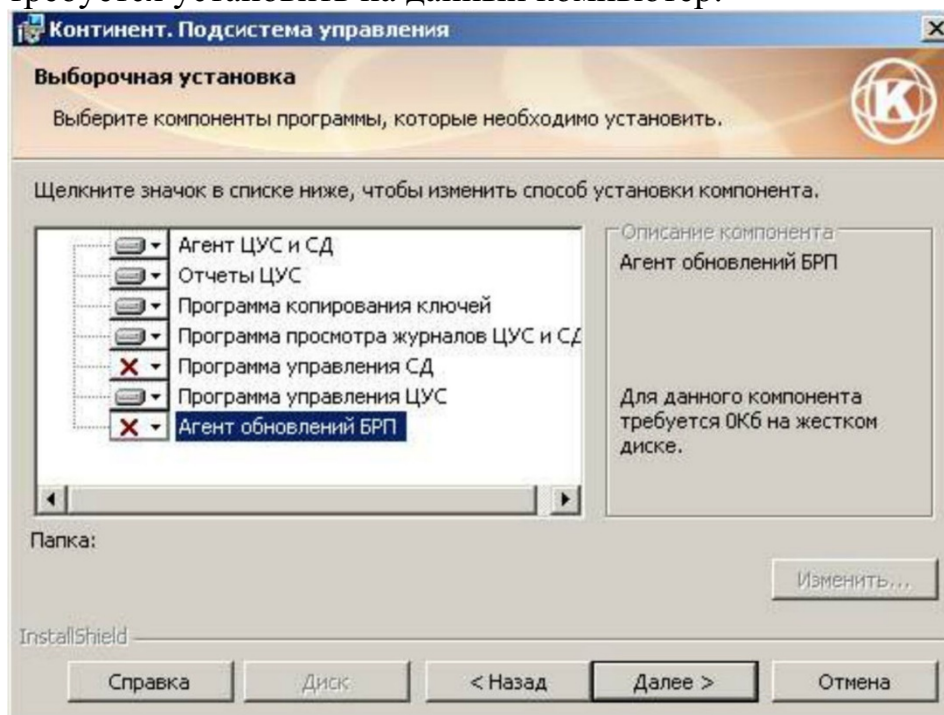
Ознакомьтесь с информацией, содержащейся в стартовом диалоге, и нажмите кнопку "Далее >" для продолжения установки.

Появится диалог с текстом лицензионного соглашения.

Ознакомьтесь с содержанием лицензионного соглашения, прочитав его до конца, согласитесь и нажмите кнопку "Далее >"

На экране появится диалог выбора варианта установки.

Укажите вариант "Выборочная" и нажмите кнопку "Далее >".
Появится диалог выбора компонентов программного обеспечения, которые требуется установить на данный компьютер:



Отметьте в списке устанавливаемые компоненты, как указано на рисунке.
(Установку Программы управления СД и агента обновления БРП выполним позже).

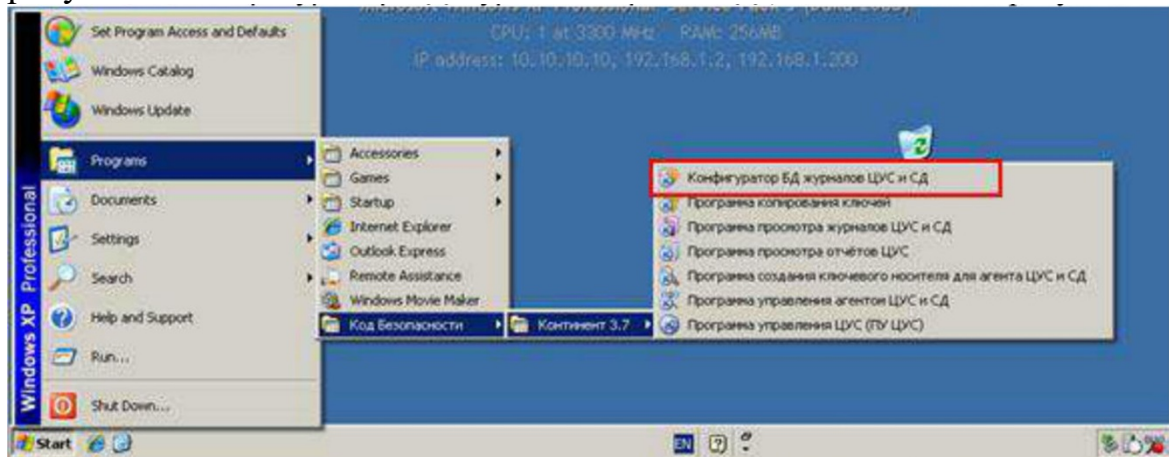
В сети под управлением одного ЦУС может быть установлен только один Агент ЦУС и СД.

Для продолжения установки нажмите кнопку "Далее >", а в появившемся окне кнопку "Установить".

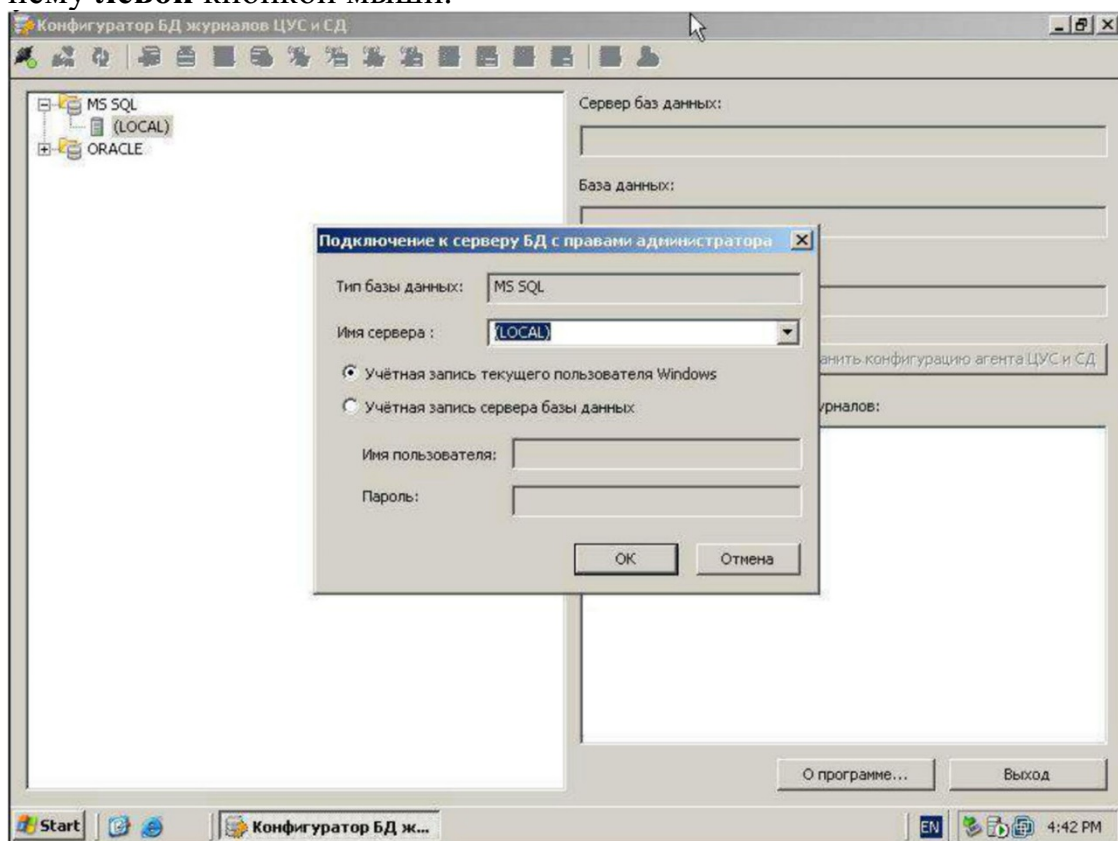
После установки программы, в появившемся окне нажмите "Готово", далее

перезагрузите операционную систему виртуальной машины PU1.

После загрузки операционной системы зайдите в меню и запустите программу Конфигуратор БД журналов ЦУС и СД: "Пуск\ Программы\ Код безопасности\ Континент 3.7\ Конфигуратор БД журналов ЦУС и СД", как показано на рисунке:



В открывшемся окне выберите сервер баз данных MS SQL -> (LOCAL) и щелкните по нему **левой** кнопкой мыши.

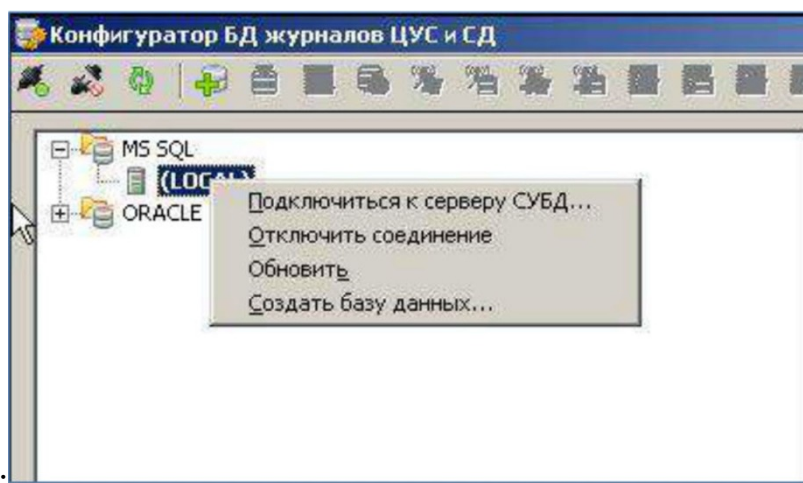


Проверьте настройки в соответствии с теми, как показано на рисунке: Имя сервера:

(LOCAL); Учетная запись текущего пользователя Windows.

Нажмите кнопку "OK", при этом выполнится подключение к базе данных MS SQL.

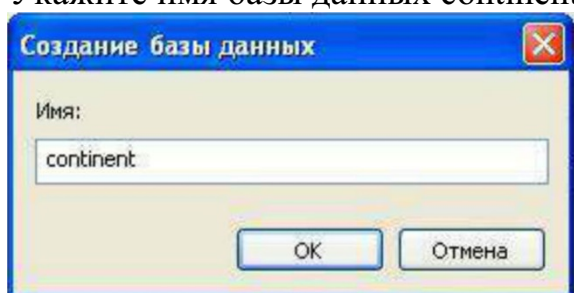
Нажмите **правой** кнопкой мыши на обозначение сервера MS SQL -> (LOCAL),



как показано на рисунке:

В выпадающем меню выберите пункт «Создать базу данных...».

Укажите имя базы данных continent.

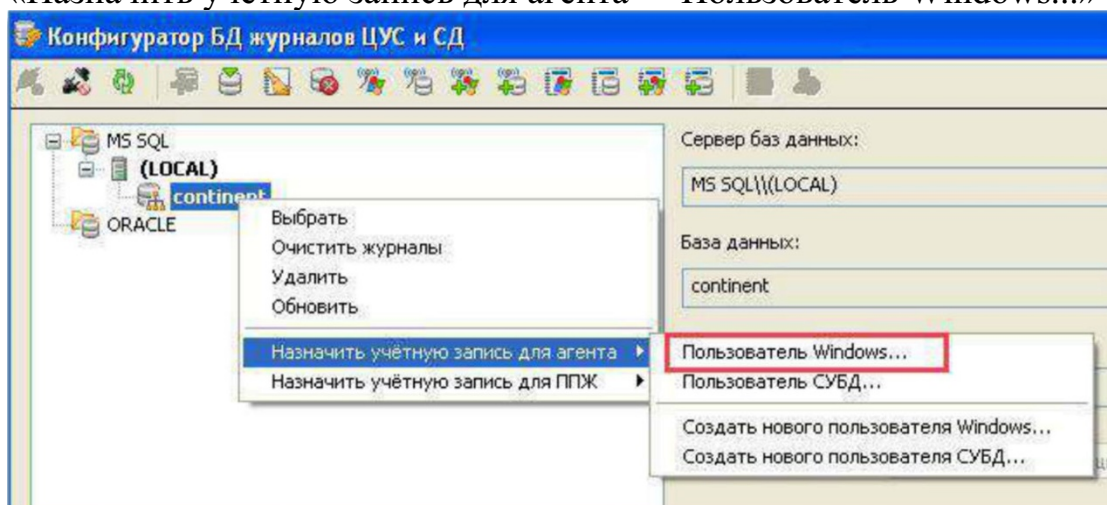


Нажмите кнопку "OK" и подождите появления символа новой базы данных continent.

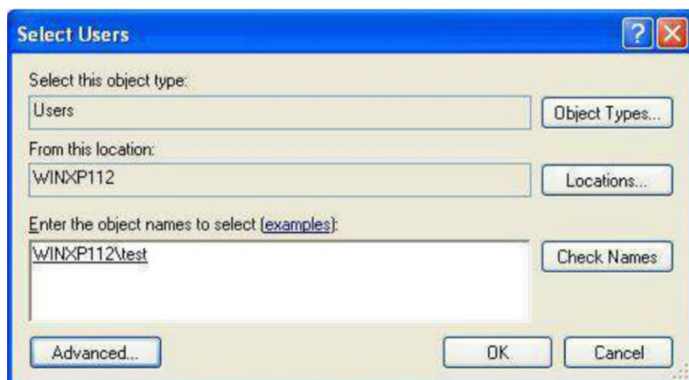
В окне конфигуратора БД **правой** кнопкой мыши нажмите изображение новой базы continent и выберите меню «Выбрать», после этого станут активными пункты меню для

ввода учетной записи пользователя базы данных:

«Назначить учетную запись для агента -> Пользователь Windows...»

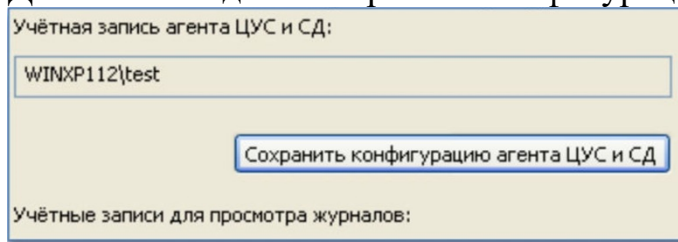


Выберите пользователя Windows - пользователь «test» (заведенного ранее, в п.5).

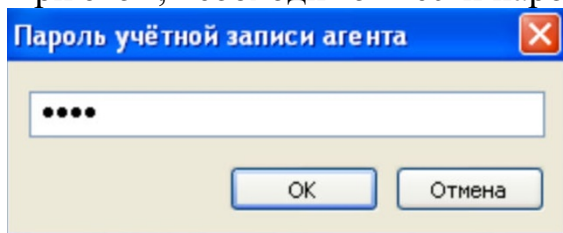


Нажмите кнопку "OK".

Далее необходимо сохранить конфигурацию агента ЦУС и СД:

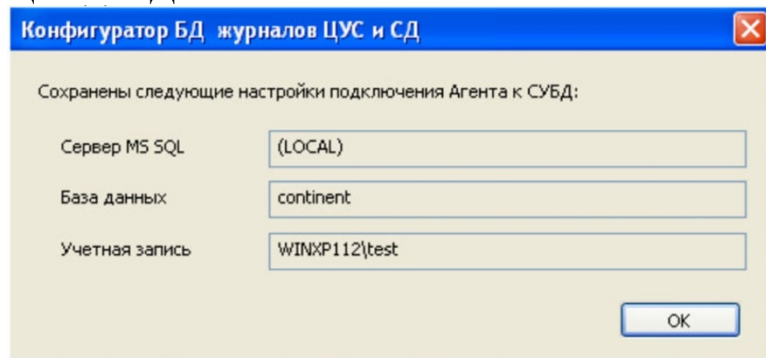


При этом, необходимо ввести пароль учетной записи "test":



Далее программа покажет сообщение, удостоверяющее сохраненную конфигурацию

ЦУС и СД:



Нажмите кнопку "OK".

Закройте программу Конфигуратор БД журналов ЦУС и СД кнопкой «Выход».

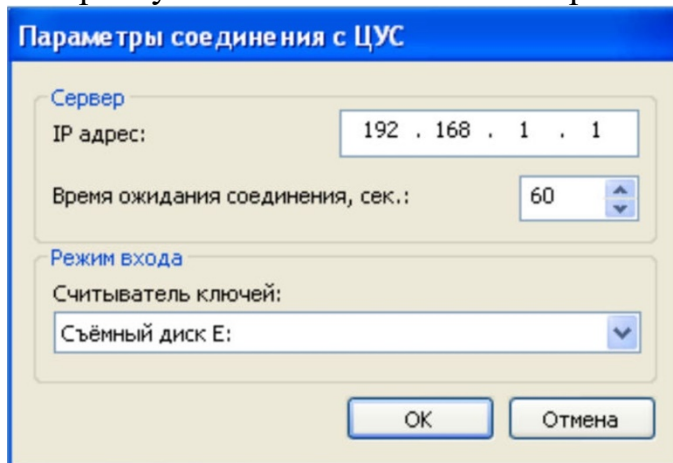
Подключите USB Flash к виртуальной машине. Для этого перейдите в виртуальную машину NCC1 и отключите USB Flash от нее.

Далее, снова перейдите в виртуальную машину PU1 и подключите USB Flash к ней.

В окне «Настройка соединения с ЦУС» заполните поля данного диалога:

- укажите IP-адрес ЦУС 192.168.1.1;
- укажите время ожидания соединения - по умолчанию 60 сек;

- выберите из списка тип ключевого носителя администратора: Съёмный диск.
- Список содержит названия тех устройств идентификации, драйверы которых установлены на компьютере.

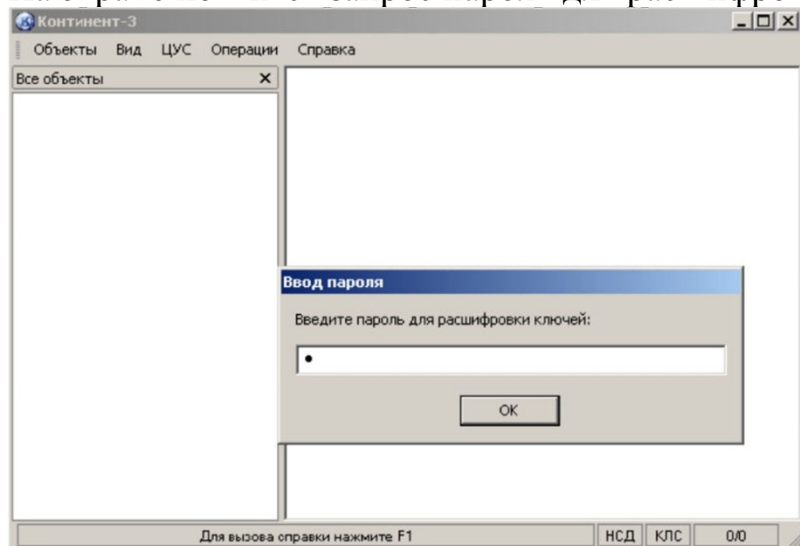


Нажмите кнопку "ОК".

Запуск Программы управления

Активируйте команду "Программы\Код Безопасности\Континент 3.7\Программа управления ЦУС (ПУ ЦУС)" в главном меню Windows или ярлык Программы управления на рабочем столе.

На экране появится запрос пароля для расшифровки ключей администратора.



Введите пароль, который Вы вводили при инициализации ЦУС (в первой практической работе) и нажмите кнопку "ОК".

При успешном чтении служебной информации с идентификатора на экране появится диалог для регистрации лицензий ЦУС.

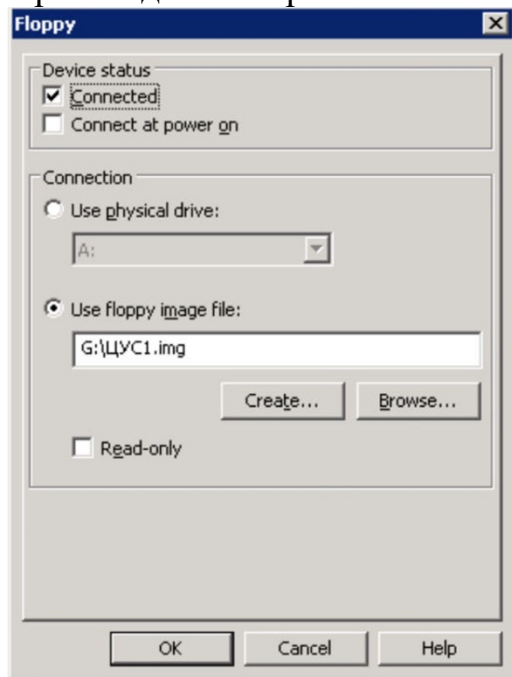
Зарегистрируйте приобретенные лицензии на работу с ЦУС. Для каждой лицензии

укажите в поле ввода серийный номер лицензии и нажмите кнопку "Добавить";

(тестовые лицензионные ключи можно скопировать из файла Licens 3_7.txt, находящегося в папке курса)

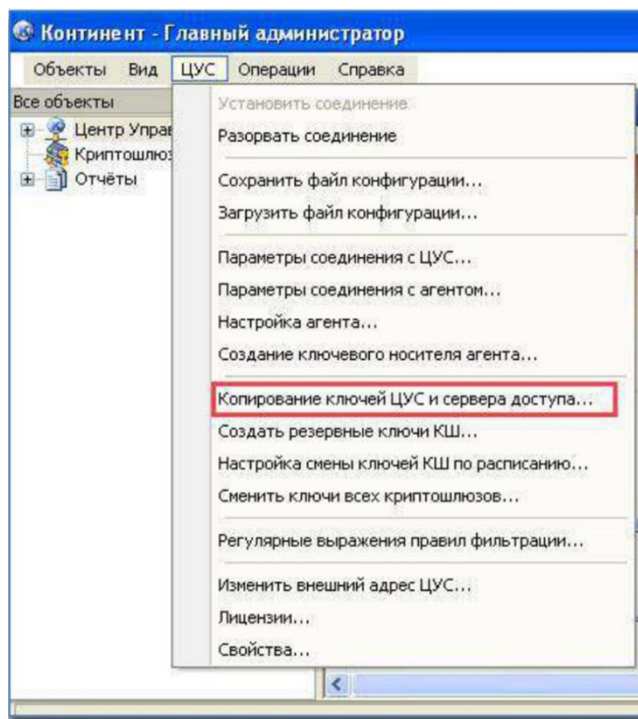
Копирование ключей администратора на другой носитель.

Произведем копирование ключей с USB Flash на дискету. Для этого



Подключим к виртуальной машине образ дискеты ЦУС1.img (образ находится в папке курса).

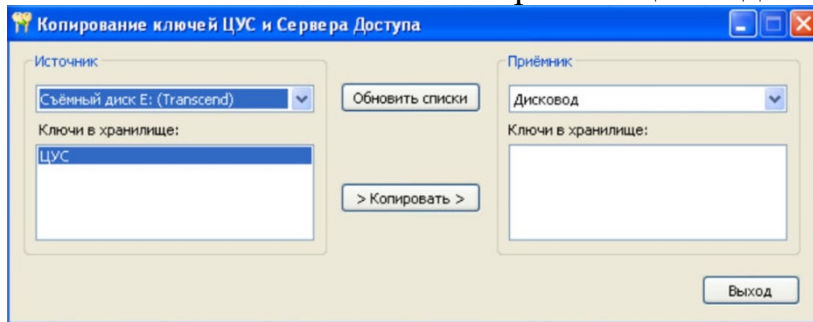




Выберете в ПУ ЦУС пункт меню "ЦУС -> Копирование ключей ЦУС и сервера доступа...":

В появившемся окне выберете

- Источник: Съёмный диск
- Приемник: Дисковод
- В левом окне “Ключи в хранилище” выделите: ЦУС

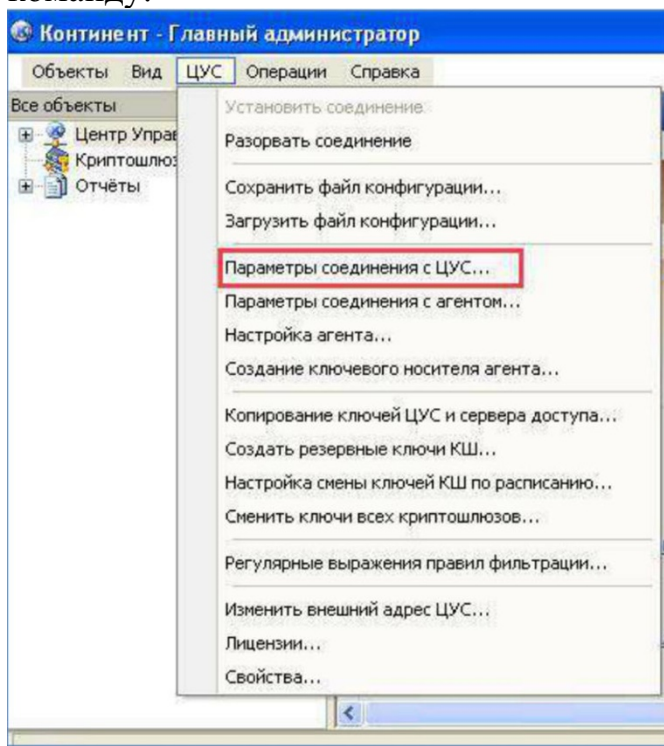


- И нажмите «Копировать». Программа произведет копирование ключей ЦУС.

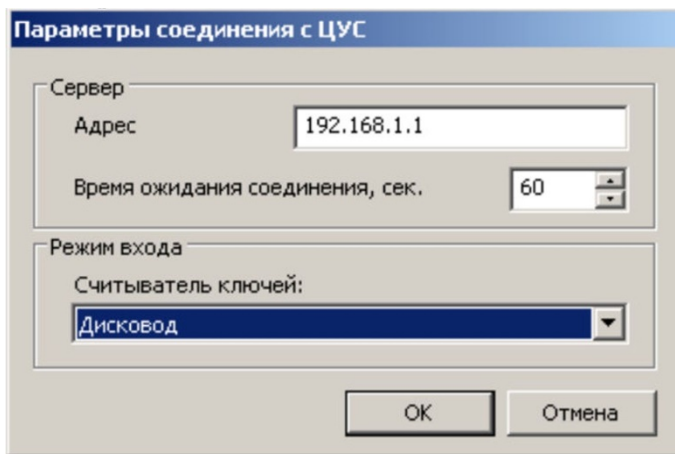
Увидев подтверждение, что копирование ключей закончено и ключи в хранилище

источника совпадают с ключами в хранилище приемника нажмите кнопку «Выход».

В ПУ ЦУС установите новый считыватель ключей. Для этого выполните команду:



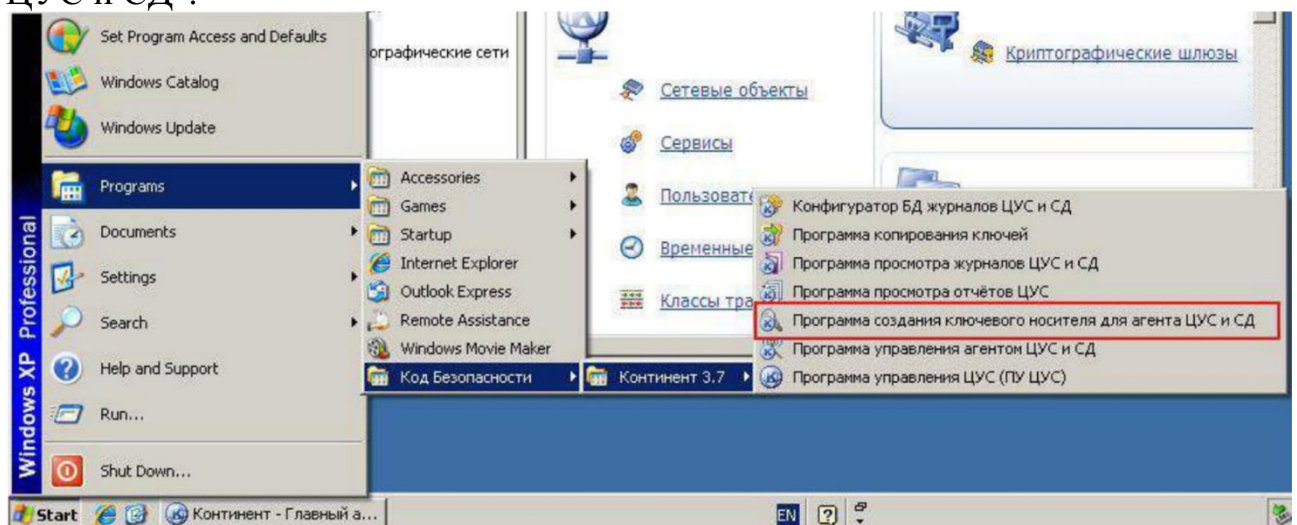
Выберете Считыватель ключей: Дисковод



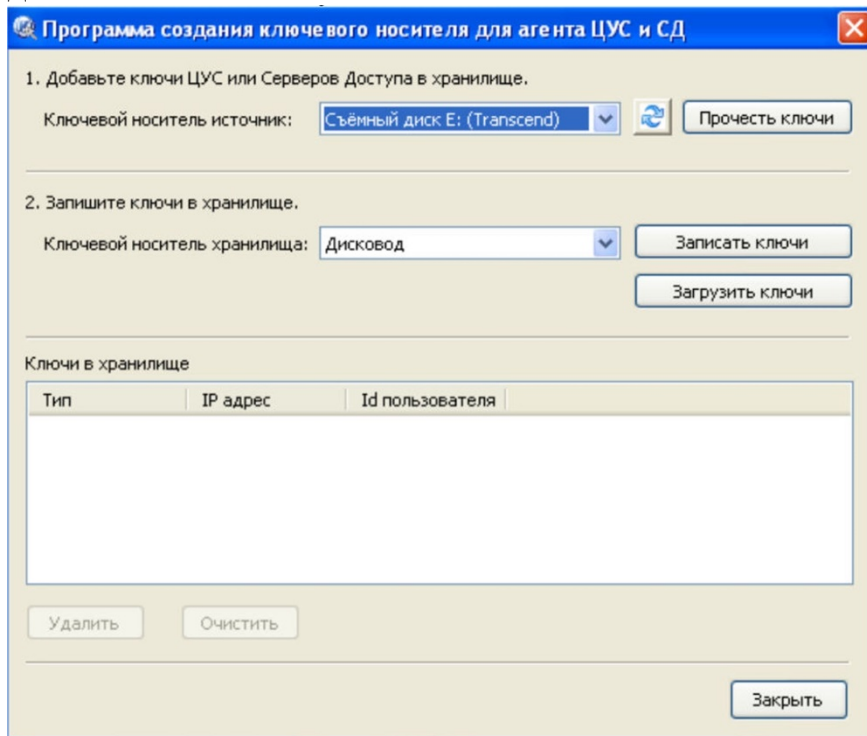
"ЦУС -> Параметры соединения с ЦУС..."

Формирование Единого ключевого носителя для запуска Агента.

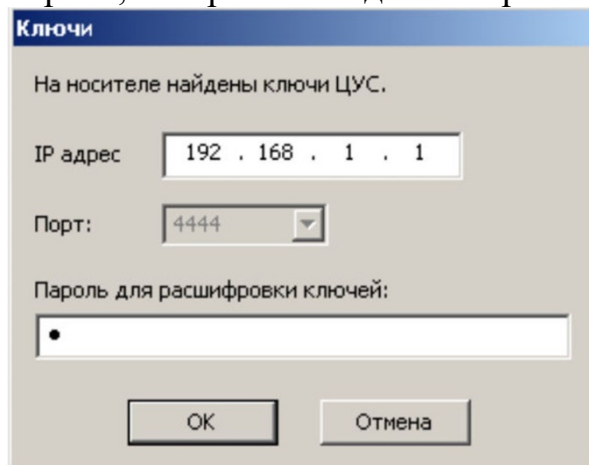
Запустите Программу создания ключевого носителя "Программы\Код Безопасности\Континент 3.7\Программа создания ключевого носителя для агента ЦУС и СД".



В появившемся окне укажите “Ключевой носитель источник”: Съёмный диск



Нажмите кнопку "Прочитать ключи". На экране появится диалоговое окно, в котором введите IP адрес 192.168.1.1 (внутренний интерфейс КШ+ЦУС) и пароль, который вы задавали при инициализации ЦУС1. И нажмите ОК.



В окне Программы создания ключевого носителя отобразиться информация о ключах

Программа создания ключевого носителя для агента ЦУС и СД

1. Добавьте ключи ЦУС или Серверов Доступа в хранилище.

Ключевой носитель источник: Съёмный диск E:  Прочитать ключи

2. Запишите ключи в хранилище.

Ключевой носитель хранилища: Дискковод  Записать ключи

 Загрузить ключи

Ключи в хранилище

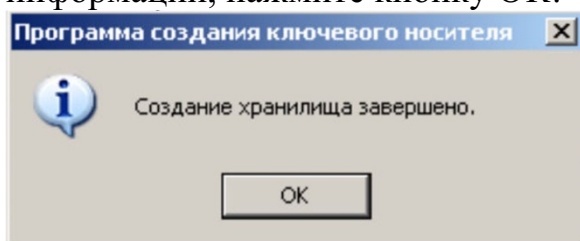
Тип	IP адрес	Id пользователя
ЦУС	192.168.1.1 (4444)	11

Удалить Очистить

Закреть

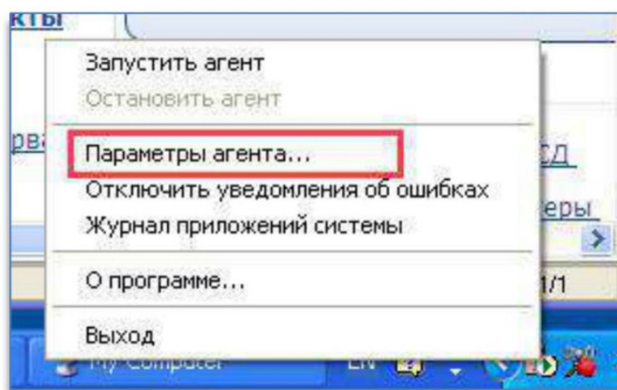
Нажмите кнопку Записать ключи.

Далее, система сообщит о успешном создании хранилища ключевой информации, нажмите кнопку ОК.

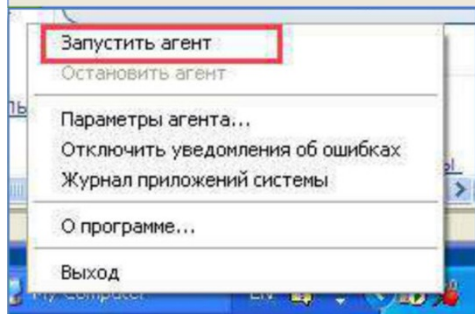


Закройте Программу создания ключевого носителя для агента ЦУС и СД.

Вызовите в контекстном меню пиктограммы Агента, расположенной в правом углу панели задач и выберите пункт «Параметры агента...».



На экране появится диалог для настройки Агента.



