Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ»

В. В. ПОДТОПЕЛЬНЫЙ

БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Учебно-методическое пособие
по выполнению лабораторных работ по дисциплине
для студентов специальности 10.05.03
«Информационная безопасность автоматизированных систем»
специализация «Безопасность открытых информационных систем»

Калининград
Издательство ФГБОУ ВО «КГТУ»
2022

УДК 004.4 (075)

Рецензент

Доцент кафедры информационной безопасности института информационных технологий ФГБОУ ВО «Калининградский государственный технический университет» А. Г. Жестовский

Подтопельный, В. В.

Безопасность вычислительных сетей: учебно-методическое пособие по выполнению лабораторных работ по дисциплине для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» / В. В. Подтопельный – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. – 42 с.

Учебно-методическое пособие включает в себя рассмотрение практических вопросов в области защиты информации по дисциплине «Безопасность вычислительных сетей». В учебно-методическом пособии приведен список лабораторных работ для изучения и закрепления материала дисциплины. Представлены методические указания по изучению дисциплины. Пособие подготовлено в соответствии с требованиями утвержденной рабочей программы дисциплины.

Учебно-методическое пособие предназначено для студентов 4–5 курсов специальности 10.05.03 «Информационная безопасность автоматизированных систем» и смежных специальностей.

Учебно-методическое пособие рассмотрено и одобрено в качестве электронного методического материала кафедрой информационной безопасности 19 мая 2022 г., протокол № 7

Учебно-методическое пособие по изучению дисциплины рекомендовано к использованию в учебном процессе в качестве локального электронного методического материала методической комиссией института цифровых технологий ФГБОУ ВО «Калининградский государственный технический университет» 28 июня 2022 г., протокол № 4

УДК 004.4 (075)

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Данное учебно-методическое пособие предназначено для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация: «Безопасность открытых информационных систем», изучающих дисциплину «Безопасность вычислительных сетей».

Лабораторный практикум содержит 16 лабораторных работ.

В результате выполнения лабораторных работ студент должен:

знать:

– принципы построения и функционирования, примеры реализаций современных вычислительных сетей;

– функции средств защиты сетей;

– принципы организации и структуру подсистем защиты маршрутизаторов и маршрутизирующих протоколов;

уметь:

– использовать средства сетевой безопасности для обеспечения эффективного и безопасного функционирования автоматизированных систем;

– оценивать эффективность и надежность защиты вычислительных сетей;

– планировать политику безопасности вычислительных сетей;

владеть:

– навыками работы, восстановления вычислительных сетей после сбоев;

– навыками установки и настройки вычислительных сетей учетом требований по обеспечению информационной безопасности.

Программное обеспечение

1. Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription (срок действия: три года).

2. Программное обеспечение, распространяемое по лицензии GNU General Public License (лицензия на свободное программное обеспечение, созданная в рамках проекта GNU , по которой автор передаёт программное обеспечение в общественную собственность): операционная система Linux, ПО Virtual Box.

Критерии положительной оценки изложены в таблице 1.

Таблица 1. Шкала оценок уровня

Оценка			
неудовлетво-рительная	пороговая	углубленная	продвинутая
«2» (неудовлетво-рительно)	«3» (удовлетвори-тельно)	«4» (хорошо)	«5» (отлично)
Работа выполнена в полном объеме. Отчет не оформлен и представлен. При защите отчетных материалов правильные ответы даны менее чем на 50 % включительно. Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по работе	Работа выполнена в полном объеме. Отчет оформлен и представлен. При защите отчетных материалов правильные ответы на 51–64 % вопросов. Допускаются нарушения в последовательности изложения. Демонстрируются поверхностные знания вопроса. Имеются затруднения с выводами. Допускаются нарушения норм литературной речи	Работа выполнена в полном объеме. Отчет оформлен и представлен. При защите отчетных материалов правильные ответы на 65–94 % вопросов. Ответы на поставленные вопросы излагаются систематизировано и последовательно. Материал излагается уверенно. Демонстрируется умение анализировать материал, однако не все выводы носят аргументи-рованный и доказательный характер	Работа выполнена в полном объеме. Отчет оформлен и представлен. При защите отчетных материалов правильные ответы даны на 95–100 % вопросов. Ответы на поставленные в билете вопросы излагаются логично, последовательно и не требуют дополнительных пояснений. Делаются обоснованные выводы. Демонстрируются глубокие знания предмета

Лабораторная работа № 1
Cisco Packet Tracer

1. Цель работы

Целью лабораторной работы является освоение пакета «Cisco Packet Tracer», изучение его интерфейса и основных элементов, а также получение навыка создания сетей с дальнейшим их тестированием. В заключительной части работы необходимо собрать сеть, изображенную на рисунке, и проверить её работу.

Программное обеспечение: ОС Microsoft Windows XP/2003/ 2008R2/Vista/7/8/8.1/10/2012/2012R2, Cisco Packet Tracer

Теоретический материал

Сетевые технологии лучше всего изучать на практике, посредством подключения устройств к сетям и наблюдения соответствующих процессы. Инновационное средство визуализации и моделирования сетей Cisco Packet Tracer поможет надежно закрепить навыки конфигурирования – результаты вашей работы отображаются непосредственно на экране настольного или мобильного устройства. Packet Tracer поможет вам:

- закрепить свои навыки при подготовке к собеседованию;
- подготовиться к сертификационному экзамену;
- опробовать на практике знания, полученные в ходе учебных курсов;
- овладев необходимыми навыками, вы сможете приступить к построению карьеры в сфере Интернета вещей.

В данной лабораторной работе будут рассмотрены устройства, работающие на трех уровнях сетевой модели OSI: первый уровень OSI – физический, второй уровень – уровень передачи данных и третий уровень – сетевой.

Маршрутизатор или роутер (транслитерация английского слова) – специализированный сетевой компьютер, имеющий два или более сетевых интерфейса и пересылающий пакеты данных между различными сегментами сети. Маршрутизатор может связывать разнородные сети различных архитектур. Для принятия решений о пересылке пакетов используется информация о топологии сети и определённые правила, заданные администратором. Маршрутизаторы работают на сетевом (третьем) уровне сетевой модели OSI.

Сетевой мост или коммутатор (жарг. свич от англ. switch – переключатель) – устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. Коммутатор работает на канальном (втором) уровне модели OSI.

Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты.

В отличие от концентратора или хаба (1 уровень OSI), который распространяет трафик от одного подключённого устройства ко всем остальным, коммутатор передаёт данные только получателю (исключение составляет широковещательный трафик всем узлам сети и трафик для устройств, для которых неизвестен исходящий порт коммутатора). Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

Задание на лабораторную работу

1. Необходимо создать малую сеть, для этого понадобятся маршрутизаторы, сетевые коммутаторы и несколько компьютеров. В логической рабочей среде выберите маршрутизатор модели 1941.
2. Создайте коммутатор модели 2960 и соедините его с маршрутизатором кабелем «Copper Cross-Over». Все кабели находятся в группе со значком молнии. При соединении маршрутизатора и коммутатора необходимо выбирать гигабитный интерфейс.
3. Разместите точку доступа Wi-fi, один персональный компьютер и один ноутбук. Точки доступа Wi-fi находятся в разделе «Wireless Devices», компьютеры – во вкладке «End Devices». Выбирайте устройства модели «Generic»
4. Соедините устройства кабелем «Copper Straight-Through», как показано на. Необходимо подключать FastEthernet порты.
5. Показать успешную отправку PDU-пакета по сети.
6. Составить по проделанной работе отчет.

Контрольные вопросы

1. Что представляет собой пакет «Tracer»?
2. Что такое маршрутизатор?
3. Чем маршрутизатор отличается от сетевого коммутатора?
4. Как настроить обмен пакетами между маршрутизаторами?
5. Что означает цвет кружков на линии связи между двумя устройствами?
6. Какие есть способы настройки маршрутизации в пакете «Tracer»?
7. Для чего используется инструмент Inspect?
8. Какие рабочие среды (workspace) есть в пакете «Tracer» и для чего они нужны?
9. Как подключить ПК к сети в пакете «Tracer»?
10. Для чего нужен Serial DTE кабель?

Лабораторная работа № 2
Cisco Packet Tracer. Виртуальные локальные сети

Цель работы

Целью данной работы является изучение работы с VLAN в пакете «Tracer» от Cisco, создание и тестирование собственной VLAN. Будет рассмотрена настройка оборудования CISCO при помощи CLI (англ. Command Line Interface).

Программное обеспечение: ОС Microsoft Windows XP/2003/ 2008R2/Vista/7/8/8.1/10/2012/2012R2, Cisco Packet Tracer

Теоретический материал

Сетевые технологии лучше всего изучать на практике, посредством подключения устройств к сетям и наблюдения соответствующих процессы. Инновационное средство визуализации и моделирования сетей Cisco Packet Tracer поможет надежно закрепить навыки конфигурирования – результаты вашей работы отображаются непосредственно на экране настольного или мобильного устройства. Packet Tracer поможет вам:

- закрепить свои навыки при подготовке к собеседованию;
- подготовиться к сертификационному экзамену;
- опробовать на практике знания, полученные в ходе учебных курсов;
- овладев необходимыми навыками, вы сможете приступить к построению карьеры в сфере Интернета вещей.