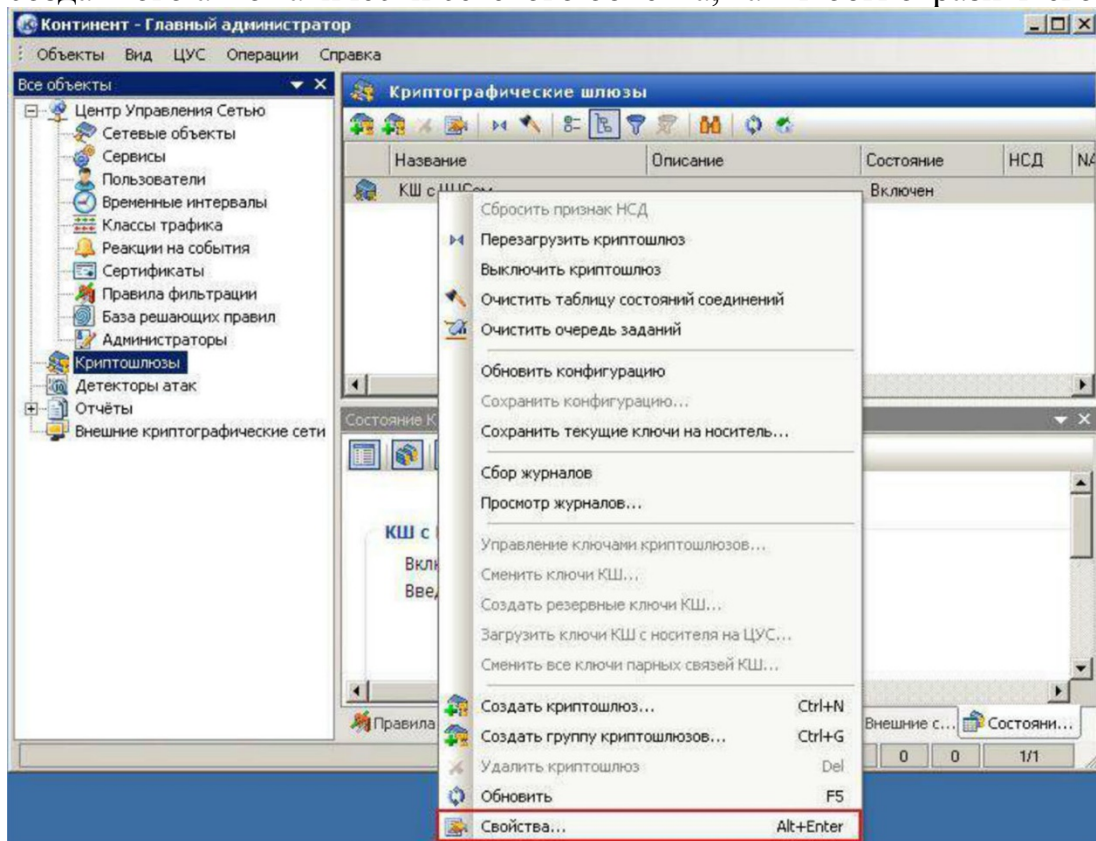
Поменяйте тип ключевого носителя на «Дисковод» и нажмите «ОК».

Запустите Агент нажав правой кнопкой мыши пиктограмму Агента в трее.

9.6 Методические пояснения и рекомендации по выполнению третьего вопроса

Вопрос 3 Необходимая настройка ЦУС из ПУ ЦУС

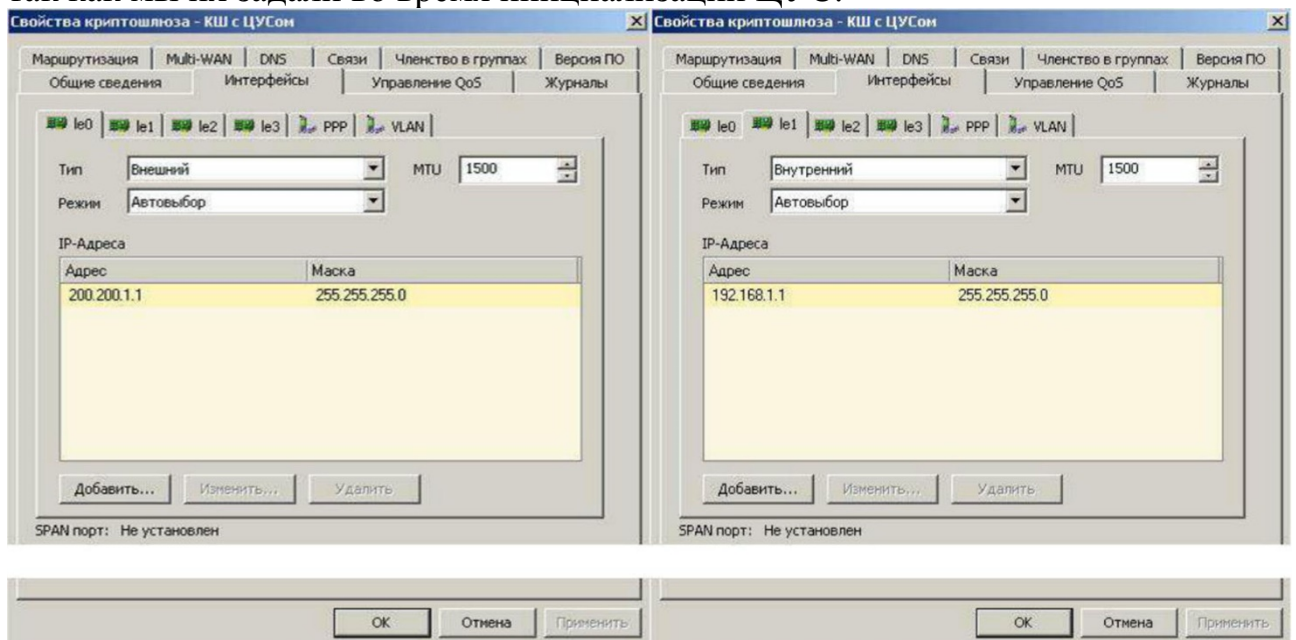
Необходимо задать параметры на интерфейсе 1пс2 ЦУС и изменить название созданного автоматически сетевого объекта, так чтобы отразить его суть.



На экране появится окно "Свойства криптошлюза"

Перейдите к вкладке "Интерфейсы". Интерфейсы le0 и le1 будут уже определены,

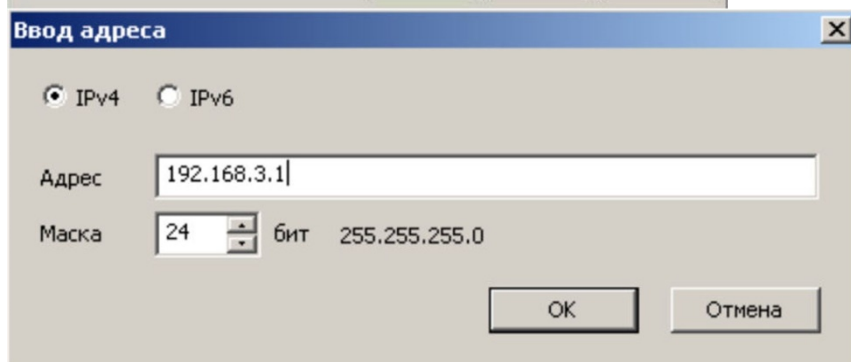
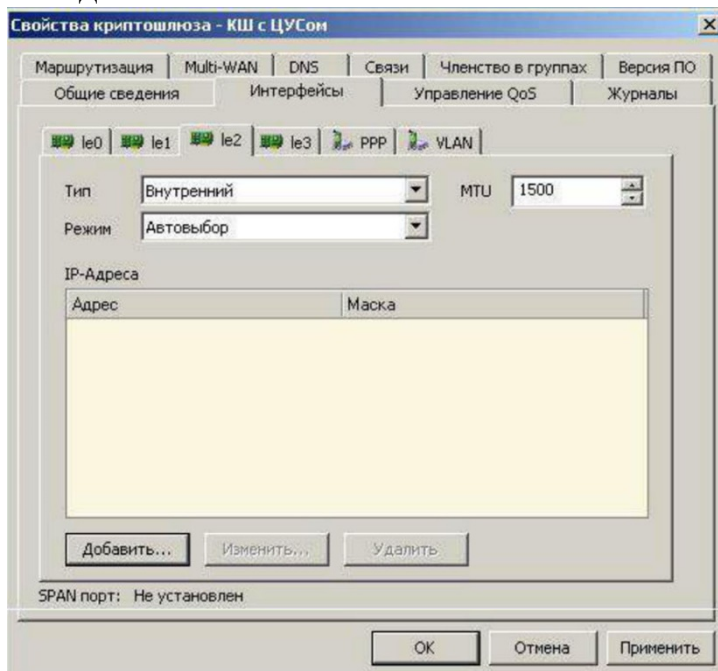
так как мы их задали во время инициализации ЦУС.



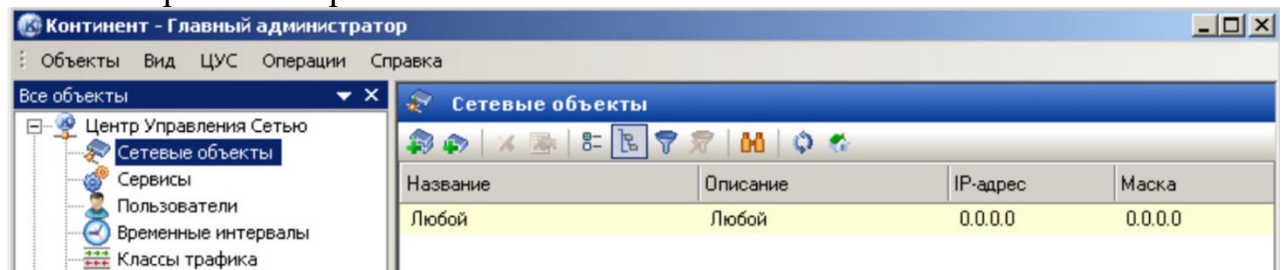
1. В правом окне управления криптографическими шлюзами правой кнопкой

мышью вызовите контекстное меню КШ с ЦУСом и активируйте команду **"Свойства..."**.

Осталось **здать параметры** для интерфейса **1e2**. Для этого перейдите к вкладке 1e2.



В окне управления свойствами криптошлюза нажмите кнопку **Применить**. Для вызова списка сетевых объектов в левой части окна программы управления выберите папку **"Центр управления сетью \ Сетевые объекты"**. В правой части окна отобразится перечень сетевых объектов



Определите IP-адреса интерфейса в соответствии со схемой. Для этого нажмите кнопку **"Добавить"** и введите в соответствующие поля диалога **"Ввод адреса"** IP-адрес **192.168.3.1** и маску подсети в виде префикса **24** (255.255.255.0) для данного интерфейса и нажмите кнопку **"ОК"**. Указанный адрес будет добавлен в перечень IP-адресов данного интерфейса.

Создайте объект «Главный офис»: Левой кнопкой мыши щелкните пиктограмму Сетевые объекты -> Создать сетевой объект.

Задайте описание объекта «Защищаемая сеть КШ «КШ с ЦУСом»

Задайте IP адрес сети 192.168.1.0 и маску 255.255.255.0

Тип привязки: **Защищаемый.**

Криптошлюз: **КШ с ЦУСом.**

Интерфейс: **le1**

Сетевой объект

Общие | Членство в группах

Название: Главный офис

Описание: Защищаемая сеть КШ «КШ с ЦУСом»

☒ Unicast ☐ Multicast

IP-адрес / Маска: 192 . 168 . 1 . 0 / 255 . 255 . 255 . 0

Тип привязки: Защищаемый

Криптошлюз: КШ с ЦУСом

Интерфейс: le1

☐ Трансляция адреса внутри VPN

Виртуальный адрес: 0 . 0 . 0 . 0 / 255 . 255 . 255 . 0

OK Отмена

Нажмите кнопку ОК.

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1-2

ЛАБОРАТОРНАЯ РАБОТА № 4-6.

Тема: Правила фильтрации и трансляции.

1. Цель работы :

1. Изучить правила фильтрации и трансляции.
2. Приобретение практических навыков использования правил фильтрации и трансляции.

Формируемые компетенции: ОПК-9, ОПК-10.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал, посвящённый правилам фильтрации и трансляции.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

3. Распределение времени занятия:

Всего: 270 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 70 мин

1. Исследование правил фильтрации и трансляции 70 мин

Проверка выполнения практического занятия 10 мин

Заключительная часть 3 мин

4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

4.1. Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

4.2. Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию;

- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;

- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

4.3. Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

6. Программное обеспечение

АПКШ «Континент», виртуальная машина DMZ.

7. Основные теоретические сведения

См. рекомендованную к ознакомлению литературу по изучаемой дисциплине

8. Литература

1. James Boney, Cisco IOS in a Nutshell, O'Reilly, 2010
2. Wendell Odom, Interconnecting Networking Devices Cisco, Part 2, Cisco Press, 2010

9. Методические рекомендации по выполнению лабораторной

работы

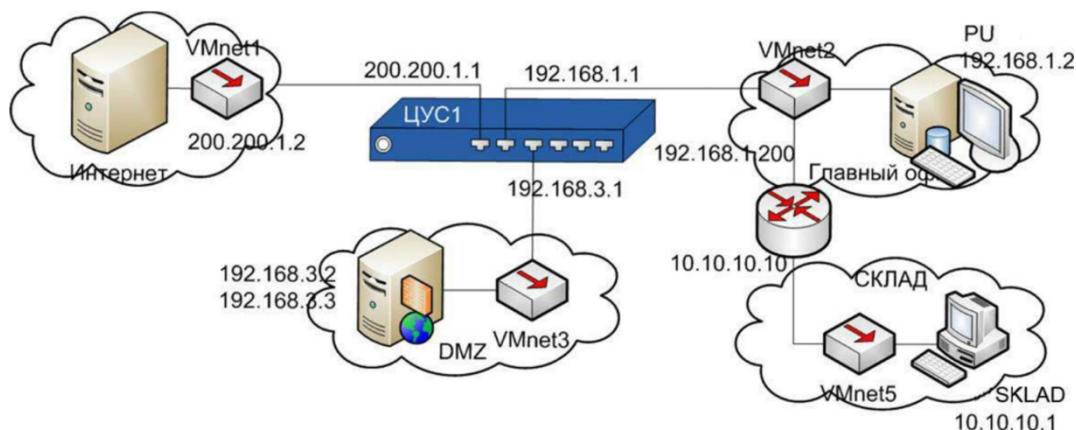


Рисунок 2 - Топология

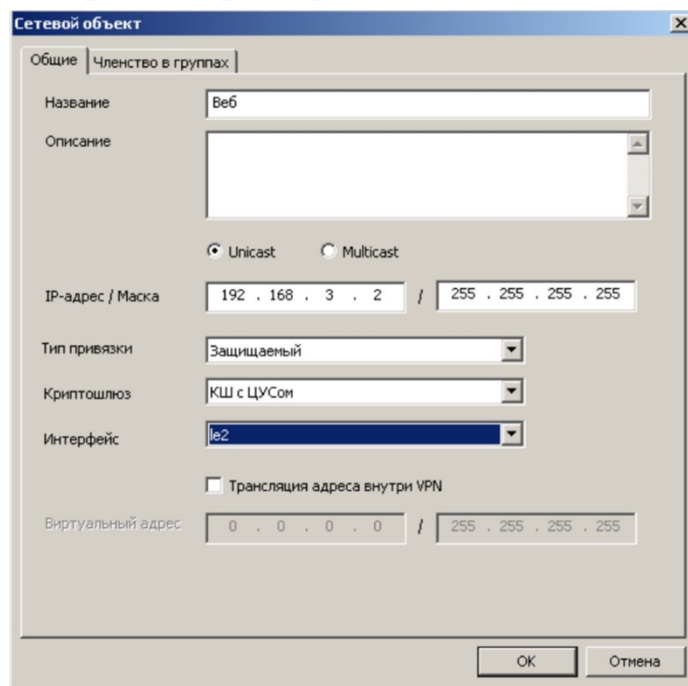
9.1 Методические рекомендации и пояснения по выполнению первого вопроса

Вопрос 1. Доступ внутренних пользователей сети «Главный офис» к ДМЗ по протоколу icmp и http

1. Вызовите список сетевых объектов, для этого в левой части окна программы управления выберите папку "Центр управления сетью \ Сетевые объекты". В правой части окна отобразится перечень сетевых объектов.

Вызовите меню "Операции" и активируйте команду "Создать сетевой объект" или нажмите  на панели управления. На экране появится окно настройки параметров сетевого объекта.

Настройте параметры создаваемого объекта в соответствии с рисунком:



Нажмите кнопку "OK".

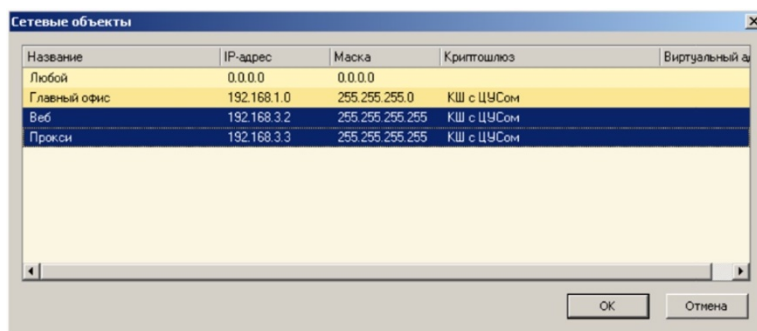
2. Создайте еще один сетевой объект - Прокси.

В списке появится имя нового объекта, а сведения о нем будут сохранены в базе данных ЦУС.

3. Создадим группу ДМЗ. Для этого нажмите «Создать группу»  на панели инструментов.

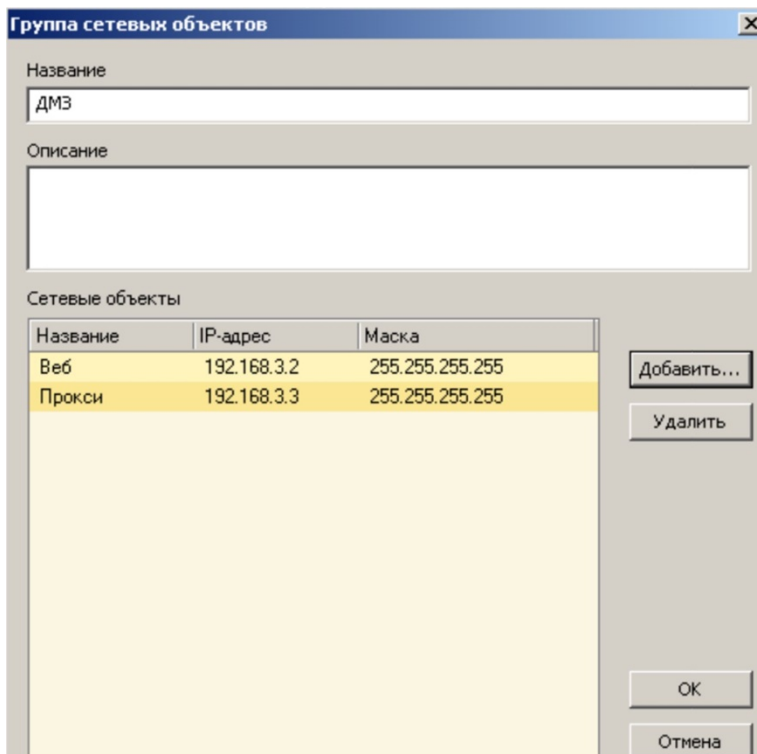
Название	IP-адрес	Маска

Нажмите кнопку «Добавить...», в появившемся окне выберите два объекта “Веб” и “Прокси” (левой кнопкой мыши, нажав предварительно кнопку «Ctrl»).



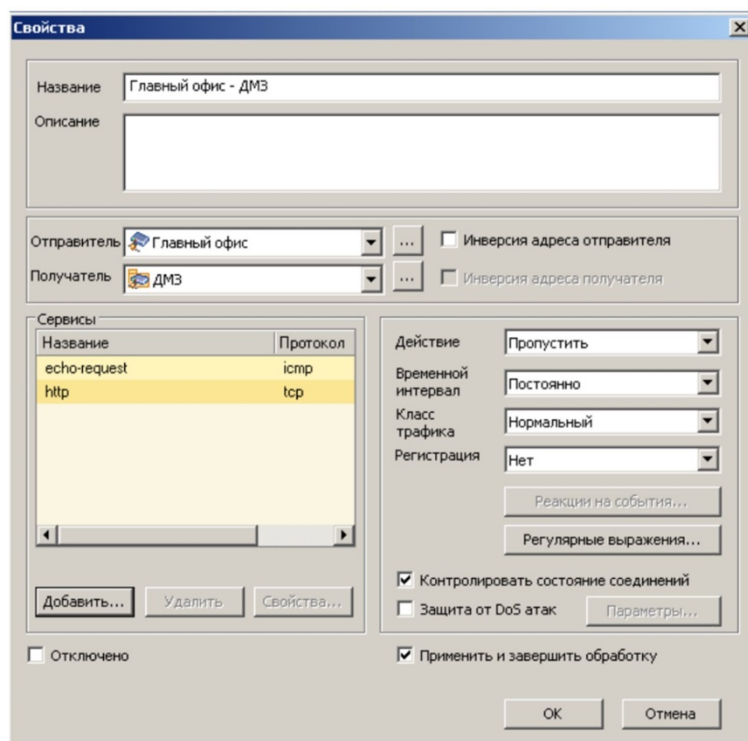
Нажмите кнопку «ОК».

И в диалоговом окне «Группа сетевых объектов» нажмите «ОК».



4. Выберите папку "Центр управления сетью \ Правила фильтрации". В правой части окна отобразится список правил фильтрации IP-пакетов.

Для создания правила вызовите контекстное меню в любом месте списка правил и активируйте команду "Создать правило фильтрации" или нажмите одноименную кнопку на панели инструментов. На экране появится диалог "Правило фильтрации".



5. Введите название, выберите отправителя и получателя, сервисы. Действие поставьте «Пропустить». Поставьте «Контролировать состояние соединений» и «Применить и завершить обработку» и нажмите «ОК».

Для того, чтобы это правило применилось необходимо нажать кнопку "Сохранить изменения"  на панели инструментов.

Проверка работы правила

Запустите виртуальную машину DMZ.

С виртуальной машины РШ выполните команду ping на адреса узлов сети DMZ и заход на веб сервер <http://192.168.3.2>

```
C:\Documents and Settings\Administrator>ping 192.168.3.2
Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=3ms TTL=127
Reply from 192.168.3.2: bytes=32 time<1ms TTL=127
Reply from 192.168.3.2: bytes=32 time<1ms TTL=127
Reply from 192.168.3.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms
C:\Documents and Settings\Administrator>
```

```
C:\Documents and Settings\Administrator>ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=2ms TTL=127
Reply from 192.168.3.3: bytes=32 time=1ms TTL=127
Reply from 192.168.3.3: bytes=32 time=1ms TTL=127
Reply from 192.168.3.3: bytes=32 time<1ms TTL=127

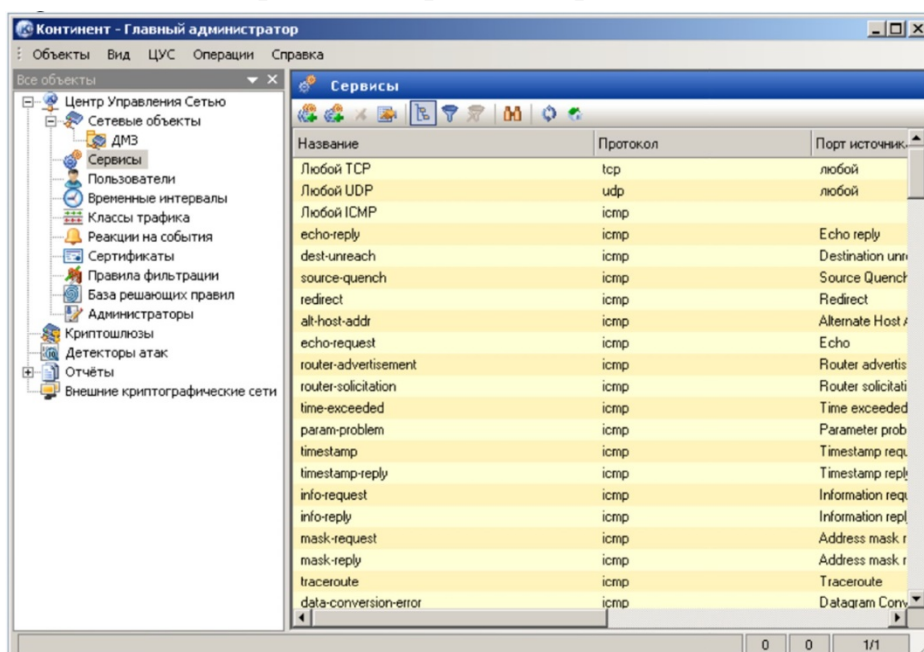
Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms
C:\Documents and Settings\Administrator>
```



9.2 Методические рекомендации и пояснения по выполнению второго вопроса

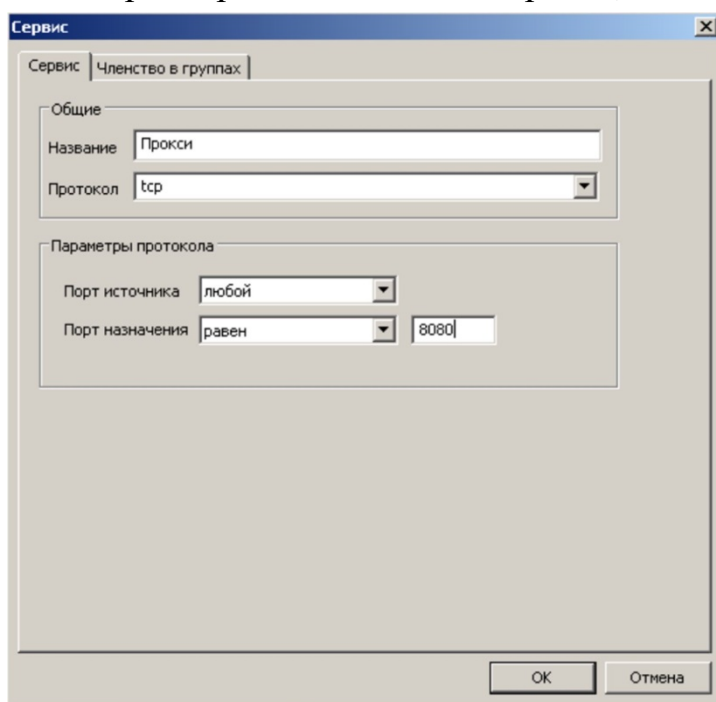
Вопрос 2 Доступ внутренних пользователей сети «Главный офис» к внешним ресурсам (через Прокси)

5. Для вызова списка сервисов в левой части окна программы управления выберите папку "Центр управления сетью \ Сервисы". В правой части окна отобразится перечень сервисов:



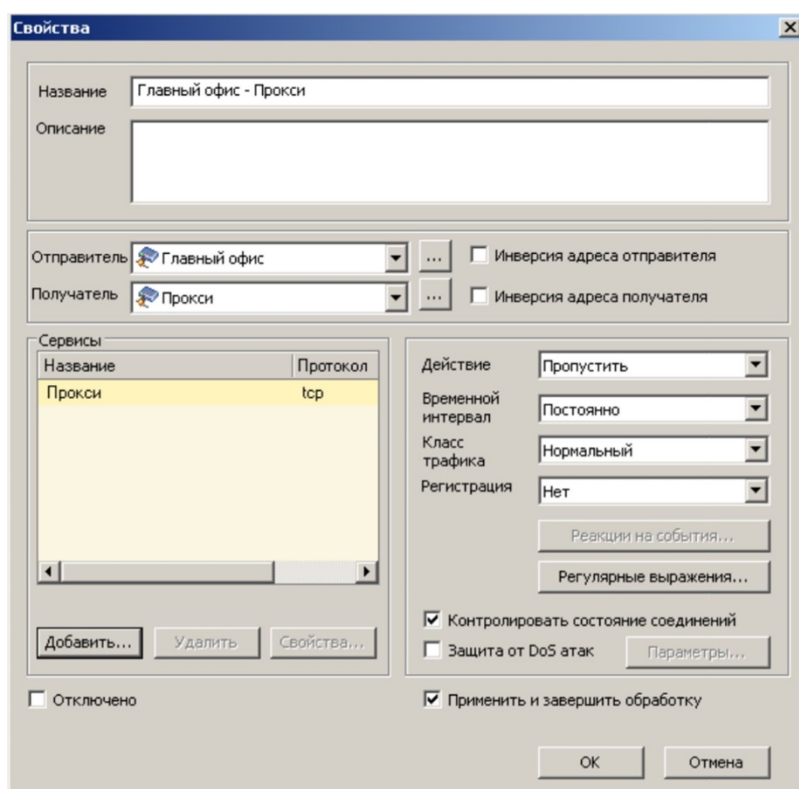
6. Вызовите меню "Операции" и активируйте команду "Создать сервис" или нажмите на кнопку «Создать сервис»  на панели

инструментов. На экране появится окно настройки параметров сервиса. Настройте параметры создаваемого сервиса, как это описано ниже.



Нажмите кнопку "OK". В списке появится имя нового сервиса, а сведения о нем будут сохранены в базе данных ЦУС.

7. В левой части окна программы управления выберите папку "Центр управления сетью \ Правила фильтрации". Создайте правило фильтрации "Главный офис - Прокси" и настройте параметры создаваемого правила, как это описано ниже:

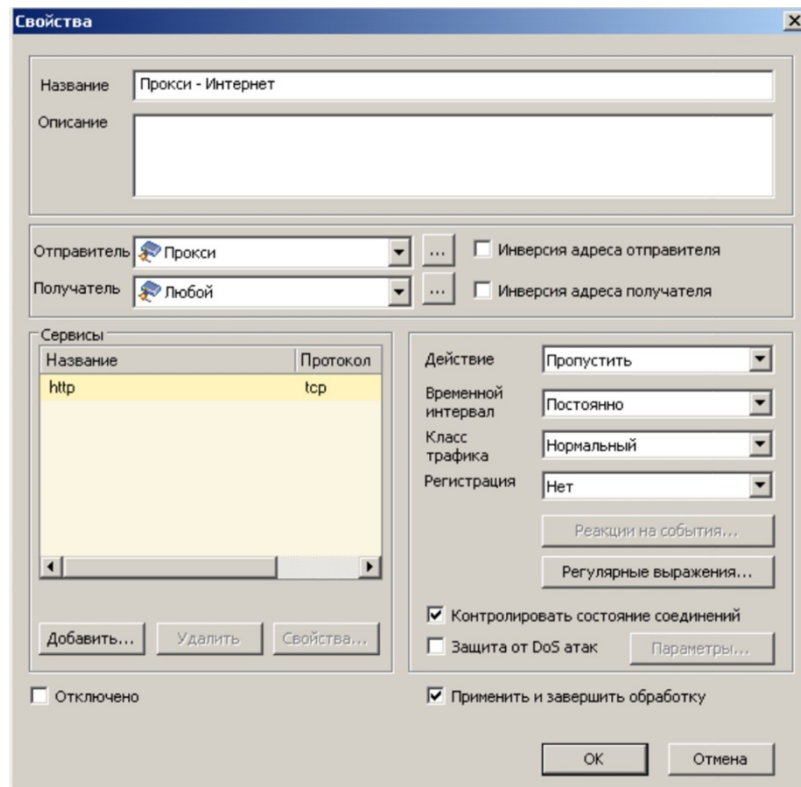


Нажмите «ОК».

8. Нажмите кнопку "Сохранить изменения"  на панели инструментов.

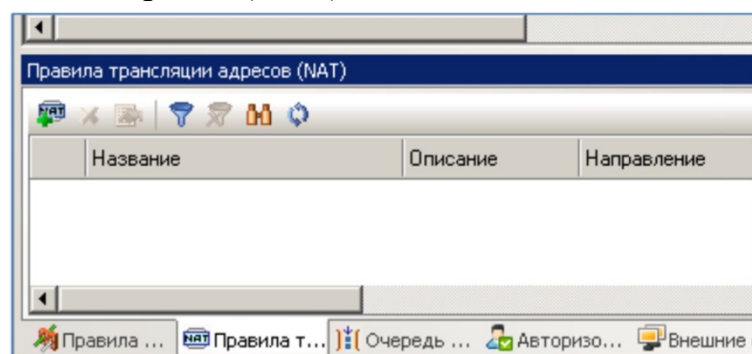
9. Используйте сетевой объект «Любой», созданный при инициализации ЦУС1 автоматически с параметрами «по умолчанию».

10. Создайте правило фильтрации “Прокси - Интернет”



11. Нажмите кнопку "Сохранить изменения"  на панели инструментов.

12. В левой части окна программы управления выберите папку "Криптошлюзы". В правом окне программы выберите криптошлюз КШ с ЦУСом. В правом нижнем углу интерфейса программы выберите вкладку “Правила трансляции адресов (NAT)” и создайте правило трансляции “Прокси — Интернет”, настройте его в соответствии с рисунком “Правило трансляции адресов (NAT)”:



Застройки правил трансляции:

Источник - **Прокси**;

Получатель - **Любой**;

Интерфейс - **1e0**;

Изменить на - **200.200.1.1 255.255.255.255**

Правило трансляции адресов (NAT)

Название: Прокси - Интернет

Описание:

Направление: Исходящие

Временной интервал: Постоянно

Источник: Прокси

Класс трафика: Нормальный

Получатель: Любой

Регистрация: Нет

Интерфейс: 1e0

Реакции на события...

Трансляция адреса источника

IP-адрес: 192 . 168 . 3 . 3

изменить на: 200 . 200 . 1 . 1

Маска: 255 . 255 . 255 . 255

Маска: 255 . 255 . 255 . 255

Сервисы и трансляция портов

Название сервиса	Протокол	Порт назначения	Порт трансляции

Добавить... Удалить Свойства... Порт трансляции...

☒ Отключено

OK Отмена

Нажмите «OK».

Проверка работы правила

На реальной (не виртуальной !) машине перейдите в каталог курса
(расположение директории может меняться в зависимости от номера аудитории):

E:\T007\http\Abyss Web Server.

Отредактируйте файл abyss.conf: задайте правильный путь в строке, указывающей расположение каталога программы (путь не может содержать символы Кириллицы!).

```
<server>
  <parameters>
    <root> E:\T007\vm\http\Abyss web server\
    </root>
    <timeout>
      30
    </timeout>
  </parameters>
</server>
```

Запустите файл abyssws.exe.

Перейдите на виртуальную машину PШ и настройте Internet Explorer следующим образом.

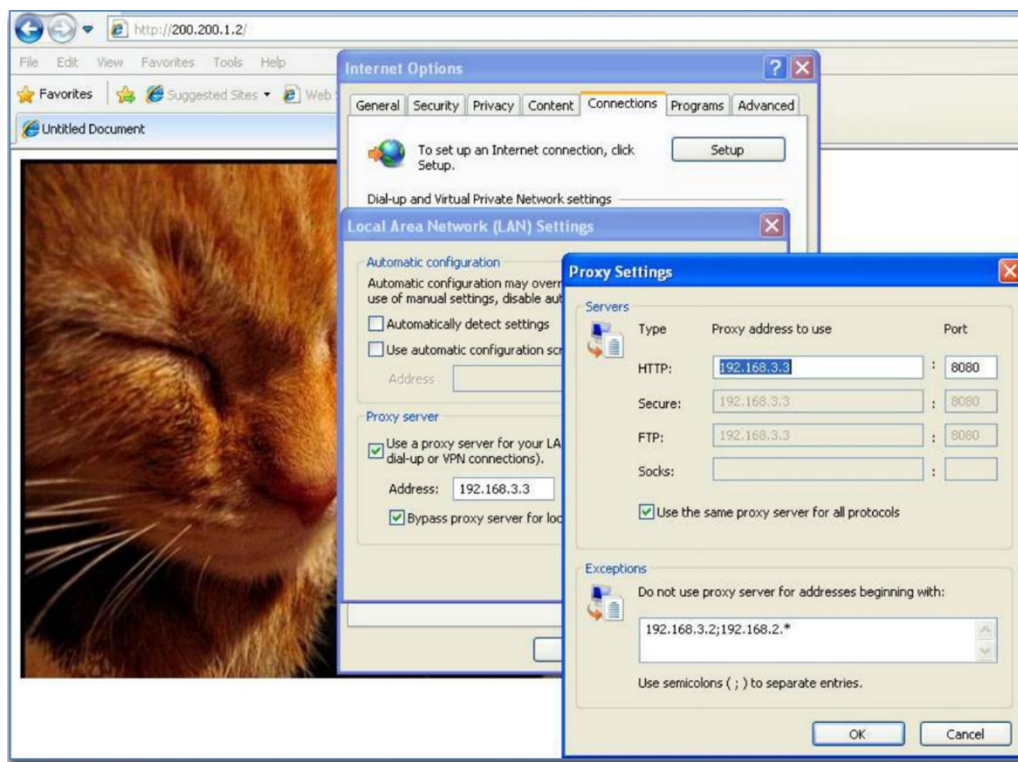
Выберите в меню "Tools\Options".

На вкладке Connections нажмите кнопку Advanced и настройте

параметры proxy , как показано на рисунке.

Proxy address 192.168.3.3 Port 8080.

Не использовать проху для адресов 192.168.3.2; 192.168.2.*

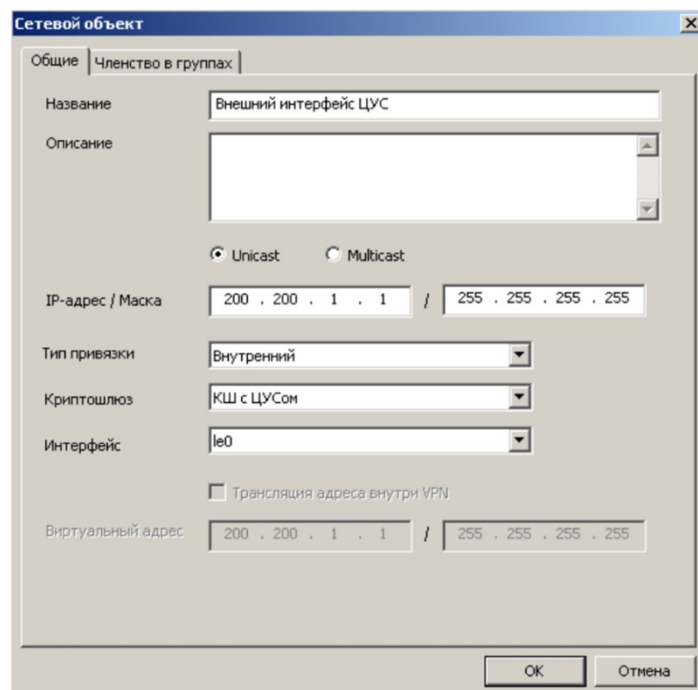


С виртуальной машины **РШ** зайдите на веб страницу по ссылке <http://200.200.L2>

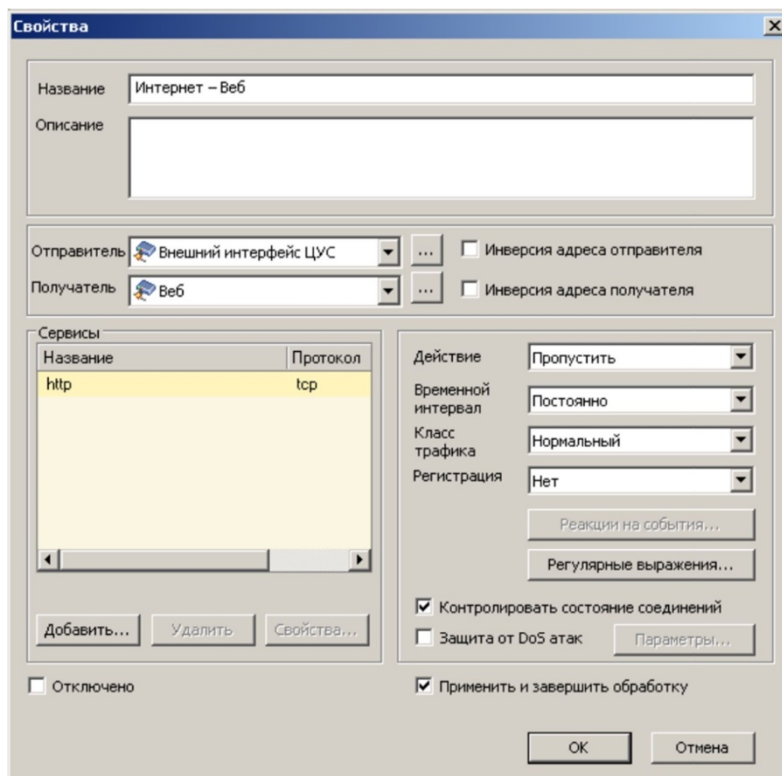
9.3 Методические рекомендации и пояснения по выполнению третьего вопроса

Вопрос 3. Доступ внешних пользователей к веб серверу в ДМЗ

1. Создайте сетевой объект «Внешний интерфейс ЦУС».

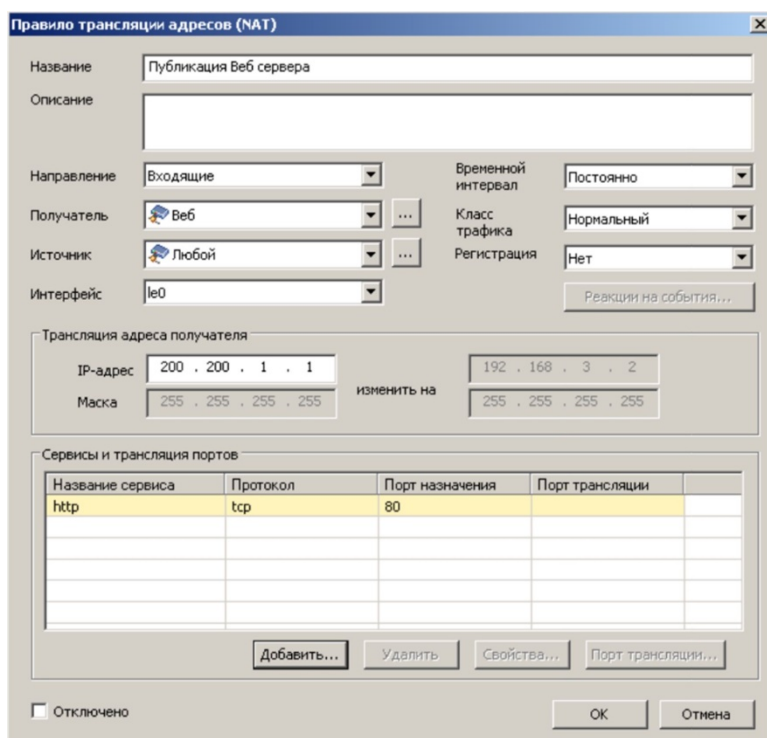


2. Создайте правило фильтрации «Интернет - Веб».



На панели инструментов нажмите кнопку "Сохранить изменения" 

3. Создайте правило трансляции с названием «Публикация Веб сервера». Для входящего правила трансляции список «Сервисы и трансляция портов» не должен быть пустым. Добавьте сервис http (порт назначения tcp 80).



4. Для того, чтобы проверить на основной машине (не виртуальной) запустите Internet Explorer, отключите в нем прокси и в адресной строке

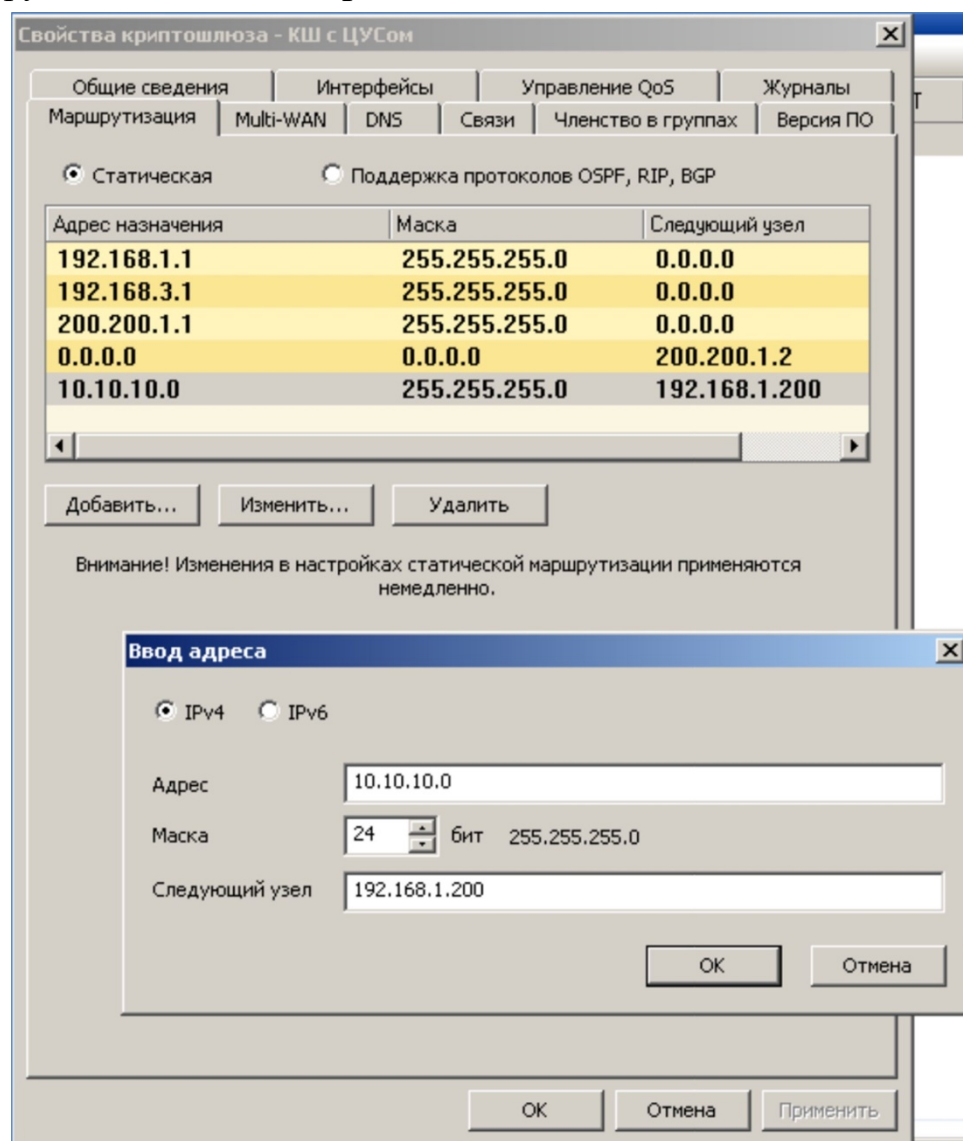
введите адрес <http://200.200.1.1>

9.4 Методические рекомендации и пояснения по выполнению первого вопроса

Вопрос 4. Доступ внутренних пользователей сети СКЛАД к ДМЗ

Для настройки правил маршрутизации в правом окне программы управления вызовите контекстное меню КШ с ЦУСом, и активируйте команду «Свойства...». На экране появится окно «Свойства криптошлюза».

13. Перейдите к вкладке «Маршрутизация» и задайте новый маршрут как показано на рисунке, затем нажмите кнопку "Добавить". Введите данные маршрута в окне «Ввод адреса».



Для сохранения изменений нажмите кнопку "OK".

14. Создайте сетевой объект «Склад».

Сетевой объект

Общие | Членство в группах

Название: Склад

Описание:

Unicast Multicast

IP-адрес / Маска: 10 . 10 . 10 . 0 / 255 . 255 . 255 . 0

Тип привязки: Защищаемый

Криптошлюз: КШ с ЦУСон

Интерфейс: le1

☐ Трансляция адреса внутри VPN

Виртуальный адрес: 0 . 0 . 0 . 0 / 255 . 255 . 255 . 0

OK Отмена

15. Создайте правило фильтрации «Склад — ДМЗ», разрешающее трафик для сервисов **icmp** и **http**.

Свойства

Название: Склад - ДМЗ

Описание:

Отправитель: Склад

Получатель: ДМЗ

☐ Инверсия адреса отправителя

☐ Инверсия адреса получателя

Сервисы

Название	Протокол
echo-request	icmp
http	tcp

Действие: Пропустить

Временной интервал: Постоянно

Класс трафика: Нормальный

Регистрация: Нет

☒ Контролировать состояние соединений

☐ Защита от DoS атак

☐ Применить и завершить обработку

OK Отмена

На панели инструментов нажмите кнопку «Сохранить изменения» 

16. Для проверки запустите виртуальную машину SKLAD.
Авторизуйтесь в системе (User:Administrator password: 1111)

Выполните с виртуальной машины SKLAD команду ping 192.168.3.2 и зайдите по ссылке <http://192.168.3.2>

```
Ethernet adapter VMnet5:
    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 10.10.10.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.10

C:\Documents and Settings\Administrator>ping 192.168.3.2
Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time=2ms TTL=62
Reply from 192.168.3.2: bytes=32 time=1ms TTL=62
Reply from 192.168.3.2: bytes=32 time=1ms TTL=62
Reply from 192.168.3.2: bytes=32 time=1ms TTL=62
Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

ЛАБОРАТОРНАЯ РАБОТА № 7-8

ИССЛЕДОВАНИЕ РАБОТЫ ПРОСТЫХ СПИСКОВ КОНТРОЛЯ ДОСТУПА

Формируемые компетенции: ОПК-9, ОПК-10.

1. Настройка и проверка стандартных ACL-списков
2. Приобретение практических навыков настройки и проверки стандартных ACL-списков.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал, посвящённый настройке и проверке стандартных ACL-списков.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

3. Распределение времени занятия:

Всего: 180 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 70 мин

1. Исследование стандартных ACL – списков 70 мин

Проверка выполнения практического занятия 10 мин

Заключительная часть 3 мин

4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

4.1. Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

4.2. Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

4.3. Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

6. Программное обеспечение

Программа эмуляции терминала.

7. Основные теоретические сведения

См. рекомендованную к ознакомлению литературу по изучаемой дисциплине

8. Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1-2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению практических работ
по дисциплине «Программно-аппаратные средства защиты информации»
для студентов направления подготовки
10.03.01 «Информационная безопасность»
Направленность (профиль)
«Организация и технологии защиты информации (по отрасли или в сфере
профессиональной деятельности)»

Ставрополь
2026

Содержание:

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1 Обход межсетевых экранов	55
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 2 Модели систем обнаружения вторжений 61	
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №3 Методы обхода систем обнаружения вторжений.....	75
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №4 Протоколы VPN канального уровня	90
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 5 Типы вредоносного программного обеспечения и защита от угроз	96
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №6 ОТЛАДКА БАЗОВОГО PPP С АУТЕНТИФИКАЦИЕЙ.....	113
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 7 Типы вредоносного программного обеспечения и защита от угроз	138
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 8-9 Атаки на сетевые протоколы и защита от них	154

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1

Тема: Настройка и подготовка к работе Cisco ASA 5505

1. Цель работы

1. Минимальная настройка ASA5505.
2. Приобретение практических навыков настройки ASA5505.

Формируемые компетенции: ОПК-9, ОПК-10.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал, посвящённый настройке ASA5505.
2. Ознакомиться с программой работы.
3. Подготовить отчет о работе.
4. Ответить на контрольные вопросы.

3. Распределение времени занятия:

Всего: 4,5 часов

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 70 мин

1. Минимальная настройка ASA5505 70 мин
 2. Проверка выполнения практического занятия 10 мин
- Заключительная часть 3 мин

4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

4.1. Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

4.2. Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование,

соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию;

- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;

- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

4.3. Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

6. Программное обеспечение

Программа эмуляции терминала Tera Term.

7. Основные теоретические сведения

См. рекомендованную к ознакомлению литературу по изучаемой дисциплине

8. Литература

1. James Boney, Cisco IOS in a Nutshell, O'Reilly, 2013
2. Wendell Odom, Interconnecting Networking Devices Cisco, Part 2, Cisco Press, 2013

9. Методические рекомендации по выполнению работы

9.1 Исходные данные

ASA5505 с чистой конфигурацией.

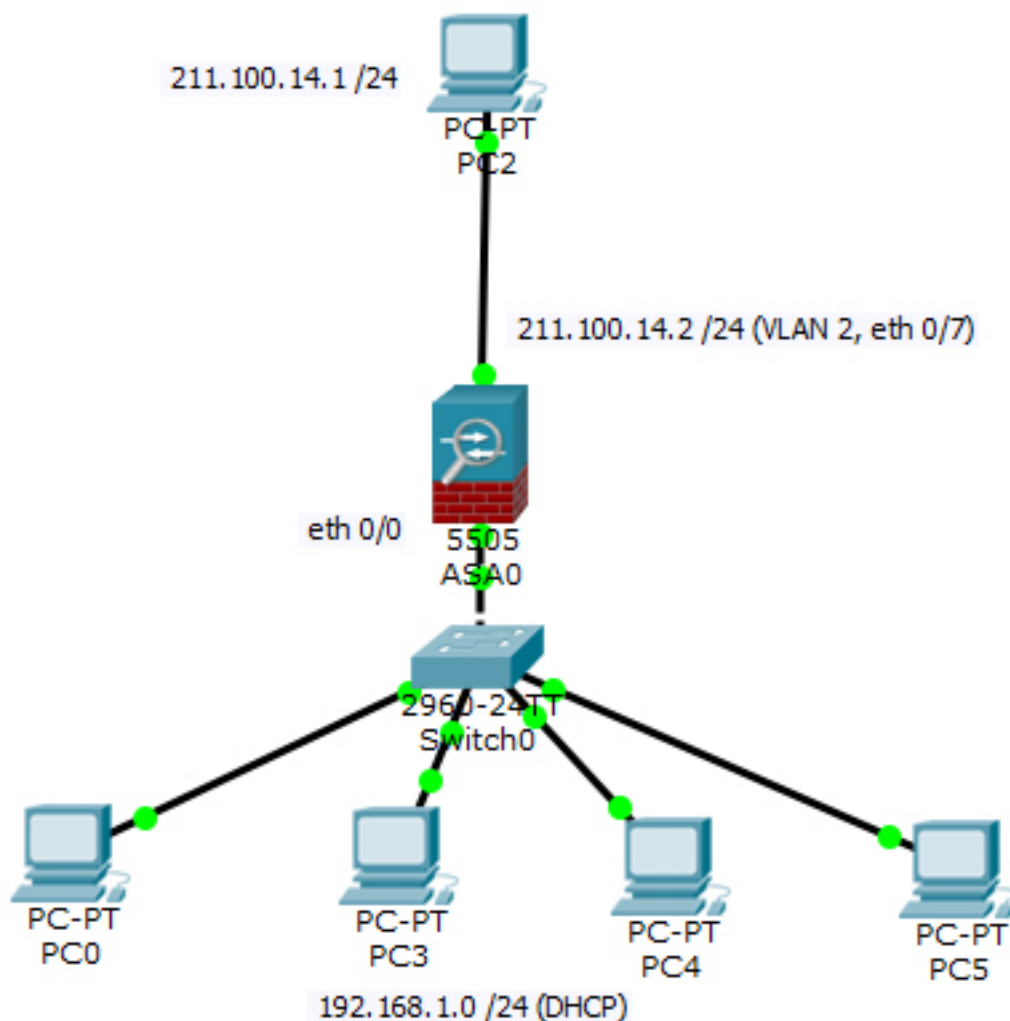


Рисунок 9 – Топология

9.2 Задача

Настроить внутреннюю сеть с раздачей IP по DHCP, NAT для доступа в интернет.

9.3 Вопросы

1. Настроить Vlan'ы.
2. Привязать Vlan к интерфейсам
3. Настроить DHCPD и прописать маршрут по умолчанию
4. Настроить NAT

9.4 Методические пояснения и рекомендации по выполнению первого вопроса

Вопрос 1 Настроить Vlan'ы.

В ASA по умолчанию есть только Vlan1. Так как он по умолчанию привязан ко всем портам, стоит его использовать для локальной сети. Указываем в нем IP-адрес ASA во внутренней сети, фактически основной шлюз. А так же устанавливаем security-level 100 - это позволяет трафику из внутренней сети спокойно проходить в Vlan с меньшим приоритетом, но запрещает установку соединений в обратную сторону (если не указано отдельное правило).

Параметр «уровень безопасности» (security level) – это число от 0 до 100, которое позволяет сравнить 2 интерфейса и определить, кто из них более «безопасен». Параметр используется качественно, а не количественно, т.е. важно только отношение «больше-меньше». По умолчанию трафик, идущий «наружу», т.е. с интерфейса с большим уровнем безопасности на интерфейс с меньшим уровнем безопасности, пропускается, сессия запоминается и обратно пропускаются только ответы по этим сессиям. Трафик идущий «внутри» по умолчанию запрещен.

Как правило, уровень безопасности интерфейсов подбирается таким образом, чтобы максимально соответствовать логической топологии сети. Сама топология представляет из себя зоны безопасности и правила взаимодействия между ними. Классической схемой считается присвоение разным интерфейсам разных уровней безопасности.

Никто не запрещает сделать уровень безопасности на разных интерфейсах одинаковым, однако по умолчанию обмен трафиком между такими интерфейсами запрещен. Такой трафик можно сознательно разрешить, дав команду

```
same-security-traffic permit inter-interface
```

Однако надо понимать, что между интерфейсами с одинаковым уровнем безопасности не возникает межсетевого экранирования, а только маршрутизация. Поэтому такой подход применяется для интерфейсов, относящихся к одной и той же логической зоне безопасности (например, 2 локальные сети пользователей, объединяемые при помощи ASA)

Настройка интерфейсов LAN

```
interface Vlan1  
nameif LAN
```

```
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
```

Так же создадим Vlan2, который будем использовать для подключения к интернет.

```
interface Vlan2
nameif WAN
security-level 0
ip address 211.100.14.2 255.255.255.0
no shutdown
```

В этот раз приоритет 0, для самого недоверенного трафика.

Имена vlan'ов можно выбрать любые, но желательно что бы они были вам понятны, в дальнейшем их придется часто использовать для настройки.

9.5 Методические пояснения и рекомендации по выполнению второго вопроса

Привязать Vlan к интерфейсам.

Теперь нам необходимо указать, на каких интерфейсах какой VLAN. Как уже сказано, VLAN по умолчанию настроен на всех. Интерфейсы ASA настраиваются аналогично интерфейсам коммутатора 2го уровня:

```
interface Ethernet0/7<
switchport access vlan 2
no shutdown
interface Ethernet0/0
no shutdown
```

9.6 Методические пояснения и рекомендации по выполнению третьего вопроса

Настроить DHCPD и прописать маршрут по умолчанию

Теперь настроим раздачу IP-адресов в нашей сети.

```
dhcpd address 192.168.1.2-192.168.1.254 LAN
dhcpd dns 8.8.8.8 interface WAN
dhcpd enable LAN
route 0.0.0.0 0.0.0.0 211.100.14.2
```

dhcpd address 192.168.1.2-192.168.1.254 LAN - какие адреса раздавать и в каком VLAN

dhcpd dns 8.8.8.8 - какой адрес DNS, который надо использовать.
dhcpd enable LAN - включаем раздачу адресов в конкретном VLAN.
route 0 0 1.1.1.1 - это означает маршрут на все адреса, где 1.1.1.1 next-hope, указанный вашим провайдером как маршрут по умолчанию.

9.7 Методические пояснения и рекомендации по выполнению четвёртого вопроса

Настроить NAT

В ASA есть два варианта прописать NAT - в глобальной настройке и в настройке объекта типа network. Сейчас мы пропишем его в объекте:

```
object network LAN
subnet 192.168.1.0 255.255.255.0
nat (LAN,WAN) dynamic interface
```

Далее этот объект, в котором мы записали нашу локальную сеть мы сможем использовать при составлении списков доступа и т.д., пригодиться еще. Если вы настраиваете только что купленную ASA, то возможно NAT - правило было создано автоматически при указании security-level на vlan.

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1-2

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 2

Тема: Разработка расширенных acl

1. Цель работы

1. Настройка и проверка расширенных ACL-списков.
2. Приобретение практических навыков настройки расширенных ACL-списков.

Формируемые компетенции: ОПК-9, ОПК-10.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал, посвящённый настройке расширенных ACL-списков.
2. Ознакомиться с программой работы.
3. Подготовить отчет о работе.
4. Ответить на контрольные вопросы.

3. Распределение времени занятия:

Всего: 4,5 часов

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 70 мин

1. Настройка расширенных ACL-списков 70 мин
2. Проверка выполнения практического занятия 10 мин

Заключительная часть 3 мин

4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

4.1. Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

4.2. Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать

только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию;

- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;

- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

4.3. Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

6. Программное обеспечение

Программа эмуляции терминала Tera Term.

7. Основные теоретические сведения

См. рекомендованную к ознакомлению литературу по изучаемой дисциплине

8. Литература

1. James Boney, Cisco IOS in a Nutshell, O'Reilly, 2013
2. Wendell Odom, Interconnecting Networking Devices Cisco, Part 2, Cisco Press, 2013

9. Методические рекомендации по выполнению работы

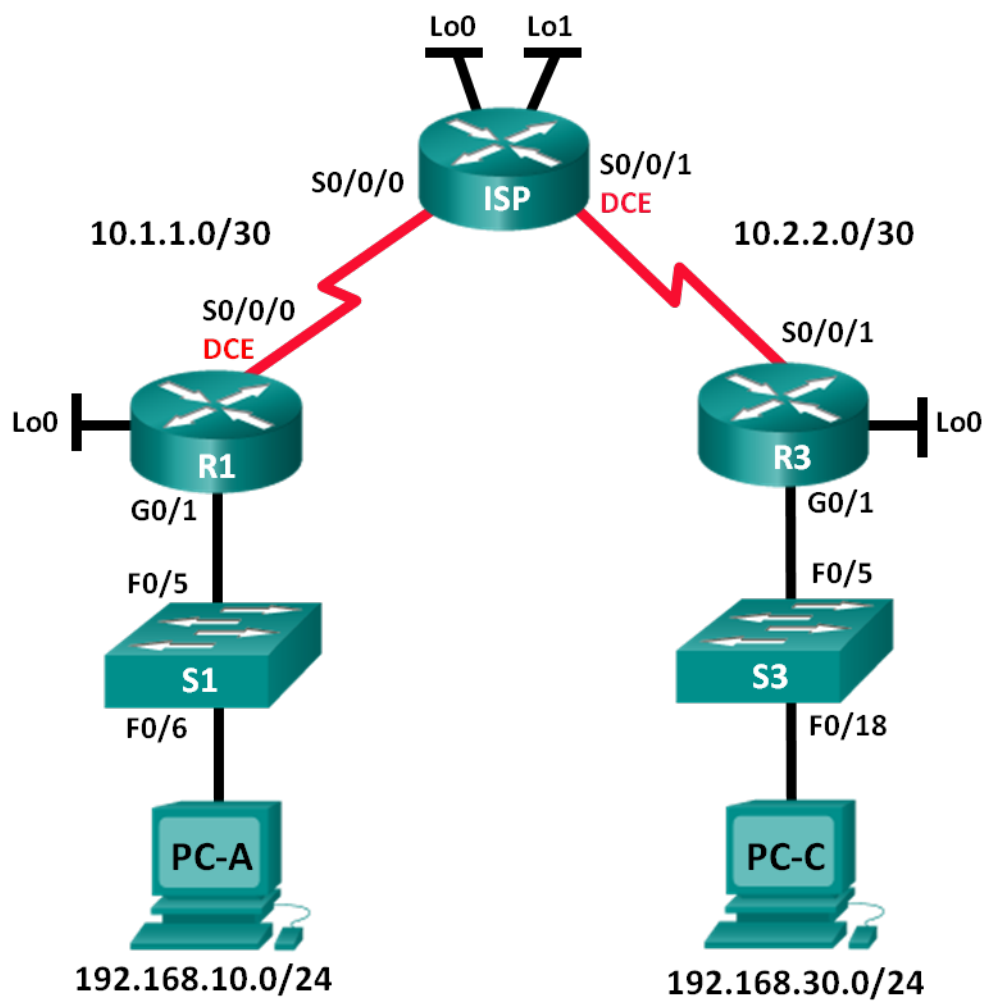


Рисунок 10 - Топология

Таблица 12. Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.10.1	255.255.255.0	N/A
	Lo0	192.168.20.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
	Lo1	209.165.201.1	255.255.255.224	N/A
R3	G0/1	192.168.30.1	255.255.255.0	N/A
	Lo0	192.168.40.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S3	VLAN 1	192.168.30.11	255.255.255.0	192.168.30.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1

9.1 Задачи

1. Настройка топологии и установка исходного состояния устройства

2. Конфигурация устройств и проверка подключения

- Настройте базовые параметры на компьютерах, маршрутизаторах и коммутаторах.
- Настройте маршрутизацию EIGRP на маршрутизаторах R1, ISP и R3.

3. Настройка и проверка расширенных нумерованных и именованных ACL-списков

- Настройте, примените и проверьте нумерованные расширенные ACL-списки.
- Настройте, примените и проверьте именованные расширенные ACL-списки.

4. Изменение и проверка расширенных ACL-списков

9.2 Исходные данные/сценарий

Расширенные списки контроля доступа (ACL) демонстрируют высокую эффективность. Они предлагают более высокий уровень управления, чем

стандартные ACL-списки, как по отношению к типам фильтруемого трафика, так и к тому, где трафик создан и куда он направлен.

В данной лабораторной работе вы настроите правила фильтрации для двух офисов, представленных маршрутизаторами R1 и R3. Руководство определило некоторые правила в рамках политики безопасности для сетей LAN, расположенных на маршрутизаторах R1 и R3, которые вы должны реализовать. На маршрутизаторе ISP, расположенном между R1 и R3, не настроены ACL-списки. У вас не будет прав административного доступа к маршрутизатору ISP, поскольку вы можете управлять только собственным оборудованием.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсе маршрутизатора в конце этой лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

9.3 Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

9.4 Методические пояснения и рекомендации по выполнению первого вопроса

Часть 1: Настройка топологии и инициализация устройств

В первой части вам предстоит создать топологию сети и при необходимости удалить все конфигурации.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

9.5 Методические пояснения и рекомендации по выполнению второго вопроса

Часть 2: Настройка устройств и проверка подключения

Во второй части вам предстоит настроить базовые параметры маршрутизаторов, коммутаторов и компьютеров. Имена и адреса устройств указаны в топологии и таблице адресации.

Шаг 1: Настройте IP-адреса на PC-A и PC-C.

Шаг 2: Настройте базовые параметры на маршрутизаторе R1.

- a. Отключите поиск DNS.
- b. Настройте имя устройства в соответствии с топологией.
- c. Создайте loopback-интерфейс на маршрутизаторе R1.
- d. Настройте IP-адреса интерфейсов в соответствии с топологией и таблицей адресации.
- e. Установите пароль **class** для доступа к привилегированному режиму EXEC.
- f. Установите тактовую частоту для интерфейса S0/0/0 на значение **128000**.
- g. Назначьте **cisco** в качестве пароля для VTY и активируйте доступ к Telnet. Настройте **logging synchronous** для консоли и каналов vty.
- h. Активируйте сетевой доступ на маршрутизаторе R1, чтобы смоделировать веб-сервер с локальной аутентификацией для пользователя **admin**.

```
R1(config)# ip http server
```

```
R1(config)# ip http authentication local
```

```
R1(config)# username admin privilege 15 secret class
```

Шаг 3: Настройте базовые параметры на ISP.

- a. Настройте имя устройства в соответствии с топологией.
- b. Создайте loopback-интерфейсы на ISP.
- c. Настройте IP-адреса интерфейсов в соответствии с топологией и таблицей адресации.
- d. Отключите поиск DNS.
- e. Назначьте **class** в качестве пароля привилегированного режима EXEC.
- f. Установите тактовую частоту на значение **128000** для интерфейса S0/0/1.
- g. Назначьте **cisco** в качестве пароля для VTY и активируйте доступ к Telnet. Настройте **logging synchronous** для консоли и каналов vty.
- h. Активируйте веб-доступ на ISP. Используйте те же параметры, что и на шаге 2h.

Шаг 4: Настройте базовые параметры на маршрутизаторе R3.

- a. Настройте имя устройства в соответствии с топологией.
- b. Создайте loopback-интерфейс на маршрутизаторе R3.
- c. Настройте IP-адреса интерфейсов в соответствии с топологией и таблицей адресации.
- d. Отключите поиск DNS.
- e. Назначьте **class** в качестве пароля привилегированного режима EXEC.
- f. Назначьте **cisco** в качестве пароля консоли и настройте **logging synchronous** на канале консоли.
- g. Включите SSH на S3.

```
R3(config)# ip domain-name cisco.com
```

```
R3(config)# crypto key generate rsa modulus 1024
```

```
R3(config)# line vty 0 4
```

```
R3(config-line)# login local
```

```
R3(config-line)# transport input ssh
```

- h. Активируйте веб-доступ на R3. Используйте те же параметры, что и на шаге 2h.

Шаг 5: Настройте базовые параметры на коммутаторах S1 и S3 (дополнительно).

- a. Настройте имена узлов в соответствии с топологией.

- b. Настройте IP-адреса административного интерфейса в соответствии с топологией и таблицей адресации.
- c. Отключите поиск DNS.
- d. Установите пароль **class** для доступа к привилегированному режиму EXEC.
- e. Настройте адрес основного шлюза.

Шаг 6: Настройте маршрутизацию EIGRP на маршрутизаторах R1, ISP и R3.

- a. Настройте автономную систему (AS) номер 10 и объявите все сети на маршрутизаторах R1, ISP и R3. Отключите автоматическое суммирование маршрутов.
- b. После настройки EIGRP на маршрутизаторах R1, ISP и R3 убедитесь, что все маршрутизаторы имеют заполненные таблицы маршрутизации с необходимыми для работы сетями. В случае необходимости выполните поиск и устранение неполадок.

Шаг 7: Проверьте наличие подключения между всеми устройствами.

Примечание. Наличие соединения важно проверять **перед** настройкой и применением списков контроля доступа! Прежде чем приступить к фильтрации трафика, проверьте работоспособность сети.

- a. От узла PC-A отправьте эхо-запросы на PC-C, loopback-интерфейс и последовательные интерфейсы на маршрутизаторе R3.

Успешно ли выполнены эхо-запросы? _____

- b. От маршрутизатора R1 отправьте эхо-запросы на PC-C, loopback-интерфейс и последовательный интерфейс на маршрутизаторе R3.

Успешно ли выполнены эхо-запросы? _____

- c. От узла PC-C отправьте эхо-запросы на PC-A, loopback-интерфейс и последовательный интерфейс на маршрутизаторе R1.

Успешно ли выполнены эхо-запросы? _____

- d. От маршрутизатора R3 отправьте эхо-запросы на PC-A, loopback-интерфейс и последовательный интерфейс на маршрутизаторе R1.

Успешно ли выполнены эхо-запросы? _____

- e. От узла PC-A отправьте эхо-запросы на loopback-интерфейсы на маршрутизаторе ISP.

Успешно ли выполнены эхо-запросы? _____

f. От узла PC-C отправьте эхо-запросы на loopback-интерфейсы на маршрутизаторе ISP.

Успешно ли выполнены эхо-запросы? _____

g. Откройте веб-браузер на узле PC-A и перейдите по адресу <http://209.165.200.225> интернет-провайдера. Появится окно с запросом имени пользователя и пароля. Используйте admin как имя пользователя и class как пароль. Если появится запрос принять подпись, подтвердите приём подписи. В отдельном окне маршрутизатор загрузит приложение Cisco Configuration Professional (CCP) Express. Появится окно с запросом имени пользователя и пароля. Используйте admin как имя пользователя и class как пароль.

h. Откройте веб-браузер на узле PC-C и перейдите по адресу <http://10.1.1.1> на маршрутизаторе R1. Появится окно с запросом имени пользователя и пароля. Используйте admin как имя пользователя и class как пароль. Если появится запрос принять подпись, подтвердите приём подписи. В отдельном окне маршрутизатор загрузит приложение CCP Express. Появится окно с запросом имени пользователя и пароля. Используйте admin как имя пользователя и class как пароль.

9.6 Методические пояснения и рекомендации по выполнению третьего вопроса

Часть 3: Настройка и проверка расширенных нумерованных и расширенных именованных ACL-списков

Расширенные ACL-списки позволяют фильтровать трафик различными способами. Расширенные ACL-списки позволяют фильтровать трафик на основе IP-адреса отправителя, порта отправителя, IP-адреса назначения, порта назначения, а также на основе различных протоколов и служб.

Данные списки контроля доступа работают в соответствии со следующими правилами безопасности:

1. Разрешать доступ веб-трафика из сети 192.168.10.0/24 в любую сеть.
2. Разрешать подключение SSH к последовательному интерфейсу R3 от узла PC-A.
3. Разрешать пользователям в сети 192.168.10.0.24 сетевой доступ к сети 192.168.20.0/24.
4. Разрешать доступ веб-трафика из сети 192.168.30.0/24 к маршрутизатору R1 через веб-интерфейс и сеть интернет-провайдера

209.165.200.224/27. Доступ сети 192.168.30.0/24 к какой-либо другой сети должен быть ЗАПРЕЩЁН.

Для выполнения этих правил безопасности вам потребуется как минимум два ACL-списка. Рекомендуется разместить ACL-списки как можно ближе к источнику. Мы последуем этой рекомендации для соблюдения вышеупомянутых правил безопасности.

Шаг 1: Для расширенных нумерованных ACL-списков на маршрутизаторе R1 настройте номера 1 и 2.

На маршрутизаторе R1 вы будете использовать нумерованный расширенный список. Укажите диапазоны для расширенных ACL-списков.

а. Настройте ACL-список на маршрутизаторе R1. В качестве номера списка доступа используйте 100.