VLAN (аббр. от англ. Virtual Local Area Network) – логическая («виртуальная») локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств

Широковещательный домен – область сети, в которой происходит обмен широковещательными сообщениями и устройства могут отправлять друг другу сообщения непосредственно, без участия маршрутизатора.

Задание на лабораторную работу

1. Ознакомиться с теорией.

2. Настроить правую часть сети самостоятельно, чтобы обе части могли через маршрутизаторы обмениваться данными, например, Комп 0 мог успешно отправить данные Комп 5.

3. После настройки подтвердить успешную отправку PDU пакета по сети.

Контрольные вопросы

1. Что такое VLAN?
2. Зачем используются VLAN?
3. Может ли компьютер, подключенный к VLAN 1, увидеть компьютер, подключенный к VLAN 2, без маршрутизатора?
4. Что такое CLI?
5. Как с помощью CLI можно задать адрес интерфейсу?
6. Зачем настраивают протокол RIP на маршрутизаторе?
7. Для чего используют режим интерфейса «access»?
8. Для чего используют режим интерфейса «trunk»?
9. За счет чего реализуется VLAN в Packet «Tracer»?
10. Как с помощью CLI сделать виртуальный интерфейс?

Лабораторная работа № 3
Одноранговые сети

Цель работы

Целью данной работы является получение навыков работы в локальных компьютерных сетях с ОС Windows.

Программное обеспечение: ОС Microsoft Windows XP/2003/ 2008R2/Vista/7/8/8.1/10/2012/2012R2, Cisco Packet Tracer

Теоретический материал

Одноранговая сеть – это сеть равноправных компьютеров, каждый из которых имеет уникальное имя и может иметь пароль для входа во время загрузки ОС. Имя компьютера и пароль входа назначаются владельцем компьютера средствами ОС. Каждый компьютер такой сети может одновременно являться и сервером, и клиентом сети, хотя допустимо назначение одного компьютера только сервером, а другого только клиентом.

Достоинством одноранговых сетей является их высокая гибкость: в зависимости от конкретной задачи сеть может использоваться очень активно, либо совсем не использоваться. Из-за большой самостоятельности компьютеров в таких сетях редко бывает ситуация перегрузки, тем более, что количество компьютеров в таких сетях обычно невелико. Установка одноранговых сетей довольно проста, для них не требуются дополнительные дорогостоящие серверы. Кроме того, нет необходимости в системном администрировании, пользователи могут сами управлять своими ресурсами.

В одноранговых сетях допускается определение различных прав пользователей на доступ к сетевым ресурсам, но система разграничения прав не слишком развита. Если каждый ресурс защищен своим паролем, то пользователю приходится запоминать большое число паролей.

К недостаткам одноранговых сетей относятся также слабая система контроля и протоколирования работы сети, трудности с резервным копированием распределенной информации. Выход из строя любого компьютера-сервера приводит к потере части общей информации, по возможности все компьютеры должны быть высоконадежными. Эффективная скорость передачи информации по одноранговой сети часто оказывается недостаточной, поскольку трудно обеспечить быстродействие процессоров, большой объем оперативной памяти и высокие скорости обмена с жестким диском для всех компьютеров сети. К тому же компьютеры сети работают не только на сеть, но и решают другие задачи.

Задание на лабораторную работу

Данная лабораторная работа выполняется на двух виртуальных машинах под управлением операционной системы Windows 7.

Для работы с рабочими группами на виртуальных машинах необходимо проверить, что в параметрах сетевого адаптера установлен пункт «Внутренняя сеть».

1. Создать рабочую группу из двух компьютеров.
2. Настроить общий доступ и проверить его работу.
3. Написать отчет по проделанной работе и защитить его у преподавателя.

Контрольные вопросы

1. Что такое одноранговая сеть?
2. Каковы достоинства и недостатки одноранговых сетей?
3. Что нужно сделать, чтобы создать рабочую группу?
4. Какое условие должно выполняться, чтобы компьютеры могли взаимодействовать?
5. Какую команду необходимо ввести в командной строке для просмотра компьютеров рабочей группы?
6. Что такое удаленный доступ?
7. Как настроить удаленный доступ?
8. Существуют ли альтернативные способы создания рабочей группы в вычислительных сетях Windows? Если да, то какие?
9. Как просмотреть компьютеры рабочей группы в графическом интерфейсе?
10. Как присоединить гостевую ОС к рабочей группе?

Лабораторная работа № 4
Настройка домена. Групповые политики

Цель работы

Целью данной работы является получение навыков работы в локальных компьютерных сетях с ОС Windows с доменной структурой и управления пользователями и компьютерами домена с помощью групповых политик безопасности домена.

Программное обеспечение: ОС Microsoft Windows XP/2003/ 2008R2/Vista/7/8/8.1/10/2012/2012R2, Cisco Packet Tracer

Теоретический материал

Доменом называется отдельная область безопасности в компьютерной сети Microsoft Windows.

В домене один или несколько компьютеров являются серверами.

Администраторы сети используют серверы для контроля безопасности и разрешений для всех компьютеров домена. Это позволяет легко изменять настройки, так как изменения автоматически производятся для всех компьютеров.

Пользователи домена должны указывать пароль или другие учетные данные при каждом доступе к домену. Если пользователь имеет учетную запись в домене, он может войти в систему на любом компьютере. Для этого не требуется иметь учетную запись на самом компьютере.

В домене могут быть тысячи компьютеров. Компьютеры могут принадлежать к различным локальным сетям. В каждом домене действует своя политика безопасности и свои отношения безопасности с другими доменами. Если несколько доменов связаны доверительными отношениями и имеют одни и те же схему, конфигурацию и глобальный каталог, их называют деревом доменов. Несколько деревьев доменов могут быть объединены в лес.

Под групповой политикой понимается совокупность параметров и настроек системы, определяющая конкретное окружение пользователя. Администратор может использовать механизм групповых политик для централизованного управления средой пользователей. Политика безопасности позволяет единообразно конфигурировать большое количество субъектов безопасности. Например, определить уровень доступа к системному реестру или задать порядок осуществления аудита событий.

Папка Мои документы традиционно рассматривается как место хранения пользовательских документов. Посредством механизма групповой

политики администратор может задать перенаправление всех обращений пользователей к этой папке на некоторый сетевой ресурс.

Параметры групповой политики хранятся в виде объектов групповой политики (Group Policy Object, GPO). Эти объекты хранятся в каталоге подобно другим объектам. Различают два вида объектов групповой политики – объекты групповой политики, создаваемые в контексте службы каталога, и локальные объекты групповой политики.

Локальные объекты групповой политики (Local Group Policy Object, LGPO) создаются в процессе установки операционной системы Windows и используются, если компьютер не включен в состав домена. Как только компьютер подключается к домену, компьютер и пользователь, работающий на нем, подпадают под действие объектов GPO, определенных в контексте данного домена.

Любой объект групповой политики может быть привязан к некоторому сайту, домену или подразделению, тогда параметры данного объекта групповой политики будут распространяться на все объекты службы каталога, зарегистрированные в данном контейнере. Один объект групповой политики может быть привязан к множеству контейнеров. Так же несколько объектов групповой политики могут быть привязаны к одному контейнеру.

Множество параметров, определяемых в рамках объекта групповой политики, разделено на две части: конфигурирование компьютера и конфигурирование среды пользователя. Конфигурирование компьютера предполагает определение значений для параметров, влияющих на формирование окружения любых пользователей, регистрирующихся на данном компьютере. Конфигурирование среды пользователя дает возможность управлять процессом формирования окружения конкретного пользователя, независимо от того, на каком компьютере он регистрируется в сети. Категории параметров групповой политики организованы в три контейнера в соответствии со своим назначением:

- Конфигурация программ. В контейнере размещаются категории параметров групповой политики, посредством которых можно управлять перечнем приложений, доступных пользователям.
- Конфигурация Windows. В контейнере размешаются категории параметров групповой политики, определяющие настройки непосредственно самой операционной системы. Содержимое данного контейнера может быть различным, в зависимости от того, определяются параметры групповой политики для пользователя или для компьютера.
- Административные шаблоны. Этот контейнер содержит категории параметров групповой политики, применяемых для управления содержимым системного реестра компьютера.

Задание на лабораторную работу

1. Задать серверу роль контроллера домена.

2. Присоединить рабочую станцию к домену.

3. Создать новый объект групповой политики и привязать его к созданному подразделению.

4. С помощью нового объекта групповой политики выполнить следующие действия:

- установить на рабочей станции приложение;
- задать ограничения на параметры парольной системы защиты;
- запретить запуск определенных программ на компьютере пользователя;
- настроить перенаправление папки «Мои документы» на одну из сетевых папок сервера;
- установить несколько административных шаблонов, запрещающих пользователю какие-либо действия

5. На рабочей станции проверить работу настроек, которые заданы в групповой политике.

6. Написать отчет и защитить его у преподавателя.

Контрольные вопросы

1. Что такое домен?

2. Сколько компьютеров может находиться в домене?

3. Что понимается под групповой политикой?

4. В чем различие между локальными политиками безопасности и групповыми политиками домена?

5. Какова структура объекта групповой политики, в какой последовательности применяются разделы объекта групповой политики?

6. Каково назначение административных шаблонов в групповой политике, как создать новый административный шаблон?

7. Для кого чего можно применять режимы планирования и ведения журналов?

8. Для чего нужен журнал паролей?

9. Что содержится в контейнере Конфигурация программ?

10. Что содержится в контейнере Конфигурация Windows?

Лабораторная работа № 5
Установка программного обеспечения через домен

Цель работы

Целью лабораторной работы является ознакомление с основными способами автоматизации установки программного обеспечения в локальной вычислительной сети при помощи Active Directory.

Программное обеспечение: ОС Microsoft Windows XP/2003/ 2008R2/Vista/7/8/8.1/10/2012/2012R2, Cisco Packet Tracer

Теоретический материал

Для централизованного управления средой пользователей используется механизм групповых политик. Под групповой политикой понимается совокупность параметров и настроек системы, определяющая конкретное окружение пользователя.

Групповые политики позволяют управлять настройками операционной системы. Все параметры операционной системы, определяющие ее функциональность, а также режимы работы ее служб и их настройки, хранятся в системном реестре. Посредством механизма групповой политики администратор может контролировать содержимое отдельных, наиболее важных ключей реестра.

С помощью групповой политики администратор может определить сценарии, которые будут выполняться при запуске и выключении компьютера, а также при входе пользователя в систему и выходе из нее.

Групповые политики могут применяться при определении параметров системы безопасности. С каждым пользователем или компьютером ассоциирован определенный набор настроек системы безопасности. Политика безопасности позволяет единообразно конфигурировать большое количество субъектов безопасности.

Управление приложениями также может осуществляться при помощи групповых политик. Используя механизм групповой политики, администратор может назначать и публиковать приложения, выполнять их централизованное обновление и восстановление

Задание на лабораторную работу

1. Изучить теоретические сведения.

2. С помощью групповых политик установить программное обеспечение на рабочую станцию, обновить его и проверить правильность работы.

3. Написать отчет и защитить его у преподавателя.

Контрольные вопросы

1. Какие недостатки имеет способ установки программного обеспечения при помощи групповой политики на компьютеры в организации?
2. Как вы думаете, для чего может понадобиться установка программ при помощи групповой политики?
3. Объясните, что из себя представляют публичный, назначенный и особый методы развертывания программ?
4. Как проходит установка программ с помощью групповой политики?
5. Как проходит удаление программ с помощью групповой политики?
6. Существуют ли другие методы установки ПО в организации? Если да, то какие?
7. Есть ли какие-то особенности назначенного способа развертывания программ? Если да, то какие?
8. Какие есть варианты удаления приложений?
9. Почему нужно указывать полный путь к месту расположения загрузочного файла?
10. Зачем нужно открывать общий доступ к папке с загрузочными файлами?

Лабораторная работа № 6
Обновление программного обеспечения и операционной системы

Цель работы

Целью данной работы является овладение основными способами обновления программного обеспечения при помощи программного продукта SUMo, предназначенного для обновления всего программного обеспечения на компьютере пользователя. Будут получены навыки обновления ОС Windows посредством службы Windows Server Update Services (WSUS), предназначенной для централизованного управления обновлениями и исправлениями корпоративных продуктов Microsoft.

Программное обеспечение: ОС Microsoft Windows XP/2003/ 2008R2/Vista/7/8/8.1/10/2012/2012R2, Cisco Packet Tracer

Теоретический материал

SUMo (Software Update Monitor) – это бесплатная утилита, работающая под управлением операционной системы Windows, которая позволяет

пользователям производить мониторинг обновлений для программного обеспечения, установленного на компьютере.

SUMo предоставляет простой и интуитивно понятный графический интерфейс, оснащённый многоязычной поддержкой для отслеживания в сети наличия новых версий для установленного программного обеспечения.

Утилита детально сканирует систему и выводит список всех программ, а также номера их версий и сведения о разработчиках.

SUMo может проверять наличие обновлений сразу для всех, или только для выборочных программ, без их предварительного запуска, и в случае обнаружения в сети более новой версии выводит окно с предложением обновить программу, предоставляя ссылку для её загрузки.

Возможности SUMo:

– автоматическое определение установленного программного обеспечения;

– обнаружение необходимых обновлений/патчей/бета-версий;

– чёрный список (отслеживает только необходимые конкретные релизы программного обеспечения);

– интернациональная поддержка;

– по заявлению пользователей имеет хорошую совместимость и выдаёт ложные обновления реже, чем другие утилиты для мониторинга обновлений.

Windows Server Update Services (WSUS) – сервер обновлений вычислительных сетей и продуктов Microsoft. Программа бесплатно может быть скачана с сайта Microsoft и установлена на серверную ОС семейства Windows Server. Сервер обновлений синхронизируется с сайтом Microsoft, скачивая обновления, которые могут быть распространены внутри корпоративной локальной сети. Это экономит внешний трафик компании и позволяет быстрее устанавливать исправления ошибок и уязвимостей в вычислительных сетейах Windows на рабочих местах, а также позволяет централизованно управлять обновлениями серверов и рабочих станций.

Задание на лабораторную работу

Работа с программой SUMo

До начала работы с программой SUMo необходимо войти в систему с правами администратора. Для запуска программы на рабочем столе найдите папку sumo и запустите приложение.

При первом запуске SUMo проверяет весь компьютер и собирает сведения обо всех установленных программах и их версиях, затем сравнивает номера версий с данными из базы данных, находящейся на сервере разработчиков. Если номер версии программы, установленной на компьютере пользователя, меньше максимальной в базе данных на сервере, то SUMo предложит обновить эту программу.

1. Изучить теоретические сведения.

2. Задать серверу роль контроллера домена.

3. Присоединить рабочую станцию к домену.

4. Создать новый объект групповой политики и привязать его к созданному подразделению.

5. С помощью нового объекта групповой политики выполнить следующие действия:

- установить на рабочей станции приложение;
- задать ограничения на параметры парольной системы защиты;
- запретить запуск определенных программ на компьютере пользователя;
- настроить перенаправление папки «Мои документы» на одну из сетевых папок сервера;
- установить несколько административных шаблонов, запрещающих пользователю какие-либо действия

6. На рабочей станции проверить работу настроек, которые заданы в групповой политике.

7. Написать отчет и защитить его у преподавателя.

Контрольные вопросы

1. Для чего предназначена программа SUMo?
2. Каковы функции программы SUMo?
3. Что такое WSUS?
4. Какие есть значения у параметра «Настройка автоматического обновления»?
5. Зачем нужно было приостанавливать службу Sqlservr?
6. Какие группы компьютеров имеются по умолчанию в среде WSUS?
7. Как создать тестовую группу?
8. Как назначить компьютер в тестовую группу?
9. Для каких узлов отображается сводный отчет о состоянии обновлений?
10. Для чего нужны отчеты об обновлениях?

Лабораторная работа № 7
Высокоуровневые службы

Цель работы

Целью данной работы является изучение теоретических сведения о высокоуровневых службах и получение практических навыков в их установке и настройке.

Программное обеспечение: ОС Microsoft Windows XP/2003/ 2008R2/Vista/7/8/8.1/10/2012/2012R2, Cisco Packet Tracer

Теоретический материал

Веб-сервер – это сервер, принимающий HTTP-запросы от клиентов и выдающий им HTTP-ответы, обычно вместе с запрошенными ресурсами. Веб-сервером называют как программное обеспечение, выполняющее функции веб-сервера, так и непосредственно компьютер, на котором это программное обеспечение работает. Клиент, которым обычно является веб-браузер, передаёт веб-серверу запросы на получение ресурсов, обозначенных URL-адресами. Ресурсы – это HTML-страницы, изображения, файлы, медиа-потоки или другие данные, которые необходимы клиенту. В ответ веб-сервер передаёт клиенту запрошенные данные. Этот обмен происходит по протоколу HTTP.

Веб-серверы могут иметь различные дополнительные функции, например:

- автоматизация работы веб страниц;
- ведение журнала обращений пользователей к ресурсам;
- аутентификация и авторизация пользователей;
- поддержка динамически генерируемых страниц;
- поддержка HTTPS для защищённых соединений с клиентами.

В качестве HTTP сервера могут использоваться такие программные продукты, как Apache, IIS, ngnix.

FTP-сервер – это удаленный компьютер, с файловой системой которого можно работать через специальный одноименный протокол. Протокол FTP – один из стандартных протоколов передачи данных через Интернет, он позволяет переносить файлы с одного компьютера на другой. Чтобы установить соединение и обменяться файлами в Интернете, согласно протоколу FTP, необходимо запустить специальную прикладную программу, называемую клиентской частью FTP. Клиентское программное обеспечение устанавливается вместе с коммуникационными утилитами TCP/IP. FTP-клиент – программа, позволяющая подключаться к удаленному FTP-серверу и получать/передавать файлы по протоколу FTP. Получить доступ к другому компьютеру для обмена файлами можно, указав пользовательское имя и пароль.