```
R1(config)# access-list 100 remark Allow Web & SSH Access
```

```
R1(config)# access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22
```

```
R1(config)# access-list 100 permit tcp any any eq 80
```

Что означает 80 в вышеуказанных выходных данных?

На каких интерфейсах должен быть применён ACL-список под номером 100?

На каком направлении следует применить ACL-список 100?

б. Примените ACL-список 100 на интерфейсе S0/0/0.

```
R1(config)# int s0/0/0
```

```
R1(config-if)# ip access-group 100 out
```

с. Проверьте работу ACL-списка 100.

1) Откройте веб-браузер на узле PC-A и проверьте доступ к <http://209.165.200.225> (маршрутизатор ISP). Всё должно работать; в обратном случае выявите и устраните неполадки.

2) Установите SSH-подключение от узла PC-A к маршрутизатору R3, используя 10.2.2.1 в качестве IP-адреса. Войдите в систему, используя учётные данные **admin** и **class**. Всё должно работать; в обратном случае выявите и устраните неполадки.

3) Из командной строки привилегированного режима на маршрутизаторе R1 выполните команду **show access-lists**.

```
R1# show access-lists
```

```
Extended IP access list 100
```

```
10 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22 (22 matches)
```

```
20 permit tcp any any eq www (111 matches)
```

4) Из командной строки узла PC-A выполните эхо-запрос на адрес 10.2.2.1. Поясните полученные результаты.

Шаг 2: Настройте именованный расширенный ACL-список на маршрутизаторе R3 для соблюдения правила безопасности под номером 3.

а. Настройте политику безопасности на маршрутизаторе R3. Имя ACL-списка: WEB-POLICY.

```
R3(config)# ip access-list extended WEB-POLICY
```

```
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq 80
```

```
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 209.165.200.224
0.0.0.31 eq 80
```

b. Примените ACL-список WEB-POLICY на интерфейсе S0/0/1.

```
R3(config-ext-nacl)# int S0/0/1
```

```
R3(config-if)# ip access-group WEB-POLICY out
```

с. Проверьте работу ACL-списка WEB-POLICY.

1) Из командной строки привилегированного режима маршрутизатора R3 выполните команду **show ip interface s0/0/1**.

Укажите имя ACL-списка (если имеется).

На каком направлении применён ACL-список?

2) Откройте веб-браузер на узле PC-C и получите доступ к <http://209.165.200.225> (маршрутизатор ISP). Всё должно работать; в обратном случае выявите и устраните неполадки.

3) На узле PC-C откройте веб-сеанс на адрес <http://10.1.1.1> (R1). Всё должно работать; в обратном случае выявите и устраните неполадки.

4) На узле PC-C откройте веб-сеанс на адрес <http://209.165.201.1> (маршрутизатор ISP). Эхо-запрос не должен пройти; в противном случае выявите и устраните неполадки.

5) Из командной строки узла PC-C отправьте эхо-запрос на узел PC-A. Какой получен результат? Почему?

9.7 Методические пояснения и рекомендации по выполнению четвёртого вопроса

Часть 4: Изменение и проверка расширенных ACL-списков

Вследствие применения ACL-списков на маршрутизаторах R1 и R3, ни эхо-запросы, ни какие-либо другие виды трафика не могут проходить между локальными сетями на маршрутизаторах R1 и R3. Руководство решило

разрешить весь трафик между сетями 192.168.10.0/24 и 192.168.30.0/24.

Необходимо внести изменения в ACL-списки на маршрутизаторах R1 и R3.

Шаг 1: Измените ACL-список 100 на маршрутизаторе R1.

a. В привилегированном режиме маршрутизатора R1 выполните команду **show access-lists**.

Сколько строк имеется в списке контроля доступа?

b. Войдите в режим глобальной конфигурации и измените ACL-список на маршрутизаторе R1.

```
R1(config)# ip access-list extended 100
```

```
R1(config-ext-nacl)# 30 permit ip 192.168.10.0 0.0.0.255 192.168.30.0  
0.0.0.255
```

```
R1(config-ext-nacl)# end
```

c. Выполните команду **show access-lists**.

Где именно в ACL-списке 100 появился только что добавленный канал?

Шаг 2: Измените ACL-список WEB-POLICY на маршрутизаторе R3.

a. В привилегированном режиме маршрутизатора R3 выполните команду **show access-lists**.

Сколько строк имеется в списке контроля доступа?

b. Войдите в режим глобальной конфигурации и измените ACL-список на маршрутизаторе R3.

```
R3(config)# ip access-list extended WEB-POLICY
```

```
R3(config-ext-nacl)# 30 permit ip 192.168.30.0 0.0.0.255 192.168.10.0  
0.0.0.255
```

```
R3(config-ext-nacl)# end
```

с. Выполните команду **show access-lists**, чтобы убедиться, что в конце ACL-списка была добавлена новая строка.

Шаг 3: Проверьте работу изменённых ACL-списков.

а. От узла PC-A отправьте эхо-запрос на IP-адрес узла PC-C. Успешно ли выполнен эхо-запрос?

б. От узла PC-C отправьте эхо-запрос на IP-адрес узла PC-C. Успешно ли выполнен эхо-запрос?

Почему изменения ACL-списков незамедлительно подействовали на эхо-запросы?

9.8 Вопросы на закрепление

1. Почему необходимо тщательно планировать и проверять работу ACL-списков?

2. Какой тип ACL-списка лучше — стандартный или расширенный?

3. Почему скрытый запрет **deny any** или аналогичная явная запись ACL-списков, применённых на маршрутизаторах R1 и R3, не блокирует пакеты приветствия (hello) EIGRP и обновления маршрутизации?

Таблица 13. Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	Последовательный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

Список литературы, рекомендуемый к использованию по данной теме.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №3

Тема: Настройка и проверка асl-списков для ipv6

1. Цель работы

1. Настройка и проверка ACL-списков для IPv6.
2. Приобретение практических навыков настройки ACL-списков для IPv6.

Формируемые компетенции: ОПК-9, ОПК-10.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал, посвящённый настройке ACL-списков для IPv6.
2. Ознакомиться с программой работы.
3. Подготовить отчет о работе.
4. Ответить на контрольные вопросы.

3. Распределение времени занятия:

Всего 4,5 часов

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 70 мин

1. Настройка и проверка ACL-списков для IPv6 70 мин
2. Проверка выполнения практического занятия 10 мин

Заключительная часть 3 мин

4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

4.1. Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

4.2. Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать

только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию;

- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;

- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

4.3. Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

6. Программное обеспечение

Программа эмуляции терминала Tera Term.

7. Основные теоретические сведения

См. рекомендованную к ознакомлению литературу по изучаемой дисциплине

8. Литература

1. James Boney, Cisco IOS in a Nutshell, O'Reilly, 2013
2. Wendell Odom, Interconnecting Networking Devices Cisco, Part 2, Cisco Press, 2013

9. Методические рекомендации по выполнению работы

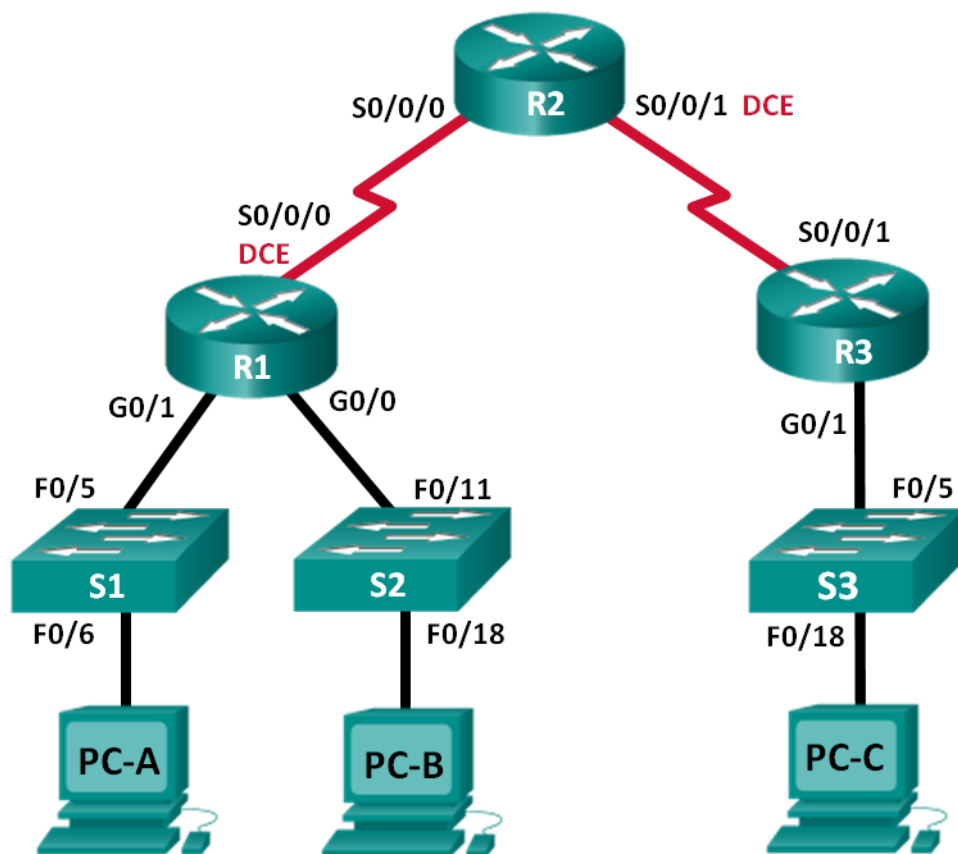


Рисунок 11 - Топология

Таблица 14. Таблица адресации

Устройство	Интерфейс	IP-адрес	Шлюз по умолчанию
R1	G0/0	2001:DB8:ACAD:B::1/64	N/A
	G0/1	2001:DB8:ACAD:A::1/64	N/A
	S0/0/0 (DCE)	2001:DB8:AAAA:1::1/64	N/A
R2	S0/0/0	2001:DB8:AAAA:1::2/64	N/A
	S0/0/1 (DCE)	2001:DB8:AAAA:2::2/64	N/A
R3	G0/1	2001:DB8:CAFE:C::1/64	N/A
	S0/0/1	2001:DB8:AAAA:2::1/64	N/A
S1	VLAN1	2001:DB8:ACAD:A::A/64	N/A
S2	VLAN1	2001:DB8:ACAD:B::A/64	N/A
S3	VLAN1	2001:DB8:CAFE:C::A/64	N/A
PC-A	NIC	2001:DB8:ACAD:A::3/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::3/64	FE80::1
PC-C	NIC	2001:DB8:CAFE:C::3/64	FE80::1

9.1 Задачи

1. Настройка топологии и установка исходного состояния устройства
2. Конфигурация устройств и проверка подключения
3. Настройка и проверка ACL-списков для IPv6
4. Редактирование ACL-списков для IPv6

9.2 Исходные данные/сценарий

Фильтрация IPv6-трафика путём создания ACL-списков для IPv6 и их применения на интерфейсах аналогична способу, по которому вы создавали именованные ACL-списки для IPv4. В IPv6 определены расширенные и именованные ACL-списки. Стандартные и нумерованные ACL-списки больше не используются для IPv6. Чтобы применить ACL-список IPv6 на интерфейсе vty, следует использовать новую команду **ipv6 traffic-filter**. Команда **ipv6 access-class** до сих пор используется для применения ACL-списков IPv6 на интерфейсах.

В рамках лабораторной работы вам предстоит применить правила фильтрации IPv6, а затем убедиться в правильной работе списков для ограничения доступа. Также вам нужно будет внести изменения в ACL-список IPv6 и очистить счётчики совпадений.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под

управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсе маршрутизатора в конце этой лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

9.3 Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 3 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель);
- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

9.4 Методические пояснения и рекомендации по выполнению первого вопроса

Часть 5: Настройка топологии и инициализация устройств

В первой части лабораторной работы вам нужно настроить топологию сети и при необходимости удалить все конфигурации.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

9.5 Методические пояснения и рекомендации по выполнению второго вопроса

Часть 6: Настройка устройств и проверка подключения

Во второй части вам предстоит настроить базовые параметры маршрутизаторов, коммутаторов и компьютеров. Имена и адреса устройств

можно найти в топологии и таблице адресации в начале этой лабораторной работы.

Шаг 1: Настройте IPv6-адреса на всех ПК.

Настройте глобальный индивидуальный IPv6-адрес в соответствии с таблицей адресации. Используйте локальный адрес канала **FE80::1** для шлюза по умолчанию на всех ПК.

Шаг 2: Настройте коммутаторы.

- a. Отключите поиск DNS.
- b. Назначьте имя узла.
- c. Назначьте имя домена для **ccna-lab.com**.
- d. Зашифруйте все незашифрованные пароли.
- e. Создайте баннер MOTD, предупреждающий пользователей о том, что неавторизованный доступ запрещён.
- f. Создайте базу данных локального пользователя с именем пользователя **admin** и паролем **classadm**.
- g. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
- h. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.
- i. Активируйте возможность входа на линии VTY с помощью локальной базы данных.
- j. Создайте ключ шифрования RSA для SSH с длиной 1024 бит.
- k. Измените настройку линий VTY transport input на настройку all только для протоколов SSH и Telnet.
- l. Назначьте IPv6-адрес для VLAN 1 в соответствии с таблицей адресации.
- m. От имени администратора отключите все неактивные интерфейсы.

Шаг 3: Настройте базовые параметры на всех маршрутизаторах.

- a. Отключите поиск DNS.
- b. Назначьте имя узла.
- c. Назначьте имя домена для **ccna-lab.com**.
- d. Зашифруйте все незашифрованные пароли.
- e. Создайте баннер MOTD, предупреждающий пользователей о том, что неавторизованный доступ запрещён.
- f. Создайте базу данных локального пользователя с именем пользователя **admin** и паролем **classadm**.

- g. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
- h. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.
- i. Активируйте возможность входа на линии VTY с помощью локальной базы данных.
- j. Создайте ключ шифрования RSA для SSH с длиной 1024 бит.
- k. Измените настройку линий VTY transport input на настройку all только для протоколов SSH и Telnet.

Шаг 4: Настройте IPv6-параметры на маршрутизаторе R1.

- a. Настройте индивидуальный IPv6-адрес на интерфейсах G0/0, G0/1 и S0/0/0.
- b. Настройте локальный IPv6-адрес канала на интерфейсах G0/0, G0/1 и S0/0/0. На всех трёх интерфейсах используйте **FE80:: 1** в качестве локального адреса канала.
- c. На интерфейсе S0/0/0 установите тактовую частоту 128000.
- d. Включите интерфейсы.
- e. Включите IPv6-маршрутизацию одноадресной передачи.
- f. Настройте маршрут IPv6 по умолчанию для использования интерфейса S0/0/0.

```
R1(config)# ipv6 route ::/0 s0/0/0
```

Шаг 5: Настройте параметры IPv6 на маршрутизаторе R2.

- a. Настройте индивидуальный IPv6-адрес на интерфейсах S0/0/0 и S0/0/1.
- b. Настройте локальный IPv6-адрес канала на интерфейсах S0/0/0 и S0/0/1. На обоих интерфейсах используйте **FE80:: 2** в качестве локального адреса канала.
- c. На интерфейсе S0/0/1 установите тактовую частоту со значением 128000.
- d. Включите интерфейсы.
- e. Включите IPv6-маршрутизацию одноадресной передачи.
- f. Настройте статические IPv6-маршруты для маршрутизации трафика на подсети LAN, подключенные к маршрутизаторам R1 и R3.

```
R2(config)# ipv6 route 2001:db8:acad::/48 s0/0/0
```

```
R2(config)# ipv6 route 2001:db8:cafe:c::/64 s0/0/1
```

Шаг 6: Настройте параметры IPv6 на маршрутизаторе R3.

- a. Настройте индивидуальный IPv6-адрес на интерфейсах G0/1 и S0/0/1.

- b. Настройте локальный IPv6-адрес канала на интерфейсах G0/1 и S0/0/1. На обоих интерфейсах используйте **FE80:: 1** в качестве локального адреса канала.
- c. Включите интерфейсы.
- d. Включите IPv6-маршрутизацию одноадресной передачи.
- e. Настройте маршрут IPv6 по умолчанию для использования интерфейса S0/0/1.

```
R3(config)# ipv6 route ::/0 s0/0/1
```

Шаг 7: Проверка соединения.

- a. Все компьютеры должны успешно выполнять эхо-запросы ко всем остальным компьютерам, указанным в топологии.
- b. Подключитесь по Telnet к маршрутизатору R1 со всех компьютеров в топологии.
- c. Подключитесь по SSH к маршрутизатору R1 со всех компьютеров в топологии.
- d. Подключитесь по Telnet к коммутатору S1 со всех компьютеров в топологии.
- e. Подключитесь по SSH к коммутатору S1 со всех компьютеров в топологии.
- f. Теперь выявите и устраните неполадки с подключением, поскольку ACL-списки, которые вы создадите в третьей части лабораторной работы, ограничат доступ к определённым областям сети.

Примечание. В соответствии с требованиями Tera Term IPv6-адрес назначения должен быть в скобках. Введите IPv6-адрес, как показано, нажмите **ОК**, а затем нажмите **Continue (Продолжить)**, чтобы принять предупреждение системы безопасности и подключиться к маршрутизатору.

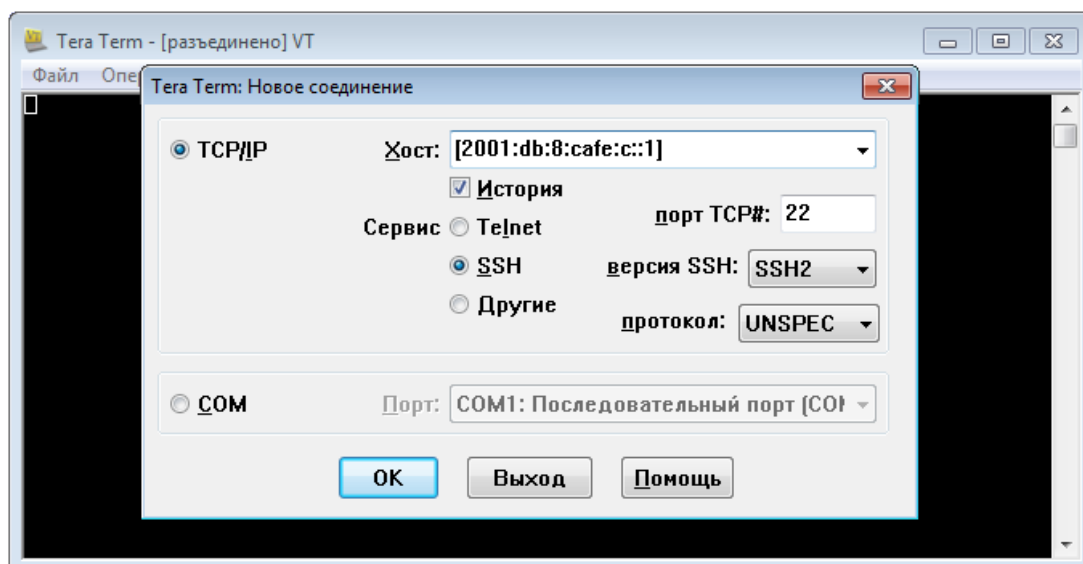


Рисунок 12 - Проверка соединения

Введите настроенные учётные данные пользователя (имя пользователя **admin**, пароль **classadm**) и в диалоговом окне SSH Authentication (Аутентификация SSH) выберите **Use plain password to log in** (Использовать незашифрованный пароль). Для продолжения нажмите кнопку **OK**.

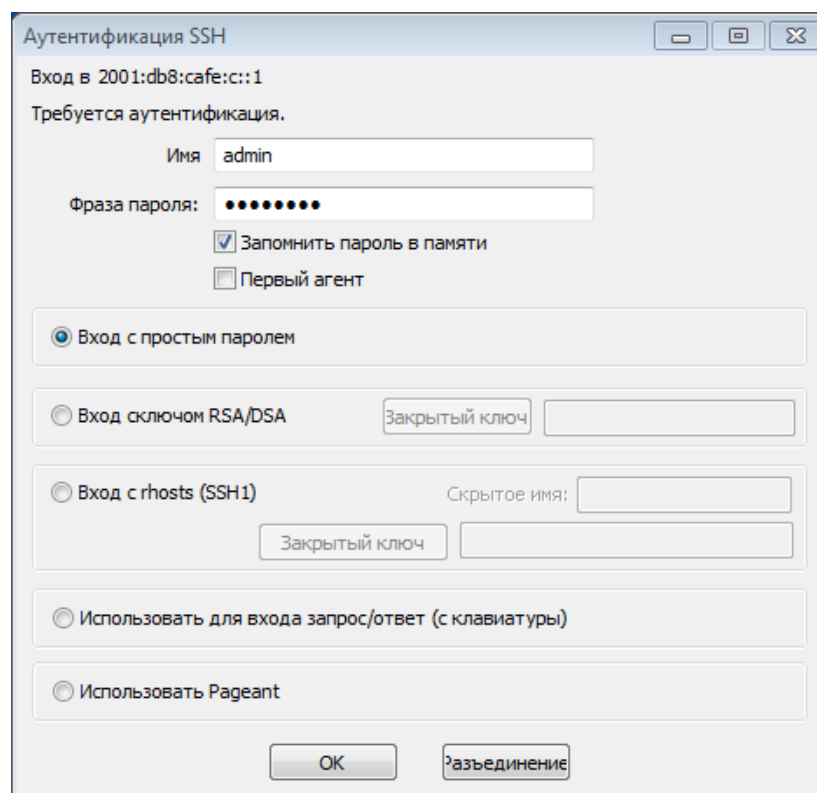


Рисунок 13 - Диалоговое окно «Аутентификация SSH»

9.6 Методические пояснения и рекомендации по выполнению третьего вопроса

Часть 7: Настройка и проверка ACL-списков для IPv6

Шаг 1: Настройте и проверьте ограничения VTY на маршрутизаторе R1.

- a. Создайте ACL-список, в соответствии с которым доступ к маршрутизатору R1 через Telnet разрешён только для узлов из сети 2001:db8:acad:a::/64. Все узлы должны обладать доступом к маршрутизатору R1 только через telnet.

```
R1(config)# ipv6 access-list RESTRICT-VTY
R1(config-ipv6-acl)# permit tcp 2001:db8:acad:a::/64 any
R1(config-ipv6-acl)# permit tcp any any eq 22
```

- b. Примените ACL-список под именем RESTRICT-VTY на линиях VTY маршрутизатора R1.

```
R1(config-ipv6-acl)# line vty 0 4
R1(config-line)# ipv6 access-class RESTRICT-VTY in
R1(config-line)# end
R1#
```

- c. Отобразите новый ACL-список.

```
R1# show access-lists
IPv6 access list RESTRICT-VTY
    permit tcp 2001:DB8:ACAD:A::/64 any sequence 10
    permit tcp any any eq 22 sequence 20
```

- d. Убедитесь, что ACL-список RESTRICT-VTY пропускает только Telnet-трафик из сети 2001:db8:acad:a::/64.

Каким образом ACL-список RESTRICT-VTY разрешает доступ к маршрутизатору R1 через Telnet только для узлов из сети 2001:db8:acad:a::/64?

Какую функцию выполняет второе правило permit в ACL-списке RESTRICT-VTY?

Шаг 2: Ограничьте доступ через Telnet к сети 2001:db8:acad:a::/64.

- a. Создайте ACL-список под именем RESTRICTED-LAN, который заблокирует доступ через Telnet к сети 2001:db8:acad:a::/64.

```
R1(config)# ipv6 access-list RESTRICTED-LAN
R1(config-ipv6-acl)# remark Block Telnet from outside
R1(config-ipv6-acl)# deny tcp any 2001:db8:acad:a::/64 eq telnet
R1(config-ipv6-acl)# permit ipv6 any any
```

- b. Примените ACL-список RESTRICTED-LAN на интерфейсе G0/1 для всего исходящего трафика.

```
R1(config-ipv6-acl)# int g0/1
R1(config-if)# ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

- c. Подключитесь по Telnet к коммутатору S1 от узлов PC-B и PC-C, чтобы проверить ограничение Telnet. Подключитесь по SSH к коммутатору S1 от узла PC-B, чтобы убедиться, что к этому узлу по-прежнему можно получить доступ через SSH. При необходимости выявите и устраните любые неполадки.

- d. Используйте команду **show ipv6 access-list**, чтобы просмотреть ACL-список RESTRICTED-LAN.

```
R1# show ipv6 access-lists RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet (6 matches) sequence 20
    permit ipv6 any any (45 matches) sequence 30
```

Обратите внимание, что каждое правило определяет количество попаданий или совпадений, возникших с момента применения ACL-списка на интерфейс.

- e. Используйте команду **clear ipv6 access-list**, чтобы сбросить счётчики совпадений для ACL-списка RESTRICTED-LAN.

```
R1# clear ipv6 access-list RESTRICTED-LAN
```

- f. Снова отобразите ACL-список с помощью команды **show access-lists**, чтобы убедиться, что счётчики удалены.

```
R1# show access-lists RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
    permit ipv6 any any sequence 30
```

9.7 Методические пояснения и рекомендации по выполнению четвёртого вопроса

Часть 8: Редактирование ACL-списков для IPv6

В четвёртой части вам предстоит внести изменения в ACL-список RESTRICTED-LAN, созданный в предыдущей части лабораторной работы. Перед внесением изменений в ACL-список рекомендуется удалить его из

интерфейса, на котором он применён. Завершив редактирование, снова примените ACL-список на интерфейсе.

Примечание. Многие сетевые администраторы делают копию ACL-списка и вносят изменения в копии. После изменения копии администратор удаляет старый ACL-список и применяет на интерфейсе отредактированный вариант. Благодаря этому ACL-список можно не удалять, пока отредактированная копия не будет готова для применения.

Шаг 1: Удалите ACL-список из интерфейса.

```
R1(config)# int g0/1
R1(config-if)# no ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

Шаг 2: Используйте команду `show access-lists`, чтобы просмотреть ACL-список.

```
R1# show access-lists
IPv6 access list RESTRICT-VTY
    permit tcp 2001:DB8:ACAD:A::/64 any (4 matches) sequence 10
    permit tcp any any eq 22 (6 matches) sequence 20
IPv6 access list RESTRICTED-LAN
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
    permit ipv6 any any (36 matches) sequence 30
```

Шаг 3: Создайте новую запись в ACL-списке, используя последовательную нумерацию.

```
R1(config)# ipv6 access-list RESTRICTED-LAN
R1(config-ipv6-acl)# permit tcp 2001:db8:acad:b::/64 host
2001:db8:acad:a::a eq 23 sequence 15
```

Какую функцию выполняет добавленная разрешающая запись `permit`?

—

Шаг 4: Создайте новое правило ACL, вставив его в конец списка.

```
R1(config-ipv6-acl)# permit tcp any host 2001:db8:acad:a::3 eq www
```

Примечание. Данная разрешающая запись используется только для того, чтобы продемонстрировать добавление записи в конец ACL-списка. Для данной строки списка не должно быть совпадений, поскольку предыдущая запись `permit` совпадает со всем.

Шаг 5: Используйте команду `show access-lists`, чтобы просмотреть изменения ACL-списка.

```
R1(config-ipv6-acl)# do show access-list
IPv6 access list RESTRICT-VTY
    permit tcp 2001:DB8:ACAD:A::/64 any (2 matches) sequence 10
    permit tcp any any eq 22 (6 matches) sequence 20
```

```
IPv6 access list RESTRICTED-LAN
  permit tcp 2001:DB8:ACAD:B::/64 host 2001:DB8:ACAD:A::A eq telnet sequence 15
  deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
  permit ipv6 any any (124 matches) sequence 30
  permit tcp any host 2001:DB8:ACAD:A::3 eq www sequence 40
```

Примечание. Для выполнения любой команды привилегированного режима в режиме глобальной конфигурации или подрежиме можно использовать команду **do**.

Шаг 6: Удалите запись ACL-списка.

Используйте команду **no**, чтобы удалить только что добавленное правило **permit**.

```
R1(config-ipv6-acl)# no permit tcp any host 2001:DB8:ACAD:A::3 eq www
```

Шаг 7: Используйте команду **do show access-lists RESTRICTED-LAN**, чтобы просмотреть ACL-список.

```
R1(config-ipv6-acl)# do show access-list RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
  permit tcp 2001:DB8:ACAD:B::/64 host 2001:DB8:ACAD:A::A eq telnet sequence 15
  deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
  permit ipv6 any any (214 matches) sequence 30
```

Шаг 8: Снова примените список ACL RESTRICTED-LAN на интерфейсе G0/1.

```
R1(config-ipv6-acl)# int g0/1
R1(config-if)# ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

Шаг 9: Проверьте изменения в ACL-списке.

От узла PC-B подключитесь к коммутатору S1 по Telnet. При необходимости выявите и устраните любые неполадки.

9.8 Вопросы на закрепление

1. Из-за чего счётчик совпадений для записи **permit ipv6 any any** списка RESTRICTED-LAN продолжает расти?

2. Какую команду следует использовать, чтобы сбросить счётчики для ACL-списка на каналах VTY?

Таблица 15. Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	Последовательный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.				

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1-2

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №4

Тема: Изучение программного обеспечения для мониторинга сети

1.Цель работы :

1. Изучение программного обеспечения для мониторинга сети.
2. Приобретение практических навыков настройки программного обеспечения для мониторинга сети.

Формируемые компетенции: ОПК-9, ОПК-10.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал, посвящённый настройке программному обеспечению для мониторинга сети.
2. Ознакомиться с программой работы.
3. Подготовить отчет о работе.
4. Ответить на контрольные вопросы.

3. Распределение времени занятия:

Всего: 4,5 часов

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 70 мин

1. Изучение программного обеспечения для мониторинга сети 70 мин
2. Проверка выполнения практического занятия 10 мин

Заключительная часть 3 мин

4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

4.1. Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

4.2. Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать

только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию;

- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;

- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

4.3. Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

6. Программное обеспечение

Программа эмуляции терминала Tera Term.

7. Основные теоретические сведения

См. рекомендованную к ознакомлению литературу по изучаемой дисциплине

8. Литература

1. James Boney, Cisco IOS in a Nutshell, O'Reilly, 2013
2. Wendell Odom, Interconnecting Networking Devices Cisco, Part 2, Cisco Press, 2013

9. Методические рекомендации по выполнению работы

9.1 Задачи

- 1. Проверка вашего понимания мониторинга сети**
- 2. Исследование средств мониторинга сети**
- 3. Выбор средства мониторинга сети**

9.2 Исходные данные/сценарий

Мониторинг необходим для сетей любого размера. Профилактическое наблюдение за сетевой инфраструктурой поможет администраторам сети выполнять ежедневные обязанности. Существуют различные средства мониторинга сети, которые отличаются по стоимости в зависимости от возможностей, количества сетей и поддерживаемых узлов.

В этой лабораторной работе будет исследоваться доступное ПО для наблюдения за сетью. Вашей задачей будет сбор информации о программных продуктах и функциях этих продуктов. Один продукт вы рассмотрите более подробно и перечислите некоторые из его основных функций.

9.3 Необходимые ресурсы:

- ПК с доступом к Интернету.

9.4 Методические пояснения и рекомендации по выполнению первого вопроса

Часть 9: Проверка знакомства с процессом наблюдения за сетью

Опишите, в чём, по вашему мнению, заключается процесс мониторинга сети. Приведите пример его использования в производственной сети.

Мониторинг сети осуществляется с помощью ПО (обычно средства или инструментария), которое помогает сетевым администраторам в поиске и устранении неполадок, наблюдении и изменении устройств в сети. Это программное средство может предоставлять следующие возможности: отчеты, графики производительности, учёт аппаратных средств, учёт программных средств, сопоставление топологий сети, создание уведомлений по электронной почте и/или текстовые сообщения для сетевого администратора. Администратор может настроить отправку уведомления по электронной почте, если потеря пакетов на маршрутизаторе превысит определенное предельное значение.

9.5 Методические пояснения и рекомендации по выполнению второго вопроса

Часть 10: Изучение средств мониторинга сети

Шаг 1: Проведите исследование и найдите три средства мониторинга сети.

Перечислите эти три найденных средства.

Возможны различные варианты ответов. В числе возможных примеров — Solar Winds, PRTG и Nagios.

Шаг 2: Заполните следующую форму для выбранных средств мониторинга сети.

Таблица 16. Сравнительные характеристики средств мониторинга сети

Поставщик	Название продукта	Функциональные возможности
Solar Winds: www.solarwinds.com	Network Performance Monitor	Наблюдение за производительностью, автоматизированное обнаружение сетевых устройств, оповещения о сетевых событиях, поддержка устройств различных производителей
Paessler: www.paessler.com	PRTG	Журналирование, контроль пропускной способности, перехват пакетов, поддержка NetFlow
Nagios: www.nagios.org	Nagios XI	Наблюдение за событиями в режиме реального времени, планирование производительности и пропускной способности, мастера настройки, пользовательские настройки уведомлений

9.6 Методические пояснения и рекомендации по выполнению третьего вопроса

Часть 11: Выберите средство мониторинга сети

Шаг 1: Выберите одно или несколько средств мониторинга из исследования.

Укажите одно или несколько средств из исследования, которые бы вы выбрали для мониторинга сети. Назовите эти средства и объясните свой выбор, перечислив конкретные функциональные возможности, которые по вашему мнению важны.

Возможны различные варианты ответов. Из-за огромного числа доступных продуктов очень важно выбрать правильный продукт. Пробные версии на 30 дней позволяют администратору оценить продукт перед покупкой. С каждым продуктом предоставляются материалы по обучению его использованию.

10. Содержание отчета о лабораторной работе

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1-2

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 5

Тема: Настройка syslog и ntp

1. Цель работы:

1. Настройка Syslog и NTP.
2. Приобретение практических навыков настройки Syslog и NTP.

Формируемые компетенции: ОПК-9, ОПК-10.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал, посвящённый настройке Syslog и NTP.
2. Ознакомиться с программой работы.
3. Подготовить отчет о работе.
4. Ответить на контрольные вопросы.

3. Распределение времени занятия:

Всего: 4,5 часов

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 70 мин

1. Настройка Syslog и NTP 70 мин
 2. Проверка выполнения практического занятия 10 мин
- Заключительная часть 3 мин

4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

4.1. Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

4.2. Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование,

соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию;

- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;

- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

4.3. Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

6. Программное обеспечение

Программа эмуляции терминала Tera Term.