При работе с FTP широко используются два понятия: скачивание и закачивание. Скачивание (download) означает процесс сохранения папок и файлов с FTP-сервера на ваш компьютер. Закачивание (upload) – это передача папок и файлов с вашего компьютера на FTP-сервер. Обычно каждой папке (реже – файлу) на FTP-сервере назначают права доступа: чтение, запись и выполнение. Право на чтение означает, что вы можете просматривать файл

или содержимое папки. Право на запись позволяет изменять содержимое файлов. Право на выполнение даёт возможность запускать исполняемые файлы и скрипты на сервере. С управлением правами доступа вы можете столкнуться, например, при разработке веб-сайта, когда посетителям нужно запретить доступ в одни каталоги сайта и разрешить выполнение скриптов из других каталогов. Для FTP-сервера наиболее распространенным программным продуктом является FileZilla.

Почтовым сервером (сервером электронной почты) в системе пересылки электронной почты называют агент пересылки сообщений (mail transfer agent, MTA). Это компьютерная программа, которая передаёт сообщения от одного компьютера к другому. Обычно почтовый сервер работает «за кулисами», а пользователи имеют дело с другой программой – клиентом электронной почты (англ. mail user agent, MUA).

Когда пользователь набрал сообщение и отправляет его получателю, почтовый клиент взаимодействует с почтовым сервером, используя протокол SMTP. Почтовый сервер отправителя взаимодействует с почтовым сервером получателя (напрямую или через промежуточный сервер – релей). На почтовом сервере получателя сообщение попадает в почтовый ящик, откуда при помощи агента доставки сообщений (mail delivery agent, MDA) доставляется клиенту получателя. Часто последние два агента совмещены в одной программе (к примеру, sendmail), хотя есть специализированные MDA, которые в том числе занимаются фильтрацией спама. Для финальной доставки полученных сообщений используется не SMTP, а другой протокол – POP3 или IMAP, который также поддерживается большинством почтовых серверов. Хотя в простейшей реализации MTA достаточно положить полученные сообщения в личный каталог пользователя в файловой системе центрального сервера («почтовый ящик»).

В качестве почтового сервера используются такие программные продукты, как Exchange Server, Courier Mail Server или Office mail Server (для ОС семейства Windows); для Unix-подобных ОС – sendmail или сочетание exim (MTA) и dovecot (MDA). В данной лабораторной работе рассматривается IIS (Internet Information Services) – проприетарный набор серверов для нескольких служб Интернета от компании Майкрософт. IIS распространяется с операционными системами семейства Windows NT. Основным компонентом IIS является веб-сервер, который позволяет размещать в Интернете сайты. IIS поддерживает протоколы HTTP, HTTPS, FTP, POP3, SMTP, NNTP

Задание на лабораторную работу

1. Изучить теоретические сведения.
2. Создать Web-сервер. Проверить его работу.
3. Настроить FTP-сервер и проверить его работу.

4. Создать почтовый сервер. Изучить его работу.

5. Написать отчет и защитить его у преподавателя.

Контрольные вопросы

1. Что такое HTTP-сервер?

2. Что из себя представляет клиент для HTTP-сервера?

3. Приведите примеры программных продуктов, которые можно использовать в качестве HTTP-серверов?

4. Что такое FTP-сервер?

5. Что такое почтовый сервер?

6. Что такое MTA и MDA?

7. Что такое IIS? Каким образом устанавливается?

8. Какие протоколы поддерживает IIS?

9. Почему письма не отображаются во «Входящих», пока не пройдет синхронизация с сервером? В чем особенность протокола POP3?

10. Какой каталог предназначен для работы с Веб-сервером по умолчанию?

Лабораторная работа № 8
Настройка операционной системы Cisco IOS

Цель работы: целью лабораторной работы является обучение методам и средствам первоначальной настройки специализированной ОС Cisco IOS, под управлением которой работают маршрутизаторы.

Программное обеспечение: ОС Microsoft Windows XP/2003/ 2008R2/Vista/7/8/8.1/10/2012/2012R2, Cisco Packet Tracer

Теоретический материал

Cisco IOS – это специализированная ОС, обеспечивающая функционирование сетевого оборудования компании «Cisco Systems, Inc». Взаимодействие с данной ОС возможно либо через webбраузер, либо через интерфейс командной строки (CLI-интерфейс). Данная ОС поддерживает удаленный доступ к интерфейсу командной строки по протоколам Telnet или SSH. В Cisco IOS существует несколько режимов.

Пользовательский режим (user mode) – стандартный режим первоначального доступа к ОС. В этот же режим ОС переходит автоматически при продолжительном отсутствии ввода в режиме администратора. В режиме пользователя доступны только простые команды, не влияющие на конфигурацию оборудования. Приглашение командной строки имеет следующий вид: router>

Административный режим (privileged mode). Открывается командой *enable*, введенной в режиме пользователя:

router> **enable**

В административном режиме доступны команды, позволяющие получить полную информацию о конфигурации оборудования и его состоянии, а также команды перехода в режим конфигурирования, команды сохранения и загрузки конфигурации. Приглашение командной строки имеет следующий вид:

router#

Обратный переход в пользовательский режим производится по команде *disable* или по истечении установленного времени неактивности. Завершение сессии – команда *exit*.

Глобальный режим конфигурирования (конфигурационный режим). Активизируется командой *config terminal*, введенной в административном режиме:

router# **configure terminal**

Глобальный режим конфигурирования организован иерархически – он содержит как непосредственно команды конфигурирования оборудования, так и команды перехода в режимы конфигурирования его подсистем (например, интерфейсов, протоколов маршрутизации, механизмов защиты).

Приглашения командной строки в наиболее часто используемых конфигурационных режимах имеют следующий вид:

router(config)# router(config-if)#

rounter(config-router)# router(config-ext-nacl)# switch(config-

line)# switch(vlan)#

Выход из любого режима конфигурирования в режим верхнего уровня производится командой *exit* или комбинацией клавиш *Ctrl-Z*. Кроме того, команда *end*, поданная в любом из режимов конфигурирования немедленно завершает процесс конфигурирования и возвращает пользователя в администраторский режим.

Любая команда изменения конфигурации вступает в действие немедленно после ввода. Все команды и параметры могут быть сокращены (например, "*enable*" – "*en*", "*configure terminal*" – "*conf t*", "*show running-config*" – "*sh run*").

В любом месте командной строки для получения помощи может быть использован вопросительный знак, например: router#**?** router#**co?** router#**conf ?**

Имена сетевых интерфейсов также могут быть сокращены, например, вместо "*fast ethernet*0/1" достаточно написать "*fa*0/1".

Отмена любой команды (отключение опции или режима, включаемых командой, снятие или удаление параметров, назначаемых командой) производится подачей этой же команды с префиксом "*no*", например:

router(config)#**int fa0/1** router(config-if)#**shutdown** router(config-if)#**no shutdown**

При загрузке сетевого оборудования, работающего под управлением Cisco IOS, происходит считывание команд конфигурации из изменяемого постоянного запоминающего устройства (NVRAM), где они хранятся в виде текстового файла, называемого *рабочей конфигурацией* (running config). Конфигурация, сохраненная в NVRAM, называется *начальной конфигурацией* (startup config). В процессе работы оборудования администратор может вводить дополнительные конфигурационные команды, в результате чего рабочая конфигурация становится отличной от начальной.

Просмотр начальной и рабочей конфигураций маршрутизатора производится в административном режиме: router#**show startup-config** router#**show running-config**

Вывод последней команды позволяет просмотреть текущую конфигурацию. Однако если администратор не менял значения параметров, используемых в ОС по умолчанию, то они при выводе не отобразятся.

При копировании одной конфигурации поверх другой возможны два варианта: перезапись и слияние. При перезаписи старая конфигурация предварительно удаляется. При слиянии команды новой конфигурации добавляются к командам старой, как если бы они вводились вручную.

Ниже приведен список команд копирования конфигурации, первая из которых выполняется в режиме перезаписи, а последняя в режиме слияния:

router#**copy running-config startup-config** router#**copy startup-config running-config**

Рассмотрим базовые команды получения информации о работе оборудования и его подсистем.

Просмотр информации об оборудовании (модель, объемы памяти, версия IOS, число и тип интерфейсов) выполняется по следующей команде:

router#**show version**

Просмотр содержимого флэш-памяти: router#**show flash:**

Мониторинг загрузки процессора: router#**show processes**

Рассмотрим основные команды первоначальной конфигурации маршрутизатора.

Установить имя маршрутизатора:

router(config)#**hostname** *my_router*

Установить пароль администратора, требуемый при переходе в вводе команды *enable*:

router(config)#**enable secret** *my_secret* Отключение разрешения DNS-имен:

router(config)#**no ip domain-lookup**

Базовая настройка FastEthernet-интерфейса: router#**configure terminal** router(config)#**interface fastEthernet 0/1** router(config-if)#**ip address**

192.168.0.1

255.255.255.0 router(config-if)#**speed 100** router(config-if)#**duplex full** router(config-if)#**no shutdown** router(config-if)#**exit**

Для последовательного интерфейса устройства, выполняющего роль DCE, необходимо указывать тактовую частоту (пропускную способность), при этом данная команда выполняется только на одной стороне линии связи:

router(config)#**interface serial0** router(config-if)#**clock rate 125000**

Если на последовательном интерфейсе необходимо использовать другой протокол 2-го уровня (например, Frame Relay), то это делается с помощью команды:

router(config-if)#**encapsulation frame-relay**

Параметры интерфейсов, протоколов 2-го уровня, а также статистика отправленных и полученных кадров может быть просмотрена следующей командой в режиме администратора:

router#**show interface**

Подробная информация о параметрах протокола IP доступна в режиме администратора по команде:

router#**show ip interface** *interface*

Краткая сводная таблица состояний IP-интерфейсов: router#**show ip interface brief**

Рассмотрим настройку статической маршрутизации. Маршруты, ведущие в сети, к которым маршрутизатор подключен непосредственно, автоматически добавляются в маршрутную таблицу после конфигурирования интерфейса при условии, что интерфейс корректно функционирует.

Для назначения дополнительных статических маршрутов в режиме глобальной конфигурации вводится команда:

router(config)#**ip route** *prefix mask ip_address* Маршрут по умолчанию (стандартный маршрут) назначается следующей командой:

router(config)#**ip route** 0.0.0.0 0.0.0.0 *ip_address*

Просмотреть таблицу маршрутов можно по команде: router#**show ip route**

Задание на лабораторную работу

Выполнить первоначальную настройку сетевых параметров ОС Cisco IOS маршрутизатора Cisco 2811 с рабочей станции администратора сети, используя данные в таблице 2:

Таблица 2. **Параметры настройки маршрутизатора**

Параметр	*Значение*
IP-адрес интерфейса Fa0/0	10.194.7.1/24
IP-адрес интерфейса Fa0/1	192.168.100.26/30
Стандартный шлюз	192.168.100.25
Имя маршрутизатора	R7
Домен	net.bank
Пароль доступа enable	xkld7Hn434!2&^
Локальный пользователь/пароль	noc/nTefa#51

Контрольные вопросы

1. Разработать шаблон конфигурационного файла маршрутизатора для удобства настройки, включить в него основные изученные команды.
2. Предложить набор учетных записей и прав доступа для эксплуатации маршрутизаторов в крупной корпоративной сети.
3. Изучить порядок наименование модулей линейных карт и сетевых интерфейсов на маршрутизаторах и коммутаторах Cisco.

Лабораторная работа № 9
Защита инфраструктуры маршрутизации

Цель работы: целью лабораторной работы является обучение методам и средствам проектирования и защиты инфраструктуры маршрутизации отказоустойчивых иерархических компьютерных сетей на основе протокола маршрутизации OSPF.

Программное обеспечение: ОС Microsoft Windows XP/2003/ 2008R2/Vista/7/8/8.1/10/2012/2012R2, Cisco Packet Tracer

Теоретический материал

Маршрутизация является одной из критически важных задач, обеспечивающей корректное функционирование, доступность, надежность и отказоустойчивость компьютерной сети. Выделяют следующие угрозы нарушения безопасности маршрутизации:

– угрозы, направленные на сеансы обмена маршрутной информацией: сброс TCP-сессий, исчерпание ресурсов;

– угрозы, направленные на маршрутизирующие сетевые устройства: отказ в обслуживании, подбор паролей, переполнение буфера, повышение привилегий;

– угрозы, направленные на маршрутную информацию: внедрение ложных маршрутов, создание циклов, удаление корректных маршрутов, чтение маршрутной информации, раскрытие параметров маршрутизации.

– Для защиты инфраструктуры маршрутизации СПД используются следующие основные методы:

– управление распространением маршрутной информации с применением фильтров маршрутизации, управление обменом маршрутной информацией между узлами и процессами маршрутизации;

– ограничение множества систем, использующих протоколы маршрутизации, использование методов аутентификации, ограничение сеансов маршрутизации только доверенными узлами;

– регистрация событий маршрутизации, регистрация изменения состояний сеансов маршрутизации со смежными или соседними узлами.

Рассмотрим команды настройки, реализующие базовые методы защиты инфраструктуры маршрутизации.

Настройка аутентификации маршрутизаторов по алгоритму MD5 выполняется следующими командами:

interface Ethernet0/1 ip ospf message-digest-key 10 md5 *mysecret* **ip ospf authentication message-digest** Назначение интерфейсов маршрутизатора, по которым не распространяется маршрутная информация, выполняется командами:

router ospf 10 passive interface Ethernet 0/0

или командами:

router ospf 10 passive interface default no passive interface Ethernet 0/0

Включение регистрации событий маршрутизации выполняется командами:

router ospf 10 log-adjacency-changes

Задание на лабораторную работу

На маршрутизаторах СПД выполнить настройки протокола OSPF, обеспечивающие корректную работу сети и защиту инфраструктуры маршрутизации.

Контрольные вопросы

1. Определить в схеме СПД механизмы и средства обеспечения отказоустойчивости и масштабирования. Перечислить задачи, решаемые на каждом уровне иерархической модели данной СПД.

2. Найти и изучить описание всех команд, используемых для настройки протокола OSPF.

3. Для каждого маршрутизатора определить его характеристики, роли и свойства в рамках протокола OSPF.

Лабораторная работа № 10
Защита инфраструктуры коммутации

Цель работы: целью лабораторной работы является обучение методам и средствам защиты инфраструктуры коммутации при использовании технологии виртуальных ЛВС (VLAN), их настройке и маршрутизации**.**

Теоретический материал

Виртуальная ЛВС или *VLAN* – широковещательный домен второго уровня. Порты коммутаторов, принадлежащие одной VLAN, могут обмениваться кадрами между собой, но не могут обмениваться кадрами с портами других VLAN.

Для централизованного управления VLAN на коммутаторах может быть использован протокол VTP.

Для передачи кадров нескольких VLAN между коммутаторами используются *магистральные соединения,* или *транки*.

Порты коммутаторов, образующие магистральный канал, называются *магистральными,* или *транковыми* портами. На магистральных портах (в отличие от портов доступа) производится идентификация и инкапсуляция кадров VLAN с помощью протоколов ISL или IEEE 802.1Q.

Для динамического создания магистрального канала между коммутаторами может использоваться протокол DTP. Порты коммутатора, передающие кадры только одной VLAN, называются *портами доступа* (access port). Как правило, по умолчанию все порты коммутаторов являются портами доступа и находятся в VLAN с номером 1, называемой *собственной* или *стандартной* VLAN (native VLAN). Для собственных VLAN не применяются никакие протоколы инкапсуляции.

Различают статические и динамические VLAN. В *статических VLAN* назначение порта осуществляется администратором на этапе настройки коммутатора. В *динамических* VLAN назначение порта осуществляется по некоторому протоколу и, как правило, на основе MAC-адреса узла сети. В настоящее время в основном используются статические VLAN.

Компьютеры, находящиеся в разных VLAN могут обмениваться данными только через маршрутизатор (или любое другое устройство уровня L3), имеющий интерфейсы в этих VLAN. Такие VLAN называются маршрутизируемыми, иначе – изолированными.

В настоящее время рекомендуется использовать следующие принципы при создании и настройке защищенных коммутируемых ЛВС:

1. Не использовать для распространения информации об используемых VLAN в ЛВС протокол VTP (включать режим transparent).

2. В качестве протокола инкапсуляции использовать протокол IEEE 802.1Q.

3. Запретить передавать кадры собственной VLAN по магистральным каналам. В качестве native VLAN использовать специально для этого выделенную VLAN, не используемую ни для каких других целей.

4. Не использовать стандартную VLAN 1 в ЛВС ни для каких целей, особенно для управления сетевым оборудованием.

5. На магистральных портах использовать только необходимые VLAN – VLAN, которым принадлежат порты коммутаторов на другой стороне. Все другие VLAN запрещать.

6. Не использовать одинаковые VLAN на разных коммутаторах. Наиболее предпочтительный вариант проектирования – один коммутатор, одна VLAN, одна IP-подсеть.

7. Все неиспользуемые порты коммутатора переводить в режим shutdown и назначать их в специально созданную для этого немаршрутизируемую и изолированную VLAN.

8. На портах доступа отключать использование протокола DTP. Для минимизации времени восстановления функционирования системы при подключении канала на магистральных портах устанавливать протокол DTP в режимах On/On и Nonegotiate (отключать согласование).

2. Задание на лабораторную работу

ЛВС филиала банка построена на базе двух коммутаторов уровня доступа филиала Cisco Catalyst 2960 (SW4-2, SW4-3), коммутатора уровня ядра-распределения филиала Cisco Catalyst 3560 (SW4-1) и маршрутизатора доступа Cisco 2811 (R4).

Требуется создать VLAN с номерами для рабочих станций, принтеров и серверов банка в соответствии со схемой, представленной на рис. 2, настроить маршрутизацию между этими VLAN при их подключении к маршрутизатору R4 по магистральному каналу, а также выполнить настройки в соответствии с приведенными выше рекомендациями.