7. Основные теоретические сведения

См. рекомендованную к ознакомлению литературу по изучаемой дисциплине

8. Литература

1. James Boney, Cisco IOS in a Nutshell, O'Reilly, 2013
2. Wendell Odom, Interconnecting Networking Devices Cisco, Part 2, Cisco Press, 2013

9. Методические рекомендации по выполнению работы

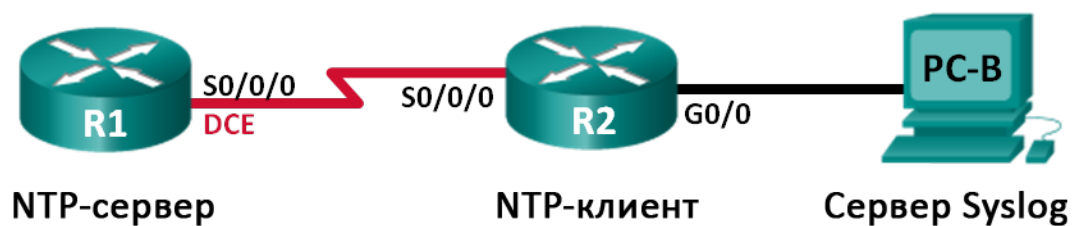


Рисунок 14 - Топология

Таблица 17. Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Недоступно
R2	S0/0/0	10.1.1.2	255.255.255.252	Недоступно
	G0/0	172.16.2.1	255.255.255.0	Недоступно
PC-B	NIC	172.16.2.3	255.255.255.0	172.16.2.1

9.1 Задачи

1. Базовая настройка устройств
2. Настройка NTP
3. Настройка Syslog

9.2 Исходные данные/сценарий

Сообщения Syslog, создаваемые сетевыми устройствами, могут собираться и архивироваться на сервере Syslog. Эту информацию можно использовать для наблюдения, отладки и поиска и устранения неполадок.

Администратор может настраивать место сохранения и отображения сообщений. Сообщения Syslog могут сопровождаться метками времени для анализа последовательности сетевых событий; поэтому важно синхронизировать часы всех сетевых устройств с помощью сервера NTP. В этой лабораторной работе необходимо настроить маршрутизатор R1 в качестве сервера NTP, а маршрутизатор R2 в качестве клиента Syslog и NTP. Приложение сервера Syslog, например Tftp32d или другая аналогичная программа, будет выполняться на ПК В. Кроме того, необходимо настроить уровень важности сообщений журнала, которые будут собираться и архивироваться на сервере Syslog.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). Возможно использование других маршрутизаторов и версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не содержат файла загрузочной конфигурации. Если вы не уверены в этом, обратитесь к инструктору.

9.3 Необходимые ресурсы:

- 2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 1 компьютер (с ОС Windows 7, Vista или XP или с программой эмуляции терминала, например Tera Term, и ПО Syslog, например tftpd32);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

9.4 Методические пояснения и рекомендации по выполнению первого вопроса

Часть 12: Базовая настройка устройств

В части 1 необходимо настроить топологию сети и базовые параметры, например IP-адреса интерфейсов, маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните запуск и перезагрузку маршрутизаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

- а. Отключите поиск DNS.
- б. Настройте имя устройства.
- в. Зашифруйте незашифрованные пароли.
- г. Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.

- e. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.
- f. Назначьте **cisco** в качестве пароля для консоли и виртуального терминала VTU и активируйте учётную запись.
- g. Настройте ведение журнала состояния консоли на синхронный режим.
- h. Примените IP-адреса к интерфейсам Serial и Gigabit Ethernet в соответствии с таблицей адресации и включите физические интерфейсы.
- i. Установите тактовую частоту **128000** для последовательного интерфейса DCE.

Шаг 4: Настройте маршрутизацию.

Включите на маршрутизаторах протокол OSPF с одной областью с идентификатором процесса 1. Добавьте все сети в процесс OSPF для области 0.

Шаг 5: Настройте ПК В.

Настройте IP-адрес и шлюз по умолчанию для ПК В согласно таблице адресации.

Шаг 6: Проверьте связь между конечными устройствами.

Убедитесь, что все устройства могут отправлять эхо-запросы на каждое другое устройство в сети. Если нет, устраните неполадки, чтобы установить связь между конечными устройствами.

Шаг 7: Сохраните текущую конфигурацию в загрузочную.

9.5 Методические пояснения и рекомендации по выполнению второго вопроса

Часть 13: Настройка NTP

В части 2 необходимо настроить маршрутизатор R1 в качестве сервера NTP, а маршрутизатор R2 в качестве клиента NTP маршрутизатора R1. Необходимо выполнить синхронизацию времени для Syslog и отладочных функций. Если время не синхронизировано, сложно определить, какое сетевое событие стало причиной данного сообщения.

Шаг 1: Выведите на экран текущее время.

Введите команду **show clock** для отображения текущего времени на R1.

```
R1# show clock
```

```
*12:30:06.147 UTC Tue May 14 2013
```

Запишите отображаемые сведения о текущем времени в следующей таблице.

Таблица 18. Текущее время маршрутизатора R1

Дата	Возможны различные варианты ответов. В данном примере: May 14, 2013
Время	Возможны различные варианты ответов. В данном примере: 12:30:06.147
Часовой пояс	Возможны различные варианты ответов. В данном примере: UTC

Шаг 2: Установите время.

С помощью команды **clock set** установите время на маршрутизаторе R1. Ниже приводится пример настройки даты и времени.

```
R1# clock set 9:39:00 05 july 2013
R1#
*Jul  5 09:39:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from
12:30:54 UTC Tue May 14 2013 to 09:39:00 UTC Fri Jul 5 2013, configured from
console by console.
```

Примечание. Время можно также настроить с помощью команды **clock timezone** в режиме глобальной конфигурации. Для получения дополнительной информации о команде **clock timezone** посетите веб-сайт www.cisco.com и определите часовой пояс для вашего региона.

Шаг 3: Настройте главный сервер NTP.

Настройте маршрутизатор R1 в качестве главного сервера NTP с помощью команды **ntp master stratum-number** в режиме глобальной конфигурации. Значение **stratum** показывает в каком количестве переходов NTP от доверенного источника времени находится сервер. В этой лабораторной работе в качестве **stratum** данного сервера NTP используется число 5.

```
R1(config)# ntp master 5
```

Шаг 4: Настройте клиент NTP.

- Введите команду **show clock** на маршрутизаторе R2. Запишите текущее время, отображаемое на маршрутизаторе R2, в следующей таблице.

Таблица 19. Текущее время маршрутизатора R2

Дата	Возможны различные варианты ответов.
Время	Возможны различные варианты ответов.
Часовой пояс	Возможны различные варианты ответов.

- Настройте R2 в качестве клиента NTP. Используйте команду **ntp server**, чтобы указать на IP-адрес или имя компьютера сервера NTP. Команда **ntp update-calendar** периодически обновляет календарь на основе времени NTP.

```
R2(config)# ntp server 10.1.1.1
R2(config)# ntp update-calendar
```

Шаг 5: Проверьте настройку NTP.

- a. Используйте команду **show ntp associations**, чтобы проверить, что маршрутизатор R2 связан через NTP с маршрутизатором R1.

```
R2# show ntp associations
```

address	ref clock	st	when	poll	reach	delay	offset	disp
*~10.1.1.1	127.127.1.1	5	11	64	177	11.312	-0.018	4.298

* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

- b. Введите команду **show clock** на маршрутизаторах R1 и R2 и сравните метку времени.

Примечание. Синхронизация метки времени на маршрутизаторе R2 с меткой времени на маршрутизаторе R1 может занять несколько минут.

```
R1# show clock
```

```
09:43:32.799 UTC Fri Jul 5 2013
```

```
R2# show clock
```

```
09:43:37.122 UTC Fri Jul 5 2013
```

9.6 Методические пояснения и рекомендации по выполнению третьего вопроса

Часть 14: Настройте Syslog

Сообщения Syslog от сетевых устройств могут собираться и архивироваться на сервере Syslog. В этой лабораторной работе в качестве программного обеспечения сервера Syslog используется Tftpd32.

Администратор может настраивать типы сообщений, которые можно отправлять на сервер Syslog.

Шаг 6: (Дополнительно) Установите сервер Syslog.

Если сервер Syslog еще не установлен на компьютере, загрузите и установите последнюю версию сервера Syslog, например Tftpd32.

Последнюю версию Tftpd32 можно найти по следующей ссылке:

<http://tftpd32.jounin.net/>

Шаг 7: Запустите сервер Syslog на компьютере ПК В.

После запуска приложения Tftpd32 перейдите на вкладку **Syslog server**.

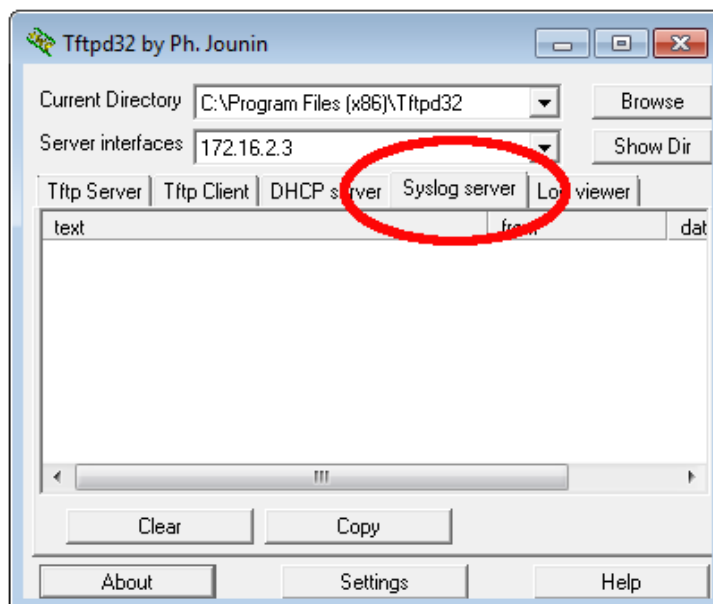


Рисунок 15 - Вкладка Syslog server

Шаг 8: Убедитесь, что на маршрутизаторе R2 включена служба меток времени.

С помощью команды **show run** проверьте, что служба меток времени включена для журналирования на маршрутизаторе R2.

```
R2# show run | include timestamp
service timestamps debug datetime msec
service timestamps log datetime msec
```

Если служба меток времени не включена, используйте следующую команду, чтобы включить её.

```
R2(config)# service timestamps log datetime msec
```

Шаг 9: Настройте R2 для сохранения сообщений журнала на сервере Syslog.

Настройте R2 для отправки сообщений Syslog на сервер Syslog — ПК В. IP-адрес сервера Syslog ПК В — 172.16.2.3.

```
R2(config)# logging host 172.16.2.3
```

Шаг 10: Выведите на экран параметры по умолчанию для журналирования.

Используйте команду **show logging**, чтобы вывести на экран параметры журналирования по умолчанию.

```
R2# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes,
0 overruns, xml disabled, filtering disabled)
```

```
No Active Message Discriminator.
```

```
No Inactive Message Discriminator.
```

```
Console logging: level debugging, 47 messages logged, xml disabled,
```

```
filtering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled,
filtering disabled
Buffer logging: level debugging, 47 messages logged, xml disabled,
filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
```

No active filter modules.

```
Trap logging: level informational, 49 message lines logged
Logging to 172.16.2.3 (udp port 514, audit disabled,
link up),
6 message lines logged,
0 message lines rate-limited,
0 message lines dropped-by-MD,
xml disabled, sequence number disabled
filtering disabled
Logging Source-Interface: VRF Name:
```

Назовите IP-адрес сервера Syslog.

Какие протокол и порт использует сервер Syslog?

Какой уровень сообщений настроен? _____

Шаг 11: Настройте и проверьте результат настройки уровней важности для журналирования на маршрутизаторе R2.

- а. Используйте команду **logging trap ?** для определения доступности различных уровней ловушек. При настройке уровня сообщений, отправляемые на сервер Syslog, будут включать сообщения настроенного уровня и сообщения более низких уровней.

```
R2(config)# logging trap ?
<0-7> Logging severity level
alerts Immediate action needed (severity=1)
critical Critical conditions (severity=2)
debugging Debugging messages (severity=7)
emergencies System is unusable (severity=0)
errors Error conditions (severity=3)
informational Informational messages (severity=6)
notifications Normal but significant conditions (severity=5)
warnings Warning conditions (severity=4)
<cr>
```

Если введена команда **logging trap warnings**, сообщения с какими уровнями важности будут регистрироваться?

предупреждения (уровень 4) ошибки (уровень 3), критические (уровень 2), тревоги (уровень 1) и чрезвычайные ситуации (уровень 0)

- b. Укажите уровень важности для журналирования равный 4.

```
R2(config)# logging trap warnings
```

или

```
R2(config)# logging trap 4
```

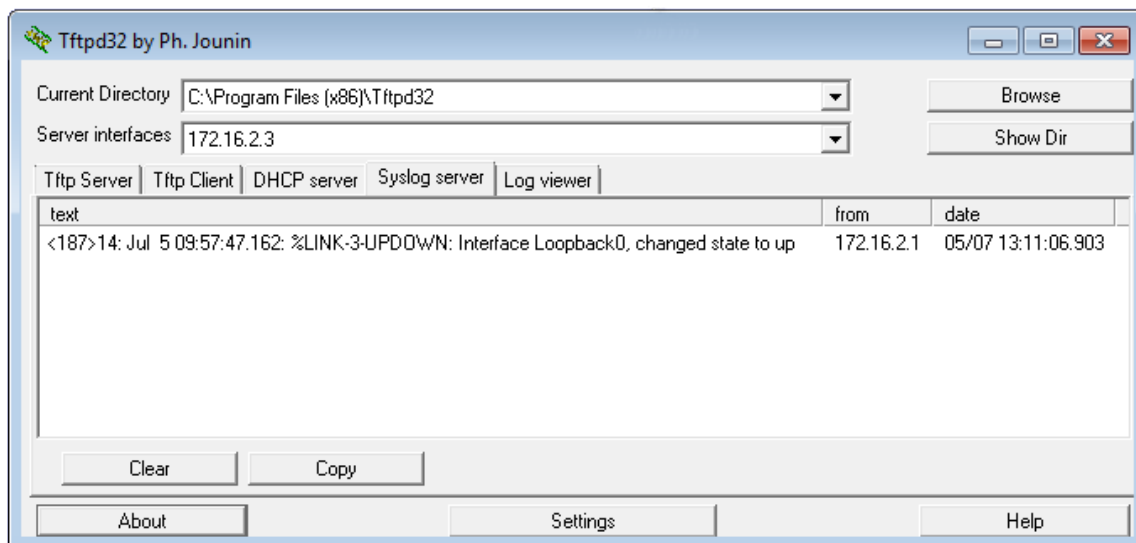
- c. Создайте интерфейс Loopback0 на маршрутизаторе R2 и просмотрите сообщения журнала как в окне терминала, так и в окне сервера Syslog на ПК В.

```
R2(config)# interface lo 0
```

```
R2(config-if)#
```

```
Jul  5 09:57:47.162: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
```

```
Jul  5 09:57:48.162: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
```



- d. Удалите интерфейс Loopback 0 на маршрутизаторе R2 и просмотрите сообщения журнала.

```
R2(config-if)# no interface lo 0
```

```
R2(config)#
```

```
Jul  5 10:02:58.910: %LINK-5-CHANGED: Interface Loopback0, changed state to administratively down
```

```
Jul  5 10:02:59.910: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to down
```

Отображаются ли какие-либо сообщения на сервере Syslog при выборе уровня серьёзности 4? Если какие-либо сообщения журнала отображаются, объясните, какие сообщения отображаются и почему.

Отобразилось сообщение журнала с общим предупреждением об изменении состояния интерфейса. Добавления интерфейса недостаточно для вызова и отправки более подробных информационных сообщений на сервер Syslog при выборе уровня 4.

- е. Укажите уровень важности для журналирования равный 6.

```
R2(config)# logging trap informational
```

или

```
R2(config)# logging trap 6
```

- ф. Удалите записи Syslog на ПК В. Нажмите кнопку **Clear** (Очистить) в диалоговом окне Tftpd32.

- г. Создайте интерфейс Loopback 1 на маршрутизаторе R2.

```
R2(config)# interface lo 1
```

```
Jul  5 10:05:46.650: %LINK-3-UPDOWN: Interface Loopback1, changed state to up
```

```
Jul  5 10:05:47.650: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
```

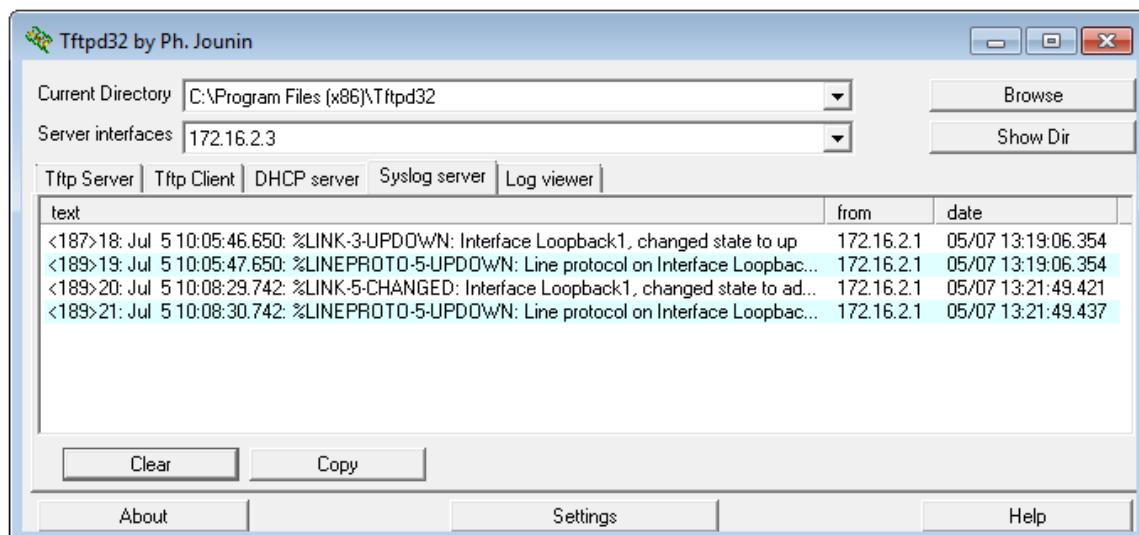
- h. Удалите интерфейс Loopback 1 с маршрутизатора R2.

```
R2(config-if)# no interface lo 1
```

```
R2(config-if)#
```

```
Jul  5 10:08:29.742: %LINK-5-CHANGED: Interface Loopback1, changed state to administratively down
```

```
Jul  5 10:08:30.742: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to down
```



- i. Проанализируйте выходные данные сервера Syslog. Сравните эти результаты с результатами на уровне важности 4. Каковы ваши наблюдения?

При настройке уровня важности 6 (информационный) создаётся больше сообщений, чем при настройке уровня 4 (предупреждения).

9.7 Вопросы на закрепление

Какая проблема возникает при настройке слишком высокого (самый маленький номер) или слишком низкого (самый большой номер) уровня важности для Syslog?

Если настроен слишком высокий уровень важности (самый маленький номер), в журнале могут отсутствовать важные, но не критичные сообщения. Однако при выборе слишком низкого (самый большой номер) уровня важности может создаваться слишком много записей, переполняющих журнал ненужной информацией.

Таблица 20. Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet № 2	Последовательный интерфейс № 1	Последовательный интерфейс № 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

9.8 Настройки устройств

Маршрутизатор R1

```
R1#show run
Building configuration...

Current configuration : 1572 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
!
!
!
```

```
!  
no ip domain lookup  
no ipv6 cef  
!  
multilink bundle-name authenticated  
!  
!  
!  
!  
!  
!  
redundancy  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
interface Embedded-Service-Engine0/0  
no ip address  
shutdown  
!  
interface GigabitEthernet0/0  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/1  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface Serial0/0/0  
ip address 10.1.1.1 255.255.255.252  
clock rate 128000  
!  
interface Serial0/0/1  
no ip address  
shutdown  
!  
router ospf 1  
network 10.1.1.0 0.0.0.3 area 0  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
!  
!  
!  
control-plane  
!
```

```

!
banner motd ^CUnauthorized access is prohibited.^C
!
line con 0
  password 7 110A1016141D
  logging synchronous
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password 7 01100F175804
  login
  transport input all
!
scheduler allocate 20000 1000
ntp master 5
!
end

```

Маршрутизатор R2

Building configuration...

```

Current configuration : 1742 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
!
!
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
redundancy
!

```

```
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
interface Embedded-Service-Engine0/0  
  no ip address  
  shutdown  
!  
interface GigabitEthernet0/0  
  ip address 172.16.2.1 255.255.255.0  
  duplex auto  
  speed auto  
!  
interface GigabitEthernet0/1  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
!  
interface Serial0/0/0  
  ip address 10.1.1.2 255.255.255.252  
!  
interface Serial0/0/1  
  no ip address  
  shutdown  
  clock rate 2000000  
!  
router ospf 1  
  network 10.1.1.0 0.0.0.3 area 0  
  network 172.16.2.0 0.0.0.3 area 0  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
!  
logging host 172.16.2.3  
!  
!  
!  
control-plane  
!  
!  
banner motd ^CUnauthorized access is prohibited.^C  
!  
line con 0  
  password 7 121A0C041104  
  logging synchronous  
  login  
line aux 0  
line 2  
  no activation-character  
  no exec  
  transport preferred none  
  transport input all  
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
```

```
stopbits 1
line vty 0 4
password 7 01100F175804
login
transport input all
!
scheduler allocate 20000 1000
ntp update-calendar
ntp server 10.1.1.1
!
end
```

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1-2

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №6

Тема: Отладка базового PPP с аутентификацией

1. Цель работы:

1. Отладка базового PPP с аутентификацией.
2. Приобретение практических навыков настройки ASA5505.

Формируемые компетенции: ОПК-9, ОПК-10.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал, посвящённый отладке базового PPP с аутентификацией.
2. Ознакомиться с программой работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

3. Распределение времени занятия:

Всего: 4,5 часов

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 70 мин

1. Отладка базового PPP с аутентификацией 70 мин
2. Проверка выполнения практического занятия 10 мин

Заключительная часть 3 мин

4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

4.1. Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

4.2. Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование,

соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию;

- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;

- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

4.3. Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

6. Программное обеспечение

Программа эмуляции терминала Tera Term.

7. Основные теоретические сведения

См. рекомендованную к ознакомлению литературу по изучаемой дисциплине

8. Литература

1. James Boney, Cisco IOS in a Nutshell, O'Reilly, 2013
2. Wendell Odom, Interconnecting Networking Devices Cisco, Part 2, Cisco Press, 2013

9. Методические рекомендации по выполнению работы

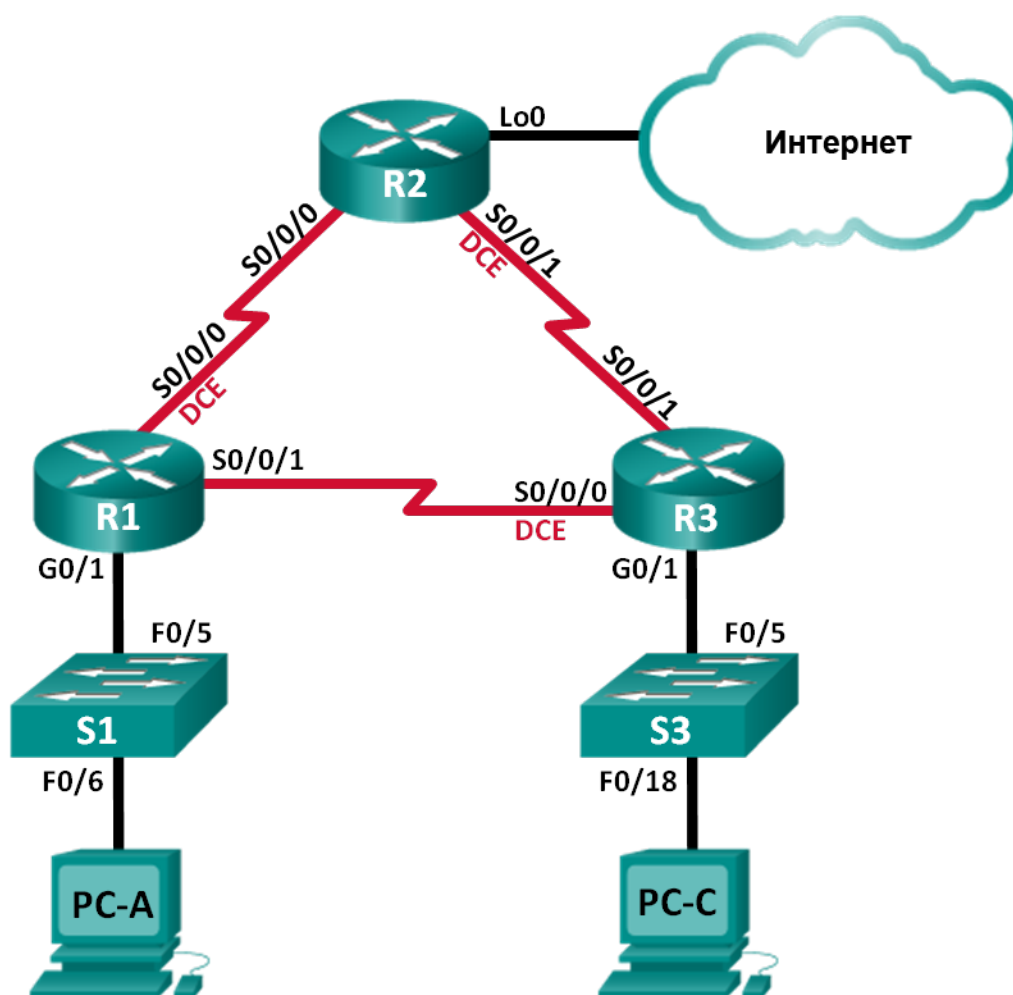


Рисунок 16 - Топология

Таблица 21. Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252	Недоступно
	S0/0/1	192.168.13.1	255.255.255.252	Недоступно
R2	Lo0	209.165.200.225	255.255.255.252	Недоступно
	S0/0/0	192.168.12.2	255.255.255.252	Недоступно
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	Недоступно
R3	G0/1	192.168.3.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	Недоступно
	S0/0/1	192.168.23.2	255.255.255.252	Недоступно
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

9.1 Задачи

1. Построение сети и загрузка настроек устройств
2. Поиск и устранение неполадок канального уровня
3. Поиск и устранение неполадок сетевого уровня

9.2 Исходные данные/сценарий

Маршрутизаторы в сети вашей компании были настроены неопытным сетевым инженером. В результате нескольких ошибок в настройках возникли проблемы со связью. Начальник попросил вас найти и устранить неполадки в настройке и задокументировать работу. Найдите и исправьте ошибки, используя свои знания PPP и стандартные методы тестирования. Убедитесь, что на всех последовательных каналах используется аутентификация CHAP PPP и что все сети доступны.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы Cisco Catalyst серии 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от

данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены и они не имеют загрузочных настроек. Если вы не уверены в этом, обратитесь к инструктору.

9.3 Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);
- 2 ПК (Windows 7, Vista и XP с программой эмуляции терминала, например, Tera Term)
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

9.4 Методические пояснения и рекомендации по выполнению первого вопроса

Часть 15: Построение сети и загрузка настроек устройств

В части 1 вам предстоит создать топологию сети, настроить базовые параметры для узлов ПК и загрузить настройки маршрутизаторов.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Настройте узлы ПК.

Шаг 3: Загрузите настройки маршрутизатора.

Загрузите в соответствующий маршрутизатор следующие настройки. На всех маршрутизаторах настроены одинаковые пароли. Пароль привилегированного режима — **class**. Пароль для консоли и доступа vty — **cisco**. Все последовательные интерфейсы должны быть настроены с инкапсуляцией PPP и аутентификацией по протоколу CHAP с паролем **chap123**.

Настройка маршрутизатора R1:

```
hostname R1
enable secret class
no ip domain lookup
banner motd #Unauthorized Access is Prohibited!#
```

```

username R2 password chap123
username R3 password chap123
interface g0/1
    ip address 192.168.1.1 255.255.255.0
    no shutdown
interface s0/0/0
    ip address 192.168.12.1 255.255.255.252
    clock rate 128000
    encapsulation ppp
    ppp authentication chap
! no shutdown
interface s0/0/1
    ip address 192.168.31.1 255.255.255.252
! ip address 192.168.13.1 255.255.255.252
    encapsulation ppp
    ppp authentication pap
! ppp authentication chap
! no shutdown
exit
router ospf 1
    router-id 1.1.1.1
    network 192.168.1.0 0.0.0.255 area 0
    network 192.168.12.0 0.0.0.3 area 0
    network 192.168.13.0 0.0.0.3 area 0
    passive-interface g0/1
    exit
line con 0
    password cisco
    logging synchronous
    login
line vty 0 4
    password cisco
    login

```

Настройка маршрутизатора R2:

```

hostname R2
enable secret class
no ip domain lookup
banner motd #Unauthorized Access is Prohibited!#
username R1 password chap123
username r3 password chap123
! username R3 password chap123
! no username r3 password chap123
interface lo0
    ip address 209.165.200.225 255.255.255.252
interface s0/0/0
    ip address 192.168.12.2 255.255.255.252
    encapsulation ppp
    ppp authentication chap
    no shutdown
interface s0/0/1

```

```

ip address 192.168.23.1 255.255.255.252
clock rate 128000
! encapsulation ppp
! ppp authentication chap
no shutdown
exit
router ospf 1
router-id 2.2.2.2
network 192.168.12.0 0.0.0.3 area 0
network 192.168.23.0 0.0.0.3 area 0
default-information originate
exit
ip route 0.0.0.0 0.0.0.0 loopback0
line con 0
password cisco
logging synchronous
login
line vty 0 4
password cisco
login

```

Настройка маршрутизатора R3:

```

hostname R3
enable secret class
no ip domain lookup
banner motd #Unauthorized Access is Prohibited!#
username R2 password chap123
username R3 password chap123
!no username R3 password chap123
!username R1 password chap123
interface g0/1
ip address 192.168.3.1 255.255.255.0
no shutdown
interface s0/0/0
ip address 192.168.13.2 255.255.255.252
clock rate 128000
encapsulation ppp
ppp authentication chap
no shutdown
interface s0/0/1
ip address 192.168.23.2 255.255.255.252
encapsulation ppp
ppp authentication chap
no shutdown
exit
router ospf 1
router-id 3.3.3.3
! network 192.168.3.0 0.0.0.255 area 0
network 192.168.13.0 0.0.0.3 area 0
network 192.168.23.0 0.0.0.3 area 0
passive-interface g0/1

```

```

line con 0
password cisco
logging synchronous
login
line vty 0 4
password cisco
login

```

Шаг 4: Сохраните текущую конфигурацию.

9.5 Методические пояснения и рекомендации по выполнению второго вопроса

Часть 16: Поиск и устранение неполадок канального уровня

В части 2 следует использовать команды **show** для устранения неполадок канального уровня. Не забудьте проверить такие параметры, как тактовая частота, инкапсуляция, СНАР и имена и пароли пользователей.

Шаг 1: Изучите настройку маршрутизатора R1.

- а. Используйте команду **show interfaces**, чтобы определить, установлен ли PPP на обоих последовательных каналах.

```

R1# show interfaces s0/0/0
Serial0/0/0 is administratively down, line protocol is down
  Hardware is GT96K Serial
  Internet address is 192.168.12.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Closed, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:04:41
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations  0/0/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
  DCD=down DSR=down DTR=up  RTS=down  CTS=down

```

```

R1# show interfaces s0/0/1
Serial0/0/1 is administratively down, line protocol is down

```

```

Hardware is GT96K Serial
Internet address is 192.168.31.1/30
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Closed, loopback not set
Keepalive set (10 sec)
Last input never, output never, output hang never
Last clearing of "show interface" counters 00:09:10
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/0/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 1158 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
    DCD=down DSR=up DTR=down RTS=down CTS=down

```

Основываясь на результатах работы команды **show interfaces** для S0/0/0 и S0/0/1, укажите возможные неполадки в каналах PPP.

Выходные данные команды говорят о том, что оба интерфейса, S0/0/0 и S0/0/1, отключены. Инкапсуляция PPP была применена к обоим интерфейсам: S0/0/0 и S0/0/1. Помимо того факта, что последовательный интерфейс отключен администратором, сохраняются проблемы, связанные с настройками PPP, например несоответствующая аутентификация.

- b. В процессе поиска и устранения неполадок используйте команду **debug ppp authentication** для просмотра результатов аутентификации PPP в реальном времени.

```

R1# debug ppp authentication
PPP authentication debugging is on

```

- c. Для исследования настроек на S0/0/0 используйте команду **show run interface s0/0/0**.

```

R1# show run interface s0/0/0

```

Building configuration...

Current configuration : 143 bytes

```
!  
interface Serial0/0/0  
 ip address 192.168.12.1 255.255.255.252  
 encapsulation ppp  
 shutdown  
 ppp authentication chap  
 clock rate 128000  
end
```

Устраните все неполадки, связанные с S0/0/0. Запишите команды, использованные для исправления настройки.

```
R1(config)# interface s0/0/0  
R1(config-if)# no shutdown
```

Укажите выходные данные команды debug, выполненной после устранения неполадки.

```
R1(config-if)# no shutdown  
*Jun 18 12:01:23.931: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up  
*Jun 18 12:01:23.931: Se0/0/0 PPP: Using default call direction  
*Jun 18 12:01:23.931: Se0/0/0 PPP: Treating connection as a dedicated line  
*Jun 18 12:01:23.931: Se0/0/0 PPP: Session handle[F900005A] Session id[90]  
*Jun 18 12:01:23.943: Se0/0/0 CHAP: O CHALLENGE id 1 len 23 from "R1"  
*Jun 18 12:01:23.947: Se0/0/0 CHAP: I CHALLENGE id 1 len 23 from "R2"  
*Jun 18 12:01:23.947: Se0/0/0 PPP: Sent CHAP SENDAUTH Request  
*Jun 18 12:01:23.947: Se0/0/0 PPP: Received SENDAUTH Response PASS  
*Jun 18 12:01:23.947: Se0/0/0 CHAP: Using hostname from configured hostname  
*Jun 18 12:01:23.947: Se0/0/0 CHAP: Using password from AAA  
*Jun 18 12:01:23.947: Se0/0/0 CHAP: O RESPONSE id 1 len 23 from "R1"  
*Jun 18 12:01:23.947: Se0/0/0 CHAP: I RESPONSE id 1 len 23 from "R2"  
*Jun 18 12:01:23.951: Se0/0/0 PPP: Sent CHAP LOGIN Request  
*Jun 18 12:01:23.951: Se0/0/0 PPP: Received LOGIN Response PASS  
*Jun 18 12:01:23.951: Se0/0/0 CHAP: O SUCCESS id 1 len 4  
*Jun 18 12:01:23.951: Se0/0/0 CHAP: I SUCCESS id 1 len 4
```

Выходные данные команды debug показывают, что процесс согласования CHAP выполнен успешно. PPP настроен на канале, соединяющем R1 S0/0/0 и R2 S0/0/0.