Контрольные вопросы

1. Пояснить рекомендации по настройке механизмов защиты виртуальных ЛВС.
2. Реализовать в ЛВС атаку типа «VLAN hopping» при настройке различных собственных VLAN на транковых портах, соединяющих коммутаторы.
3. Настроить распространение базы данных VLAN через протокол VTP в соответствии с рекомендуемыми параметрами.
4. Настроить терминирование и маршрутизацию VLAN на коммутаторе уровня ядра-распределения ЛВС.

Лабораторная работа № 11
Защита ЛВС от петель на канальном уровне

Цель работы:

Целью лабораторной работы является изучение методов и средств построения, защиты и оптимизации отказоустойчивых ЛВС на основе протокола STP.

Программное обеспечение: ОС Microsoft Windows XP/2003/ 2008R2/Vista/7/8/8.1/10/2012/2012R2, Cisco Packet Tracer

Теоретический материал

Протоколы и механизмы оптимизации и защиты семейства STP предназначены для предотвращения петель (циклов) в сетях с множественными маршрутами на канальном уровне ЛВС. За счет обмена служебными BPDU-кадрами коммутаторы, на которых запущен протокол STP, строят топологию, в которой между любыми двумя коммутаторами существует только один активный в данный момент маршрут на канальном уровне.

В настоящее время семейство протоколов STP включает протоколы и механизмы IEEE 802.1d, IEEE 802.1w, IEEE 802.1s, IEEE 802.1t, а также расширение Cisco Spanning Tree Toolkit.

Одним из основных элементов протокола STP является корневой коммутатор. Некорректный выбор корневого коммутатора, вызванный ошибками конфигурирования оборудования или атаками нарушителей, может привести к нарушению штатного функционирования сетевой инфраструктуры или перенаправлению и перехвату информационных потоков на канальном уровне.

В настоящее время используются следующие принципы при проектировании, настройке и оптимизации протоколов семейства STP.

1. Использовать протоколы семейства STP с целью построения отказоустойчивых ЛВС только при необходимости. По возможности для обеспечения отказоустойчивости и высокой доступности ЛВС использовать механизмы и протоколы маршрутизации сетевого уровня.

2. Применение протокола STP является обязательным в случае передачи данных в одной и той же виртуальной ЛВС, организованной на разных коммутаторах, а также для защиты от действий пользователей на портах доступа коммутаторов ЛВС и ошибок обслуживающего персонала.

3. В семействе протоколов STP рекомендуется использовать протокол Rapid-PVST+.

4. Административно определять и назначать корневые коммутаторы. Использовать дополнительные механизмы и средства защиты протокола STP (Root Guard, Loop Guard, UplinkFast, UDLD) для предотвращения получения роли корневого коммутатора другими коммутаторами.

5. На портах доступа коммутаторов ЛВС выполнять настройки по предотвращению возможности появления или фильтрации BPDU-пакетов протокола STP (механизмы BPDU Guard и BPDU Filter соответственно), а также выполнять настройки для быстрого включения и защиты корневого коммутатора (механизмы PortFast и Root Guard соответственно).

Задание на лабораторную работу

На коммутаторах ЛВС филиала банка выполнить настройки протокола STP и механизмов его защиты. Построенная ЛВС должна обеспечивать состояние доступности при отказе:

- одного из коммутаторов SW7-1 или SW7-2;
- активного коммутируемого порта маршрутизатора R7;
- одной из линий связи канала EtherChannel;
- активного порта линии связи между коммутатором уровня доступа и коммутатором уровня ядра-распределения.

Контрольные вопросы

1. Пояснить различия в работе между механизмами BPDU Guard, BPDU Filter и Root Guard. Описать области применения и назначение каждого из этих механизмов защиты.
2. Пояснить выбор портов активации механизма Root Guard на коммутаторах уровня ядра-распределения филиала.
3. Разработать проект внедрения механизма Loop Guard для защиты ЛВС от образования однонаправленных каналов связи.
4. Смоделировать DoS-атаку на сетевую инфраструктуру при подключении к ЛВС коммутатора с наименьшим значением параметра BID.
5. Смоделировать атаку типа BPDU spoofing на протокол STP путем подключения к ЛВС коммутатора нарушителя и получения им роли корневого моста.

Лабораторная работа № 12
Защита ЛВС от атак канального уровня

Цель работы

Целью лабораторной работы является изучение методов проектирования, развертывания и настройки механизмов защиты в коммутируемых ЛВС от атак канального уровня типа MAC-flooding и MAC-spoofing.

Теоретический материал

Одним из механизмов защиты ЛВС от атак является механизм *port security*, реализованный на коммутаторах. Механизм *port security* позволяет осуществлять фильтрацию кадров, поступающих на отдельные порты коммутатора ЛВС, на основе MAC-адреса источника.

При активизации данного защитного механизма на порту коммутатора создается список ассоциированных (разрешенных) с ним MAC-адресов. Кадры, поступающие на порт коммутатора с активизированной функцией *port security*, MAC-адреса которые не принадлежат данному списку, уничтожаются. При этом сам порт коммутатора может переходить в режим shutdown.

Существует два метода построения списка разрешенных MACадресов – метод статического назначения и метод динамического изучения.

Метод статического назначения разрешенных MAC-адресов применяется на коммутаторах доступа ДМЗ, центров обработки данных и т. д. При этом на порту коммутатора указывается конкретный MAC-адрес.

Метод динамического изучения адресов определяет максимальное количество MAC-адресов, ассоциируемых коммутатором с портом в течение некоторого времени. Такой способ построения таблицы адресов, как правило, применять на уровне доступа ЛВС или в сетях филиалов.

При нарушении безопасности – при поступлении на защищаемый порт коммутатора кадра с запрещенным MAC-адресом – возможно одно из трех событий: порт отключается (режим защиты shutdown), кадр отвергается коммутатором (режим защиты protect), кадр отвергается коммутатором, увеличивается счетчик нарушений порта и генерируется SNMP-сообщение (режим защиты restrict).

В динамически изменяемой сетевой инфраструктуре рекомендуется ограничиваться одним MAC-адресом для порта коммутатора и использовать режим protect, в серверных группах – статически задавать списки MAC-адресов и использовать режим shutdown, в VoIP- сегментах – ограничиваться двумя или тремя MAC-адресами с активизацией режима restrict.

Дополнительным механизмом формирования списка MACадресов является механизм sticky. Он позволяет добавить статически заданные или

динамически выученные MAC-адреса в конфигурационный файл ОС коммутатора.

Задание на лабораторную работу

В сегменте ЛВС филиала, построенном на базе двух коммутаторов уровня доступа Cisco Catalyst 2960 и коммутатора уровня ядра-распределения Cisco Catalyst 3560, обеспечить защиту от атак типа MAC-flooding и MAC-spoofing.

Контрольные вопросы

1. Описать назначение и принцип работы механизма port security sticky для статического метода формирования MACадресов.
2. Объяснить рекомендацию задания максимального количества MAC-адресов на порту коммутатора с динамическим методом формирования списка из двух или трёх разрешенных MAC-адресов.
3. Возможно ли применение механизма port security для защиты от атак типа ARP spoofing и DHCP spoofing?

Лабораторная работа № 13
Построение маршрутизируемой ЛВС

Цель работы

Целью лабораторной работы является обучение методам построения и настройки маршрутизируемой ЛВС с высокой доступностью на основе протокола маршрутизации OSPF.

Программное обеспечение: ОС Microsoft Windows XP/2003/ 2008R2/Vista/7/8/8.1/10/2012/2012R2, Cisco Packet Tracer

Теоретический материал

Архитектура современных корпоративных ЛВС должна обладать следующими основными свойствами: иерархичность, модульность, устойчивость и масштабируемость. Классическая иерархическая модель ЛВС состоит из трех уровней – ядра, распределения (агрегирования) и доступа. В современных корпоративных ЛВС, как правило, можно выделить блок распределения и блок сервисов, объединяемых ядром сети. От правильного проектирования блока распределения зависит стабильность и корректность работы всей ЛВС.

В настоящее время основными вариантами архитектуры блока распределения является многозвенная архитектура (multi-tier), архитектура с маршрутизируемым доступом (routed access) и архитектура с виртуальной коммутацией. Подходы различаются в границе между уровнями реализации,

используемыми сетевыми технологиями и протоколами уровней L2 и L3, а также возможностями в реализации отказоустойчивости, избыточности и балансировки нагрузки.

Альтернативой традиционному блоку распределения с классической многозвенной архитектурой служит архитектура блока распределения с реализацией функций маршрутизации на уровне доступа, что позволяет построить полностью маршрутизируемую ЛВС. В такой архитектуре коммутаторы доступа функционируют как устройства третьего уровня, магистральные каналы между коммутаторами уровней доступа и распределения заменены маршрутизируемыми каналами уровня L3.

Таким образом, граница сопряжения сетевых уровней L2 и L3 перемещена в иерархии ЛВС с уровня распределения на уровень доступа. При этом на всех коммутаторах доступа создаются уникальные виртуальные ЛВС, для которых шлюзами являются коммутаторы доступа.

Создание стандартного маршрутизатора для каждой виртуальной ЛВС на коммутаторе доступа выполняется через механизм Switch Virtual Interface (SVI). Для обеспечения высокой доступности используются механизмы маршрутизации, а не специализированные протоколы семейств FHRP и STP.

Данный подход содержит существенные преимущества по сравнению с классическим подходом: простота проектирования и реализации, простота отладки и управления, единые механизмы восстановления и управления.

При проектировании и конфигурировании маршрутизируемой ЛВС на основе протокола OSPF используются следующие основные принципы:

1. Создание двухуровневой модели маршрутизации – магистраль (область 0), реализуемая в ядре сети, и остальные области, реализуемые в сегментах сети, подключенных к магистрали через коммутаторы уровня распределения. Последние выступают в качестве пограничных маршрутизаторов области. Ограничение рассылки OSPF-сообщений путем определения и настройки пассивных интерфейсов на коммутаторах уровня доступа.

2. Наличие L3-соединения между коммутаторами уровня распределения, а также между коммутаторами уровня доступа и уровня распределения. Использование треугольных топологий между уровнями доступа, распределения и ядра.

3. Уменьшение количества рассылаемых OSPF-сообщений о состоянии связей и размера таблиц маршрутизации путем определения и настройки тупиковых и полностью тупиковых областей, а также путем выполнения суммирования маршрутов на пограничных маршрутизаторах.

Достоинства полностью маршрутизируемых ЛВС:

- простота реализации и сопровождения;
- наличие развитых средств диагностики и устранения неисправностей;
- высокая скорость и предсказуемость восстановления после отказов;
- унификация средств и механизмов построения всех уровней.

Основным требованием для обеспечения возможности построения маршрутизируемой ЛВС является наличие на всех коммутаторах уникальных VLAN.

Задание на лабораторную работу

Выполнить настройки коммутаторов ЛВС банка, обеспечивающие реализацию архитектуры полностью маршрутизируемой ЛВС с высокой доступностью.

Контрольные вопросы

1. Определить в схеме маршрутизации ЛВС механизмы и средства обеспечения отказоустойчивости и масштабирования.
2. Какие сложности могут возникнуть в процессе реализации политик безопасности (межсетевом экранировании, организации VPN) при построении маршрутизируемых ЛВС?
3. Смоделировать процесс асимметричной маршрутизации ЛВС. Каким требованиям должны удовлетворять средства защиты информации при поддержке асимметричной маршрутизации?

Лабораторная работа № 14
Защита сетевой инфраструктуры

Цель работы

Целью лабораторной работы является изучение методов и средств защиты сетевой инфраструктуры от НСД, а также принципов проектирования сетей управления.

Программное обеспечение: ОС Microsoft Windows XP/2003/ 2008R2/Vista/7/8/8.1/10/2012/2012R2, Cisco Packet Tracer

Теоретический материал

Для защиты устройств сетевой инфраструктуры от НСД, обеспечения ее устойчивости и безотказного функционирования используются следующие основные настройки безопасности:

1. Отключение неиспользуемых протоколов, сетевых служб и механизмов (DNS, CDP, TELNET, DHCP, FINGER, ECHO, маршрутизация от источника, proxy-arp, ICMP redirect, ICMP maskreply и др.).
2. Настройка планировщика задач для обеспечения возможности передачи ресурсов процессам управления.
3. Ограничение доступа к сетевой инфраструктуре только из сети управления или с автоматизированных рабочих мест администраторов.
4. Обеспечение синхронизации времени на всех устройствах для корректного анализа событий (в том числе и событий безопасности). Для этого

настраивается синхронизация времени с внешним источником по протоколу NTP с аутентификацией пакетов.

5. Уведомление и сохранение информации о сбоях (SNMP, SYSLOG, автоматическое сохранение файлов crashinfo, создаваемых ОС при фатальных сбоях аппаратного или программного обеспечения).

6. Предупреждение лиц, подключившихся к устройству, о запрете тех или иных действий. Для этого на всех устройствах настраивается выдача предупреждающего сообщения о запрещении НСД к данному устройству. Регистрация и учет для всех видов доступа. Регистрация лиц, осуществляющих доступ к устройству, выполняемых ими действий и времени для последующего аудита.

7. Разрешение управления устройством только по защищенным протоколам типа SSH и SNMP с узлов сети управления и установлением ограничений на продолжительность сессий.

8. Настройка механизмов парольной защиты: использование стойких паролей, включение хэширования и шифрования паролей.

В архитектуре сетей с высоким уровнем безопасности, как правило, выделенная строится сеть управления, выполняющая отдельные функции передачи информационных потоков уровня управления. Сеть управления, использующая физически выделенные каналы, называется сетью внеполосного управления (out-of-band network). Сеть управления, использующая каналы передачи данных, называется сетью внутриполосного управления (in-band network).

Как правило, сеть внеполосного управления строится в корпоративных ЛВС и ЦОД. При этом используются выделенные, виртуальные коммутаторы и маршрутизаторы.

Сети внутриполосного управления используются для управления сетями филиалов и внешними устройствами периметра. При построении сетей управления активно используются современные технологии виртуализации сетей – технологии VLAN, VRF, path isolation, механизмы MPLS.

Задание на лабораторную работу

Организовать управление сетевым оборудованием филиала из сети внеполосного управления. Выполнить настройки по обеспечению защиты маршрутизаторов СПД. Для централизованного управления доступом администраторов к сетевому оборудованию банка использовать технологию AAA.

Контрольные вопросы

1. В сети одного из филиалов банка построить сеть внутриполосного управления.

2. Убедиться в невозможности доступа в сеть управления из ЛВС передачи данных и наоборот.

Лабораторная работа № 15
Защита периметра сети

Цель работы

Целью лабораторной работы является изучение основных технологий межсетевого экранирования, методов и средств управления безопасностью информационных потоков на межсетевых экранах и сетевых маршрутизаторах.

Теоретический материал

Межсетевой экран (далее – МЭ) – аппаратный, программно-аппаратный или программный комплекс, реализующий функции управления, контроля и фильтрации сетевых информационных потоков между двумя и более АС по некоторому набору правил, определяемых политикой безопасности.

МЭ подразделяются на различные типы в зависимости от следующих характеристик:

- обеспечивается соединение между одним узлом и сетью или между двумя или более различными сетями;
- происходит контроль потока данных на сетевом уровне или более высоких уровнях эталонной модели ISO/OSI;
- отслеживаются состояния активных соединений или нет.

В зависимости от охвата контролируемых потоков данных МЭ, как правило, делятся на:

- традиционные МЭ, которые обычно представляют собой специализированное устройство или компьютер, размещённый на границе двух или более сетей. Такие типы экранов контролируют входящие и исходящие потоки данных в каждой из подключенных сетей;
- персональные МЭ – программные МЭ или модули антивирусного ПО, устанавливаемые на отдельном компьютере и предназначенные для защиты только этого компьютера от несанкционированного доступа.
- В зависимости от уровня, на котором происходит управление доступом, существует разделение на:
- МЭ, работающие на сетевом уровне, когда фильтрация происходит на основе сетевых адресов отправителя и получателя пакетов, номеров портов транспортного уровня и статических правил, заданных администратором;
- МЭ, работающие на уровне приложений, осуществляющие контроль за передаваемыми данными на более высоких уровнях модели *OSI*. Такие типы экранов позволяют блокировать передачу нежелательной и потенциально опасной информации в зависимости от принятой администратором политики и настроек устройства. Такие типы МЭ обычно

работают в режиме прокси-сервера различных приложений, а не маршрутизации на сетевом уровне.

В зависимости от реализации возможности отслеживания активных соединений МЭ бывают:

- без инспекции состояний – не отслеживают текущие соединения (например, *TCP*), а фильтруют поток данных исключительно на основе статических правил;
- с инспекцией состояний – с отслеживанием текущих соединений и пропуском только таких пакетов, которые удовлетворяют логике и алгоритмам работы соответствующих протоколов и приложений. Данные МЭ позволяют эффективнее бороться с различными типами *DoS*-атак и уязвимостями некоторых сетевых протоколов. Кроме того, они обеспечивают функционирование таких протоколов, как *H*.323, *SIP*, *FTP* и т.п., использующие сложные схемы передачи данных между узлами, плохо поддающиеся описанию статическими правилами, и зачастую несовместимы со стандартными МЭ без инспекции состояний.

Дополнительными механизмами защиты и управления информационными потоками, реализуемыми, как правило, в МЭ, являются технологии NAT, AAA, VPN и IDPS.

Технология NAT применяется как для обеспечения доступа узлов с немаршрутизируемыми адресами к ГВС Интернет, так и для реализации механизмов защиты сети, например, для изоляции сетей управления или прохождения пакетов через VPN-шлюз.

Существуют следующие виды NAT: динамическая трансляция адресов на уровне портов, динамическая трансляция на уровне портов с выборкой IP-адресов, трансляция с динамической выборкой IP-адресов и статическая трансляция.