- d. Для исследования параметров на S0/0/1 используйте команду **show run interface s0/0/1** .

```
R1# show run interface s0/0/1  
Building configuration...
```

Current configuration : 123 bytes

```
!  
interface Serial0/0/1  
  ip address 192.168.31.1 255.255.255.252  
  encapsulation ppp  
  shutdown  
  ppp authentication pap  
end
```

Устраните все неполадки, связанные с S0/0/1. Запишите команды, использованные для исправления настройки.

```
R1(config)# interface s0/0/1  
R1(config-if)# ppp authentication chap  
R1(config-if)# no shutdown
```

Укажите выходные данные команды debug, выполненной после устранения неполадки.

```
*Jun 18 12:13:57.819: %LINK-3-UPDOWN: Interface Serial0/0/1, changed state to up  
*Jun 18 12:13:57.819: Se0/0/1 PPP: Using default call direction  
*Jun 18 12:13:57.819: Se0/0/1 PPP: Treating connection as a dedicated line  
*Jun 18 12:13:57.819: Se0/0/1 PPP: Session handle[F300005B] Session id[91]  
*Jun 18 12:13:57.831: Se0/0/1 CHAP: O CHALLENGE id 1 len 23 from "R1"  
*Jun 18 12:13:57.831: Se0/0/1 CHAP: I CHALLENGE id 1 len 23 from "R3"  
*Jun 18 12:13:57.831: Se0/0/1 PPP: Sent CHAP SENDAUTH Request  
*Jun 18 12:13:57.831: Se0/0/1 PPP: Received SENDAUTH Response PASS  
*Jun 18 12:13:57.831: Se0/0/1 CHAP: Using hostname from configured hostname  
*Jun 18 12:13:57.831: Se0/0/1 CHAP: Using password from AAA  
*Jun 18 12:13:57.831: Se0/0/1 CHAP: O RESPONSE id 1 len 23 from "R1"  
*Jun 18 12:14:01.819: Se0/0/1 PPP: Using default call direction  
*Jun 18 12:14:01.819: Se0/0/1 PPP: Treating connection as a dedicated line  
*Jun 18 12:14:01.819: Se0/0/1 PPP: Session handle[BC00005C] Session id[92]  
*Jun 18 12:14:01.831: Se0/0/1 CHAP: O CHALLENGE id 1 len 23 from "R1"  
*Jun 18 12:14:01.851: Se0/0/1 CHAP: I CHALLENGE id 1 len 23 from "R3"  
*Jun 18 12:14:01.851: Se0/0/1 PPP: Sent CHAP SENDAUTH Request  
*Jun 18 12:14:01.851: Se0/0/1 PPP: Sending AAA radius abort  
R1(config-if)#  
*Jun 18 12:14:04.860: %LINEPROTO-5-UPDOWN: Line protocol on Interface  
Serial0/0/1, changed state to up  
*Jun 18 12:14:04.868: %LINEPROTO-5-UPDOWN: Line protocol on Interface  
Serial0/0/1, changed state to down  
*Jun 18 12:14:06.856: Se0/0/1 PPP: Using default call direction
```

Выходные данные команды debug показывают, что согласование CHAP не выполнено, и интерфейс включается и выключается. Имеются дополнительные ошибки настройки канала, соединяющего R1 S0/0/1 и R3 S0/0/0.

- e. Для отключения вывода данных команды debug PPP используйте команду **no debug ppp authentication** или **undebug all**.
- f. Для проверки правильности настроек имени и пароля пользователя используйте команду **show running-config | include username**.

```
R1# show running-config | include username
username R2 password 0 chap123
username R3 password 0 chap123
```

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления настройки.

Шаг 2: Исследуйте настройку маршрутизатора R2.

- g. Используйте команду **show interfaces**, чтобы определить, установлен ли PPP на обоих последовательных каналах.

```
R2# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 192.168.12.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:06, output 00:00:01, output hang never
  Last clearing of "show interface" counters 00:18:22
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations  0/1/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    53 packets input, 3055 bytes, 0 no buffer
    Received 0 broadcasts, 0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    52 packets output, 2772 bytes, 0 underruns
    0 output errors, 0 collisions, 34 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
    1 carrier transitions
```

DCD=up DSR=up DTR=up RTS=up CTS=up

R2# **show interfaces s0/0/1**

```
Serial0/0/1 is up, line protocol is down
  Hardware is GT96K Serial
  Internet address is 192.168.23.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:11, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/1/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    230 packets input, 4370 bytes, 0 no buffer
    Received 230 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    119 packets output, 3014 bytes, 0 underruns
    0 output errors, 0 collisions, 42 interface resets
    230 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
    121 carrier transitions
  DCD=up DSR=up DTR=up RTS=up CTS=up
```

Все ли каналы установлены? _____

Если ответ отрицательный, то какие каналы следует проверить? В чем заключаются возможные причины неполадок?

- h. Для исследования связей, которые не были установлены, используйте команду **show run interface**.

R2# **show run interface s0/0/1**

Building configuration...

```
Current configuration : 89 bytes
!
interface Serial0/0/1
  ip address 192.168.23.1 255.255.255.252
  clock rate 128000
end
```

Устраните все обнаруженные неполадки, относящиеся к интерфейсам.
Запишите команды, использованные для исправления настройки.

-
-
- i. Для проверки правильности настроек имени и пароля пользователя используйте команду **show running-config | include username** .

```
R2# show running-config | include username
username R1 password 0 chap123
username r3 password 0 chap123
```

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления настройки.

-
- j. Используйте команду **show ppp interface serial** для того последовательного интерфейса, который вы отлаживаете.

```
R2# show interfaces s0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 192.168.23.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:07, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:25:09
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/1/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    506 packets input, 27348 bytes, 0 no buffer
    Received 0 broadcasts, 0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    507 packets output, 28030 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
  DCD=up DSR=up DTR=up RTS=up CTS=up
```

Связь установлена? _____

Шаг 3: Исследуйте настройку маршрутизатора R3.

- к. Используйте команду **show interfaces**, чтобы определить, установлен ли PPP на обоих последовательных каналах.

R3# **show interfaces s0/0/0**

```
Serial0/0/0 is up, line protocol is down
  Hardware is GT96K Serial
  Internet address is 192.168.13.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Closed, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:01, output 00:00:01, output hang never
  Last clearing of "show interface" counters 00:55:56
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/1/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 3 packets/sec
  5 minute output rate 0 bits/sec, 2 packets/sec
    3540 packets input, 70800 bytes, 0 no buffer
    Received 0 broadcasts, 0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    3274 packets output, 60079 bytes, 0 underruns
    0 output errors, 0 collisions, 821 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
    1573 carrier transitions
  DCD=up DSR=up DTR=up RTS=up CTS=up
```

R3# **show interfaces s0/0/1**

```
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 192.168.23.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:07, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:51:19
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/1/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
```

```
5 minute output rate 0 bits/sec, 0 packets/sec
  711 packets input, 35022 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 847 packets output, 36444 bytes, 0 underruns
  0 output errors, 0 collisions, 73 interface resets
 141 unknown protocol drops
  0 output buffer failures, 0 output buffers swapped out
 96 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

Все ли каналы установлены? _____

Если ответ отрицательный, то какие каналы следует проверить? В чем заключаются возможные причины неполадок?

1. Для исследования всех последовательных связей, которые не были установлены, используйте команду **show run interface**.

```
R3# show run interface s0/0/0
Building configuration...

Current configuration : 134 bytes
!
interface Serial0/0/0
 ip address 192.168.13.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 clock rate 2000000
end
```

Устраните все неполадки, обнаруженные на интерфейсах. Запишите команды, использованные для исправления настройки.

- m. Для проверки правильности настроек имени и пароля пользователя используйте команду **show running-config | include username**.

```
R3# show run | include username
username R2 password 0 chap123
username R3 password 0 chap123
```

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления настройки.

- n. Используйте команду **show**, чтобы убедиться, что последовательные связи установлены.

```

R3# show interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 192.168.13.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:20, output 00:00:03, output hang never
  Last clearing of "show interface" counters 01:03:35
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/1/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    4392 packets input, 88310 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    3974 packets output, 74268 bytes, 0 underruns
    0 output errors, 0 collisions, 994 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
    1919 carrier transitions
    DCD=up DSR=up DTR=up RTS=up CTS=up

```

- о. Связь по протоколу PPP установлена во всех каналах? _____
- р. Эхо-запрос от узла ПК А к Lo0 выполняется успешно? _____
- q. Успешно ли выполняется эхо-запрос от узла ПК А на узел ПК С? _____

Примечание. Для успешной передачи эхо-запросов между компьютерами может потребоваться отключение межсетевого экрана.

9.6 Методические пояснения и рекомендации по выполнению третьего вопроса

Часть 17: Поиск и устранение неполадок сетевого уровня

В части 3 вам предстоит убедиться, что подключения уровня 3 установлены на всех интерфейсах, исследуя для этого настройки IPv4 и OSPF.

Шаг 4: Убедитесь, что интерфейсы, указанные в таблице адресации, активны и настроены с правильными IP-адресами.

Выполните команду **show ip interface brief** на всех маршрутизаторах, чтобы убедиться, что все интерфейсы находятся в рабочем состоянии (up/up).

```
R1# show ip interface brief
```

Interface Protocol	IP-Address	OK?	Method	Status
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down down
GigabitEthernet0/0	unassigned	YES	unset	administratively down down
GigabitEthernet0/1	192.168.1.1	YES	manual	up up
Serial0/0/0	192.168.12.1	YES	manual	up up
Serial0/0/1	192.168.31.1	YES	manual	up up

R2# **show ip interface brief**

Interface Protocol	IP-Address	OK?	Method	Status
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down down
GigabitEthernet0/0	unassigned	YES	unset	administratively down down
GigabitEthernet0/1	unassigned	YES	unset	administratively down down
Serial0/0/0	192.168.12.2	YES	manual	up up
Serial0/0/1	192.168.23.1	YES	manual	up up
Loopback0	209.165.200.225	YES	manual	up up

R3# **show ip interface brief**

Interface Protocol	IP-Address	OK?	Method	Status
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down down
GigabitEthernet0/0	unassigned	YES	unset	administratively down down
GigabitEthernet0/1	192.168.3.1	YES	manual	up up
Serial0/0/0	192.168.13.2	YES	manual	up up
Serial0/0/1	192.168.23.2	YES	manual	up up

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления настройки.

Шаг 5: Проверка маршрутизации OSPF

Введите команду **show ip protocols**, чтобы убедиться, что OSPF запущен и что все сети объявляются.

R1# **show ip protocols**

*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 1.1.1.1

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

192.168.1.0 0.0.0.255 area 0

192.168.12.0 0.0.0.3 area 0

192.168.13.0 0.0.0.3 area 0

Passive Interface(s):

GigabitEthernet0/1

Routing Information Sources:

Gateway	Distance	Last Update
---------	----------	-------------

3.3.3.3	110	00:01:46
---------	-----	----------

2.2.2.2	110	00:01:46
---------	-----	----------

Distance: (default is 110)

R2# **show ip protocols**

*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 2.2.2.2

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

192.168.12.0 0.0.0.3 area 0

192.168.23.0 0.0.0.3 area 0

209.165.200.224 0.0.0.3 area 0

Routing Information Sources:

Gateway	Distance	Last Update
---------	----------	-------------

3.3.3.3	110	00:03:53
---------	-----	----------

1.1.1.1	110	00:07:45
---------	-----	----------

Distance: (default is 110)

R3# **show ip protocols**

*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 3.3.3.3

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

192.168.13.0 0.0.0.3 area 0

192.168.23.0 0.0.0.3 area 0

Passive Interface(s):

GigabitEthernet0/1

Routing Information Sources:

Gateway	Distance	Last Update
---------	----------	-------------

1.1.1.1	110	00:07:14
---------	-----	----------

2.2.2.2	110	00:07:14
---------	-----	----------

Distance: (default is 110)

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления настройки.

___ Успешно ли выполняется эхо-запрос от узла ПК А на узел ПК С?

Если между некоторыми узлами нет связи, продолжите поиск и устранение неполадок, чтобы устранить все имеющиеся неполадки.

Примечание. Для успешной передачи эхо-запросов между компьютерами может потребоваться отключение межсетевого экрана.

Таблица 22. Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet № 2	Последовательный интерфейс № 1	Последовательный интерфейс № 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

9.7 Настройки устройств — итоговые

Маршрутизатор R1

```

R1#show run
Building configuration...

Current configuration : 1821 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
!
username R2 password 0 chap123

```

```
username R3 password 0 chap123
!
interface Embedded-Service-Engine0/0
  no ip address
  shutdown
!
interface GigabitEthernet0/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  ip address 192.168.1.1 255.255.255.0
  duplex auto
  speed auto
!
interface Serial0/0/0
  ip address 192.168.12.1 255.255.255.252
  encapsulation ppp
  ppp authentication chap
  clock rate 128000
!
interface Serial0/0/1
  ip address 192.168.13.1 255.255.255.252
  encapsulation ppp
  ppp authentication chap
!
router ospf 1
  router-id 1.1.1.1
  passive-interface GigabitEthernet0/1
  network 192.168.1.0 0.0.0.255 area 0
  network 192.168.12.0 0.0.0.3 area 0
  network 192.168.13.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^CUnauthorized Access is Prohibited!^C
!
line con 0
  password cisco
  logging synchronous
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password cisco
  login
  transport input all
!
scheduler allocate 20000 1000
!
end
```

Маршрутизатор R2

```
R2#show run
Building configuration...

Current configuration : 1866 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
!
username R1 password 0 chap123
username R3 password 0 chap123
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.252
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.12.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
interface Serial0/0/1
 ip address 192.168.23.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 clock rate 128000
!
router ospf 1
 router-id 2.2.2.2
 network 192.168.12.0 0.0.0.3 area 0
```

```

network 192.168.23.0 0.0.0.3 area 0
default-information originate
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 Loopback0
!
control-plane
!
banner motd ^CUnauthorized Access is Prohibited!^C
!
line con 0
password cisco
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end

```

Маршрутизатор R3

```

R3#show run
Building configuration...

```

```

Current configuration : 1888 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
username R2 password 0 chap123

```

```
username R1 password 0 chap123
!
interface Embedded-Service-Engine0/0
  no ip address
  shutdown
!
interface GigabitEthernet0/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  ip address 192.168.3.1 255.255.255.0
  duplex auto
  speed auto
!
interface Serial0/0/0
  ip address 192.168.13.2 255.255.255.252
  encapsulation ppp
  ppp authentication chap
  clock rate 128000
!
interface Serial0/0/1
  ip address 192.168.23.2 255.255.255.252
  encapsulation ppp
  ppp authentication chap
!
router ospf 1
  router-id 3.3.3.3
  passive-interface GigabitEthernet0/1
  network 192.168.3.0 0.0.0.255 area 0
  network 192.168.13.0 0.0.0.3 area 0
  network 192.168.23.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^CUnauthorized Access is Prohibited!^C
!
line con 0
  password cisco
  logging synchronous
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password cisco
  login
  transport input all
!
scheduler allocate 20000 1000
!
End
```

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1-2

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 7

Тема: Сбор и анализ данных netflow

1.Цель работы:

1. Сбор и анализ данных NetFlow.
2. Приобретение практических навыков настройки ASA5505.

Формируемые компетенции: ОПК-9, ОПК-10.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал, посвящённый сбору и анализу данных NetFlow.
2. Ознакомиться с программой работы.
3. Подготовить отчет о работе.
4. Ответить на контрольные вопросы.

3. Распределение времени занятия:

Всего: 4,5 часов

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 70 мин

1. Сбор и анализ данных NetFlow 70 мин
 2. Проверка выполнения практического занятия 10 мин
- Заключительная часть 3 мин

4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

4.1. Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

4.2. Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование,

соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию;

- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;

- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

4.3. Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

6. Программное обеспечение

Программа эмуляции терминала Tera Term.

7. Основные теоретические сведения

См. рекомендованную к ознакомлению литературу по изучаемой дисциплине

8. Литература

1. James Boney, Cisco IOS in a Nutshell, O'Reilly, 2013
2. Wendell Odom, Interconnecting Networking Devices Cisco, Part 2, Cisco Press, 2013

9. Методические рекомендации по выполнению работы



Рисунок 17 - Топология

Таблица 23. Таблица адресации

Устройство	Интерфейс	IP-адрес	Шлюз по умолчанию
R1	G0/0	192.168.1.1/24	Недоступно
	S0/0/0 (DCE)	192.168.12.1/30	Недоступно
R2	G0/0	192.168.2.1/24	Недоступно
	S0/0/0	192.168.12.2/30	Недоступно
	S0/0/1 (DCE)	192.168.23.1/30	Недоступно
R3	G0/0	192.168.3.1/24	Недоступно
	S0/0/1	192.168.23.2/30	Недоступно
PC-A	NIC	192.168.1.3	192.168.1.1
PC-B	NIC	192.168.2.3	192.168.2.1
PC-C	NIC	192.168.3.3	192.168.3.1

9.1 Задачи

1. Создание сети и настройка базовых параметров устройств
2. Настройка NetFlow на маршрутизаторе
3. Анализ NetFlow с помощью интерфейса командной строки
4. Изучение ПО сбора данных и анализатора NetFlow

9.2 Исходные данные/сценарий

NetFlow — это технология Cisco IOS, предоставляющая статистические данные о пакетах, проходящих через маршрутизатор или многоуровневый

коммутатор Cisco. NetFlow обеспечивает контроль сети и безопасности, планирование сетевых ресурсов, анализ трафика и учёт IP. Важно не путать назначение и результаты NetFlow с назначением и результатами оборудования и программного обеспечения для сбора пакетов. Средства сбора пакетов записывают всю входящую и исходящую информацию сетевого устройства для последующего анализа, в то время как NetFlow собирает только определённую статистическую информацию.

Flexible NetFlow — это новейшая версия технологии NetFlow, которая расширяет возможности первоначального протокола NetFlow, позволяя настраивать параметры анализа трафика. Flexible NetFlow использует формат экспорта версии 9. Начиная с Cisco IOS версии 15.1, поддерживаются многие полезные команды Flexible NetFlow.

В этой лабораторной работе вам потребуется настроить NetFlow для сбора данных входящих и исходящих пакетов. С помощью команды **show** вы сможете проверить, что NetFlow находится в рабочем состоянии и осуществляет сбор статистических данных. Вы также рассмотрите доступные варианты ПО сборщика данных и анализатора NetFlow.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). Возможно использование других маршрутизаторов и версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не содержат файла загрузочной конфигурации. Если вы не уверены в этом, обратитесь к инструктору.

9.3 Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;

- кабели Ethernet и последовательные кабели в соответствии с топологией.

9.4 Методические пояснения и рекомендации по выполнению первого вопроса

Часть 18: Построение сети и базовая настройка устройств

В части 1 вам предстоит настроить топологию сети и сделать базовую настройку устройств.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните запуск и перезагрузку маршрутизаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

- Отключите поиск DNS.
- Настройте имена устройств в соответствии с топологией.
- Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.
- Назначьте **cisco** в качестве пароля консоли и виртуального терминала VTU и включите запрос пароля при подключении.
- Зашифруйте пароли.
- Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.
- Настройте **logging synchronous** на линии консоли.
- Настройте тактовую частоту на всех последовательных интерфейсах DCE на **128000**.
- Настройте IP-адреса, как указано в таблице адресации.
- Настройте OSPF с использованием идентификатора процесса 1 и объявите все сети. Интерфейсы Ethernet должны быть пассивными.
- Создайте учётную запись в локальной базе данных на маршрутизаторе R3 с именем пользователя **admin** и паролем **cisco** и с уровнем привилегий **15**.
- На маршрутизаторе R3 включите службу HTTP и настройте проверку подлинности пользователей HTTP с помощью локальной базы данных.
- Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4: Настройте узлы.

Шаг 5: Проверьте связь между конечными устройствами.

Все устройства должны иметь возможность отправлять эхо-запросы другим устройствам в топологии. При необходимости устраните неисправности, пока связь между конечными устройствами не будет установлена.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра на ПК.

9.5 Методические пояснения и рекомендации по выполнению второго вопроса

Часть 19: Настройка NetFlow на маршрутизаторе

В части 2 вы должны будете настроить NetFlow на маршрутизаторе R2. NetFlow собирает весь входящий и исходящий трафик на последовательных интерфейсах R2 и экспортирует данные на сборщик данных NetFlow — ПК В. Для экспорта данных на сборщик NetFlow будет использоваться Flexible NetFlow версии 9.

Шаг 1: Настройте сбор данных NetFlow.

Настройте сбор данных NetFlow на обоих последовательных интерфейсах. Выполните сбор данных из входящих и исходящих пакетов.

```
R2(config)# interface s0/0/0
R2(config-if)# ip flow ingress
R2(config-if)# ip flow egress
R2(config-if)# interface s0/0/1
R2(config-if)# ip flow ingress
R2(config-if)# ip flow egress
```

Шаг 2: Настройте экспорт данных NetFlow.

С помощью команды **ip flow-export destination** определите IP-адрес и порт UDP сборщика данных NetFlow, на который маршрутизатор должен экспортировать данные NetFlow. Для данной настройки будет использоваться номер порта UDP 9996.

```
R2(config)# ip flow-export destination 192.168.2.3 9996
```

Шаг 3: Настройте версию экспорта NetFlow.

Маршрутизаторы Cisco под управлением IOS 15.1 поддерживают NetFlow версии 1, 5 и 9. Версия 9 — это наиболее универсальный формат экспорта данных, однако он не совместим с более ранними версиями. Для установки версии NetFlow используйте команду **ip flow-export version**.

```
R2(config)# ip flow-export version 9
```

Шаг 4: Выполните проверку конфигурации NetFlow.

- Введите команду **show ip flow interface** для просмотра сведений об интерфейсе сбора данных NetFlow.

```
R2# show ip flow interface
Serial0/0/0
  ip flow ingress
  ip flow egress
```

```
Serial0/0/1
  ip flow ingress
  ip flow egress
```

- b. Введите команду **show ip flow export** для просмотра сведений об экспорте данных NetFlow.

```
R2# show ip flow export
Flow export v9 is enabled for main cache
Export source and destination details :
VRF ID : Default
  Destination(1) 192.168.2.3 (9996)
Version 9 flow records
388 flows exported in 63 udp datagrams
0 flows failed due to lack of export packet
0 export packets were sent up to process level
0 export packets were dropped due to no fib
0 export packets were dropped due to adjacency issues
0 export packets were dropped due to fragmentation failures
0 export packets were dropped due to encapsulation fixup failures
```

9.6 Методические пояснения и рекомендации по выполнению третьего вопроса

Часть 20: Анализ NetFlow с помощью интерфейса командной строки

В части 3 вы должны будете генерировать трафик данных между маршрутизаторами R1 и R3 для наблюдения за работой технологии NetFlow.

Шаг 5: Создайте трафик данных между маршрутизаторами R1 и R3.

- Подключитесь по Telnet от маршрутизатора R1 к маршрутизатору R3 с использованием IP-адреса 192.168.3.1. Введите пароль **cisco** для перехода в пользовательский режим. Введите пароль **class** для включения глобального режима ввода. Введите команду **show run**, чтобы создать трафик Telnet. Не закрывайте текущий сеанс Telnet.
- На маршрутизаторе R3 введите команду **ping 192.168.1.1 repeat 1000**, чтобы отправить эхо-запрос на интерфейс G0/0 маршрутизатора R1. Будет создан трафик ICMP через маршрутизатор R2.
- На компьютере ПК А перейдите к маршрутизатору R3, используя IP-адрес 192.168.3.1. Войдите в систему с именем пользователя **admin** и паролем **cisco**. После входа в маршрутизатор R3 оставьте браузер открытым.

Примечание. Убедитесь, что в браузере отключено блокирование всплывающих окон.

Шаг 6: Выведите на экран сводную статистику NetFlow.

На маршрутизаторе R2 введите команду **show ip cache flow**, чтобы отобразить изменения в сводных данных NetFlow, включая распределение размеров пакета, информацию о потоках IP, записанные протоколы и активность интерфейса. Теперь протоколы отображают сводные данные.

```
R2# show ip cache flow
IP packet size distribution (5727 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
  .000 .147 .018 .700 .000 .001 .001 .001 .001 .011 .009 .001 .002 .000 .001

      512   544   576 1024 1536 2048 2560 3072 3584 4096 4608
      .001 .001 .097 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 114 added
 1546 aged polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 inactive, 112 added, 112 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics 00:07:35
```

Protocol	Total	Flows	Packets	Bytes	Packets	Active(Sec)	Idle(Sec)
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
TCP-Telnet	4	0.0	27	43	0.2	5.0	15.7
TCP-WWW	104	0.2	14	275	3.4	2.1	1.5
ICMP	4	0.0	1000	100	8.8	27.9	15.4

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Pkts
Total:	112	0.2	50	146	12.5	3.1	2.5

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Pkts
Se0/0/0	192.168.12.1	Null	224.0.0.5	59	0000	0000	43
Se0/0/1	192.168.23.2	Null	224.0.0.5	59	0000	0000	40

Шаг 7: Завершите сеансы Telnet и закройте браузер.

- Введите команду **exit** на маршрутизаторе R1, чтобы отключить сеанс связи по Telnet с маршрутизатором R3.
- Закройте сеанс браузера на компьютере ПК А.

Шаг 8: Удалите статистику NetFlow.

- На маршрутизаторе R2 введите команду **clear ip flow stats**, чтобы удалить статистику NetFlow.

```
R2# clear ip flow stats
```

- Повторно введите команду **show ip cache flow**, чтобы убедиться, что статистика NetFlow сброшена. Обратите внимание: даже несмотря на то, что вы больше не создаёте данные с помощью маршрутизатора R2, они

по-прежнему принимаются NetFlow. В приведенном ниже примере адрес назначения для данного трафика — групповой адрес 224.0.0.5, это данные LSA OSPF.

R2# **show ip cache flow**

IP packet size distribution (124 total packets):

1-32	64	96	128	160	192	224	256	288	320	352	384	416	448	480
.000	.000	1.00	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
512	544	576	1024	1536	2048	2560	3072	3584	4096	4608				
.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000				

IP Flow Switching Cache, 278544 bytes

2 active, 4094 inactive, 2 added

1172 age polls, 0 flow alloc failures

Active flows timeout in 30 minutes

Inactive flows timeout in 15 seconds

IP Sub Flow Cache, 34056 bytes

2 active, 1022 inactive, 2 added, 2 added to flow

0 alloc failures, 0 force free

1 chunk, 0 chunks added

last clearing of statistics 00:09:48

Protocol	Total	Flows	Packets	Bytes	Packets	Active(Sec)	Idle(Sec)
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
IP-other	2	0.0	193	79	0.6	1794.8	5.7
Total:	2	0.0	193	79	0.6	1794.8	5.7

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Se0/0/0	192.168.12.1	Null	224.0.0.5	59	0000	0000	35
SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Se0/0/1	192.168.23.2	Null	224.0.0.5	59	0000	0000	33

9.7 Методические пояснения и рекомендации по выполнению четвёртого вопроса

Часть 21: Изучение ПО сборщика данных и анализатора NetFlow

Программное обеспечение сборщика данных и анализатора NetFlow предоставляют многие производители. Некоторые программы распространяются бесплатно, другие — нет. По следующему URL-адресу размещена веб-страница с обзором некоторых бесплатных программ NetFlow:

http://www.cisco.com/en/US/prod/iosswrel/ps6537/ps6555/ps6601/networking_solutions_products_genericcontent0900aecd805ff72b.html

Посмотрите эту веб-страницу, чтобы ознакомиться с некоторыми из доступных программных продуктов сборщика данных и анализатора NetFlow.

9.8 Вопросы на закрепление

1. В чём заключается назначение ПО сборщика данных NetFlow?

Программное обеспечение сборщика данных NetFlow получает данные NetFlow, экспортируемые с маршрутизаторов и коммутаторов в сети. Оно фильтрует и объединяет данные в соответствии с политиками, настроенными сетевым администратором, и сохраняет эти обобщённые или объединённые данные вместо «сырых» данных о потоках, чтобы снизить потребление дискового пространства.

2. В чём заключается назначение программного анализатора NetFlow?

Программный анализатор NetFlow представляет собой средство визуализации практически в режиме реального времени и анализа записанных и объединённых данных потока. Он позволяет указать маршрутизатор, схему агрегации и временной интервал для просмотра данных. После этого можно выполнять сортировку и визуализацию данных удобным для пользователей способом (в виде столбчатых диаграмм, круговых диаграмм или гистограмм упорядоченных отчётов).

3. Перечислите семь основных полей, используемых первоначальным протоколом NetFlow для различения потоков данных.

IP-адрес источника, IP-адрес назначения, номер порта источника, номер порта назначения, тип протокола уровня 3, маркировка ToS (тип обслуживания), логический входной интерфейс.

Таблица 24. Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet № 2	Последовательный интерфейс № 1	Последовательный интерфейс № 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

9.9 Настройки устройств (окончательные)

Маршрутизатор R1

```
R1# show run
Building configuration...

Current configuration : 1592 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
```

```
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
ip address 192.168.12.1 255.255.255.252
clock rate 128000
!
interface Serial0/0/1
no ip address
shutdown
!
router ospf 1
passive-interface GigabitEthernet0/0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.12.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
password 7 030752180500
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password 7 02050D480809
login
transport input all
!
scheduler allocate 20000 1000
```

!
end

Маршрутизатор R2

R2# show run

Building configuration...

Current configuration : 1808 bytes

```
!  
version 15.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
!  
hostname R2  
!  
boot-start-marker  
boot-end-marker  
!  
enable secret 4 06YFDUHH6lwAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2  
!  
no aaa new-model  
memory-size iomem 15  
!  
ip cef  
!  
no ip domain lookup  
no ipv6 cef  
!  
multilink bundle-name authenticated  
!  
interface Embedded-Service-Engine0/0  
no ip address  
shutdown  
!  
interface GigabitEthernet0/0  
ip address 192.168.2.1 255.255.255.0  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/1  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface Serial0/0/0  
ip address 192.168.12.2 255.255.255.252  
ip flow ingress  
ip flow egress  
!  
interface Serial0/0/1  
ip address 192.168.23.1 255.255.255.252  
ip flow ingress  
ip flow egress  
clock rate 128000  
!  
router ospf 1  
passive-interface GigabitEthernet0/0  
network 192.168.2.0 0.0.0.255 area 0  
network 192.168.12.0 0.0.0.3 area 0  
network 192.168.23.0 0.0.0.3 area 0  
!  
ip forward-protocol nd
```

```

!
no ip http server
no ip http secure-server
ip flow-export version 9
ip flow-export destination 192.168.2.3 9996
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
  password 7 14141B180F0B
  logging synchronous
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password 7 060506324F41
  login
  transport input all
!
scheduler allocate 20000 1000
!
End

```

Маршрутизатор R3

```

R3# show run
Building configuration...

Current configuration : 1769 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
username admin privilege 15 secret 4
tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
!
interface Embedded-Service-Engine0/0
  no ip address

```

```

shutdown
!
interface GigabitEthernet0/0
ip address 192.168.3.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
ip address 192.168.23.2 255.255.255.252
!
router ospf 1
passive-interface GigabitEthernet0/0
network 192.168.3.0 0.0.0.255 area 0
network 192.168.23.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
ip http server
ip http authentication local
no ip http secure-server
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
exec-timeout 0 0
password 7 01100F175804
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password 7 0822455D0A16
login
transport input all
!
scheduler allocate 20000 1000
!
End

```

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1-2

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 8-9

Тема: Поиск и устранение неполадок в работе dhcprv4

1.Цель работы:

1. Поиск и устранение неполадок в работе DHCPv4.
2. Приобретение практических навыков настройки ASA5505.

Формируемые компетенции: ОПК-9, ОПК-10.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал, посвящённый поиску и устранению неполадок в работе DHCPv4.
2. Ознакомиться с программой работы.
3. Подготовить отчет о работе.
4. Ответить на контрольные вопросы.

3. Распределение времени занятия:

Всего: 9 часов

Вступительная часть 5 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 140 мин

1. Поиск и устранение неполадок в работе DHCPv4 140 мин
 2. Проверка выполнения практического занятия 20 мин
- Заключительная часть 10 мин

4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

4.1. Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

4.2. Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать

только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию;

- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;

- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

4.3. Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

6. Программное обеспечение

Программа эмуляции терминала Tera Term.

7. Основные теоретические сведения

См. рекомендованную к ознакомлению литературу по изучаемой дисциплине

8. Литература

1. James Boney, Cisco IOS in a Nutshell, O'Reilly, 2013
2. Wendell Odom, Interconnecting Networking Devices Cisco, Part 2, Cisco Press, 2013

9. Методические рекомендации по выполнению работы

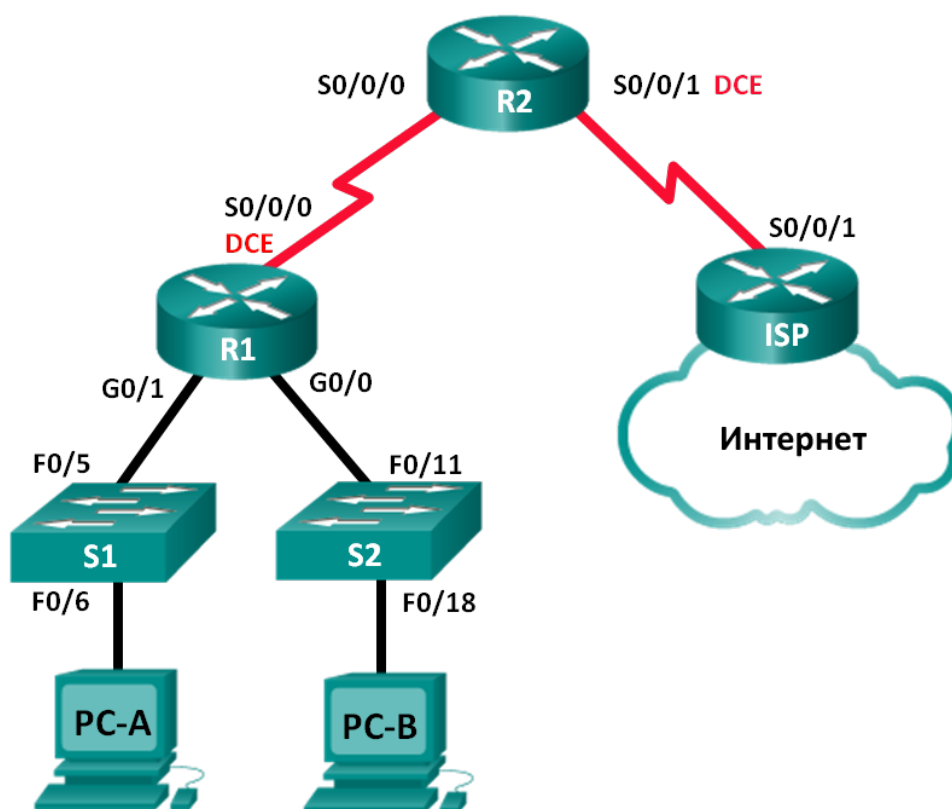


Рисунок 18 - Топология

Таблица 25. Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.0.1	255.255.255.128	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.0.253	255.255.255.252	N/A
R2	S0/0/0	192.168.0.254	255.255.255.252	N/A
	S0/0/1 (DCE)	209.165.200.22 6	255.255.255.252	N/A
ISP	S0/0/1	209.165.200.22 5	255.255.255.252	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.0.2	255.255.255.128	192.168.0.1
PC-A	NIC	DHCP	DHCP	DHCP
PC-B	NIC	DHCP	DHCP	DHCP

9.1 Задачи

1. Построение сети и настройка базовых параметров устройства
2. Выполнение поиска и устранения неполадок в работе DHCPv4

9.2 Исходные данные/сценарий

Протокол динамической конфигурации сетевого узла (DHCP) — сетевой протокол, позволяющий сетевым администраторам управлять назначением и автоматизировать назначение IP-адресов. Без использования DHCP администратору приходится вручную назначать и настраивать IP-адреса, предпочтительные DNS-серверы и шлюз по умолчанию. По мере увеличения сети и перемещении устройств из одной внутренней сети в другую это становится административной проблемой.

В предложенном сценарии размеры компании увеличились, и сетевые администраторы больше не имеют возможности назначать IP-адреса для устройств вручную. Маршрутизатор R2 был настроен в качестве сервера DHCP для назначения IP-адресов узловым устройствам в локальных сетях маршрутизатора R1. В результате нескольких ошибок в настройках возникли проблемы со связью. Вас попросили выполнить поиск и

устранение неполадок в конфигурации и написать отчёт о проделанной работе.

Убедитесь в том, что сеть соответствует следующим требованиям:

- 1) Маршрутизатор R2 должен функционировать в качестве сервера DHCP для сетей 192.168.0.0/25 и 192.168.1.0/24, подключённых к маршрутизатору R1.
- 2) Все ПК, подключённые к коммутаторам S1 и S2, должны получить IP-адрес в нужной сети с помощью DHCP.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсах маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

9.3 Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

9.4 Методические рекомендации и пояснения по выполнению первого вопроса

Часть 22: Построение сети и настройка базовых параметров устройства

В первой части лабораторной работы вам предстоит создать топологию сети и настроить основные параметры на маршрутизаторах и коммутаторах, такие как пароли и IP-адреса. Также вам предстоит настроить параметры IP для компьютеров в приведённой топологии.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 3: Настройте базовые параметры каждого маршрутизатора.

- a. Отключите поиск DNS.
- b. Присвойте имена устройствам в соответствии с топологией.
- c. Назначьте **class** в качестве пароля привилегированного режима EXEC.
- d. Назначьте **cisco** в качестве паролей консоли и VTY.
- e. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.
- f. Назначьте IP-адреса всем интерфейсам маршрутизатора.
- g. Установите тактовую частоту на **128000** для всех интерфейсов маршрутизатора DCE.
- h. Настройте EIGRP на маршрутизаторе R1.