Задание на лабораторную работу

Настроить правила управления доступом серверов и рабочих станций из ЛВС в сеть Интернет и из нее к серверам АС, расположенным в ДМЗ. Реализовать механизм первичной фильтрации пакетов на пограничном маршрутизаторе IBR. Доступ в сеть Интернет из сети 10.194.200.0/24 осуществляется по технологии NAT.

Доступ из сети 10.194.192.0/24 в Интернет запрещен и осуществляется через терминальный сервер s01-term (IP-адрес 10.194.210.11). Дополнительно в ЛВС существует прокси-сервер s01-proxy (IPадрес 10.194.210.10). Для реализации технологии NAT выделяются IP-сети 212.192.98.168/29 и 212.192.98.154/32 соответственно. В сегменте ДМЗ расположены DNS-сервер s01-dns (IP-адрес 212.192.98.162) и WWW-сервер s01-www (IP-адрес 212.192.98.163). Настроить политику управления доступом к данным серверам на основе порядка функционирования WWW- и DNS-служб.

Контрольные вопросы

1. Проанализировать политику безопасности управления информационными потоками, представленную в табл. 2.
2. Дополнить политику безопасности управления информационными потоками правилами для проектируемой вами электронной почтовой системы.
3. Обеспечить доступ к сети Интернет из сетей филиалов через ГВС. При необходимости внести изменения в политику безопасности управления информационными потоками.

Лабораторная работа № 16
Криптографическая защита каналов передачи данных

Цель работы

Целью лабораторной работы является обучение методам и средствам защиты каналов передачи данных ГВС на основе технологии виртуальных частных сетей.

Теоретический материал

При организации обмена и передачи информации в ГВС, как правило, исходят из модели нарушителя, в которой последний контролирует каналы передачи данных, а также имеет возможность искажать информацию, передаваемую между абонентами (модель активного нарушителя). Для защиты информации применяют различные специализированные протоколы безопасности, работающие на одном (или нескольких) уровнях модели ISO/OSI. Ниже представлен краткий перечень наиболее распространенных протоколов безопасности. Так, на канальном уровне работают протоколы PPTP, L2TP, L2F, на сетевом уровне работают протоколы IPv6 и IPSec, на транспортном уровне – протокол SSL/TLS и на прикладном – SSH, PGP, S/MIME. Для обмена ключевой информации в рамках одного или нескольких доменов применяют протокол Kerberos, в масштабах ГВС используют инфраструктуры обмена открытыми ключами PKI. Помимо этого, большинство протоколов передачи данных включают в себя возможность проведения аутентификации сторон прежде, чем будет установлен информационный канал связи.

Выбор протокола для защиты передаваемых данных диктуется необходимыми сервисами и возможностями предполагаемого нарушителя. Для защищенного обмена данными между сетями, расположенными удаленно друг от друга, или между абонентами и сетью, как правило, применяется семейство протоколов сетевого уровня IPSec. Защита данных на сетевом уровне обладает тем достоинством, что для транспортных и сеансовых протоколов работа по защите данных становится прозрачной. В этом случае

нет необходимости создавать специальное ПО для защиты передаваемых данных протоколами верхних уровней.

Защищенная передача данных, реализуемая на транспортном уровне, используется преимущественно в модели клиент – сервер. Соответственно клиент и сервер должны поддерживать специальный протокол. Примером может служить протокол SSL и его модификация – TLS.

Выбор схемы для распределения ключевой информации зависит от модели нарушителя. Для модели с активным нарушителем подходят только те схемы, в которых участники информационного обмена заранее знают известный только им секрет, или у них есть общий доверенный посредник.

Большое распространение получили способы распределения ключей на основе протокола Kerberos и на основе инфраструктуры открытых ключей. Оба способа предполагают общего доверенного посредника, в роли которого выступает либо контроллер домена, либо удостоверяющий центр. Схема, основанная на предварительном знании общего секрета, предполагает административноорганизационное решение, когда, например, администраторы сети договариваются об используемом пароле или ключе.

Виртуальная частная сеть (VPN) – это технология, использующая криптографические механизмы для защищенной передачи данных по общей или выделенной сетевой инфраструктуре.

В общем случае технология VPN решает следующие задачи: организация связи между филиалами, подключение партнеров и клиентов, а также мобильных сотрудников к корпоративной СПД.

Термин «частная сеть» означает принадлежность оборудования сети предприятия и гарантию конфиденциальности информации, передаваемой по этой сети. Такие сети не очень распространены, гораздо чаще предприятие арендует каналы связи для своих филиалов.

При аренде каналов предприятие делит пропускную способность магистральных каналов с другими абонентами провайдера. Полоса пропускания арендованного канала полностью выделяется предприятию и является его собственностью. Корпоративные данные практически не доступны для абонентов, не являющихся пользователями корпоративной СПД или сети провайдера.

Также возможна организация VPN на базе ГВС Интернет, что, с одной стороны, имеет преимущества в простоте и низкой стоимости реализации, но вместе с тем не гарантирует заданной пропускной способности.

Выделяют следующие виды VPN: внутрикорпоративные (intranet VPN) – для организации связей с филиалами, удаленного доступа

(remote access VPN) – для организации доступа к ресурсам компании сотрудников или клиентов, межкорпоративные (extranet VPN) – для организации связей с партнерами и клиентами.

В VPN для криптографической защиты данных на сетевом уровне предназначено семейство протоколов IPSec, обеспечивающее выполнение

следующих задач: шифрование передаваемых данных, обеспечение их аутентичности и целостности, а также разграничение доступа (фильтрация IP-потоков) и защита от повторной передачи IP-дейтаграмм.

В состав семейства IPSec входят протокол аутентификации (AH), протокол шифрования (ESP) и протокол обмена ключами (IKE). Протокол IKE разработан на основе протоколов ISAKMP, Oakley и SKEME и предназначен для согласования используемых алгоритмов, ключей, продолжительности их действия и других параметров. Результатом такого согласования является *однонаправленная безопасная ассоциация* (security association – SA). Работа протокола IKE включает два этапа. Первый – идентификация и аутентификация сторон, установление защищенного канала для согласования параметров (результат – создание IKE SA). Второй – установление защищенного канала передачи данных.

Протоколы семейства IPSec могут работать в транспортном и туннельном режимах. В *транспортном режиме* заголовок исходной дейтаграммы остается неизменным, а в *туннельном режиме* происходит формирование нового IP-заголовка для AH или ESP-пакета.

Выделяют следующие основные варианты применения протокола IPSec: узел – узел, узел – сеть и сеть – сеть. При этом основными схемами включения VPN-шлюзов в сегменте LVP являются параллельная и последовательная.

Задание на лабораторную работу

Обеспечить криптографически защищенное подключение сетей филиалов к сети центрального офиса по арендуемым каналам передачи данных, а также криптографически защищенный удаленный доступ клиентов через ГВС Интернет к АС «Клиент – Банк». Для обеспечения гарантий защиты каналов связи для подключения клиентов через ГВС Интернет использовать немаршрутизируемые IP-адреса инфраструктуры АС «Клиент-Банк». Централизованное управление доступом обеспечить путем использования протокола Radius и инфраструктуры AAA.

Контрольные вопросы

1. Изучить рекомендации к выбору параметров криптографической защиты протоколов IPSec.

2. Убедиться в невозможности доступа в сегмент АС «КлиентБанк» из ГВС и корпоративной СПД без знания параметров и ключей криптографической защиты IPSec.

ЗАКЛЮЧЕНИЕ

Правильная организация практических учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 373-ст: дата введения 2008-02-01. – URL: https://docs.cntd.ru/document/1200058320 (дата обращения: 15.04.2021). – Текст: электронный.
2. ГОСТ Р ИСО 19011-2012. Руководящие указания по аудиту систем менеджмента: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 19 июля 2012 г. N 196-ст: дата введения 2013-02-01. – URL: https://docs.cntd.ru/document/1200095049 (дата обращения: 15.04.2021). – Текст: электронный.
3. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: учеб. пособие / В. Г. Олифер, Н. А. Олифер . – 3-е изд. – Санкт-Петербург: Питер, 2008. – 958 с.: ил. – (Учебник для вузов). – Библиогр.: с. 919–921. – Алф. указ.: с. 922–957. – ISBN 9785469005049 (5 экз.)
4. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – Москва: ИД «Форум»: ИНФРА-М, 2013. – 416 с.: ил. – (Профессиональное образование). – Библиогр.: с. 401–408. – ISBN 978-5-8199-0331-5. – ISBN 978-5-16-003132-3 : (20 экз.)
5. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс]: учеб. пособие / В. Ф. Шаньгин. – Москва: ДМК Пресс, 2012. – 592 с.: ил. - ISBN 978-5-94074-637-9
6. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: учеб. пособие / В. Г. Олифер; авт. Олифер Н.А. – 2-е изд. – Санкт-Петербург: Питер, 2003. – 864 с.: ил. – ISBN 5947234785 .

Локальный электронный методический материал

Владислав Владимирович Подтопельный

БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Редактор С. Кондрашова
Корректор Т. Звада

Уч.-изд. л. 3,2. Печ. л. 2,6.

Федеральное государственное
бюджетное образовательное учреждение высшего образования
«Калининградский государственный технический университет»,
236022, Калининград, Советский проспект, 1