```
R1(config)# router eigrp 1
R1(config-router)# network 192.168.0.0 0.0.0.127
R1(config-router)# network 192.168.0.252 0.0.0.3
R1(config-router)# network 192.168.1.0
R1(config-router)# no auto-summary
```

- i. На маршрутизаторе R2 настройте EIGRP и статический маршрут по умолчанию.

```
R2(config)# router eigrp 1
R2(config-router)# network 192.168.0.252 0.0.0.3
R2(config-router)# redistribute static
R2(config-router)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.225
```

- j. Настройте суммарный статический маршрут на маршрутизаторе ISP к сетям на маршрутизаторах R1 и R2.

```
ISP(config)# ip route 192.168.0.0 255.255.254.0 209.165.200.226
```

Шаг 4: Выполните проверку сетевого соединения между маршрутизаторами.

При неудачных эхо-запросах между маршрутизаторами исправьте обнаруженные ошибки, прежде чем переходить к следующему шагу. Используйте команды **show ip route** и **show ip interface brief**, чтобы определить возможные неполадки.

Шаг 5: Настройте базовые параметры каждого коммутатора.

- Отключите поиск DNS.
- Присвойте имена устройствам в соответствии с топологией.
- Назначьте IP-адрес интерфейсу VLAN 1 и шлюз по умолчанию для каждого коммутатора.
- Назначьте **class** в качестве пароля привилегированного режима EXEC.
- Назначьте **cisco** в качестве паролей консоли и VTY.
- Настройте **logging synchronous** для консольного канала.

Шаг 6: Убедитесь в том, что на узлах включена работа с DHCP.

Шаг 7: Загрузите начальную конфигурацию DHCP для маршрутизаторов R1 и R2.

Маршрутизатор R1

```
interface GigabitEthernet0/1
ip helper-address 192.168.0.253
```

Маршрутизатор R2

```
ip dhcp excluded-address 192.168.11.1 192.168.11.9
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp pool R1G1
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
ip dhcp pool R1G0
network 192.168.0.0 255.255.255.128
default-router 192.168.11.1
```

9.5 Методические рекомендации и пояснения по выполнению второго вопроса

Часть 23: Поиск и устранение неполадок в работе DHCPv4

После настройки маршрутизаторов R1 и R2 с параметрами DHCPv4 появилось несколько ошибок в настройке DHCP, которые привели к неполадкам в подключении. Маршрутизатор R2 настроен в качестве сервера DHCP. В обоих пулах адресов DHCP первые девять адресов зарезервированы для маршрутизаторов и коммутаторов. Маршрутизатор R1 ретранслирует информацию о DHCP во все локальные сети

маршрутизатора R1. На данный момент компьютеры PC-A и PC-B не имеют доступа к сети. Используйте команды **show** и **debug** для выявления и исправления проблем с сетевым соединением.

Шаг 1: Запишите IP-параметры для компьютеров PC-A и PC-B.

- a. В командной строке компьютеров PC-A и PC-B введите **ipconfig /all** для отображения IP- и MAC-адресов.
- b. Запишите IP- и MAC-адреса в таблице ниже. MAC-адрес можно использовать для определения какой ПК упоминается в сообщении об ошибке.

Таблица 26. Сетевая конфигурация PC-A и PC-B

	IP-адрес/маска подсети	MAC-адрес
PC-A		
PC-B		

Шаг 2: Устраните неполадки в работе DHCP для сети 192.168.1.0/24 на маршрутизаторе R1.

Маршрутизатор R1 является агентом DHCP-ретрансляции для всех сетей LAN маршрутизатора R1. На данном этапе будет рассматриваться только процесс DHCP для сети 192.168.1.0/24. Первые девять адресов зарезервированы для других сетевых устройств, включающих маршрутизаторы, коммутаторы и серверы.

- a. Для наблюдения за процессом DHCP на маршрутизаторе R2 используйте команду DHCP **debug**.

```
R2# debug ip dhcp server events
```

- b. На маршрутизаторе R1 отобразите текущую конфигурацию интерфейса G0/1.

```
R1# show run interface g0/1
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip helper-address 192.168.0.253
 duplex auto
 speed auto
```

При наличии каких-либо проблем с DHCP-ретрансляцией, запишите команды, которые понадобятся для исправления ошибок конфигурации.

-
- c. В командной строке компьютера PC-A введите **ipconfig /renew**, чтобы получить адрес от сервера DHCP. Запишите полученный IP-адрес, маску подсети и шлюз по умолчанию для PC-A.
-

- d. Проследите за процессом обновления информации для PC-A с помощью отладочных сообщений на маршрутизаторе R2. Сервер DHCP пытался назначить компьютеру PC-A адрес 192.168.1.1/24. Данный адрес уже используется для интерфейса G0/1 маршрутизатора R1. Та же проблема возникла с IP-адресом 192.168.1.2/24, поскольку в начальной конфигурации адрес был назначен коммутатору S1. Поэтому компьютеру PC-A был назначен IP-адрес 192.168.1.3/24. Конфликт при назначении адреса DHCP указывает, что при настройке сервера DHCP на маршрутизаторе R2 определенные адреса могли быть не исключены из пула DHCP.

```
*Mar 5 06:32:16.939: DHCPD: Sending notification of DISCOVER:
*Mar 5 06:32:16.939:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar 5 06:32:16.939:   DHCPD: circuit id 00000000
*Mar 5 06:32:16.939: DHCPD: Seeing if there is an internally specified pool
class:
*Mar 5 06:32:16.939:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar 5 06:32:16.939:   DHCPD: circuit id 00000000
*Mar 5 06:32:16.943: DHCPD: Allocated binding 2944C764
*Mar 5 06:32:16.943: DHCPD: Adding binding to radix tree (192.168.1.1)
*Mar 5 06:32:16.943: DHCPD: Adding binding to hash tree
*Mar 5 06:32:16.943: DHCPD: assigned IP address 192.168.1.1 to client
0100.5056.be76.8c.
*Mar 5 06:32:16.951: %DHCPD-4-PING_CONFLICT: DHCP address conflict: server
pinged 192.168.1.1.
*Mar 5 06:32:16.951: DHCPD: returned 192.168.1.1 to address pool R1G1.
*Mar 5 06:32:16.951: DHCPD: Sending notification of DISCOVER:
*Mar 5 06:32:16.951:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar 5 06:32:16.951:   DHCPD: circuit id 00000000
*Mar 5 06:32:1
R2#6.951: DHCPD: Seeing if there is an internally specified pool class:
*Mar 5 06:32:16.951:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar 5 06:32:16.951:   DHCPD: circuit id 00000000
*Mar 5 06:32:16.951: DHCPD: Allocated binding 31DC93C8
*Mar 5 06:32:16.951: DHCPD: Adding binding to radix tree (192.168.1.2)
*Mar 5 06:32:16.951: DHCPD: Adding binding to hash tree
*Mar 5 06:32:16.951: DHCPD: assigned IP address 192.168.1.2 to client
0100.5056.be76.8c.
```

```
*Mar  5 06:32:18.383: %DHCPD-4-PING_CONFLICT: DHCP address conflict:  server
pinged 192.168.1.2.
*Mar  5 06:32:18.383: DHCPD: returned 192.168.1.2 to address pool R1G1.
*Mar  5 06:32:18.383: DHCPD: Sending notification of DISCOVER:
*Mar  5 06:32:18.383:   DHCPD: htype 1 chaddr 0050.56be.6c89
*Mar  5 06:32:18.383:   DHCPD: circuit id 00000000
*Mar  5 06:32:18.383: DHCPD: Seeing if there is an internally specified pool
class:
*Mar  5 06:32:18.383:   DHCPD: htype 1 chaddr 0050.56be.6c89
*Mar  5 06:32:18.383:   DHCPD: circuit id 00000000
*Mar  5 06:32:18.383: DHCPD: Allocated binding 2A40E074
*Mar  5 06:32:18.383: DHCPD: Adding binding to radix tree (192.168.1.3)
*Mar  5 06:32:18.383: DHCPD: Adding binding to hash tree
*Mar  5 06:32:18.383: DHCPD: assigned IP address 192.168.1.3 to client
0100.5056.be76.8c.
<output omitted>
```

- e. Отобразите конфигурацию сервера DHCP на маршрутизаторе R2. Первые девять адресов для сети 192.168.1.0/24 не исключены из пула DHCP.

```
R2# show run | section dhcp
ip dhcp excluded-address 192.168.11.1 192.168.11.9
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp pool R1G1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
ip dhcp pool R1G0
 network 192.168.0.0 255.255.255.128
 default-router 192.168.1.1
```

Запишите команды для решения обнаруженной проблемы на маршрутизаторе R2.

- f. В командной строке компьютера PC-A введите **ipconfig /release**, чтобы вернуть адрес 192.168.1.3 обратно в пул DHCP. За процессом можно проследить с помощью сообщений команды **debug** на маршрутизаторе R2.

```
*Mar  5 06:49:59.563: DHCPD: Sending notification of TERMINATION:
*Mar  5 06:49:59.563:   DHCPD: address 192.168.1.3 mask 255.255.255.0
*Mar  5 06:49:59.563:   DHCPD: reason flags: RELEASE
*Mar  5 06:49:59.563:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar  5 06:49:59.563:   DHCPD: lease time remaining (secs) = 85340
*Mar  5 06:49:59.563: DHCPD: returned 192.168.1.3 to address pool R1G1.
```

- g. В командной строке компьютера PC-A введите **ipconfig /renew**, чтобы компьютеру был назначен новый IP-адрес сервером DHCP. Запишите назначенные IP-адреса и данные шлюза по умолчанию.

За процессом можно проследить с помощью сообщений команды `debug` на маршрутизаторе R2.

```
*Mar 5 06:50:11.863: DHCPD: Sending notification of DISCOVER:
*Mar 5 06:50:11.863:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar 5 06:50:11.863:   DHCPD: circuit id 00000000
*Mar 5 06:50:11.863: DHCPD: Seeing if there is an internally specified pool
class:
*Mar 5 06:50:11.863:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar 5 06:50:11.863:   DHCPD: circuit id 00000000
*Mar 5 06:50:11.863: DHCPD: requested address 192.168.1.3 has already been
assigned.
*Mar 5 06:50:11.863: DHCPD: Allocated binding 3003018C
*Mar 5 06:50:11.863: DHCPD: Adding binding to radix tree (192.168.1.10)
*Mar 5 06:50:11.863: DHCPD: Adding binding to hash tree
*Mar 5 06:50:11.863: DHCPD: assigned IP address 192.168.1.10 to client
0100.5056.be76.8c.
<output omitted>
```

h. Проверьте сетевое соединение.

Можно ли отправить эхо-запрос от компьютера PC-A на назначенный шлюз по умолчанию?

Можно ли отправить эхо-запрос от компьютера PC-A на маршрутизатор R2? _____

Можно ли отправить эхо-запрос от компьютера PC-A на маршрутизатор ISP? _____

Шаг 3: Выполните поиск и устранение неполадок в работе DHCP для сети 192.168.0.0/25 на маршрутизаторе R1.

Маршрутизатор R1 является агентом DHCP-ретрансляции для всех сетей LAN маршрутизатора R1. На этом этапе будет рассматриваться только процесс DHCP для сети 192.168.0.0/25. Первые девять адресов зарезервированы для других сетевых устройств.

- a. Для наблюдения за процессом DHCP на маршрутизаторе R2 используйте команду **DHCP debug**.

```
R2# debug ip dhcp server events
```

- b. Отобразите текущую конфигурацию интерфейса G0/0 маршрутизатора R1, чтобы определить возможные проблемы в работе DHCP.

```
R1# show run interface g0/0
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.128
 duplex auto
 speed auto
```

Запишите обнаруженные проблемы и все команды, которые понадобятся для исправления ошибок конфигурации.

- c. В командной строке компьютера PC-B введите **ipconfig /renew**, чтобы получить адрес от сервера DHCP. Запишите полученный IP-адрес, маску подсети и шлюз по умолчанию для PC-B.

- d. За процессом обновления для PC-A можно проследить с помощью сообщений команды **debug** на маршрутизаторе R2. Сервер DHCP назначил компьютеру PC-B адрес 192.168.0.10/25.

```
*Mar 5 07:15:09.663: DHCPD: Sending notification of DISCOVER:
*Mar 5 07:15:09.663:   DHCPD: htype 1 chaddr 0050.56be.f6db
*Mar 5 07:15:09.663:   DHCPD: circuit id 00000000
*Mar 5 07:15:09.663: DHCPD: Seeing if there is an internally specified pool
class:
*Mar 5 07:15:09.663:   DHCPD: htype 1 chaddr 0050.56be.f6db
*Mar 5 07:15:09.663:   DHCPD: circuit id 00000000
*Mar 5 07:15:09.707: DHCPD: Sending notification of ASSIGNMENT:
*Mar 5 07:15:09.707:   DHCPD: address 192.168.0.10 mask 255.255.255.128
*Mar 5 07:15:09.707:   DHCPD: htype 1 chaddr 0050.56be.f6db
*Mar 5 07:15:09.707:   DHCPD: lease time remaining (secs) = 86400
```

- e. Проверьте сетевое соединение.

Можно ли отправить эхо-запрос от компьютера PC-B на шлюз по умолчанию, назначенный сервером DHCP? _____

Можно ли отправить эхо-запрос от PC-B на его шлюз по умолчанию (192.168.0.1)? _____

Можно ли отправить эхо-запрос от компьютера PC-B на маршрутизатор R2? _____

Можно ли отправить эхо-запрос от компьютера PC-B на маршрутизатор ISP? _____

- f. При возникновении каких-либо неполадок на шаге e, запишите обнаруженные проблемы и все команды, необходимые для устранения неполадок.

- g. Очистите и обновите настройки IP на компьютере PC-B. Повторите шаг e для проверки сетевого соединения.
- h. Прервите процесс отладки с помощью команды **undebug all**.

R2# **undebug all**

All possible debugging has been turned off

9.6 Вопросы на закрепление

Каковы преимущества использования DHCP?

Таблица 27. Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	Последовательный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

1. Цель работы:

1. Поиск и устранение неполадок конфигураций NAT.
2. Приобретение практических навыков поиска и устранения неполадок

конфигураций NAT.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал, посвящённый поиску и устранению неполадок конфигураций NAT.
2. Ознакомиться с программой работы.
3. Подготовить отчет о работе.
4. Ответить на контрольные вопросы.

3. Распределение времени занятия:

Всего: 90 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 70 мин

1. Поиск и устранение неполадок конфигураций NAT 70 мин
 2. Проверка выполнения практического занятия 10 мин
- Заключительная часть 3 мин

4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

4.1. Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

4.2. Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию;
- подключение и отключение составляющих вычислительного

комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;

- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

4.3. Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

6. Программное обеспечение

Программа эмуляции терминала Tera Term.

7. Основные теоретические сведения

См. рекомендованную к ознакомлению литературу по изучаемой дисциплине

8. Литература

1. James Boney, Cisco IOS in a Nutshell, O'Reilly, 2013
2. Wendell Odom, Interconnecting Networking Devices Cisco, Part 2, Cisco Press, 2013

9. Методические рекомендации по выполнению работы

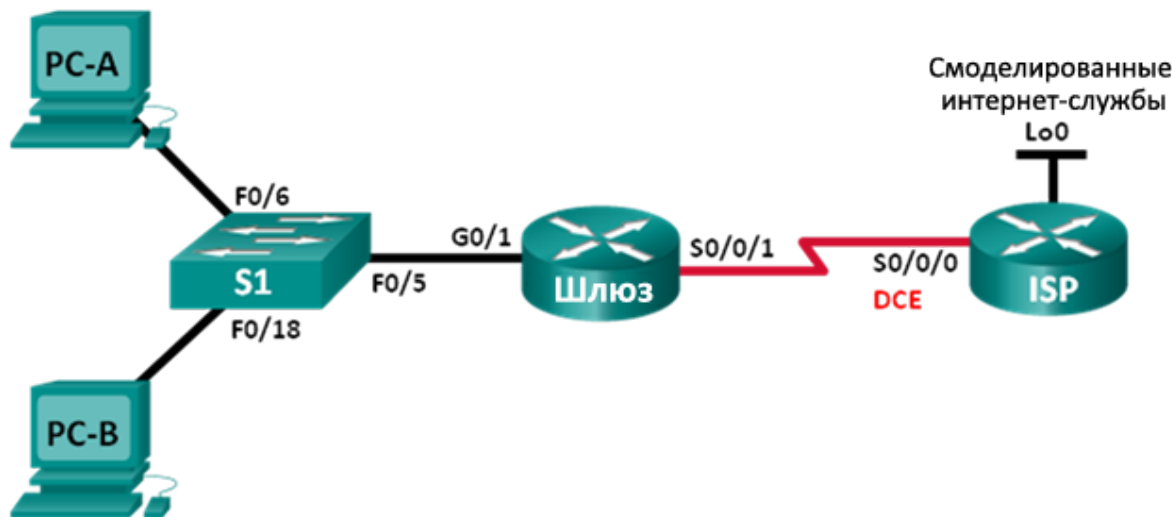


Рисунок 19 - Топология

Таблица 28. Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Шлюз	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.200.225	255.255.255.252	N/A
Интернет-провайдер	S0/0/0 (DCE)	209.165.200.226	255.255.255.252	N/A
	Lo0	198.133.219.1	255.255.255.255	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.4	255.255.255.0	192.168.1.1

9.1 Задачи

1. Построение сети и настройка базовых параметров устройства
2. Поиск и устранение неполадок статического NAT
3. Поиск и устранение неполадок динамического NAT

9.2 Исходные данные/сценарий

По сценарию лабораторной работы маршрутизатор Gateway был настроен неопытным сетевым администратором из вашей компании. Из-за нескольких ошибок в настройках возникли проблемы с процессом NAT. Начальник попросил вас найти неисправности, устранить ошибки конфигурации и составить отчёт о проделанной работе. Убедитесь в том, что сеть соответствует следующим требованиям:

- Компьютер PC-A работает в качестве веб-сервера со статическим NAT и будет доступен извне через адрес 209.165.200.254.
- Компьютер PC-B функционирует в качестве узлового компьютера и динамически получает IP-адрес от созданного пула адресов под названием NAT_POOL, который использует диапазон 209.165.200.240/29.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсах маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

9.3 Необходимые ресурсы:

- 2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 1 коммутатор (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);

- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

9.4 Методические пояснения и рекомендации по выполнению первого вопроса

Часть 24: Построение сети и настройка базовых параметров устройства

В первой части вам предстоит настроить топологию сети и настроить базовые параметры на маршрутизаторах. Дополнительные конфигурации NAT прилагаются. В конфигурации NAT для шлюзового маршрутизатора (Gateway) содержатся ошибки, которые вам нужно найти и исправить в процессе выполнения этой лабораторной работы.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Настройте узлы ПК.

Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 4: Настройте базовые параметры каждого маршрутизатора.

- Отключите поиск DNS.
- Присвойте имена устройствам в соответствии с топологией.
- Настройте IP-адреса в соответствии с таблицей адресов.
- Установите тактовую частоту на **128000** для всех последовательных интерфейсов DCE.
- Назначьте **cisco** в качестве пароля консоли и виртуального терминала VTU.
- Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.
- Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.

Шаг 5: Настройте статическую маршрутизацию.

- Создайте статический маршрут от маршрутизатора интернет-провайдера до маршрутизатора Gateway, используя диапазон публичных сетевых адресов 209.165.200.224/27.

```
ISP(config)# ip route 209.165.200.224 255.255.255.224 s0/0/0
```

- Создайте маршрут по умолчанию от маршрутизатора Gateway к маршрутизатору ISP.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 s0/0/1
```

Шаг 6: Загрузите настройки маршрутизатора.

В вашем распоряжении конфигурации для маршрутизаторов. Ошибки содержатся в конфигурации для маршрутизатора Gateway. Определите и исправьте ошибки конфигурации.

Конфигурация шлюзового маршрутизатора

```
interface g0/1
  ip nat outside
  no shutdown
interface s0/0/0
  ip nat outside
interface s0/0/1
  no shutdown
ip nat inside source static 192.168.2.3 209.165.200.254
ip nat pool NAT_POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
ip nat inside source list NAT_ACL pool NATPOOL
ip access-list standard NAT_ACL
  permit 192.168.10.0 0.0.0.255
banner motd $AUTHORIZED ACCESS ONLY$
end
```

Шаг 7: Сохраните текущую конфигурацию в загрузочную конфигурацию.

9.5 Методические пояснения и рекомендации по выполнению второго вопроса

Часть 25: Поиск и устранение неполадок статического NAT

Во второй части вам нужно исследовать статический NAT для компьютера PC-A, чтобы оценить правильность его настройки. Выполняйте поиск и устранение неполадок, пока статический NAT не будет настроено правильно.

- a. Чтобы устранить неполадки в NAT, используйте команду **debug ip nat**. Включите отладку NAT, чтобы видеть преобразования через маршрутизатор Gateway в реальном времени.

```
Gateway# debug ip nat
```

- b. Отправьте эхо-запрос с PC-A на Lo0 маршрутизатора интернет-провайдера (ISP). Появляются ли какие-либо преобразования отладки NAT на маршрутизаторе Gateway?

-
- c. На маршрутизаторе Gateway введите команду, которая позволит увидеть все текущие преобразования NAT на данном маршрутизаторе. Запишите команду в строке ниже.

Почему вы видите преобразования NAT в таблице, хотя при отправке эхо-запроса от компьютера PC-A на интерфейсе loopback маршрутизатора интернет-провайдера этого не было? Что необходимо сделать, чтобы исправить эту проблему?

- d. Запишите все команды, необходимые для исправления ошибки в конфигурации статического NAT.
-

- e. Отправьте эхо-запрос с PC-A на Lo0 маршрутизатора интернет-провайдера (ISP). Появляются ли какие-либо преобразования отладки NAT на маршрутизаторе Gateway?
-

На маршрутизаторе Gateway введите команду, которая позволит увидеть общее количество текущих преобразований NAT. Запишите команду в строке ниже.

Успешно ли проходит статическое преобразование NAT? Почему?

- f. На маршрутизаторе Gateway введите команду, которая позволит увидеть текущую конфигурацию маршрутизатора. Запишите команду в строке ниже.
-

- g. Есть ли какие-либо проблемы в текущей конфигурации, которые препятствуют статическому NAT?

-
- h. Запишите все команды, необходимые для исправления ошибок в конфигурации статического NAT.

-
- i. Отправьте эхо-запрос с PC-A на Lo0 маршрутизатора интернет-провайдера (ISP). Появляются ли какие-либо преобразования отладки NAT на маршрутизаторе Gateway?

-
- j. Чтобы убедиться в правильном функционировании статического NAT, используйте команду **show ip nat translations verbose**.

Примечание. Период истечения времени для ICMP очень короткий.

Если вы не видите все преобразования в выходных данных, повторите эхо-запрос.

Успешно ли проходит статическое преобразование NAT?

Если статическое преобразование NAT проходит неправильно, повторите вышеупомянутые действия, чтобы исправить неполадки в конфигурации.

9.6 Методические пояснения и рекомендации по выполнению третьего вопроса

Часть 26: Поиск и устранение неполадок динамического NAT

- а. Отправьте эхо-запрос с PC-B на Lo0 на маршрутизаторе интернет-провайдера (ISP). Появляются ли какие-либо преобразования отладки NAT на маршрутизаторе Gateway?

- б. На маршрутизаторе Gateway введите команду, которая позволит увидеть текущую конфигурацию маршрутизатора. Есть ли какие-либо проблемы в текущей конфигурации, которые препятствуют динамическому преобразованию NAT?

- с. Запишите все команды, необходимые для исправления ошибок в конфигурации динамического NAT.

- д. Отправьте эхо-запрос с PC-B на Lo0 на маршрутизаторе интернет-провайдера (ISP). Появляются ли какие-либо преобразования отладки NAT на маршрутизаторе Gateway?

- е. Чтобы отслеживать использование NAT, используйте команду **show ip nat statistics**.

Успешно ли проходит NAT? _____

Какой процент динамических адресов выделен? _____

- f. Отмените все операции отладки с помощью команды `undebug all`.

9.7 Вопросы на закрепление

1. В чём заключаются преимущества статического NAT?

2. Какие проблемы могли бы возникнуть, если бы десять узловых компьютеров в этой сети попытались одновременно наладить связь через Интернет?

Таблица 29. Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	Последовательный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.				

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1-2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для обучающихся по организации и проведению самостоятельной работы
по дисциплине «Программно-аппаратные средства защиты информации»
для студентов направления подготовки
10.03.01 «Информационная безопасность»
Направленность (профиль):
«Организация и технологии защиты информации (по отрасли или в сфере
профессиональной деятельности)»

СОДЕРЖАНИЕ

Введение	
1. Общая характеристика самостоятельной работы студента.....	
2. Технологическая карта самостоятельной работы студента.....	
3. Самостоятельное изучение тем лекций.....	
4. Паспорт фонда оценочных средств для проверки самостоятельной работы	
5. Список рекомендуемой литературы	

Введение

Целью изучения дисциплины «Программно-аппаратные средства защиты информации» Дисциплина «Программно-аппаратные средства защиты информации» имеет целью подготовить выпускника квалификации бакалавр к деятельности, связанной с эксплуатацией и обслуживанием аппаратуры и оборудования, содержащего современные средства вычислительной техники, получение основополагающих знаний о программно-аппаратных средствах защиты информации в операционных системах, вычислительных сетях и системах управления базами данных, средствах антивирусной защиты

Задачами дисциплины являются:

- 1.Формирование требований к системе управления ИБ конкретного объекта;
- 2.Проектирование системы управления ИБ конкретного объекта.
- 3.Эффективное управление ИБ конкретного объекта.

1. Общая характеристика самостоятельной работы студента

Основными видами учебной работы по достижению результатов освоения дисциплины являются лекции, лабораторные и практических работы и самостоятельная работа студентов (СРС).

На лекциях раскрываются основные положения и понятия курса, формируются знания в области программно-аппаратных средств защиты информации. На лабораторных и практических работах формируются умения и навыки, необходимые для решения задач профессиональной деятельности.

Приступая к изучению учебной дисциплины, необходимо ознакомиться с учебной программой, получить в библиотеке рекомендованные учебные пособия, а также получить у ведущего преподавателя в электронном виде конспекты лекций, методические рекомендации к лабораторным и практическим работам и тестовые, завести новую тетрадь для конспектирования лекций и выполнения лабораторных и практических работ.

Для изучения дисциплины предлагается список основной и дополнительной литературы. Основная литература предназначена для обязательного изучения, дополнительная – поможет более глубоко освоить отдельные вопросы, подготовить исследовательские задания и выполнить задания для самостоятельной работы.

В ходе лекционных занятий студент обязан осуществлять конспектирование учебного материала, особое внимание, обращая на категории, формулировки, раскрывающие содержание тех или иных понятий, физических явлений, процессов, эффектов. В рабочих конспектах желательно оставлять поля, на которых следует делать пометки из рекомендованной литературы, дополнять материал прослушанной лекции, формулировать научные выводы и практические рекомендации. Студент имеет право задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Самостоятельная работа студентов над материалом учебной дисциплины

является неотъемлемой частью учебного процесса и должна предполагать углубление знания учебного материала, излагаемого на аудиторных занятиях, и приобретение дополнительных знаний по отдельным вопросам самостоятельно.

Основными видами самостоятельной работы курсантов по учебной дисциплине являются:

- самостоятельное изучение учебного материала по заданным темам;
- подготовка к лабораторным работам, оформление отчета по выполненному лабораторному и практическому занятию и подготовка к собеседованию по результатам работы.

Основными методами самостоятельной работы студентов являются:

1) для овладения знаниями:

- чтение текста (конспекта лекций, учебника, дополнительной литературы) и конспектирование текста;
- работа с нормативными документами;
- поиск информации в Интернет;

2) для закрепления и систематизации знаний:

- работа с конспектом лекции (обработка текста);
- повторная работа над учебным материалом (учебника, дополнительной литературы, слайдами);
- составление плана и тезисов ответа или графическое изображение структуры ответа;

- составление таблиц для систематизации учебного материала;
- изучение нормативных документов;
- ответы на контрольные вопросы;

3) для формирования умений:

- подготовка к лабораторным и практическим занятиям;
- решение задач и практических заданий;
- подготовка отчетов по лабораторным и практическим занятиям;
- рефлексивный анализ профессиональных умений.

В случае пропуска учебного занятия студент может воспользоваться содержанием различных блоков учебно-методического комплекса (лекции, лабораторные и практические занятия, контрольные вопросы и тесты) для самоподготовки и освоения темы. Для самоконтроля необходимо использовать вопросы и задания, предлагаемые к лабораторным и практическим занятиям, а также варианты тестовых заданий.

2. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций, индикатора(ов)	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего

5 семестр					
ОПК-9 ИД-3 ОПК-10 ИД-1	Подготовка к лабораторной работе	Собеседование	12	2	14
ОПК-9 ИД-3 ОПК-10 ИД-1	Подготовка к лекции	Конспект	12	2	14
ОПК-9 ИД-3 ОПК-10 ИД-1	Подготовка доклада	Доклад	12	2	14
ОПК-9 ИД-3 ОПК-10 ИД-1	Самостоятельное изучение литературы	Конспект	12	2	14
ОПК-9 ИД-3 ОПК-10 ИД-1	Подготовка к практическому занятию	Конспект. Письменный отчет	14	2	16
Итого за 5 семестр			62	10	72
6 семестр					
ОПК-9 ИД-3 ОПК-10 ИД-1	Подготовка к экзамену	Вопросы к экзамену	4	2	
ОПК-9 ИД-3 ОПК-10 ИД-1	Подготовка к лабораторной работе	Собеседование	4	2	
ОПК-9 ИД-3 ОПК-10 ИД-1	Подготовка к лекции	Конспект	6	2	
ОПК-9 ИД-3 ОПК-10 ИД-1	Подготовка к практическому занятию	Конспект. Письменный отчет	4	2	
ОПК-9 ИД-3 ОПК-10 ИД-1	Самостоятельное изучение литературы	Конспект	10	2	
Итого за 6 семестр			28	10	28
Итого			90	10	100

1. Порядок выполнения самостоятельной работы

3.1 Методические рекомендации по изучению теоретического материала

Комплексное изучение предлагаемой студентам учебной дисциплины «Программно-аппаратные средства защиты информации» предполагает овладение материалами лекций, учебников, программы, творческую работу студентов в ходе проведения практических занятий, а также систематическое выполнение заданий для самостоятельной работы.

В ходе лекций раскрываются основные вопросы в рамках рассматриваемых тем, делаются акценты на наиболее сложные и интересные положения изучаемого материала,

которые должны быть приняты студентами во внимание. Материалы лекций являются основой для подготовки студентов к практическим занятиям.

Работа с конспектом лекций

Просмотрите конспект сразу после занятий. Отметьте материал конспекта лекций, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю.

Каждую неделю отводите время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам и тестам.

Выполнение практических занятий по дисциплине «Программно-аппаратные средства защиты информации»

На первом занятии получите у преподавателя задания по курсу, планы подготовки к практическим занятиям. Обзаведитесь всем необходимым методическим обеспечением.

Перед практическими занятиями изучите теорию вопроса, предполагаемого к исследованию, ознакомьтесь с опытом других исследователей в этом направлении.

Целью практических занятий является:

- закрепление методов приложения теории к решению практических задач анализа и синтеза психологического знания;
- проверка уровня понимания студентами вопросов, рассмотренных на лекциях и по учебной литературе, степени и качества усвоения материала;
- обучение навыкам освоения методики эксперимента и работы с нормативно-справочной литературой;
- восполнение пробелов в пройденной теоретической части курса и оказание помощи в его усвоении.

3.2 Методические рекомендации по написанию и оформлению доклада

1. Общие положения

1.1. Доклад, как вид самостоятельной работы в учебном процессе, способствует формированию навыков исследовательской работы, расширяет познавательные интересы, учит критически мыслить.

1.2. При написании доклада по заданной теме студент составляет план, подбирает основные источники.

1.3. В процессе работы с источниками систематизирует полученные сведения, делает выводы и обобщения.

1.4. К докладу по крупной теме могут привлекать несколько студентов, между которыми распределяются вопросы выступления.

2. Выбор темы доклада

2.1. Тематика доклада обычно определяется преподавателем, но в определении темы инициативу может проявить и студент.

2.2. Прежде чем выбрать тему доклада, автору необходимо выявить свой интерес, определить, над какой проблемой он хотел бы поработать, более глубоко ее изучить.

3. Этапы работы над докладом

3.1. Формулирование темы, причем она должна быть не только актуальной по своему значению, но и оригинальной, интересной по содержанию.

3.2. Подбор и изучение основных источников по теме (как правильно, при разработке доклада используется не менее 8-10 различных источников).

3.3. Составление списка использованных источников.

3.4. Обработка и систематизация информации

3.5. Разработка плана доклада.

3.6. Написание доклада.

3.7. Публичное выступление с результатами исследования.

4. Структура доклада:

- титульный лист

- оглавление (в нем последовательно излагаются названия пунктов доклада, указываются страницы, с которых начинается каждый пункт);

- введение (формулирует суть исследуемой проблемы, обосновывается выбор темы, определяются ее значимость и актуальность, указываются цель и задачи доклада, дается характеристика используемой литературы);

- основная часть (каждый раздел ее, доказательно раскрывая отдельную проблему или одну из ее сторон, логически является продолжением предыдущего; в основной части могут быть представлены таблицы, графики, схемы);

- заключение (подводятся итоги или дается обобщенный вывод по теме доклада, предлагаются рекомендации);

- список использованных источников

5. Структура и содержание доклада

5.1. Введение - это вступительная часть научно-исследовательской работы. Автор должен приложить все усилия, чтобы в этом небольшом по объему разделе показать актуальность темы, раскрыть практическую значимость ее, определить цели и задачи эксперимента или его фрагмента.

5.2. Основная часть. В ней раскрывается содержание доклада.

Как правило, основная часть состоит из теоретического и практического разделов. В теоретическом разделе раскрываются история и теория исследуемой проблемы, дается критический анализ литературы и показываются позиции автора. В практическом разделе излагаются методы, ход, и результаты самостоятельно проведенного эксперимента или фрагмента.

В основной части могут быть также представлены схемы, диаграммы, таблицы, рисунки и т.д.

5.3. В заключении содержатся итоги работы, выводы, к которым пришел автор, и рекомендации. Заключение должно быть кратким, обязательным и соответствовать поставленным задачам.

5.4. Список использованных источников представляет собой перечень использованных книг, статей, фамилии авторов приводятся в алфавитном порядке, при этом все источники даются под общей нумерацией литературы. В исходных данных источника указываются фамилия и инициалы автора, название работы, место и год издания.

5.5. Приложение к докладу оформляются на отдельных листах, причем каждое должно иметь свой тематический заголовок и номер, который пишется в правом верхнем углу, например: «Приложение 1»

6. Требования к оформлению доклада

6.1. Объем доклада может колебаться в пределах 5-15 печатных страниц; все приложения к работе не входят в ее объем.

6.2. Доклад должен быть выполнен грамотно, с соблюдением культуры изложения.

6.3. Обязательно должны иметься ссылки на используемую литературу.

6.4. Должна быть соблюдена последовательность написания библиографического аппарата.

7. Критерии оценки доклада

- актуальность темы исследования;
- соответствие содержания теме;
- глубина проработки материала; правильность и полнота использования источников;
- соответствие оформления доклада стандартам.

По усмотрению преподавателя доклады могут быть представлены на семинарах, научно-практических конференциях, а также использоваться как зачетные работы по пройденным темам.

3.3 Методические рекомендации по конспектированию первоисточников

Изучение и анализ литературных источников является обязательным видом самостоятельной работы студентов. Изучение литературы по избранной теме имеет своей задачей проследить характер постановки и решения определенной проблемы различными авторами, аргументацию их выводов и обобщений, провести анализ и систематизировать полученный материал на основе собственного осмысления с целью выяснения современного состояния вопроса.

Проработка отобранного материала обязательно должна идти с одновременным ведением записей прочитанного и своих замечаний. Запись может иметь как форму конспекта, так и выписок, а также картотеку положений, тезисов, идей, методик, что в дальнейшем облегчит классификацию и систематизацию полученного материала. Такого рода записи являются лучшим способом накопления и первичной обработки материала, одной из обязательных форм организации умственного труда.

Планом удобно пользоваться при подготовке к устному выступлению по выбранной теме. Каждый пункт плана должен раскрывать одну из сторон избранной темы, а весь план должен охватывать ее целиком.

Тезисы предполагают сжатое изложение основных положений текста в форме утверждения или отрицания. Они являются более совершенной формой записей и представляют основу для дискуссии. К тому же их легко запомнить.

Конспектирование – процесс мысленной переработки и письменной фиксации информации, в виде краткого изложения основного содержания, смысла какого-либо текста.

Результат конспектирования – запись, позволяющая конспектирующему немедленно или через некоторый срок с нужной полнотой восстановить полученную информацию. Конспект в переводе с латыни означает «обзор». По существу его и составлять надо как обзор, содержащий основные мысли текста без подробностей и второстепенных деталей. Конспект носит индивидуализированный характер: он рассчитан на самого автора и поэтому может оказаться малопонятным для других.

Для того чтобы осуществлять этот вид работы, в каждом конкретном случае необходимо грамотно решить следующие задачи:

1. Сориентироваться в общей композиции текста (уметь определить вступление, основную часть, заключение).
2. Увидеть логико-смысловую канву сообщения, понять систему изложения автором информации в целом, а также ход развития каждой отдельной мысли.
3. Выявить «ключевые» мысли, т. е. основные смысловые вехи, на которые «нанизано» все содержание текста.
4. Определить детализирующую информацию.
5. Лаконично сформулировать основную информацию, не перенося на письмо все целиком и дословно.

Во всяком научном тексте содержится информация 2-х видов: основная и вспомогательная. Основной является информация, имеющая наиболее существенное значение для раскрытия содержания темы или вопроса. К ней относятся: определения научных понятий, формулировки законов, теоретических принципов и т. д. Назначение вспомогательной информации – помочь читателю лучше усвоить предлагаемый материал. К этому типу информации относятся разного рода комментарии. Основную – записываем как можно полнее, вспомогательную, как правило, опускаем. Содержание конспектирования составляет переработка основной информации в целях ее обобщения и сокращения. Обобщить – значит представить ее в более общей, схематической форме, в виде тезисов, выводов, отдельных заголовков, изложения основных результатов и т. п. Читая, мы интуитивно используем некоторые слова и фразы в качестве опорных. Такие опорные слова и фразы называются ключевыми. Ключевые слова и фразы несут основную смысловую и эмоциональную нагрузку содержания текста.

Выбор ключевых слов – это первый этап смыслового свертывания, смыслового сжатия материала.

Важными требованиями к конспекту являются наглядность и обозримость записей и такое их расположение, которое давало бы возможность уяснить логические связи и иерархию понятий.

По форме конспекты подразделяются на формализованные и графические.

1. **Формализованные** (все записи вносятся в заранее подготовленные таблицы).

Это удобно, во-первых, при конспектировании материалов, когда перечень характеристик описываемых предметов или явлений более или менее постоянен, во-вторых, при подготовке единого конспекта по нескольким источникам. Особенно если есть необходимость сравнения отдельных данных. Разновидностью формализованного конспекта является запись, составленная в форме ответов на заранее подготовленные вопросы, обеспечивающие исчерпывающие характеристики однотипных предметов или явлений.

2. Графические (элементы конспектируемой работы располагаются в таком виде, при котором видна иерархия понятий и взаимосвязь между ними).

По каждой работе может быть не один, а несколько графических конспектов, отображающих книгу в целом и отдельные ее части. Ведение графического конспекта - наиболее совершенный способ изображения внутренней структуры книги, а сам этот процесс помогает усвоению ее содержания.

Можно выделить следующие основные **типы конспектов: плановый, текстуальный, сводный, тематический.**

Плановый – легко получить с помощью предварительно сделанного плана произведения, каждому вопросу плана отвечает определенная часть конспекта:

а) вопросно-ответный (на пункты плана, выраженные в вопросительной форме, конспект дает точные ответы);

б) схематичный плановый конспект (отражает логическую структуру и взаимосвязь отдельных положений).

Текстуальный – это конспект, созданный в основном из цитат.

Сводный конспект – сочетает выписки, цитаты, иногда тезисы; часть его текста может быть снабжена планом.

Тематический – дает более или менее исчерпывающий ответ (в зависимости из числа привлеченных источников и другого материала, например, своих же записей) на поставленный вопрос – тему: обзорный; хронологический.

Роль конспекта – чисто учебная: он помогает зафиксировать основные понятия и положения первичного текста и в нужный момент их воспроизвести, например, при написании реферата или подготовке к экзамену.

Способы конспектирования.

- **Тезисы** – это кратко сформулированные основные мысли, положения изучаемого материала. Тезисы лаконично выражают суть читаемого, дают возможность раскрыть содержание. Приступая к освоению записи в виде тезисов, полезно в самом тексте отмечать места, наиболее четко формулирующие основную мысль, которую автор доказывает (если, конечно, это не библиотечная книга). Часто такой отбор облегчается шрифтовым выделением, сделанным в самом тексте.

- **Линейно-последовательная запись текста.** При конспектировании линейно – последовательным способом целесообразно использование плакатно-оформительских средств, которые включают в себя следующие:

- сдвиг текста конспекта по горизонтали, по вертикали;
- выделение жирным (или другим) шрифтом особо значимых слов;
- использование различных цветов;
- подчеркивание;
- заключение в рамку главной информации.

- **Способ «вопросов – ответов».** Он заключается в том, что, поделив страницу тетради пополам вертикальной чертой, конспектирующий в левой части страницы самостоятельно формулирует вопросы или проблемы, затронутые в данном тексте, а в правой части дает ответы на них.

Одна из модификаций способа «вопросов – ответов» - таблица, где место вопроса занимает формулировка проблемы, поднятой автором (лектором), а место ответа – решение данной проблемы. Иногда в таблице могут появиться и дополнительные графы: например, «мое мнение» и т. п.

- **Схема с фрагментами** – способ конспектирования, позволяющий ярче выявить структуру текста, - при этом фрагменты текста (опорные слова, словосочетания, пояснения всякого рода) в сочетании с графикой помогают созданию рационально - лаконичного конспекта.

- **Простая схема** – способ конспектирования, близкий к схеме с фрагментами, объяснений к которой конспектирующий не пишет, но должен уметь давать их устно. Этот способ требует высокой квалификации конспектирующего. В противном случае такой конспект нельзя будет использовать.

- **Параллельный способ** конспектирования. Конспект оформляется на двух листах параллельно или один лист делится вертикальной чертой пополам и записи делаются в правой и в левой части листа.

Однако лучше использовать разные способы конспектирования для записи одного и того же материала.

Комбинированный конспект – вершина овладения рациональным конспектированием. При этом умело используются все перечисленные способы, сочетая их в одном конспекте (один из видов конспекта свободно перетекает в другой в зависимости от конспектируемого текста, от желания и умения конспектирующего). Именно при комбинированном конспекте более всего проявляется уровень подготовки и индивидуальность студента.

Принципы составления конспекта прочитанного.

1. Записать все выходные данные источника: автор, название, год и место издания. Если текст взят из периодического издания (газеты или журнала), то записать его название, год, месяц, номер, число, место издания.
2. Выделить поля слева или справа, можно с обеих сторон. Слева на полях отмечаются страницы оригинала, структурные разделы статьи или книги (названия параграфов, подзаголовки и т. п.), формулируются основные проблемы. Справа – способы фиксации прочитанной информации.

Один из видов чтения – углубленное – предполагает глубокое усвоение прочитанного и часто сохранение информации в целях последующего обращения к ней. Эффективность такого чтения повышается, если прочитанное зафиксировано не только в памяти, но и на бумаге. Психологи утверждают, что записанное лучше и полнее усваивается, прочнее откладывается в памяти. Установлено, что если прочитать 1000 слов и затем записать 50, подытоживающих прочитанное, то коэффициент усвоения будет выше, чем, если прочитать 10000 слов, не записав ни одного. Кроме того, при записи прочитанного формируется навык свертывания информации. И, наконец, чередование чтения и записывания уменьшает усталость, повышает работоспособность и производительность умственного труда.

1. Резюмирование.

Резюме – краткий итог прочитанного, содержащий его оценку. Резюме характеризует основные выводы книги, главные итоги.

Выбор языковых средств для построения резюме-выводов подчинен основной задаче свертывания информации: минимум языковых средств – максимум информации. Это обычно одно – три четких, кратких, выразительных предложения, раскрывающих, по мнению автора, самую суть описываемого объекта.

2. Аннотация.

Аннотация – краткая обобщенная характеристика печатной работы (книги, статьи), включающая иногда и его оценку. Это наикратчайшее изложение содержания первичного документа, дающее общее представление о теме.

Основное ее назначение – дать некоторое представление о книге (статье, научной работе) с тем, чтобы рекомендовать ее определенному кругу читателей или воспользоваться своими записями при выполнении работы исследовательского, реферативного характера. Поэтому аннотации не требуются изложения содержания произведения, в ней лишь перечисляются вопросы, которые освещены в первоисточнике (содержание этих вопросов не раскрывается). Аннотация отвечает на вопрос: «О чем говорится в первичном тексте?», дает представление только о главной теме и перечне вопросов, затрагиваемых в тексте первоисточника.

Текст аннотации не стандартизирован. В научной литературе можно встретить различные требования к составлению аннотаций. Например, текст справочной аннотации может включать следующие сведения:

- тип и название аннотируемого документа (монография, диссертация, сборник, статья и т. п.)
- задачи, поставленные автором аннотируемого документа
- метод, которым пользовался автор (эксперимент, сравнительный анализ, компиляция других источников)
- принадлежность автора к определенной научной школе или направлению
- структуру аннотируемого документа
- предмет и тему произведения, основные положения и выводы автора
- характеристику вспомогательных иллюстративных материалов, дополнений, приложений, справочного аппарата, включая указатели и библиографию.

3.4 Методические указания по подготовке к экзамену

Контроль и оценка знаний студентов является неотъемлемой составной частью учебно-воспитательного процесса в вузе. Экзаменационная сессия – самая ответственная пора в студенческой жизни: она является итогом большой работы студентов в семестре. Экзамен – это метод проверки знаний студентов по части или полному курсу учебной дисциплины, произведенный путем постановки устных или письменных вопросов. Он дает объективную официально фиксируемую оценку успехов студентов за определенный отрезок времени.

Экзамен преследует многогранную цель: во-первых, это – проверка знаний студента, во-вторых, они сами по себе являются важным звеном в овладении наукой, в-третьих, это продолжение учебного процесса; наконец, он имеет большое значение как фактор стимулирования глубокого изучения предмета.

Подготовка к экзамену состоит из двух взаимосвязанных этапов. Первый – систематический труд на протяжении семестра, учебного года, охватывающий все формы учебного процесса: лекции, изучение и конспектирование рекомендованной литературы, активное участие в семинарских (практических) и лабораторных занятиях.

Второй – подготовка непосредственно перед экзаменом. Она позволяет студентам за сравнительно короткий отрезок времени охватить всю перспективу изученного и лучше понять основные закономерности и явления.

Ограниченность времени (3-4 дня) для непосредственной подготовки к экзамену по предмету требует от студентов спокойно, без нервной суеты и спешки еще раз

внимательно продумать изученный в течение семестра материал, тщательно отработать вопросы, недостаточно изученные или плохо понятые, с тем, чтобы по возможности устранить все пробелы в своих знаниях.

Готовиться надо по строго продуманному графику, последовательно переходя от темы к теме, не пропуская ни одну из них.

Сложные вопросы, недостаточно уясненные в процессе подготовки к экзамену, необходимо записать и получить на них разъяснения у преподавателей во время предэкзаменационных консультаций.

Следует заметить, что студенты, которые не ходят на консультации из-за отсутствия, по их мнению, сложных вопросов, поступают опрометчиво. На консультациях очень часто лектор не только отвечает на заданные вопросы, но и по собственной инициативе разъясняет наиболее трудные разделы курса.

Итак, основной задачей подготовки студентов к экзамену является систематизация знаний учебного материала, его творческое осмысливание. Важнейшим учебным пособием на этом этапе работы студента является собственный конспект прослушанных лекций и самостоятельно проработанных тем курса.

В соответствии с положением об экзаменах их, как правило, принимают преподаватели, читающие курс лекций.

Получив билет, студент должен хорошо продумать содержание поставленных вопросов. Значительное число неудачных ответов объясняется неясным пониманием поставленной проблемы. Правильное понимание вопроса обеспечит успех при ответе на него. При подготовке к ответу на билет нужно составить развернутый план по каждому вопросу

Отвечая на вопросы экзаменационного билета, не следует спешить. Надо излагать материал спокойно, не торопясь, владеть собой, следить за построением фраз. Следует избегать подходов издали, общих рассуждений. Рекомендуются строить ответы четко, последовательно, конкретно, по возможности исчерпывающе. Вместе с тем весьма желательно быстро и правильно иллюстрировать свой ответ примерами.

От экзаменуемого требуется: определение понятий, обоснование выдвинутых положений, свободное оперирование фактическим материалом, дать альтернативные подходы по отдельным проблемам. Логичность, стройность, литературная грамотность изложения являются неотъемлемыми чертами полноценного ответа. Нельзя при ответе допускать ни излишней краткости, переходящей в схематизм, ни многословия. И то, и другое не оправдано. Краткость не дает преподавателю возможности понять, владеет ли студент учебным материалом, а многословие может показать, что студент не умеет акцентировать внимание на главном и говорит слишком расплывчато.

Вопросы для проверки уровня обученности

Базовый уровень

Знать:

1. Модель контроля целостности Кларка-Вилсона.
2. Модель безопасности на основе матрицы доступов HRU.
3. Модель распространения прав доступа TAKE-GRANT.
4. Модель системы безопасности Белла-Лападула.
5. Модель безопасности информационных потоков.
6. Модели нарушителя информационных систем.
7. Модели нарушения целостности программ и данных в электронно-вычислительных машинах.

8. Теория безопасных систем. ТСВ.
9. Политики безопасности. Домены безопасности. Основные типы.
10. Парольная защита Требования и атаки.
11. Криптографические методы защиты. Основные требования, модели, способы и реализации.
12. Асимметричное шифрование. Модели и алгоритмы.
13. Симметричное шифрование. Модели и алгоритмы.
14. Электронно-цифровая подпись. Модели, требования, атаки, способы обмана, реализация ЭЦП.
15. Криптографические атаки на схемы шифрования.
16. Критерии оценки безопасности компьютерных систем министерства обороны США («Оранжевая книга»).
17. Европейские критерии безопасности информационных технологий.
18. Федеральные критерии безопасности информационных технологий.
19. Руководящие документы Государственной Технической Комиссии при Президенте РФ.
20. Защита распределенных баз данных: транзакция, репликация, резервирование и другие особенности по надежности.
21. Общие положения криптографии. Имитостойкость, имитозащита.
22. Криптографические алгоритмы. Перемешивания и рассеивания. Подстановки.
23. Реализация шифров. Методы получения случайных и псевдослучайных чисел.
24. Блочные и поточные шифры на основе реализации требований ГОСТ 28147-99
25. Блочные и поточные шифры на основе симметричных криптографических алгоритмов.
26. Методы анализа симметричных криптосистем.
27. Методы криптоанализа несимметричных криптосистем
28. Протокол SSH.
29. Применение криптографических алгоритмов для обеспечения безопасности информации в информационных системах. Технология VPN.
30. Технологии WPA и WPA2.
31. Применение криптографических алгоритмов для обеспечения безопасности информации в информационных системах.
32. Основы технологии инфраструктуры открытых ключей.
33. Основные компоненты и сервисы ИОК.
34. Введение в компьютерные атаки. Модель атаки. Результат атаки.
35. Атаки с использованием промежуточных узлов и территорий.
36. Технологии обнаружения компьютерных атак и их возможности.
37. Модели нарушителей информационной безопасности
38. Модели угроз информационной безопасности
39. Программные закладки. Классификация, воздействие на компьютерную систему.
40. Методы защиты от программных закладок.

41. Методы защиты компьютерной системы от взлома.
42. Назначение межсетевых экранов.
43. Уровни сетевой модели, на которых применяется фильтрация пакетов.
44. Статическая и динамическая трансляция адресов.
45. Значение функции трансляции адресов с точки зрения обеспечения информационной безопасности.
46. Предотвращение взлома компьютерной системы на уровне СУБД
47. Предотвращение взлома компьютерной системы на уровне операционной системы.
48. Политика ИБ и политика СУИБ: сходства и различия.
49. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
50. Анализ рисков ИБ: основные понятия

Уметь, Владеть:

Задачи для проверки умений и навыков

- 1) Сформулируйте понятие виртуального сеанса.
- 2) Перечислите уровни сетевого стека TCP/IP, используемые при инспекции состояний.
- 3) Назовите состав основных параметров, которые должны содержаться в таблице состояний.
- 4) Указать, какое правило «по умолчанию» присутствует в расширенном списке доступа и отсутствует в рефлексивном.
- 5) Перечислите соответствия между классом межсетевого экрана и классом защищаемой им автоматизированной системы.
- 6) Укажите основные цели тестирования на проникновение.

Повышенный уровень:

Знать:

1. Цели и задачи процесса анализа рисков, роль процесса в рамках СУИБ.
2. Анализ рисков ИБ: основные подходы, основные этапы процесса.
3. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
4. Расследование инцидентов ИБ
5. Виды расследования инцидентов
6. Критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).
7. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
8. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках

СУИБ.

9. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.
10. Система инженерно-технической защиты информации
11. Организационная основа системы обеспечения информационной безопасности РФ
12. Источники угроз информационной безопасности.
13. Защита информации. Основные термины и определения

Уметь, Владеть:

Задачи для проверки умений и навыков

1. Разработать в эмуляторе модель распределенной сети с использованием межсетевого экрана ASA 5505 и технологии Frame Relay.
2. Разработать в эмуляторе модель распределенной сети с использованием межсетевого экрана ASA 5505 и технологии Ethernet.

Комплект разноуровневых задач и заданий

по дисциплине Программно-аппаратные средства защиты информации
при выполнении лабораторных работ

1. Тема 5. Развитие технологий межсетевого экранирования

Типовые задачи (всего 8 заданий):

Задания базового уровня:

- 1) Указать основное назначение межсетевых экранов.
- 2) Перечислить уровни сетевой модели, на которых применяется фильтрация пакетов.
- 3) Перечислить основные отличия статической и динамической трансляции адресов.
- 4) Указать значение функции трансляции адресов с точки зрения обеспечения информационной безопасности.
- 5) Перечислить основные параметры, которые обычно включаются в таблицу состояний.
- 6) Пояснить, в чем состоят особенности применения службы проху.

Задания повышенного уровня:

- 7) Разработать и реализовать в эмуляторе сегмент сети с использованием МСЭ без DMZ.
- 8) Разработать и реализовать в эмуляторе сегмент сети с использованием МСЭ и DMZ.

2. Тема 6. Списки контроля доступа.

Типовые задачи (всего 8 заданий):

Задания базового уровня:

9) Пояснить, могут ли быть применены списки контроля доступа для входящего и исходящего трафиков на одном интерфейсе маршрутизатора?

10) Пояснить, почему порядок правил в списке контроля доступом имеет важное значение.

11) Смоделировать в эмуляторе РТ создание и удаление списков контроля доступа.

12) Смоделировать в эмуляторе РТ прикрепление списка контроля доступа к интерфейсу маршрутизатора

13) Смоделировать в эмуляторе РТ прикрепление списка контроля доступа к интерфейсу межсетевого экрана.

14) Смоделировать в эмуляторе РТ прикрепление списка контроля доступа к виртуальному интерфейсу маршрутизатора

Задания повышенного уровня:

15) Настройте, примените и проверьте работу нумерованных стандартных ACL-списков.

16) Настройте, примените и проверьте работу стандартных именованных ACL-списков.

3. Тема 14. Протоколы VPN канального уровня.

Типовые задачи (всего 8 заданий):

Задания базового уровня:

17) Перечислить уровни стека протоколов TCP/IP, которые используются для создания VPN.

18) Перечислить основные типы конфигураций VPN.

19) Пояснить, что понимается под термином «туннелирование»

20) Назовите основные этапы формирования защищенного канала при использовании протокола L2TP.

21) Перечислить основные задачи, решаемые ассоциациями безопасности.

22) Перечислить основные различия транспортного и туннельного режимов

Задания повышенного уровня:

23) Провести в эмуляторе настройку маршрутизатора для реализации туннеля GRE.

24) Провести в эмуляторе настройку маршрутизатора для включения маршрутизации через туннель GRE.

4. Тема 15. Протокол IPSec.

Типовые задачи (всего 8 заданий):

Задания базового уровня:

25) Пояснить, возможно ли одновременное применение протоколов ESP и АН для организации защищенной связи.

26) Перечислить варианты защищенной связи, поддерживаемые протоколом IPSec.

27) Перечислить состав и назначение цифрового сертификата открытых

ключей.

28) Пояснить, для чего в уполномоченном центре ведутся списки отозванных сертификатов и отозванных полномочий?

29) Настроить isakmp, указав методы шифрования, хеширования, аутентификации, группы Диффи-Хелмана, lifetime соединения и идентификации.

30) Опишите процедуру создания IPSec туннеля между двумя межсетевыми экранами.

Задания повышенного уровня:

31) Создать в эмуляторе IPSec туннель между двумя Cisco ASA.

32) В эмуляторе настроить шифрование трафика от локальной сети LAN1 к PC1, расположенной в локальной сети LAN2.

5. Тема 16. Типы вредоносного ПО и защита от угроз.

Типовые задачи (всего 8 заданий):

Задания базового уровня:

33) Перечислить основные методы защиты компьютерных вирусов от обнаружения.

34) Дать определения полиморфизма и метаморфизма компьютерных вирусов.

35) Перечислить основные виды троянских коней.

36) Дать определение сетевого червя.

37) Перечислить основные методы защиты от обнаружения, применявшиеся червем Морриса.

38) Перечислить основные виды руткитов.

Задания повышенного уровня:

39). Разработать в программной среде C++ функцию тестирования ПСП на пропуски.

40) Разработать в программной среде Delphi функцию тестирования ПСП на равноб.

6. Тема 18. Атаки на сетевые протоколы и защита от них.

Типовые задачи (всего 8 заданий):

Задания базового уровня:

41) Перечислите основные угрозы при сетевом взаимодействии.

42) Пояснить, что понимается под удаленной сетевой атакой.

43) Перечислить основные типы сетевых атак и их особенности.

44) Пояснить, что понимается под уязвимостью и эксплойтом.

45) Пояснить взаимосвязь между атакой и сценарием атаки.

46) Перечислить основные шаги обобщенного сценария атаки.

Задания повышенного уровня:

47) Настроить на коммутаторе под управлением Cisco IOS режим безопасности портов с привязкой к MAC адресу конечного устройства

48). Настроить на коммутаторе под управлением Cisco IOS режим безопасности портов с привязкой к пулу MAC адресов

1. Тема 5. Развитие технологий межсетевого экранирования

Типовые задачи (всего 11 заданий):

Задания базового уровня:

- 49) Сформулируйте понятие виртуального сеанса.
- 50) Перечислите уровни сетевого стека TCP/IP, используемые при инспекции состояний.
- 51) Назовите состав основных параметров, которые должны содержаться в таблице состояний.
- 52) Указать, какое правило «по умолчанию» присутствует в расширенном списке доступа и отсутствует в рефлексивном.
- 53) Перечислите соответствия между классом межсетевого экрана и классом защищаемой им автоматизированной системы.
- 54) Укажите основные цели тестирования на проникновение.

Задания повышенного уровня:

- 55) Разработать в эмуляторе модель распределенной сети с использованием межсетевого экрана ASA 5505 и технологии Frame Relay.
- 56) Разработать в эмуляторе модель распределенной сети с использованием межсетевого экрана ASA 5505 и технологии Ethernet.

2. Тема 6. Списки контроля доступа.

Типовые задачи (всего 8 заданий):

Задания базового уровня:

- 57) Назовите возможные атаки при применении динамического списка контроля доступа.
- 58) Укажите назначение промежутка времени существования динамического списка контроля доступа.
- 59) Назовите основные отличия между рефлексивными списками контроля доступа и СВАС.
- 60) Перечислите диапазоны числовых значений для нумерованных простых и расширенных ACL.
- 61) Пояснить, почему скрытый запрет **deny any** или аналогичная явная запись ACL-списков, применённых на маршрутизаторах R1 и R3, не блокирует пакеты приветствия (hello) EIGRP и обновления маршрутизации.
- 62) Перечислите команды Cisco IOS, используемые для работы с ACL/

Задания повышенного уровня:

- 63) Настройте, примените и проверьте нумерованные расширенные ACL-списки.
- 64) Настройте, примените и проверьте именованные расширенные ACL-списки..

3. Тема 9. Модели систем обнаружения вторжений.

Типовые задачи (всего 8 заданий):

Задания базового уровня:

- 65) Перечислите задачи, выполняемые системами обнаружения аномалий протоколов.

66)Перечислить подходы, которые могут использоваться для определения «нормальности» поведения.

67)Дать определение понятия data mining.

68)Указать основные достоинства применения технологии агентов для обнаружения вторжений.

69)Перечислить подходы, которые используются для нахождения генетическими алгоритмами локальных максимумов.

70)Перечислить основные методы обхода систем обнаружения вторжений

Задания повышенного уровня:

71)Осуществить сбор сетевой статистики с использованием NagIOS.

72)Осуществить сбор сетевой статистики с использованием PRTG.

4. Тема 10. Обнаружение сигнатур.

Типовые задачи (всего 8 заданий):

Задания базового уровня:

73)Перечислить основные проблемы формирования сигнатур атак.

74)Дать определение понятий «атака» и «вторжение».

75)Пояснить, что характеризуют профили в модели Д. Деннинг.

76)Пояснить основное отличие между профилями и шаблонами профилей в модели Д. Деннинг.

77)Объясните наличие в модели CIDF двусторонних связей.

78)Пояснить, что включается в понятие «сигнатуры COB»

Задания повышенного уровня:

79)Настроить в модели сети с использованием эмулятора работу службы Syslog.

80)Настроить в модели сети с использованием эмулятора работу службы NTP.

5. Тема 14. Протоколы VPN канального уровня.

Типовые задачи (всего 8 заданий):

Задания базового уровня:

81)Пояснить механизм настройки RPTP на маршрутизаторе.

82)Пояснить механизм настройки L2TP на маршрутизаторе.

83)Пояснить механизм настройки PPPoE на маршрутизаторе.

84)Пояснить, что такое ACL и как происходит наследование разрешений NTFS.

85)Пояснить механизм инкапсуляции HDLC

86)Перечислить команды Cisco IOS для поиска и устранения неисправностей на канальном уровне.

Задания повышенного уровня:

87)Настроить на маршрутизаторах соединение PPP.

88)Настроить динамическую маршрутизацию на маршрутизаторах при использовании PPP.

6. Тема 18. Атаки на сетевые протоколы и защита от них.

Типовые задачи (всего 8 заданий):

Задания базового уровня:

89)Перечислить основные типы атак на протокол DHCP.

90)Перечислить основные типы атак на протокол TCP.

91)Перечислить основные типы атак на протокол ICMP.

92)Перечислить основные типы атак на протокол ARP.

93)Перечислить основные типы атак на протокол IP.

94)Перечислить основные типы атак на протокол UDP.

Задания повышенного уровня:

95)Настроить на коммутаторах режим безопасности портов, противостоящий атакам на DHCP

96)Настроить на коммутаторах режим безопасности портов, противостоящий атакам, связанным с переполнением MAC таблиц.

4.3 Вопросы для собеседования по темам лекций 1-18

Базовый уровень

1. Защита распределенных баз данных: транзакция, репликация, резервирование и другие особенности по надежности.
2. Общие положения криптографии. Имитостойкость, имитозащита.
3. Криптографические алгоритмы. Перемешивания и рассеивания. Подстановки.
4. Реализация шифров. Методы получения случайных и псевдослучайных чисел.
5. Блочные и поточные шифры на основе реализации требований ГОСТ 28147-99
6. Блочные и поточные шифры на основе симметричных криптографических алгоритмов.
7. Методы анализа симметричных криптосистем.
8. Методы криптоанализа несимметричных криптосистем
9. Протокол SSH.
10. Применение криптографических алгоритмов для обеспечения безопасности информации в информационных системах. Технология VPN.
11. Технологии WPA и WPA2.
12. Применение криптографических алгоритмов для обеспечения безопасности информации в информационных системах.
13. Основы технологии инфраструктуры открытых ключей.
14. Основные компоненты и сервисы ИОК.
15. Введение в компьютерные атаки. Модель атаки. Результат атаки.
16. Атаки с использованием промежуточных узлов и территорий.
17. Технологии обнаружения компьютерных атак и их возможности.
18. Модели нарушителей информационной безопасности
19. Модели угроз информационной безопасности
20. Программные закладки. Классификация, воздействие на компьютерную систему.

Повышенный уровень

21. Методы защиты от программных закладок.
22. Методы защиты компьютерной системы от взлома.
23. Назначение межсетевых экранов.
24. Уровни сетевой модели, на которых применяется фильтрация пакетов.
25. Статическая и динамическая трансляция адресов.
26. Значение функции трансляции адресов с точки зрения обеспечения информационной безопасности.
27. Предотвращение взлома компьютерной системы на уровне СУБД
28. Предотвращение взлома компьютерной системы на уровне операционной системы.
29. Политика ИБ и политика СУИБ: сходства и различия.
30. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
31. Анализ рисков ИБ: основные понятия

Вопросы к экзамену по дисциплине «Программно-аппаратные средства защиты информации»

Базовый уровень

Вопросы (задача, задание) для проверки уровня обученности

1. Модель контроля целостности Кларка-Вилсона.
2. Модель безопасности на основе матрицы доступов HRU.
3. Модель распространения прав доступа TAKE-GRANT.
4. Модель системы безопасности Белла-Лападула.
5. Модель безопасности информационных потоков.
6. Модели нарушителя информационных систем.
7. Модели нарушения целостности программ и данных в электронно-вычислительных машинах.
8. Теория безопасных систем. TCB.
9. Политики безопасности. Домены безопасности. Основные типы.
10. Парольная защита. Требования и атаки.
11. Криптографические методы защиты. Основные требования, модели, способы и реализации.
12. Асимметричное шифрование. Модели и алгоритмы.
13. Симметричное шифрование. Модели и алгоритмы.
14. Электронно-цифровая подпись. Модели, требования, атаки, способы обмана, реализация ЭЦП.
15. Криптографические атаки на схемы шифрования.
16. Критерии оценки безопасности компьютерных систем министерства обороны США («Оранжевая книга»).

17. Европейские критерии безопасности информационных технологий.
18. Федеральные критерии безопасности информационных технологий.
19. Руководящие документы Государственной Технической Комиссии при Президенте РФ.
20. Защита распределенных баз данных: транзакция, репликация, резервирование и другие особенности по надежности.
21. Общие положения криптографии. Имитостойкость, имитозащита.
22. Криптографические алгоритмы. Перемешивания и рассеивания. Подстановки.
23. Реализация шифров. Методы получения случайных и псевдослучайных чисел.
24. Блочные и поточные шифры на основе реализации требований ГОСТ 28147-99
25. Блочные и поточные шифры на основе симметричных криптографических алгоритмов.
26. Методы анализа симметричных криптосистем.
27. Методы криптоанализа несимметричных криптосистем. Протокол SSH.
28. Применение криптографических алгоритмов для обеспечения безопасности информации в информационных системах. Технология VPN.
29. Технологии WPA и WPA2.
30. Применение криптографических алгоритмов для обеспечения безопасности информации в информационных системах.
31. Основы технологии инфраструктуры открытых ключей.
32. Основные компоненты и сервисы ИОК.
33. Введение в компьютерные атаки. Модель атаки. Результат атаки.
34. Атаки с использованием промежуточных узлов и территорий.
35. Технологии обнаружения компьютерных атак и их возможности.
36. Модели нарушителей информационной безопасности
37. Модели угроз информационной безопасности
38. Программные закладки. Классификация, воздействие на компьютерную систему.
39. Методы защиты от программных закладок.
40. Методы защиты компьютерной системы от взлома.
41. Назначение межсетевых экранов.
42. Уровни сетевой модели, на которых применяется фильтрация пакетов.
43. Статическая и динамическая трансляция адресов.
44. Значение функции трансляции адресов с точки зрения обеспечения информационной безопасности.
45. Предотвращение взлома компьютерной системы на уровне СУБД
46. Предотвращение взлома компьютерной системы на уровне операционной системы.
47. Политика ИБ и политика СУИБ: сходства и различия.
48. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов

49. Анализ рисков ИБ: основные понятия

Основная литература:

1. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации Электронный ресурс / сост. И. А. Денисов. - Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации, 2022-04-04. - Москва : Московский технический университет связи и информатики, 2016. - 31 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 2227-8397
2. Платонов, В. В. Программно-аппаратные средства защиты информации : учебник для вузов / В.В. Платонов. - Москва : Академия, 2013. - 330, [1] с. : ил. ; 22. - (Высшее профессиональное образование. Информационная безопасность. Бакалавриат). - Библиогр.: с. 326-327. - ISBN 978-5-7695-9327-7

1. Ложников, П.С. Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft. Электронный ресурс : практикум / Е.М. Михайлов / П.С. Ложников. - Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft, 2020-07-28. - Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. - 264 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-4487-0080-4
2. Щеглов, А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов; под ред. М. В. Финкова. - СПб.: Наука и Техника, 2004. - 384 с. - (Профи). - Библиогр.: с. 383

Список литературы, рекомендуемый к использованию в самостоятельной работе студентов:

1. Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону : Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/237770>
2. Программно-аппаратные средства защиты информации : учебное пособие / Л. Х. Мифтахова, А. Р. Касимова, В. Н. Красильников [и др.]. — Санкт-Петербург : Интермедия, 2018. — 408 с. — ISBN 978-5-4383-0157-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/103200>

3. Ложников, П.С. Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft. Электронный ресурс : практикум / Е.М. Михайлов / П.С. Ложников. - Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft, 2020-07-28. - Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. - 264 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-4487-0080-4

4. Щеглов, А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов; под ред. М. В. Финкова. - Спб.: Наука и Техника, 2004. - 384 с. - (Профи).
- Библиогр.: с. 383

Интернет-ресурсы.